European Commission

Study on the feasibility and implications of options to digitalise visa processing

HOME/2018/ISFB/FW/VISA/0012

Final report

September 2019

Prepared by Deloitte

Migration and Home Affairs

EUROPEAN COMMISSION

Final report

Study on the feasibility and implications of options to digitalise visa processing

HOME/2018/ISFB/FW/VISA/0012

September 2019

Prepared by Deloitte

Abstract

The European Union common visa policy is an essential element in ensuring the secure and proper functioning of the Schengen Area without internal border controls. The processing of visa applications is already digital to a great extent. However, some key parts of the process remain paper-based, i.e. the submission of the visa application with the required supporting documents, and the issuing of the visa sticker, which is affixed to the travel document.

This report presents the options for improving these two steps by further digitalisation taking into account the impacts on the different stakeholders involved. In addition, the report compares the different options based on a thorough assessment in terms of legal, technical, security, data protection, operational and implementation feasibility, as well as on a cost-benefit analysis. Lastly, the report provides concrete indications for the way forward, including a high-level roadmap and recommendations for a pilot project.

Keywords: visa policy – border policy - short-stay visa - digitalisation – feasibility study.

La politique commune de l'Union européenne en matière de visas est l'un des principaux éléments concourant au fonctionnement sécurisé d'un Espace Schengen sans contrôles aux frontières internes. Le traitement des demandes de visa est déjà digital dans une grande mesure. Néanmoins, certaines étapes essentielles du processus demeurent basées sur support papier, notamment pour la soumission des demandes de visa ainsi que des documents requis, et la délivrance de la vignette apposée au document de voyage.

Cette étude propose plusieurs options pour l'amélioration de ces deux étapes au travers de leur numérisation en tenant compte des impacts sur les différents acteurs impliqués. De plus, l'étude compare les différentes options en se basant sur une analyse détaillée de leur faisabilité du point de vue légal, technique, sécuritaire, de protection des données, opérationnel et de leur implémentation, ainsi que sur une analyse coûts-avantages. Enfin, le rapport fournit des indications concrètes sur la voie à suivre, incluant une feuille de route et des recommandations pour un projet pilote.

Mots clés: politique des visas – politique des frontières – visa court séjour – numérisation – étude de faisabilité

Luxembourg: Publications Office of the European Union, 2020

Print	ISBN 978-92-76-14138-9	doi:10.2837/072646	DR-03-19-941-EN-C
PDF	ISBN 978-92-76-14139-6	doi:10.2837/510316	DR-03-19-941-EN-N

Table of Contents

List of figures

List of tables

Executive Summary

Introduction

The European Union common visa policy is an essential element for ensuring the secure and proper functioning of the Schengen Area without internal border controls. Digitalisation brings an opportunity to reinforce security at the Schengen borders by strengthening visa processing. This report presents options for further digitalisation of two aspects of the current Schengen visa procedure: the application process and the visa sticker issued at the end of the procedure.

Current situation and challenges

In 2018, the 26 Schengen countries issued 14.3 million Schengen visas. This number might further increase in the years ahead. An earlier report for the European Commission forecasted that the total number of legal crossings will rise to 887 million by 2025. It is estimated that approximately one third of these crossings are made by third country nationals aiming to enter the Schengen Area for a short-term stay.

To ensure a high level of internal security and the free movement of persons in the Schengen Area, the EU and the Schengen countries are currently working on improving the management of EU external borders. To this end, the EU is upgrading its IT border management systems, and, deploying new ones. The overhaul of existing systems such as the Visa Information System (VIS) and the Schengen Information System (SIS), and the design of future systems, such as the European Travel Information and Authorisation System (ETIAS) and the Entry-Exit System (EES) will be the backdrop of the future visa policy. In addition, the EU has enacted legal measures to ensure the interoperability of these IT systems, i.e. two new Interoperability Regulations, as well as efficient and systematic access by competent authorities to the necessary data to perform their tasks.

As illustrated by these IT changes in the border management landscape, digitalisation is increasingly part of visa processing. At national level, some Schengen countries have already launched projects for the digitalisation of the visa processing, e.g. setting up national portals. Nevertheless, some key steps remain paper-based, i.e. the submission of the visa application with the required supporting documents and the visa sticker affixed to the travel document. In relation to these two key steps, the report identifies the following main pain points for stakeholders:

- Applicants: spend considerable resources (time and money) to physically lodge an application, sometimes without proper guidance. Moreover, they also need to come back physically to the consulate (or visa application centre) to collect their travel document.
- Consulates: deal with paper-based applications files (sometimes wrong or incomplete), which need to be stored for at least two years at their premises. They also incur costs and human resources for filling in and affixing the visa stickers, which also need to be stored securely at the consulate.
- Central authorities, i.e. ministries: have little control over the application procedure at local level, i.e. in the consulates. These central authorities incur costs for procuring the visa sticker's production service and transporting the stickers securely to the consulates.
- Border control authorities: risk being inclined to check only the visa sticker at the border without carrying out biometric verification using VIS.

Digitalisation can bring unique and tailored solutions by leveraging new technologies to address each of these pain points identified in the visa processing journey, while ensuring the security of the procedure.

Options and their feasibility

Online application

Based on the current visa processing steps and the pain points relating to each, this report presents the online visa application workflow. The workflow is divided into seven main functional blocks: (1) digital visa application form, (2) travel document, (3) supporting documents, (4) collecting biometrics, (5) declaring data are accurate and complete, (6) paying the visa fee and (7) interaction with the applicant. Digitising this workflow to reduce the burden on stakeholders requires different technical solutions for each step.

For each main functional block, the report identifies and assesses possible digital solutions. Based on that assessment, and taking into account the input received from Schengen countries experts at two workshops, the report retains two options for the **business architecture**. These two options aggregate several digital solutions, and can be distinguished by their level of digitalisation:

- the 'fully digital' (option A1) aggregates the most digital and far-reaching options;
- the 'custom digital' (option A2) encompasses a mix of digital options and the status quo.

Both options introduce an advanced technical solution for the application process. For example, they both allow the applicant to complete their visa application online, provide the supporting documents online, and pay the visa fee online. Option A2 is however closer to the status quo, particularly in relation to three functional blocks: the travel document, supporting documents, and the collection of biometrics. On the other hand, Option A1 is more innovative by putting technological solutions in place to support a digital process. For instance, the physical submission of the travel document will no longer be required, nor the submission of supporting documents in paper format, and the enrolment of biometrics could be handled remotely (as long as some security requirements are respected).

The business architecture options represent the features to be enabled for the users. However, these features need to be built on a technical back-end. This back-end, or **system architecture**, represents the technical adjustments needed to the architecture landscape in terms of systems and communication channels in order to host the new features envisaged at the business level. This report presents two technical solutions for the system architecture:

- centralised architecture (option B1) encapsulates a central application portal and a centralised application file database;
- hybrid architecture (option B2) also consists of a central application portal but stores the application files at a national (decentralised) level.

The main difference between these two proposed options is the location of the stored application data. In option B1, all data provided by the applicants, including identity data and supporting documents, are stored at a central level within the Application Management System (AMS). In option B2, the visa application portal only stores data temporarily until the submission of the application files, which are ultimately stored in the different national systems owned and operated by the Schengen countries.

Digital visa

The second aspect of visa processing investigated in this study is the visa sticker. This report suggests replacing the visa sticker with a digital visa embedded within VIS. In addition, it was found that a fallback solution is necessary for security reasons in order to provide authorised authorities with another means of verifying the validity of a visa should VIS or the local area network not be available.

The report identifies three possible **fallback solutions**:

- visa issuance notification (option C1): applicants receive an email notification that their visa has been issued;
- visa issuance notification with non-signed 2D barcode (option C2): applicants receive the same visa issuance notification as described in option C1, plus a 2D barcode in which the consulate has encoded the visa information;
- visa issuance notification with digitally signed 2D barcode (option C3): applicants receive a visa issuance notification with a 2D barcode signed with a key (digital seal) issued by designated authorities in the Schengen countries.

The report assesses the different options for the visa application and the digital visa for their legal, technical, security, data protection, operational and implementation feasibility.

Cost-benefit analysis

In addition to the feasibility assessment, the reports also examines the options in terms of costs and benefits.

Online application

For the online application portal, the investments costs to be covered depend on the system architecture option selected.

Option B1 requires more effort at a central level because of the need to implement an Application Management System (AMS) (which would most likely be hosted by eu-LISA in this scenario). Over an eight-year running period (three years for implementation and five years' operation), the central systems would incur an average annual cost of EUR 3.1-5.7 million and each national system of the Schengen countries would incur an average annual cost of EUR 105,000-200,000. Over the eight years, this amounts to a total cost of EUR 24.6-45.8 million for the central systems and a cost of EUR 0.84-1.6 million for each national system. This adds up to a total cost of EUR 49-91 million for the centralised system architecture.

The option B2 requires more effort at national level because the application files would be stored nationally. Over an eight-year running period (three years for implementation and five years' operation – as above), the central systems would incur an average annual cost of EUR 1.7-3.1 million, and each national system of the Schengen countries would incur an average annual cost of EUR 275,000-500,000. Over the eight years, this amounts to a total cost of EUR 13.4-25 million for the central systems and a cost of EUR 2.2-4 million for each national system. This adds up to a total cost of EUR 75-140 million for the hybrid system architecture over the eight-year period.

In terms of benefits, the online application portal could save 708 full-time equivalents (FTEs) for Schengen countries and a total of EUR 880 million in travel costs for third country nationals each year. It would also increase the number of visa applications received, with indirect benefits for the economies of the Schengen Area.

Digital visa

The implementation costs of the digital visa will mainly depend on options of the fallback solutions. However, if the digital visa were implemented before or without any online application option, applicants would not be able to receive notification of issuance or check their visa information via the online application portal. To provide that information, a traveller web service would be required in order to notify the consulates and the applicants. This report estimates that this traveller web service would require a one-off effort costing EUR 3.5-6.4 million plus EUR 0.7-1.2 million yearly for operations and maintenance.

As regards the fall-back solutions, option C1 should impose only minor costs while option C2 would require software for encoding information in barcodes (EUR 1.1-1.9 million for the whole Schengen Area). Although this option would also require smartphones able to scan barcodes, this report assumes that border crossing points and Schengen police authorities would already be equipped with this type of device, so it does not foresee any new costs in that regard. The option C3, the most secure option identified in the report, is slightly more expensive than the option C2: EUR 0.1-0.2 million per Schengen country, i.e. EUR 3-6 million for the whole Schengen Area, for the acquisition and maintenance of software for the whole Schengen Area. The same equipment would be needed as for option C2, i.e. smartphones able to scan barcodes.

Implementation of the digital visa could bring significant benefits for the Schengen countries and some benefits for third country nationals. Schengen countries are currently spending around EUR 13.8 million annually on visa stickers (aggregated costs). Doing away with the Schengen visa sticker would lead to a significant saving on those costs. Allowing for the fact that Schengen countries would still have production and transport costs if their national visa remains paper-based, Schengen countries would nevertheless certainly save up to EUR 10 million in production, transportation, storage and filling in costs. The digital visa would also save around 554 FTEs, and

reduce the Schengen countries' environmental footprint. The digital visa would also reduce some of costs for third country nationals, such as the travel document's transportation fee, generating a saving on average of EUR 15.60-17.50 per applicant.

Recommendations

For the visa application, this report recommends an online application process consisting of a mix of digital solutions and the status quo (option A2) and relying on a hybrid system architecture (option B2) with the following core characteristics:

- a centralised online application portal through which applicants all over the world can apply for a Schengen visa;
- electronic storage of application files (including supporting documents) at the national level, i.e. each Schengen country manages national systems that electronically store the applications for which they are responsible.

For the issuance of the visa, this report suggests that the Schengen Area abolish the paper-based visa sticker in favour of a digital visa solution. The digital visa would rely on the existing and upcoming EU systems for border management, removing the need to spend resources and time on the development of a brand new system. In fact, the digital visa would consist of the visa holder's record file stored in VIS (taking into account the reforms brought in by the new VIS Regulation), verified biometrically by the Schengen authorities, e.g. from the EES at the border. The interoperability framework for border management makes it possible to implement this solution.

In some circumstances, e.g. central VIS downtime, or lack of internet connection, it will be impossible to verify the digital visa. For security reasons, a fall-back solution is needed. Out of the three options (option C1, C2, C3), this report recommends the visa issuance notification with a digitally signed 2D barcode (option C3) as it guarantees the highest security and reliability in comparison to the other options.

Way forward and roadmap

This report presents the way forward for the visa application portal and digital visa.

For the online application portal, the report suggests a pilot project to test the deployment of the solution on a smaller scale, e.g. in one third country. The report also concludes that the material scope of this pilot project should be limited, i.e. only low-risk applicant profiles should be considered. In terms of timeline, the pilot for this online application portal could be designed in the upcoming months.

The pilot project should be conducted in two phases. First, the definition phase aims at making the necessary preparation for launching the pilot project. These preparations mainly relate to the key responsibilities, expectations and requirements for all Schengen countries participating in the pilot project, as well as to the development of a prototype realisation of the online application portal. Second, the delivery phase consists of defining the technical aspects and setting up a small-scale online application portal.

The report advises adopting another approach for the digital visa as it needs to be fully implemented by all Schengen countries at the same time in order to avoid security breaches. Therefore, a pilot project would not be useful. The digital visa could be implemented once the ongoing VIS revision is implemented, most likely around 2022.

Both the digitalisation of the application process and the digital visa require legislation to amend existing regulations and create a legal basis, together with secondary legislation (delegated and implementing acts) in order to prepare for the specific technical requirements. Once that is in place, the procurement can be launched and the solution designed, developed and implemented.

1. Introduction

1.1. Context

The European Union (EU) has experienced significant pressure on its external borders in the last few years. It is likely that there will continue to be high numbers of third country nationals crossing Schengen borders in future. Consequently, there is a need to modernise border controls. A study for the European Commission has estimated that the total number of regular crossings will rise to 887 million[1] in 2025, up by more than half in little more than a decade. It is estimated that approximately one third of these crossings will be made by third country nationals aiming to enter the Schengen Area for a short-term stay. Other challenges, e.g. the abuse of the Schengen visa to enter the Schengen Area fraudulently or overstay, are also putting Europe's internal security at risk.

The EU common visa policy is an essential element in ensuring that the external Schengen borders function securely and properly. It ensures legitimate travel to the EU and has gone a long way towards harmonising the Schengen countries' visa issuing practices. To ensure a continued high level of internal security and the free movement of persons in the Schengen Area, the Schengen countries are currently working on improving the management of their common external borders.

Since the entry into force of the Visa Code in 2010[2] and the start of operations of the Visa Information System (VIS) in 2011[3], the environment in which the visa policy is applied has changed considerably. On the one hand are the migration and security challenges faced in recent years; on the other are significant technological developments, which provide new opportunities to make the Schengen visa application process smoother for both travellers and consulates.

While visa processing is already partially digitalised, with applications and decisions recorded in VIS, two important steps remain paper-based: the visa application process and the visa sticker. These two steps create a burden for all stakeholders, from national public authorities, i.e. ministries of home and foreign affairs, to consulates and applicants. Schengen countries are aware of this and a considerable number have already launched digital solutions for moving towards a more efficient and user-friendly application process.

At EU level, the Estonian Council Presidency opened the discussion in the Visa Working Party of the Council[4] on options to improve the current visa process with an online visa application[5] and a digital visa.[6]

This political impetus, together with current and future legislative changes, i.e. the revised Visa Code,[7] the VIS revision,[8] the Entry/Exit System (EES),[9] the Visa Information System (VIS),[10] and the European Travel Information

1 European Commission: Impact Assessment Report on the establishment of an EU Entry Exit system, SWD(2016) 115 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/smart_borders_package_-_20160406_-_impact_assessment_-_part_1_en.pdf

2 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0810&from=EN

3 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0767&from=EN

4 https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/visa-working-party/

5 Presidency Council of the European Union, e-Visa: Improving the current visa process with online visa application, 12546/17, October 2017.

6 Presidency Council of the European Union, e-Visa: Improving the current visa process with digital visa, 11816/17; September 2017.

7 Regulation (EU) 2019/1155 amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code).

8 Proposal for a Regulation amending the VIS Regulation: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA - amended by the European Parliament's first reading on 11 to 14 March 2019 (hereinafter: VIS Recast or Proposal for a Regulation amending the VIS Regulation).

9 Regulation (EU) No 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. (hereinafter: Entry/Exit System/EES).

10 Regulation 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Schengen countries on short-stay visas (hereinafter: VIS Regulation).

and Authorisation System (ETIAS),[11] led the Commission to issue its Communication of 14 March 2018[12] on adapting the common visa policy to new challenges to launch a reflection in view of the move towards digital visas.

Therefore, digitalisation is an opportunity to improve the visa application process, thus removing, or at least reducing, the risks, the costs and the burden on stakeholders. Moreover, the digitalisation of the visa process is in line with recent legislative developments[13] relating to the IT landscape for border management, contributing to enhanced security of the Schengen Area.

1.2. Objectives and scope of the report

1.2.1. Objectives

The general objective of this study is to assess, from a legal and technical standpoint, the feasibility and practical implications of possible options for digitalisation of the:

- Schengen visa application process;
- visa sticker issued at the end of the visa procedure.

This study thus aims to investigate to what extent digitalisation can offer applicants a better user experience during the visa process, while enabling the Schengen countries to leverage technology to their advantage in order to make the visa process more efficient and contribute to the internal security of the Schengen Area.

1.2.2. Scope

This report is restricted to the Schengen visa application process and the Schengen visa sticker.

The visa application process represents the sequence of steps and activities beginning with a third country national's decision to apply for a visa and ends with the start of the examination phase by the consulate. The examination leads to the decision to issue or refuse the visa. This report explores digital options for facilitating the application phase, thus leaving the examination phase out of scope.

Thus, any initiatives and solutions intended to make the visa application process simpler by means of digital tools, whether for use by the applicant or the consulate side, fall within the scope of the report. By contrast, initiatives or proposals to render the current application process more secure or simpler without resorting to the use of digital technologies are out of scope.

This report is restricted to the Schengen visa for short stays not exceeding 90 days in any 180-day period (hereinafter referred to as the "visa", "short-stay visa", or "Schengen visa"), including also the airport transit visa. Other types of visa issued to third country nationals by Schengen countries in accordance with national law, e.g. national long-term visas for the purposes of study, work and research, fall outside the scope of this report. Nevertheless, the possible efficiency gains from including the national visas in an online visa application portal together with the Schengen visa, and using a digital visa for national visas as well, have been taken into account.

The visa sticker is a paper mark that proves that the holder of a travel document is in possession of a valid visa. The visa sticker is filled in and affixed to the travel document.

---

11 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (hereinafter: ETIAS Regulation).

12 Communication from the Commission to the European Parliament and the Council, Adopting the common visa policy to new challenges, COM(2018) 251 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20180314_communication-commission-parliament-council-adapting-common-visa-policy-new-challenges_en.pdf

13 Such as the Interoperability Regulation (Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816).

This report aims to explore the options for replacing the physical visa sticker with a digital visa that does not need a paper support. Conversely, the report does not consider any initiatives intended to increase the security and reliability of the current paper visa sticker.

1.3. Structure of the report

This report contains the following chapters.

- Chapter 2: Current situation and challenges – This chapter presents the current situation of the Schengen countries in terms of the IT solutions deployed for the visa processing. It also illustrates the current EU legal situation relating to the visa application process and border management systems, and the main challenges and pain points of the stakeholders involved in the visa application process as well as those relating to the visa sticker.
- Chapter 3: Options – This chapter presents an overview of the options designed to address the pain points identified previously. The chapter describes the legal, technical, security, data protection, operational and implementation feasibility assessment conducted for the online application and the digital visa in relation to several criteria.
- Chapter 4: Cost-benefit analysis – This chapter presents the costs associated with, and the benefits obtained from, rolling out a Schengen online application portal and transitioning to the digital visa.
- Chapter 5: Recommended option and way forward – This chapter presents the recommended options for the online application portal and the digital visa based on the feasibility and cost-benefit analysis. In addition, it sets out how the recommended options can be implemented;
- Chapter 6: Conclusions – This chapter summarises the main outcomes of the report and outlines the next steps for the way forward to implement the recommended options.

2. Current situation and challenges

This chapter presents the current situation of the Schengen countries in terms of the IT solutions deployed for the visa application process. It also describes the current EU legal situation with regard to the visa application process and border management systems, as well as the main challenges and pain points for the stakeholders in the visa application process as well as those relating to the visa sticker.

2.1. Schengen countries' IT solutions for the visa application process

Most Schengen countries use some IT solutions to facilitate the visa application process. However, there are significant differences among them.

This section presents the main differences between the most advanced technical solutions and best practices and the least advanced, in terms both of the technical features offered by the systems and the features used by the applicants. To date, only a few countries have adopted a user-centric logic, where the IT solutions include some features easing the application process for the applicant, e.g. user accounts, an appointment management tool or status checking.

Overall, most Schengen countries experience benefits from using digital solutions in the visa application process, and, as indicated during the fieldwork interviews, are generally in favour of upgrading their current IT solutions.

To assess the features and the level of maturity of the IT solutions used in the different Schengen countries, the following technical features were considered:

- access and environment (which stakeholders can use the tool and how, i.e. website/smartphone),
- features for the applicant, e.g. account, information about the application process, list of supporting documents, status, communication,
- e-signature,[14]
- online payment,
- appointments tool,
- interaction between the IT solution and the national system,
- possibility of creating statistics and reports,
- reading passport chip content,[15]
- scanning.

In addition, the report also takes into consideration the geographical scope of the solutions.

Based on this assessment, Schengen countries can be classified in three broad categories according to the level of digitalisation of their visa process: basic, intermediate and advanced. These classifications help in assessing the different levels of maturity of Schengen countries. The figure below provides an overview of the main features included in each of the three groups. Within a given category, there may be a certain amount of variability in the IT solutions.

[14] Although this element was taken into account, none of the Schengen countries has actually included it in their IT solution.
[15] Idem.

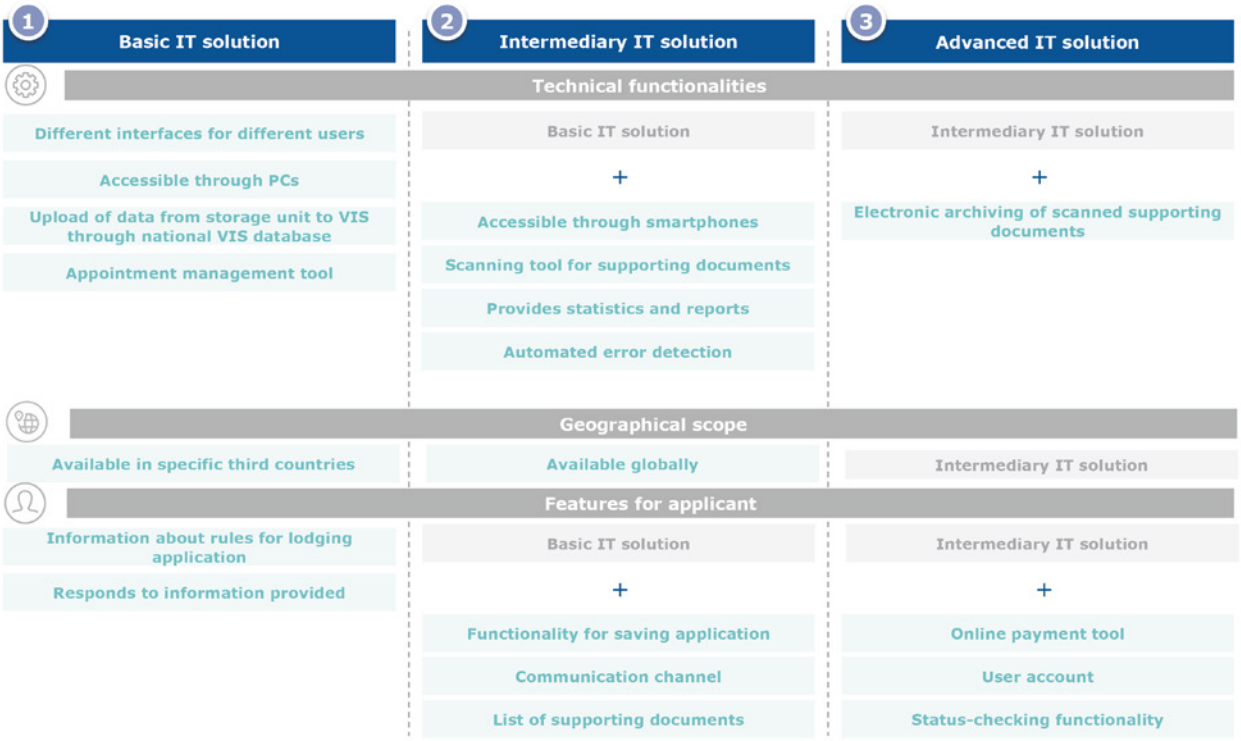

Figure 1: Overview of the levels of digitalisation in visa processing

The figure above is broken down into two main streams: technical features offered by the IT solution, and features for applicants, i.e. functions helping the applicant to complete their application successfully.

The following sections present and explain the best practices and more advanced technical solutions for each of the features.

2.1.1. Technical features

This section presents the general features of the IT solutions used by the Schengen countries, focusing on the best practices and/or most advanced technical solutions.

Access and support for users

In addition to being available globally, the four most advanced IT solutions are accessible to all stakeholders: the applicant, the external service provider (ESP) and the consulate. These stakeholders have different access rights and different features at their disposal. Depending on the profile of the user, the IT solution provides him/her with a different interface tailored to his/her specific needs.

The user features available to each user profile are described below:

- applicant: create and activate a user account (if the feature is available), fill in an application form, finalise/submit this form;
- external service provider: check the data and correct where applicable, add internal comments, add biometrics, finalise the application;
- consulate: check the data and correct where applicable, process and assess the application;
- other: additional internal profiles from the central authorities can be granted access to the tool, e.g. for reporting or monitoring purposes.

Websites or mobile websites, i.e. a website tailored to be displayed accurately on mobile devices, are the only technology supporting the IT solution so far. None of the Schengen countries has developed an app. Based on the data collected, access via a smartphone ensures a higher coverage, as some third country nationals do not have access to a PC, but do have a smartphone. For example, 37% of applicants access the French application portal using their smartphone's web browser.

Interaction with national systems

Schengen countries upload their visa data to VIS via their national systems. Most countries have a direct link between their national system(s) and the online application tool. There is, however, one Schengen country that has not created a direct link between its application tool and the national system, and uploads the data into the national IT system using 2D code. After the applicant has filled in the form online, the system creates a barcode embedding all the information from the application. The applicant subsequently prints the form and brings it to the consulate or visa application centre. The staff in the consulate reads the barcode and uploads the information into the national system.

Appointment management tool

Sixteen Schengen countries offer an appointment management tool, enabling users to book an appointment to submit their application and to provide biometrics. These appointment management tools are either included in the national online visa solutions, or are external tools, i.e. the applicant is redirected to a separate online appointment management system.

In Belgium, for example, applicants are redirected to a separate online appointment management system to book their appointments. The appointment is granted based on the data submitted, and thus only one appointment can be associated with the same data. Appointments for groups, e.g. families, are managed manually.

Appointment management tools make it possible on the one hand to prevent fraudulent activity around the bookings, and on the other hand to improve management of activities at the consulates, i.e. to avoid "no shows" and overbooking. In addition, as indicated in interviews with the ESPs and consulates, requiring applicants to pay the visa fee before booking their appointments can significantly help consulates avoid "no shows".

Scanning tool and document archiving

Thirteen Schengen countries require the ESP to scan passports and supporting documents to send them digitally to the consulates for further examination and decision-making. The creation and administration of the relevant tool varies across countries: it is either created and administered by both a governmental institution and by a private entity, e.g. an ESP, or created, administered and supervised exclusively by a private entity. Only three Schengen countries uses their own custom document-scanning tool.

Of the 13 Schengen countries, eight use the scanned documents for archiving purposes.

Data quality mechanisms

Most of the IT solutions include some data quality mechanisms. The IT solutions of 12 Schengen countries respond to the information provided or fields filled in. This ensures that the application form is complete and no data are missing. An error detection feature is also included (in the IT solutions of 14 countries). Such features avoid spelling mistakes and ensure that the data are provided in the correct format, e.g. alphanumeric.

Statistics and reports

The most advanced IT solutions enable retrieval of statistics and reports on their use. This feature is available in eight IT solutions and provides data on the following:

- number of visits and users;

- waiting list for appointments;
- peak time, indicating when the highest number of applicants are using the IT solution;
- average time taken to fill in a form;
- support used to access the IT solution, e.g. PC versus smartphone.

These statistics and reports are used to monitor the use of the IT solution, but also to identify improvement opportunities.

2.1.2. Other characteristics of the IT solutions

Geographical scope

The most advanced IT solutions are accessible globally. This means that the IT solution has been deployed in all third countries, and can thus be used by all third country applicants.

The IT solutions of some Schengen countries are only accessible in some specific third countries. There are several reasons:

- progressive implementation in third countries for technical reasons;
- national strategic priorities;
- some of these IT solutions can only be used by a specific service provider in the third countries where it is available.

2.1.3. Features for applicants

This section presents the features included in the IT solutions for the applicants.

Visa application information

General information on the visa application process is available on most of the Schengen countries' websites, as well as tailored information for each third country. In addition, some IT solutions assist the applicant in the visa application process. This interactive guidance consists of a set of questions to which the applicant must reply. Based on the information provided, the IT solution informs the applicants which visa is needed and the next steps in lodging the application. This is the case of the French and Dutch IT solutions, for example. These determine whether and which visa the applicants need based on their replies to a set of questions, i.e. country of origin, destination and duration of the trip.

User account

Applicants are in some cases invited to create an account in order to lodge an application. In six countries, this step is mandatory, while in one other, it is optional. This feature makes filling in the application form and submitting future applications easier. There are, however, some differences between the options offered by these six countries. In Sweden, the account created by the applicant is a one-time account for one specific application, i.e. the account created cannot be used for future applications. The French IT solution displays all the applications lodged by an applicant.

Although such user accounts offer a technically advanced solution, applicants must still print the application form, sign it and submit it in a paper-based format as this is required by law.

Supporting documents

Applicants are required to provide several supporting documents. The exact documents required mainly depend on their country of residence and purpose of travel. In order to make this step in the application easier, some IT solutions provide a tailored list of the documents needed for the application. This information is either displayed on the website, e.g. France, or shared in an email, e.g. Norway. Currently nine countries include this feature in their IT solutions. Currently, none of the IT solutions developed by the Schengen countries offers applicants the

possibility of uploading the supporting documents directly. However, such a feature is in the pipeline in several countries, e.g. Belgium and France.

Features to communicate with the applicant

Communication features in the IT solutions ensure that applicants are kept informed of their applications. This best practice is available in only five IT solutions. The purpose of such communication features varies across countries. It can be used, for example, to inform and remind the applicant about the date of an appointment or receipt of the electronic version of the application.

Status checking feature

Some IT solutions allow the applicants to verify the status of their application. This feature is included in 12 IT solutions with some differences. In six countries, the information about the status is provided directly in the system. In five others, this feature is outsourced, i.e. using an externally implemented tracking tool, which can be accessed by the users online. A status checking best practice has been identified in three countries, which communicate with the applicant directly via email or text message.

Online payment tool

Four Schengen countries have included an online payment tool in their IT solution. Online payment is a mandatory step to confirm submission of the application for three of these four countries. As explained above, requiring payment of the visa fee before submission of the application and booking an appointment contribute to reducing the number of "no shows", and/or fraudulent activities with the timeslots.

2.2. Visa processing ecosystem

The EU legal situation is explained in the sections below by detailing how visa processing is carried out currently as well as how the current and future border management systems help or will help improve the security of the Schengen borders.

2.2.1. Current visa process (application, examination and verification)

This section provides a detailed description of the current visa process.

As shown in the figure below, it is useful to distinguish between three stages within the whole visa life cycle:

- apply for a visa: starts with the individual's decision to apply for a visa and ends with the consulate's decision to examine the application;
- examine visa application: starts with the risk assessment (fulfilment of entry conditions) performed by the consulate and ends with the applicant collecting the travel document;
- verify the visa: starts with the visa holder's journey to the Schengen Area and ends once the visa holder leaves that area.

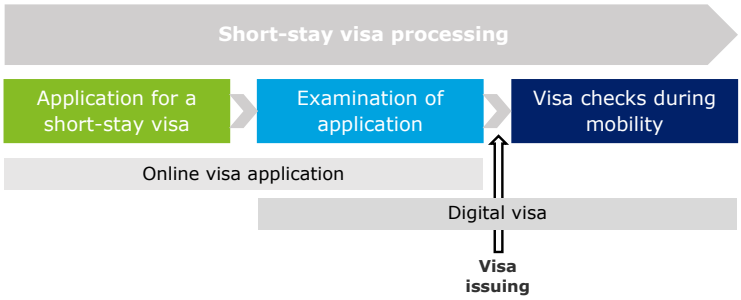

Figure 2: Stages of the short-stay visa processing

The main topics of the study, i.e. the digitalisation of the paper-based visa application process and the elimination of the physical visa sticker, are considered as separate steps of one continuous process that starts with the application process and ends with the checks on the visa issued/the visa holder. Therefore, to ease the reading of the rest of this report, the complete process is explained in more detail below.

Apply for a visa

A third country national subject to the visa requirement, who intends to enter the Schengen Area, must apply for and obtain a short-stay visa, unless the applicant is covered by a specific visa waiver, e.g. diplomatic or service passport holder. These third country nationals must apply at a consulate or visa application centre (operated by an ESP) of the Schengen country they intend to visit (or in which they plan to spend most of their time during the trip). The administrative steps are outlined in the figure below. The figure gives an overview of the activities performed by the applicant and by the case handler in two separate rows. Each activity is described in more detail below. Please refer to Annex I for a more detailed visualisation.

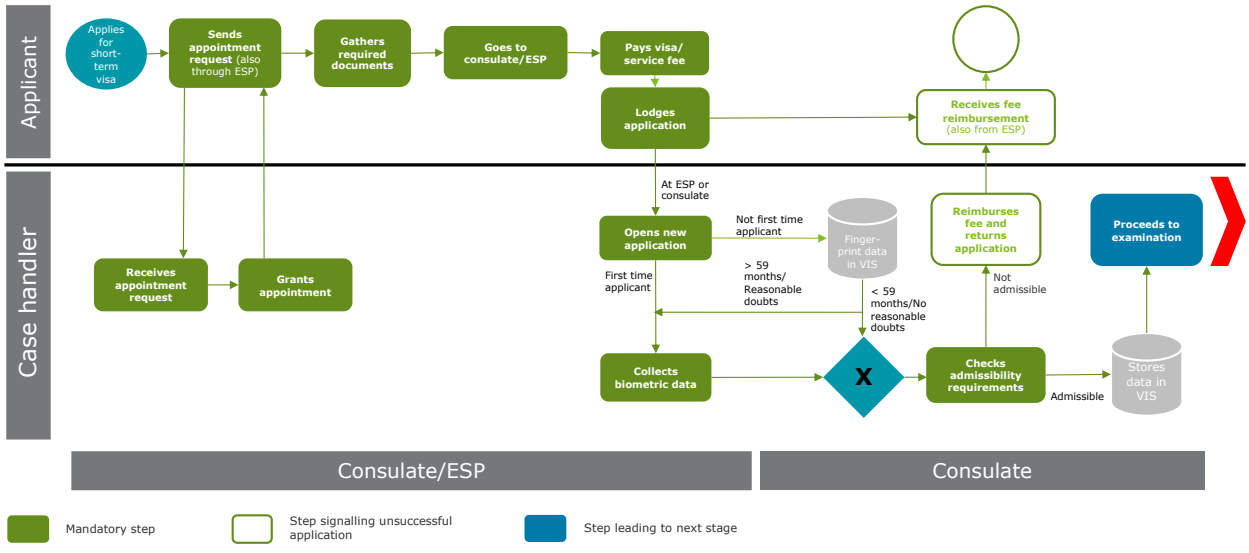

Figure 3: Application stage

Schedule appointment

When an applicant decides to apply for a short-stay visa, they lodge the application directly at the consulate or through an ESP. Generally, the applicant's first contact with the consulate/ESP consists of booking an appointment to lodge the application.[16] Once the consulate or the ESP receives the appointment request, a notification confirming the date and time of the appointment is sent to the applicant.

Gather required documents

The next step for the applicant is to gather the documents required by the relevant Schengen country to support his/her application. Such documents include:

- the (currently paper-based) application form,[17]
- the travel document,[18]
- the supporting documents, e.g. proof of purpose of stay, of sufficient means of subsistence covering the intended period of stay, and of will to return,[19]
- travel medical insurance.[20]

Even if the Schengen country concerned provides the option to submit (part of) the application online, all applicants (or their representatives) must still appear in person to lodge the application at a consulate or visa application centre run by an ESP.

Pay visa fee

When submitting the application, applicants who are not exempted from the visa fee must pay a fee of EUR 60[21], and, if applicable, a service fee charged by the ESP.[22]

Collect biometrics (fingerprints and facial image)

The collection of biometric identifiers[23] depends on whether the applicant is a first-time applicant or not, and on certain conditions, as explained below. Applicants who are not required to provide their fingerprints are listed in Article 13(7) of the Visa Code.[24]

If the applicant is a first-time applicant or their fingerprints were collected more than 59 months previously, they will have to be present at the consulate or ESP for the fingerprints to be collected. Currently the facial image can be provided as a paper photograph and scanned. Once the VIS Recast is adopted and implemented, the facial image will also be taken live at the consulate (together with the fingerprints). The facial image will then be uploaded to the VIS-BMS (Visa Information System – Biometric Matching Service) as a biometric identifier.

If the applicant is not a first-time applicant and his/her fingerprints have been taken and stored in VIS in the previous 59 months, they are copied to the new application. However, if the applicant's fingerprints cannot be found in VIS and/or the applicant's identity cannot be checked with reasonable reliability, applicants will have their biometric identifiers collected again.

---

16 The Visa Code does not oblige Schengen countries to have applicants request an appointment, but this is a common practice amongst Schengen countries and External Service Providers.

17 Article 11 of the Visa Code.

18 Articles 12, 15 and 16 of the Visa Code.

19 Article 14 of the Visa Code.

20 Article 15 of the Visa Code.

21 Article 16 of the Visa Code. The amendment to the current Visa Code would increase the standard fee from EUR 60 to EUR 80.

22 Article 17 of the Visa Code.

23 Article 3 of the Visa Code.

24 Children under the age of 12; persons for whom fingerprints are physically impossible; heads of State or government and members of a national government with accompanying spouses, and the members of their official delegation when invited by Schengen countries' governments or by international organisations for an official purpose; and Sovereigns and other senior members of a royal family when invited by Member States' governments or by international organisations for an official purpose.

Either way, the final application must be accompanied by valid biometric identifiers of the applicant. If the ESP needs to collect new biometric identifiers, the ESP must transfer them, along with all other application data, to the consulate for upload into VIS.

At this point, the ESP ceases to have a role in the application creation process. Only the consulate is entitled to check whether the application is admissible, i.e. whether it complies with the criteria (the required documents and data – including biometric identifiers – and payment of the visa fee). If the application is not deemed admissible, the application will be erased and the visa fee reimbursed to the applicant.

Examine visa application

If the application is admissible, the consulate initiates the examination stage, displayed in the figure below. Please refer to Annex I for a more detailed visualisation.

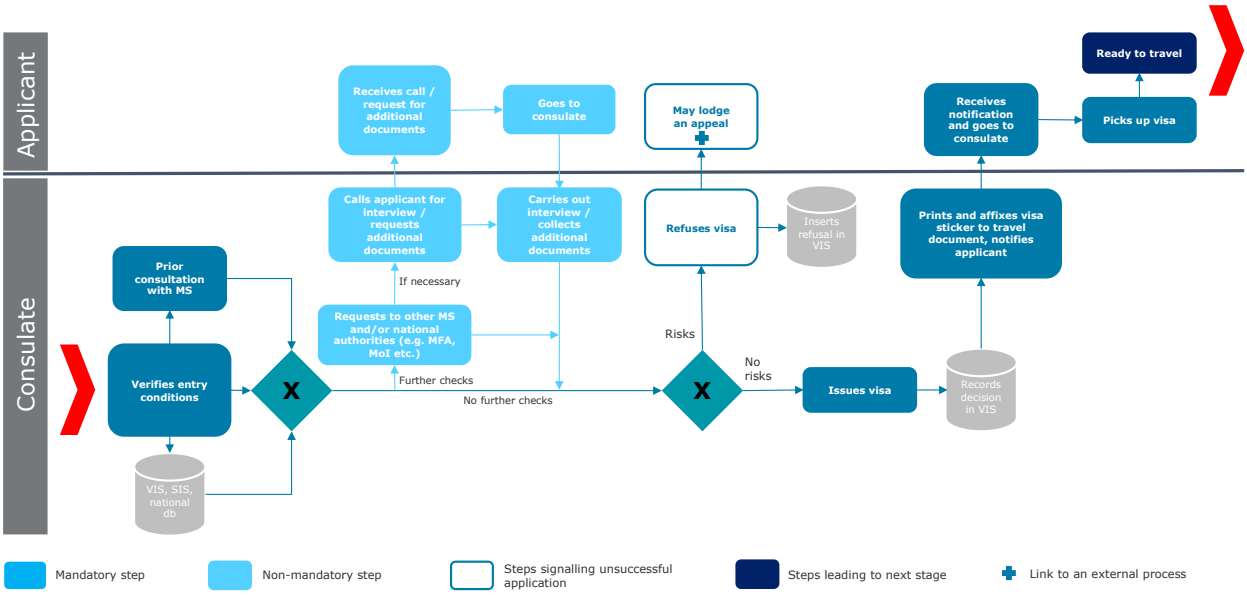

Figure 4: Examination stage

During the examination stage, the consulate assesses the information stored in VIS, checks whether any alert has been entered on the applicant in the Schengen Information System,[25] and whether the applicant is considered a threat by other Schengen countries.[26] It then carries out a risk assessment of the visa applicant and verifies his/her compliance with the entry conditions.

If the consulate needs more information, it may request that the applicant submit additional documents and/or undergo an interview about his/her planned trip.[27] Based on this information, the consulate decides either to grant or to refuse a visa.

The proof of a valid visa consists of a physical sticker, i.e. a personalised sticker (with holder's name and photo) affixed to the holder's travel document indicating the type of visa issues and the validity.

When a decision has been taken, the consulate or the ESP notifies the applicant that they should collect their travel document at the consular or ESP premises.

25 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

26 Article 22 of the Visa Code.

27 Article 21(8) of the Visa Code.

Verify the visa

After collecting the travel document with the visa sticker, the visa holder may present himself/herself at the external borders of the Schengen Area. The visa verification stage formally starts when the visa holder undergoes the first checks in his/her journey to the Schengen Area.

The figure below outlines the main types of checks a visa holder may have to go through during his/her journey and stay in the Schengen territory. Please refer to Annex I for a more detailed visualisation.

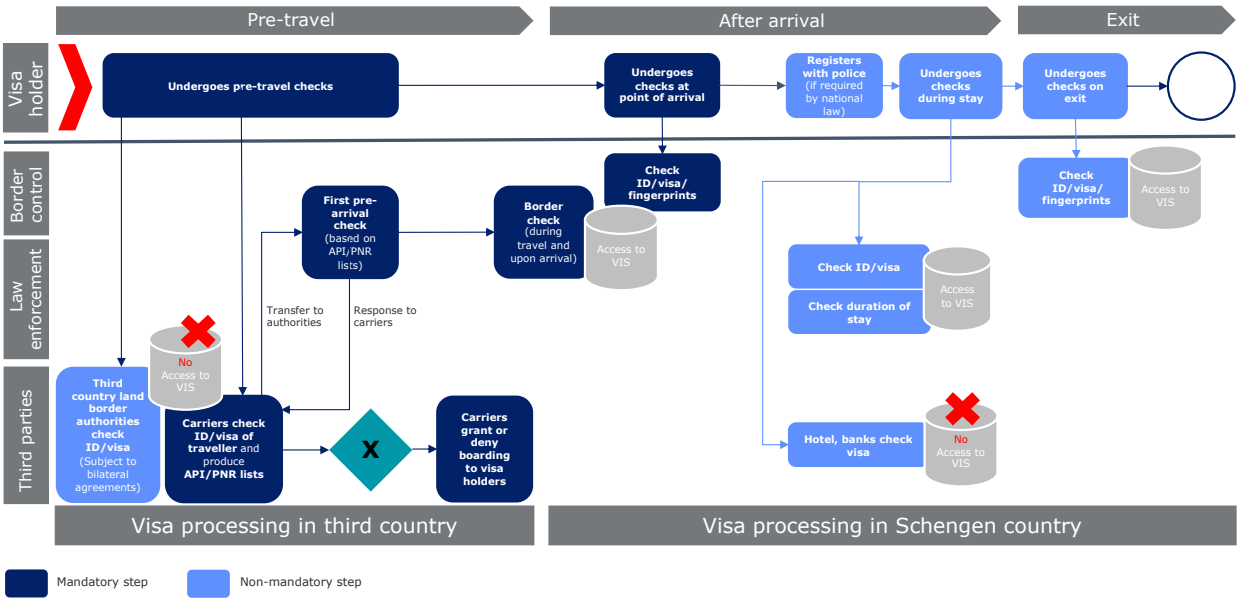

Figure 5: Visa verification before and after entering the Schengen Area

The issued visa can be checked by three main categories of stakeholder:

- Schengen country border control authorities;
- Schengen country immigration and police authorities (law enforcement);
- designated third parties, such as border control authorities in third countries, carriers and service providers (e.g. banks and hotels).

Verify visa validity pre-travel

Carriers are likely to be the first stakeholders to check the visa of a third country national intending to enter the Schengen Area. Carriers are required to ensure that third country nationals are in possession of the required travel documents and a valid visa.

Currently, carriers are not authorised to access VIS for consulting visa information stored there. They therefore rely on the physical visa sticker affixed to the travel document. However, with the implementation of the EES Regulation and the future revised VIS Regulation,[28] carriers will be able to consult a web service linked to the specific databases. In practice, this web service will launch a query about the existence of a valid visa and authorised stay for the person looking to enter the Schengen Area and provide an "OK/NOT OK" answer.

[28] Proposal for a Regulation amending the VIS Regulation: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA - amended by the European Parliament's first reading on 11 to 14 March 2019 (hereinafter: VIS Recast or Proposal for a Regulation amending the VIS Regulation).

The check on the validity of the visa by third country border authorities before departure is not a mandatory step. It depends on the bilateral agreements concluded between the particular Schengen country and the third country. Third country border authorities have no access to VIS but may be required to check the physical visa sticker.

Verify visa validity on arrival

When the third country national arrives at the Schengen border, border control authorities are required by the Schengen Borders Code (SBC)[29] to make sure that the person fulfils the conditions for entering the Schengen Area. For visa holders, this entails, among others:

- checking the authenticity of his/her travel documents, including the Schengen visa;[30]
- checking whether the travel document belongs to its holder;
- checking whether the visa belongs to its holder via two processes: 1) scanning the visa sticker number which is checked against VIS, and 2) comparing one or two fingerprints with the fingerprint set stored in the VIS record retrieved in step 1, i.e. biometric verification.

Under the VIS Regulation, border control authorities are required to run these checks in VIS for entry verification purposes.

If the third country national does not fulfil the entry conditions at the border, then they are refused entry to the Schengen Area. If the third country national fulfils the entry conditions, they are allowed to enter the territory of the Schengen country of arrival.

Once the EES is in place, border control authorities will record in the system the date, time and place of entry of third country national crossing the borders of the Schengen countries.

Once in the territory of a Schengen country, national law may require visa holders to register with the police and/or immigration authorities, which would then verify the visa holder's identity and entitlement to stay.

Moreover, private parties, such as hotels and banks operating in the Schengen Area, may also be required under the national law of certain Schengen countries to ask third country nationals to provide their travel document with a visa in order to verify their identity and legal stay in the territory. These are optional checks, and such private parties cannot have access to any data stored in VIS under any circumstances.

Verify visa on exit

At end of his/her stay, the visa holder is also checked when departing from the Schengen Area. As stated in the Schengen Borders Code (SBC)[31] (Article 8 (3)), every individual should undergo a minimal set of thorough exit checks. However, the verification that an individual is in possession of a valid visa is optional during the exit checks.

Once the EES is in place, border control authorities will record in the system the date, time and place of exit of third country national leaving the Schengen Area.

2.2.2. Border management systems

To ensure internal security and the free movement of persons in the Schengen Area in the face of challenges such as security and increasing migratory pressure, the European Union is introducing new systems such as the Entry-Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) with the aim of strengthening and securing the Schengen Area borders.

---

29 Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0818&from=EN

30 Article 8(3)(b) of the Schengen Borders Code read in conjunction with Article 18 of the VIS Regulation.

31 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

In addition, the European Union has also adopted an Interoperability Framework for borders and visas[32] and for police and judicial cooperation[33]. The aim of this framework is to provide the competent authorities with seamless, efficient and systematic access to the information they need to perform their duties. For this purpose, the current IT systems for border management need to be connected in order to complement each other and, crucially, be able to exchange data. In order to enable such interoperability, the following interoperability components need to be developed: a European Search Portal (ESP – not to be confused with External Service Provider), a shared Biometric Matching Service (shared BMS), a Common Identity Repository (CIR), a Central Repository for Reporting and Statistics (CRRS) and a Multiple-Identity Detector (MID).

The VIS is a central system linked to the national systems of all Schengen countries, which is used in consulates in countries subject to the visa requirement and at all external border crossing points of the Schengen Area to exchange data on visa applications and decisions on visas.[34] In addition to the adoption of the Interoperability Framework, the existing VIS will be upgraded[35] in order to better respond to the security and migratory challenges.

The revised VIS will be fully interoperable with other EU large-scale information systems for border and migration management, enhancing the overall security of visa processing. The VIS will run additional checks against the new IT systems to be implemented in the coming years, i.e. EES, ETIAS, ECRIS-TCN[36] and existing systems (SIS II, Europol, Eurodac and Interpol databases). These additional checks will reinforce the security checks in the application phase, rendering them more thorough and comprehensive.

Taken together, the adoption of new IT systems, the Interoperability Framework and the upgrade of current systems such as VIS will improve the security checks at the visa application stage and at the Schengen Areas external borders. This will make it possible to improve the detection of security threats and risks, while preventing irregular immigration.

2.3. Challenges

This section presents the challenges relating to, on the one hand, the current paper-based visa application, and, on the other, the visa sticker.

2.3.1. Challenges relating to the current paper-based visa application

Applicants are very much impacted by the paper-based visa application. This process is burdensome. It requires them to appear in person, either at the consulate or Visa Application Centre (VAC), to lodge their paper–based application, submit the required supporting documents (which it is sometimes mandatory to submit as originals) and to provide their biometric identifiers. In addition, the process can be expensive for applicants who have to travel to a city where there is a consulate or VAC. Moreover, applicants may make mistakes when filling in the application form or forget to submit documents due to a lack of knowledge or understanding of the information required. This can lead to them submitting an incomplete application, which could require the submission of missing documents and a second trip to the consulate/ESP or lead to the visa being refused.

---

32 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

33 Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0818&from=EN

34 This system stores the data and decisions on applications for short-stay visas to visit, or to transit through the Schengen Area. The data registered in the system include the data from the visa application, i.e. alphanumeric data on the applicant and on visas requested, links to other applications, and the facial image and the fingerprints of the applicants, as well as the decisions taken by Member States' authorities (visas issued, refused, extended, annulled or revoked).

35 The main additional measures to be included in the system are: (i) enhanced security checks across all databases: all visa applications registered in VIS will be automatically checked against other information systems, i.e. EES, ETIAS, SIS, ECRIS-TCN, Interpol and Europol; (ii) improved data and information exchange: the scope of VIS will be broadened in order to include long-stay visas and residence permits; (iii) more efficient return procedures: copies of the visa applicants travel document will be included in the system; (iv) strengthened capacity to prosecute and prevent crime: both law enforcement authorities and Europol (under strict conditions) will have a more structured access to the system for prevention, detection or investigation of terrorist offences or other serious crimes; and (v) lowering of fingerprinting age for minors from 12 to 6 years.

36 Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019, establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726

Consulates are also impacted by the current procedure, as they have to handle a significant number of paper-based applications, follow up on incomplete applications, i.e. contact applicants to provide missing information, archive those documents for at least two years, and then destroy them at the end of the retention period.

The central authorities, i.e. the ministries, need to supervise the visa procedure, but in fact have little control over application procedures and practices. In addition, the central authorities have to rent or buy real estate in order to store the paper-based applications. Some Schengen countries have considered outsourcing the storage of physical application files but this raises issues of data protection.

The table below summarises the challenges of the current paper-based visa application process that would be mitigated or disappear in an online application process. The challenges are presented for each of the different stakeholders involved.

Table 1: Main challenges of the current paper-based visa application

Stakeholder	Pain points
Visa applicants	• may not fully understand visa requirements and procedure/may not be sure about the information to be provided (as operational procedures and requirements vary across Schengen countries); • may make mistakes when filling in data; • may drop application due to complexities or low quality of services; • spend time and money to apply, especially if they live far from consulate/VAC; • repeated procedure for frequent travellers.
Consulates	Time and resources spent on: • wrong or incomplete applications; • managing paper workflow in consulates; • having to store all applications for 2 years (paper archiving).
Central authorities	• little control over the application process at local level, with practices varying widely across consulates of the same Schengen country; • need to rent premises or outsource the service in order to archive paper applications.

2.3.2. Challenges relating to the visa sticker

The physical visa is a paper sticker with security features embedding evidence that the Schengen visa has been issued, thus linking the visa application process and the visa verification process. It displays important information about the visa holder,[37] and is checked by carriers and Schengen border authorities[38] when holders are travelling to and arriving in the Schengen Area. Furthermore, the sticker can be checked by police or immigration services within the territory.

Pre-travel phase

The Schengen countries need to select, via a public tender procedure, a sticker-manufacturing company complying with the requirements. The competent authorities of the Schengen countries spend time and staff resources in the tendering process (drafting the contract; tendering and adjudication procedures), and have to allocate public expenditure to purchase the required amount of stickers. Once purchased, the Schengen countries have to securely store a large amount of stickers and at the later stage transport the requested number of stickers securely to their consulates, thus also bearing transportation costs.

Upon receipt of the blank visa stickers, consulates need to store them securely. Then, at the end of the application process, consulate staff need to fill in and affix the visa sticker to the travel document. This process requires both purchase and maintenance of the equipment for filling in stickers, and human resources to carry out these tasks.

[37] Pursuant to Annex VII of the Visa Code, the sticker displays information about; the type of visa issued, i.e. airport transit visa, long-stay visa, or Schengen visa; the period of validity and duration of the visa, i.e. the number of days during which the holder may stay in the territory, including the first and last day of validity; the territorial validity of the visa, i.e. whether it is valid in the whole Schengen Area or just in certain countries; the place and date of issuance; the number of the travel document to which the sticker has been affixed; name, surname and personal data about the visa holder.

[38] The Schengen border control authorities do not merely use the traveller's visa sticker to verify his/her identity; they are obliged by the VIS Regulation to verify the traveller's biometric identifiers (fingerprints) against the data stored in VIS.

The use of paper-based visa stickers also entails challenges and costs for the applicants. First, applicants need to leave their travel document at the consulate (or VAC) for an authenticity assessment and for the sticker to be affixed to it, reducing their international mobility (if they do not hold another travel document). Moreover, once granted a visa, applicants have to collect their travel document from the consulate/visa application centre or pay a courier fee in cases where the ESP arranges home delivery of the travel document upon issuance of the visa. Applicants thus incur costs, in money and time, twice.[39]

After-arrival phase

The sticker also has an impact on the verification process. In order to verify the traveller's identity, the Schengen border control authorities are required by law to use inter alia the visa sticker number to launch a query in VIS and proceed to the biometric verification. However, according to eu-LISA's statistics, border control authorities only check, on average, 50% of visa holders against the biometric data in VIS at entry. The main reasons for this low percentage are the time pressure and the high number of third country nationals to be cleared. Border control authorities therefore rely heavily on the visa sticker to conduct the security verification check, instead of on VIS and the biometric identification. This could lead to potential immigration and security challenges as the visa sticker can be counterfeited and the counterfeit not detected by the border control authorities (despite their expertise and training in this).

Furthermore, carriers need to check whether travellers have the documents required for entry, including a valid visa. However, carriers are not required to check that third country nationals fulfil the entry conditions. They are only required to check the documents. Other third parties (such as hotels, banks and employers) may be affected depending on whether they are required under national law to verify the visa of a third country national.[40]

The following table sums up the main challenges arising from the production and use of the visa sticker.

Table 2: Main pain points relating to the current visa sticker

Stakeholder	*Challenges*	
	Pre-travel phase	*After-arrival phase*
Visa applicants/ visa holders	• need to come back to consulate/visa application centre to collect travel document with sticker affixed; • have reduced mobility while application is being examined, because the passport stays at consulates.	Spend more time at the border to allow authorities to check the sticker on top of their biometrics (*if authorities carry out all required checks*).
Central authorities and consulates	Incur costs for: • procuring the sticker production service and paying the sticker manufacturing company; • transporting stickers to the consulates securely; • storing stickers securely; • consulate staff dedicated to low added-value activities, such as filling in and affixing the sticker and maintaining related equipment.	
Border authorities		Risk being inclined to check only the sticker (for counterfeiting and forgery) at the border without carrying out biometric verification against VIS.

[39] The first time being in the application phase, to lodge the application.

[40] For example, hotel and accommodation services in Italy are required to collect data from the guests' travel documents and send those data to the State Police for verification.

3. Options

The challenges identified in the previous chapter highlighted two areas where digitalisation can lead to improvements:

- the current paper-based visa application process;
- the use of a physical visa sticker.

The transition from paper-based to digital solutions would apply to the whole visa process, including the steps that take place after the Schengen countries issue visas to third country nationals.

Although the two areas cover fundamentally different processes, digitalisation aims to:

1. offer the applicants a better user experience during the visa process;
2. enable the Schengen countries to leverage technology to their advantage in order to make the visa process more efficient and contribute to the internal security of the Schengen Area.

This chapter identifies a number of options for the digitalisation of these areas, in line with these objectives, and assesses their feasibility. These options entail proposing new processes for the Schengen countries, and the development of new systems at both central and national level.

3.1. Online application

This section deals with the first area of improvement, i.e. the application process that is currently paper-based, despite certain Schengen countries having introduced online application tools. To digitalise the current application process, this study explores an *online* application process. This online application process involves the creation of an EU-level online application portal covering all Schengen countries for Schengen visa applicants worldwide. Instead of each Schengen country operating their own national portals, this new approach will offer a single interface through which all applicants can lodge their visa applications. The process has been designed based on the steps that applicants and consulates need to accomplish.

This proposal requires a modification of the visa application process in the following key phases.

- **Application:** identification and determination of the application type by asking key questions to applicants. Based on the answers provided, the online application portal will inform applicants of the visa type, competent Schengen country, supporting documents to be provided, need for an appointment and where to go, visa fee, etc.
- **Appointment (where needed):** physical touchpoint of the applicant with the consulate or ESP to provide the necessary documents (travel document or supporting documents in paper) or biometric identifiers. With the introduction of the new process, this appointment would only be needed when:
    - an applicant needs to provide his/her biometric identifiers (first time and every five years thereafter);
    - an applicant acquires a new travel document which has not yet been registered in VIS; or
    - an applicant needs to submit specific supporting documents that can only be checked in paper format, e.g. for authenticity checks.
- **Processing:** automated admissibility and completeness check. At this point, and with the introduction of the advances in interoperability, VIS triggers multiple queries to the other EU IT systems and other databases, e.g. Interpol and Europol, in order to detect whether the applicant does not have identity data, i.e. biographic and biometric, inconsistencies and hits across different systems, e.g. against SIS.

The figure below visualises the steps in each phase. In order to propose a consistent and coherent online application process, digitalisation would entail a number of options at both business and system level:

- digitalisation at business level includes the options to introduce digital technologies at each step of the application process, e.g. the submission of the travel document and the payment of the visa fee.

- digitalisation at system level includes the options to adjust the current IT architecture landscape for the Schengen visa and introduce the technical components hosting the features envisaged at business level.

The table below zooms in on each phase of the application process and, for each step, highlights:

1. the current situation;
2. how the future solution envisaged by the online application process would look;
3. the challenges stemming from the future solution;
4. the technical option(s) proposed.

The following sections then detail possible options and their feasibility for both the business and system architectures. In particular, the feasibility assessment analyses the legal, technical, security, data protection, operational and implementation implications and challenges of the proposed options.

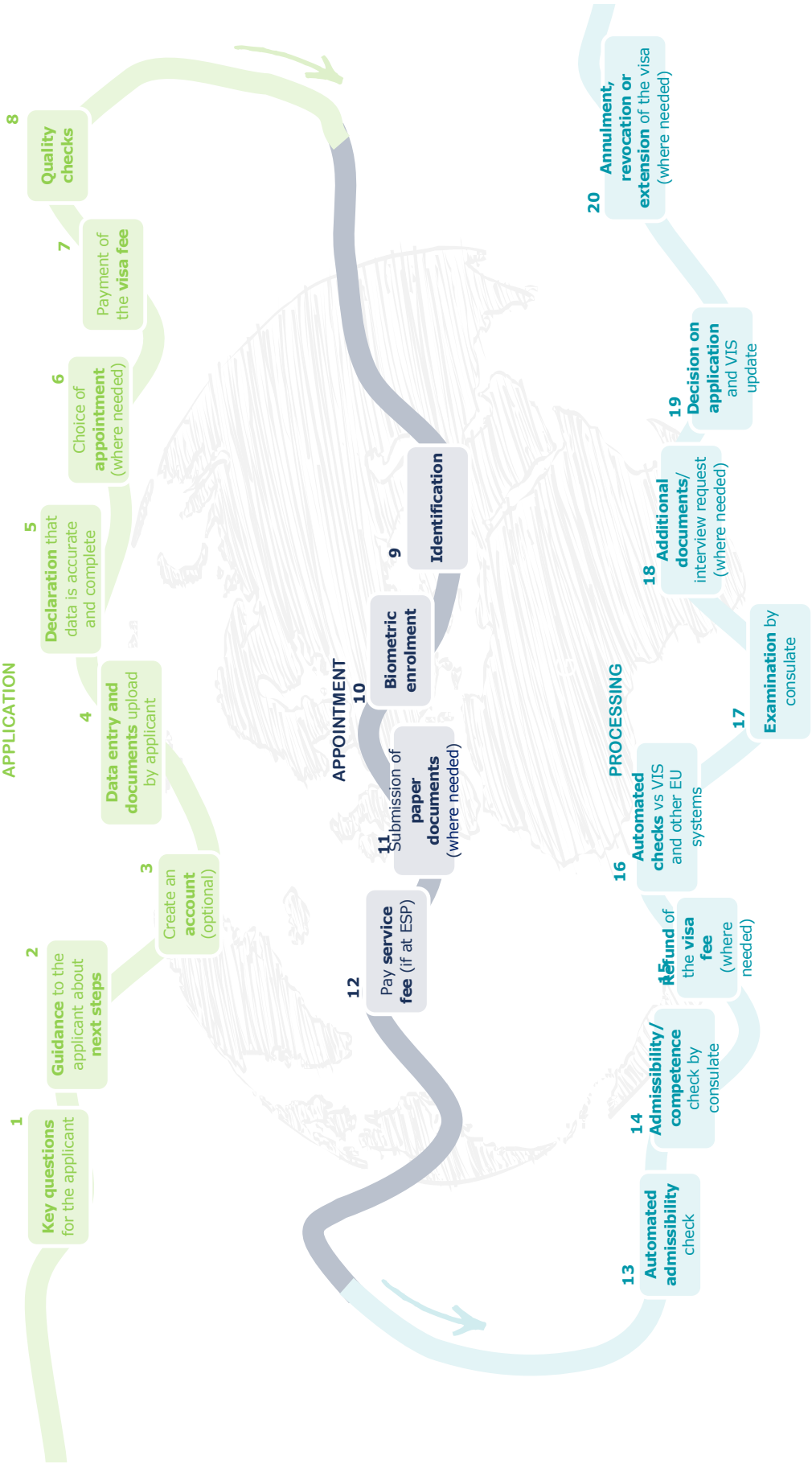

Figure 6: The proposed new visa application process

Table 3: Detailed overview of the considerations relating to different steps in the visa application process

Step	Current situation	Future Solution	Challenges	Option(s)
Application phase				
1) Key questions for the applicant	Static information provided on the website of each consulate. Limited guidance on what type of visa is required for which type of travel.	Online application portal with a unique source of dynamic information for the applicant covering the whole Schengen Area. This depends on the answer to different questions, such as: • nationality, • residence, • length of stay, • main destination, • travel purpose, • previous applications and date, • travel document type and number, • date of birth, • family member of EU citizen.	Schengen countries must be able to configure the key questions in the online application portal, such as the following: • locations of consulates and ESP • Optional visa exemptions, e.g. for diplomats • Optional visa fee exemptions • Supporting documents required (where no harmonised list exists).	A set of configurable questions (per Schengen country) to which an applicant must provide answers.
2) Guidance to the applicant about the next steps	Information on the website of each Schengen country; no consolidated source of detailed information for the whole Schengen Area. Phone call (to consulate/ESP).	Online application portal that informs applicant of: • visa type required; • visa fee or fee waiver, e.g. for Visa Facilitation Agreements (VFA), children, family member; • competent Schengen country issuing visa; • supporting documents required; • need for appointment or possibility of applying online without any appointment. By guiding the applicant, the "first-time right" percentage of applicants can be increased.	Ensuring information is presented to the applicant according to specific requirements of the different Schengen countries. Ensuring the portal can check in VIS whether biometrics have been provided in the previous 59 months or whether it is a known travel document to determine whether an appointment is necessary.	Interactive, dynamic website informing applicant in accordance with his/her answers to key questions, e.g. by means of a chatbot, FAQ sections, tool tips next to data entry fields, etc.
3) Create an account (optional)	Generally N/A. Some countries already require applicants to create an account.	Possibility of creating an account with email address and password and saving progress (to complete the application in different stages). Data from draft applications are stored for a predefined period. Creating an account can give the applicant the ability to check the information about his/her visa such as: • status of the visa application • status of the visa; • expiry date of the biometrics • notifications on documents necessary for the application process.	Authenticating and authorising users (access & identity management). Secure storage of personal identification data.	Use of Multi-Factor Authentication (MFA) by, for instance, means of a password, reference number, email verification and/or text message.

Step	Current situation	Future Solution	Challenges	Option(s)
4) Data entry and documents upload by applicant	Fill in application form (manually or electronically; in the latter case it still needs to be printed). Physically submit document at the consulate or ESP.	Online application portal with digital application form: • data entry (manual or automated, for certain fields); • quality checks to ensure data are filled in accurately; • data from prior applications can be used for this purpose. Upload of: • supporting documents • travel medical insurance • copy of travel document's biographic page. The online application portal should differentiate between which documents can be provided electronically and which must be provided physically.	Documents provided: • ensuring data are transmitted securely to the portal; • deciding which documents can be provided digitally (upload/scan) and which in paper form; • ensuring that documents provided electronically are authentic. Storage: • moving from paper-based archive to a digital repository of documents; • secure storage, e.g. by use of a private cloud.	Documents provided: • provide in paper format; • upload a scanned version of the supporting document; • upload electronic format of the supporting documents (in native format, e.g..pdf,.docx, etc.); or • direct access through third-party gateways. Storage: • centralised: documents are stored in the databases of eu-LISA; • decentralised: documents are stored locally in the databases of the Schengen country.
5) Declaration that data are accurate and complete	Handwritten signature on application form confirming consent.	Consent "tick box" declaration (similar to ETIAS).	Ensuring that the "tick box" complies with the legally relevant definition of 'signature'.	Embed a "tick box" in the digital application form, which needs to be checked before submitting the application.
6) Choice of appointment (where needed)	Appointment tool specific to Schengen country (consulate/ESP) or phone call to the consulate/ESP.	Redirection from the online application portal to the appointment tool or details of the competent Schengen country consulate/ESP; and/or Central appointment tool (on the portal, managed by the consulates and ESPs).	Redirecting to the application tool only when a physical meeting is required; URL link management: dealing with broken links or changed domains; Receipt of confirmation on the appointment to be able to continue with the process.	Decentralised booking tool redirecting the user from the online application portal to the specific tool of each consulate or ESP. Central appointment tool (on the portal, managed by the consulates and ESPs).
7) Payment of the visa fee	Direct payment to the consulate or ESP using different methods offered in euro or local currency (depending on the Schengen country).	Use of a third party payment gateway linked to the online application portal. Payments are directly transferred to appropriate Schengen country (or consulate). The payment tool offers different methods of payment such as credit cards, debit cards, mobile payment or online payment parties, such as PayPal.	Choice of third party provider with required capabilities. Ensuring: • payment is transferred to the rightful party; • ability to refund applicants in event of a wrong payment.	Central gateway, single account: applicants pay their fee through a uniform gateway, after which the money is collected in a single account, and then distributed to the appropriate country afterwards. Central gateway, multiple accounts: applicants pay their fee through a uniform gateway, after which the money is immediately allocated to the correct Schengen country's account. Multiple gateways: each Schengen country is responsible for operating and maintaining their own payment gateway to which the applicants will be redirected from the application portal.

Step	Current situation	Future Solution	Challenges	Option(s)
8) Quality checks	Quality check by the ESP / at the counter of the consulate.	During the application process automatic quality checks are performed. These inform the applicant if there are errors in the information provided or if the applicant does not meet the specified requirements.	Agreeing on a common set of quality parameters assessing the quality of data and documents provided, e.g. resolution, format, size, readability index, brightness.	Two complementary options: • "real-time" data quality checks, i.e. while typing/uploading; • final data validation check prior to sending for review to the consulate.
Appointment phase (where needed)				
9) Identification of the applicant	Physical identification at the consulate or ESP by providing travel document and application reference number.	No change, but this requires ESP/consulate access to the data stored on the online portal.	Ensuring: • access for consulate/ESP staff to the online portal; • access is only given to the intended individuals; • applicants provide consent to consulate/ESP to access the application file.	Different user profiles managed by the digital application portal depending on the user. Use of access and identity management systems to authenticate and authorise these users.
10) Biometric enrolment (where needed)	Provide fingerprints and facial image at consulate or ESP.	No change.		Enrolment only for first-time applicants or expired biometrics. "Enrol from anywhere" using technology to send biometric identifiers, e.g. using mobile phone.
11) Submission of paper documents (where needed)	Physically submit document to consulate or ESP. The document may also be scanned by the consulate/ESP for electronic archiving.	No change.		
12) Pay service fee (if at ESP)	Direct payment to ESP.	No change.		
Processing phase				
13) Automated admissibility / completeness check	Generally N/A – as much of the processing is still paper-based, automated checks are not possible. However, some countries, e.g. France, have this feature as they use an online portal.	Within the online application portal an automated check is performed. The check ensures that the information provided fulfils the requirements for the requested visa, e.g. if three documents are required, the system checks if three documents were actually uploaded. The system notifies the applicant if a document is missing, biometrics are not recorded in VIS, etc. and the system provides the applicant with the possibility of correcting the application.	Implementing the checks in a way that takes into account requirements of different Schengen countries. Notifying applicants (automated email).	Online application portal with integrated business logic.
14) Admissibility/ competence check by consulate	Manual check by consulate staff.	No change, but this will have to be done "on screen" instead of "on paper".	Organising checks when data are stored centrally or within each Schengen country. Notifying applicants (automated/manual email).	

Step	Current situation	Future Solution	Challenges	Option(s)
15) Refund of the visa fee (where needed)	Via the same means as payment, which depends on the consulate or ESP (credit card, bank transfer, cash, etc.)	Third party gateway (used for initial payment) refunds the applicant.	Ensuring consulates are able to specify which individuals need to be refunded and share this information with the requisite service provider.	Third party payment gateway.
16) Automated check against VIS and other EU systems	VIS search and SIS check (through the national system). After the VIS Revision, these checks will be automated.	No change.		
17) Examination by consulate	Manual check and assessment against information from third countries or private companies, e.g. insurance, hotels, banks etc.	No change, but this will have to be done "on screen" instead of "on paper".		
18) Additional documents/ interview request (where needed)	Contact applicant by phone or by email.	Online application portal informing applicant using the built-in notification tool.	Notifying applicants (automated/manual email). Individualising messages. Informing and teaching case workers how to use the online application portal for communication with the applicant.	Use of a notification tool linked to the applicant's account.
19) Decision on application and VIS update	Decision on the visa Different ways of notification that the decision has been taken (tracking tool / text message). Pick-up of travel document Necessary to visit consulate or ESP to obtain the travel document with visa sticker.	Decision on the visa Notification tool informs the applicant when status changes. Pick-up of travel document No visit necessary. The proof of the visa is sent electronically.	Ensuring that: • in event of inability to reach VIS, border guards can still check if a traveller has a valid visa; • Schengen police authorities and third country authorities are able to check visas without stickers.	Different fallback solutions exist should one or more systems fail: • email notification with confirmation (alphanumeric); • email notification with barcode; • email notification with digitally signed barcode.
20) Annulment, revocation or extension of the visa (where needed)	Appearance in person, if revocation or extension requested by visa holder. Where needed, the consulate provides information by means of a letter or phone call.	• Communication tool allows applicant to request withdrawal or extension of the application or revocation of the issued visa. • Notification tool informs the applicant when status changes.	Informing the visa holder that the visa is revoked or extended before trip is initiated.	A notification tool informs the traveller of any changes relating to his/her visa; A communication tool to request extension or revocation of a visa; In the event of an extension, the traveller receives a confirmation with an updated barcode.

3.1.1. Proposed options

The following section highlights and describes the proposed options for both the business and the system architecture.

Business architecture options for the online application portal

The business architecture options cover the features required for the new online application portal from an applicant's point of view. The steps in the online application process, as described in Figure 6 above, can be grouped into seven main functional blocks: (1) filling in the online visa application form, (2) providing the travel document, (3) providing supporting documents, (4) collecting biometrics, (5) declaring data are accurate and complete, (6) paying the visa fee and (7) interacting with the applicant.

Taking into account the desk research, national and strategic interviews, and the multiple workshops carried out for this study, two options have been developed as aggregated solutions to manage the whole online application process. These two options can be distinguished by their level of digitalisation:

- The **fully digital (option A1)** aggregates the most digital and far-reaching options developed during the study.
- The **custom digital (option A2)** encompasses a mix of digital options and the status quo, mainly in terms of the travel document, supporting documents and collecting biometrics.

The following subsection briefly describes both options so the differences become apparent.

The 'fully digital' online application portal (option A1)

Option A1 offers a fully digital user experience with multiple features aimed mostly at guiding the applicant during the entire application process and ensuring data are submitted accurately and correctly.

During the application process, applicants will need to submit their travel document information (alphanumerical data) and provide a scan of their travel document's biographic data page. The fully digital online application portal will only support the electronic submission of this travel document information (by filling out a form or scanning the travel document's Machine Readable Zone). The physical submission of the travel document will no longer be required.

Applicants must also submit supporting documents during the application process. In this option, along the same lines as for the travel document, the physical submission of these documents is no longer necessary. This option allows for the uploading of documents in their native digital format or a scanned version. Furthermore, the fully digital online application portal introduces a new concept: the submission of supporting documents through permission gateways. In this concept, the consulates would, with the applicant's permission, be able to request supporting documents directly from third parties (such as bank statements from banks, or reservations from hotels). This process ensures the authenticity of the documents and reduces the burden on the applicant of collecting these documents.

For the collection of biometric identifiers, an applicant can submit their biometric identifiers from any location with internet access using a specific application, thereby exempting them from the obligation to present themselves at a consulate or at a visa application centre.

In the visa application process, an applicant must declare that the data provided are correct and complete. Currently, this happens through a paper-based signature. Option A1 does not require any specific action from an applicant to make this declaration. The online application portal assumes that this declaration is implicit with the submission of the application and the payment of the visa fee.

For the payment of the visa fee, the applicant will be redirected to a central payment gateway. All payments will be collected by a central account and subsequently distributed to the appropriate Schengen country.

Finally, the online application portal will enable interaction with the applicant. This feature will include:

- notifications (custom/automated messages to provide information on visa issuance, on the revocation or extension of the visa and on the status on his/her biometric data);
- appointment scheduling;
- the ability for the applicant to check the status of his/her visa application;
- the status of the applicant's visa, i.e. validity and remaining stay;
- the status of applicant's biometric data.

All the required application data can be submitted online via option A1. Therefore, no visit to the consulate/ESP would ever be necessary.

The 'custom digital' online application portal (Option A2)

Option A2 offers, similar to option A1, a fully digital user experience with multiple features aimed mostly at guiding the applicant during the entire application process and ensuring data are submitted accurately and correctly.

During the application process, applicants will need to submit their travel document information and provide a scan of their travel document's biographic data page. Option A2 supports the electronic submission of this travel document information (by filling out a form or scanning the travel document with a smartphone). Nevertheless, the status quo, in which the travel document is physically submitted at a consulate or ESP, will be necessary for first-time applicants or applicants who have acquired a new travel document.

Applicants must also submit supporting documents during the application process. In this option, along the lines of the travel document, the physical submission of these documents is still an option (where considered necessary). This option also allows the uploading of documents in their native format or for upload of a scan. This option does not provide for third-party gateways to submit supporting documents.

For the collection of biometric identifiers, the custom digital online application does not change the status quo: the applicant would still be required to present themselves physically at a consulate, or at a visa application centre, if the person is applying for the first time (or every five years thereafter).

In the visa application process, an applicant must declare that the data provided are correct and complete. Currently, this is achieved by means of a paper-based signature. Option A2 replaces this physical signature with a 'tick box'. By 'ticking' this tick box, an applicant declares that the information filled out and uploaded is correct, complete and reliable.

For the payment of the visa fee, the applicant is redirected to a central payment gateway, which automatically redirects the money to the appropriate Schengen country.

Finally, the online application portal will offer interaction with the applicant. This feature will include:

- notifications (custom/automated messages to provide information on visa issuance, on the revocation or extension of the visa and on the status of his/her biometric data);
- appointment scheduling;
- the ability for the applicant to check the status of his/her visa application;
- the status of the applicant's visa, i.e. validity and remaining stay;
- the status of the applicant's biometric data.

Overview

The table below shows an overview of the descriptions above of both business architecture options. For a detailed description of each functional block's possible options, please refer to Annex E.

Table 4: Summary of the options per business architecture

	Functional blocks	Analysed options	Option A1	Option A2
1	**Filling in online application form**	Premium (a digitally enhanced application form including configurable questions and automated field completion)	✓	✓
2	**Providing travel document**	Physical submission of the travel document (*status quo*)		✓
		Scan of travel document's biographic data page (*status quo*) – this is a required step for all applicants[41]	✓	✓
3	**Providing supporting documents**	Provide supporting documents in paper (*status quo*)		✓
		Scan documents	✓	✓
		Upload documents	✓	✓
		Third-party gateways	✓	
4	**Collecting biometrics**	Enrol biometric identifiers on the premises of the consulate or VAC (*status quo*)		✓
		Enrol biometric identifiers electronically from any place	✓	
5	**Declaring data are accurate and complete**	Tick box declaration		✓
		Implicit declaration	✓	
6	**Paying the visa fee**	Central gateway, one account	✓	
		Central gateway, multiple accounts		✓
		Multiple payment gateways		
7	**Interacting with the applicant**	Centralised appointment management tool	✓	
		Decentralised appointment tool offering redirections to local appointment tools.		✓
		Status checking tool	✓	✓
		Electronic notification tool	✓	✓

Supporting system architecture of the online application process

This section presents and describes the different options for the system architecture. To construct these system architecture options to digitalise the visa process, the regulation of the existing and future landscape of EU information systems was taken into account. The implementation of new systems (EES, ETIAS, ECRIS-TCN), the adaptation of existing systems (VIS, SIS and Eurodac) and the interoperability components[42] will strengthen the security of border management within the Schengen Area by providing responsible authorities with fast, controlled and streamlined access to facilitate the checks on third country nationals.

In addition, moving towards an online visa application process opens up opportunities to leverage and reuse components of the EU landscape, e.g. EES and ETIAS, and reflecting on how different architecture scenarios will process the required operations, e.g. the application status retrieval through the read-only database (similar to the process in ETIAS).

Based on this approach and using the status quo system architecture as a reference (see Figure 7), two main system architecture options were developed. Before detailing both options, the status quo must be presented since it is considered the baseline of the present study.

[41] Future Article 9(7) VIS Regulation
[42] CIR, MID, sBMS, ESP and CRRS.

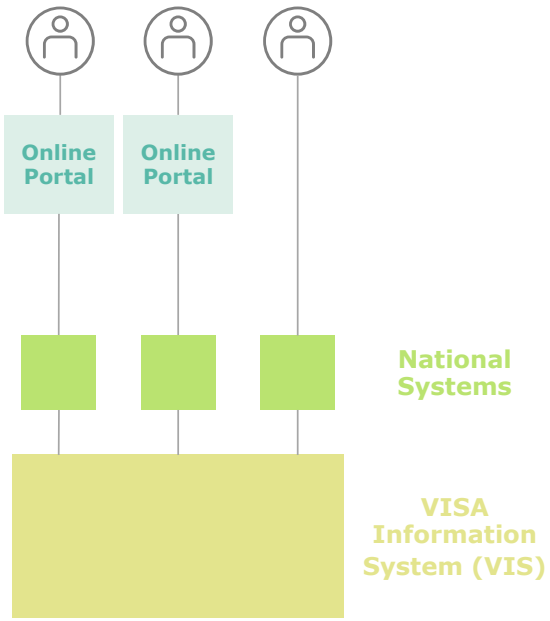

Figure 7: Status quo (system architecture)

Some Schengen countries have adopted their own online application solution with different levels of maturity and sets of features, while others still rely on a manual and paper-based visa application process. The image above demonstrates both positions. Although the visit of the applicants to consulates or visa application centres is currently mandatory, e.g. to submit supporting documents in paper and for the collection of biometric identifiers, applicants can use to the Schengen countries' online portals to submit part of their application online, e.g. to submit the application form and pay the visa fee. In both cases, i.e. with or without an existing portal in place, the application data are stored and processed in the national systems and is then pushed to the central VIS.

It is not the aim of the proposed options to modify the current process performed by Schengen countries significantly. As is the case today, the final decision-making remains at the consulate level through the national systems. Furthermore, the management and creation of new records in VIS also remains the responsibility of the Schengen countries. The core difference between the status quo and the proposed system architectures is the creation of a centralised online application portal, available to all applicants. This common portal will be the unique point of entry for all applicants wanting to apply for a Schengen visa, regardless of their country of origin and the country/ies they plan to visit.

The following figure presents the conceptual representation of both proposed system architectures, B1 (central portal and storage) and B2 (central portal and decentralised storage):

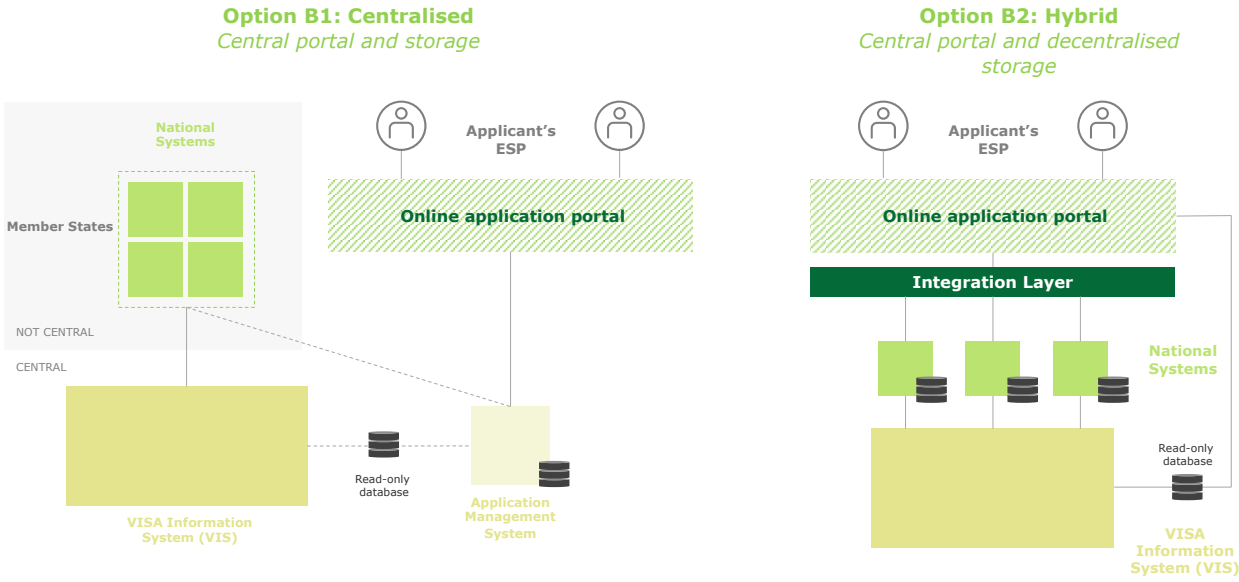

Figure 8: System architecture options

The main difference between the proposed options is the location of application data storage before being recorded in VIS. In option B1, all data provided by the applicants, including identity data and supporting documents, are stored at a central level within the Application Management System (AMS). In option B2, all these data are stored in the different national systems owned by the Schengen countries.

The description of the data flow of both options makes it possible to understand their functional and technical particularities.

In **option B1**, a third country national who wants to apply for a Schengen visa has to access the online application portal. The applicant must fill in all the data required and submit the supporting documents via the portal.[43] In order to enable applicants to save the application for a later submission, the online application portal should store data temporarily (possibly in a private cloud solution, such as the Common Shared Infrastructure, which is operated and maintained by eu-LISA[44]).

Once the applicant has submitted the online application, the application file is transferred to the Application Management System. This system is composed of a database[45] and an integration layer to transfer the relevant data to the national systems.[46] In order to take the decision on whether to grant a visa, the visa officer from the consulate can consult the supporting documents stored in the AMS for examination purposes.

Once the decision is made, the central VIS will be updated through the existing channels between the national systems and VIS in accordance with the current VIS Regulation.[47] At this moment, the applicant is notified of the decision whether the visa has been granted. For this purpose, the Application Management System must retrieve the data from the central VIS (the access would be through a replicated read-only database). Furthermore, the AMS will also use this read-only database to consult:

43 Unless the applicant needs to submit some supporting documents to the consulate or visa application centre.

44 The Common Shared Infrastructure (CSI) can be considered a private cloud for EU central information systems. The CSI will be hosted at the eu-LISA premises and serve as an IaaS (and later PaaS) for the systems for which eu-LISA is responsible. This cloud will be hosted by eu-LISA, and will be shared by all systems and components. A more detailed description of this CSI is out of scope for this study. However, as it will be shared by all these systems, the required security and data protection principles will be in place. Furthermore, as the scale of the temporary storage of application files is minimal compared to the other systems the CSI needs to support, no technical infeasibilities are foreseen.

45 The AMS would store application files submitted (biographic data, biometric identifiers, supporting documents, photograph etc.). Once a visa application has been processed and the visa data entered in VIS, the AMS is updated so as to delete the data inserted in VIS (to avoid data duplication). Furthermore, the data remaining in the AMS (e.g. supporting documents) is retained for a period of one year in case it is needed for appeal procedures. A link is maintained during this retention period between the data in the AMS and the data inserted in VIS.

46 Article 9, VIS Regulation

47 Articles 10, 11, 12, 13 and 14, VIS Regulation

- the status of the visa;
- the status of the biometrics;
- whether a travel document is already registered.

The tools enabling the interaction with applicants (visa status checking tool and electronic notification tool) will be embedded in the online application portal and can be linked to the AMS.

In **option B2,** as in option B1, applicants have to access the online application portal directly in order to fill in the required data and submit the application form and supporting documents. In order to enable applicants to save the application for submission later, the online application portal should be able to store data temporarily (possibly in a private cloud solution, such as the Common Shared Infrastructure operated and maintained by eu-LISA).

Once the applicant has submitted the online application, the application file is transferred to the different national systems via an integration layer. This decentralised storage is similar to that currently used by some Schengen countries: some Schengen countries operate a direct link between their online application portals and their national systems, which contain a national database on which the application files are stored. This option envisions something similar, with the particularity that the entry point is common for all applicants, hence requiring an integration layer to connect this online visa application portal to the different national systems. Consulate case workers consult the information stored at a national level and push the data to the central VIS.[48]

In order to interact with the applicant, the online application portal must consult the VIS data through a replicated read-only database. This read-only database stores the necessary information so that applicants can check the visa status, application status, biometric status and whether a travel document has already been registered.

3.1.2. Feasibility assessment

This section analyses and compares the proposed options for the online application portal.

Business architecture

To compare the possibilities for the online application portal, the following subsections analyse the functional blocks individually, highlighting the key aspects of options A1 and A2.

Filling in the online application form

The 'premium' electronic application form allows a user to fill out the required identity and travel document information in an electronic form, supported by dynamic user guidance.

The premium option offers applicants an alternative for filling out part of his/her application form, namely the travel document information section:

- manually fill out the travel document information; or
- scan the travel document's Machine Readable Zone (MRZ).

In the first alternative, applicants simply enter their travel document data in the corresponding fields, similar to other identity information in other parts of the application form.

The option to scan the travel document's MRZ, allows the applicant to scan the travel document's MRZ, which will then automatically fill out the required fields. This could be achieved by uploading a photo of the MRZ or the use of a hardware scanner, which both require a certain level of technical knowledge and capacity of the applicant. Furthermore, not all the 104 countries that are currently subject to the visa requirement offer a MRZ on their travel document. Therefore, this option only applies to a limited number of countries so the online portal should always retain the possibility for the applicants to fill out the required fields manually.

[48] Articles 9, 10, 11, 12, 13 and 14, VIS Legislation.

As both option A1 and option A2 adopt the premium application form, there are no differences between the options.

Providing travel document

The 'providing travel document' functional block envisages two actions that could be adopted to verify the validity of the travel document. These actions are *not* alternatives, and could be adopted together. The two actions to be given consideration are:

- physical submission of the travel document (status quo);
- submitting a scan of the travel document's biographic data page (status quo).[49]

Both proposed business architectures are the same, except that option A1 will no longer require the physical submission of the travel document. Option A2 maintains this requirement for first-time applicants and applicants who have acquired a new travel document that has not yet been registered by a consulate.

The first action, the physical submission of the travel document, is the current status quo, which means the required processes are already in place, and the option is feasible on all domains. However, it has become apparent from interviews and workshops with stakeholders that the physical submission of the travel document at a consulate or a visa application centre will remain necessary for the foreseeable future for security reasons for first-time applicants and in the event of new travel documents. By requiring an applicant to appear in person, the link between the travel document holder and the authentic travel document can be established. This process requires an authenticity check of the travel document (which can currently only be done physically) as well as the physical presence of the travel document holder.

The second action, where a scan of the travel document's biographic page, is uploaded, is necessary to comply with a requirement that will apply under the future revised VIS Regulation. Therefore, this feature has to be included in both system architectures. As this process involves attaching an image file to the application, no infeasibilities are foreseen for this process.

In conclusion, the preferred business architecture would always need to support the upload of a scan of the travel document's biographic page. Furthermore, an assessment has been made that for security reasons first time applicants and applicants who have acquired a new travel document would need to present their travel document at a consulate/ESP. This leads to a solution where both actions are adopted simultaneously. This corresponds to the actions supported by option A2.

Providing supporting documents

The 'providing supporting documents' functional block envisages four options:

- provide supporting documents in paper (status quo);
- scan documents;
- upload electronic documents;
- third-party gateways.

These options are four routes to achieving the same goals.

There are differences between the two business architectures in two areas: option A2 offers applicants the ability to provide supporting documents in paper, while option A1 introduces third-party gateways to acquire supporting documents. Both options support the uploading of scans or native format documents.

The differentiation element in option A2, namely **providing supporting documents in paper**, is the current status quo. Thus, means the required processes are already in place, and the option is feasible on all domains. During discussions with the Schengen countries' representatives, it was noted that the current status quo would need to remain in place for the foreseeable future. Two reasons for maintaining the status quo were put forward.

[49] Future Article 9(7) VIS Regulation

- An applicant should retain the right to bring originals if they do not have the technical means to acquire electronic scans/documents; and
- Some supporting documents, e.g. civil status, currently need to be provided in paper format in order to be able to check their authenticity. Therefore, to prevent an increase in fraud, the status quo process needs to be retained.

The second and third options entail the same technical process: attaching an electronic document to the application file. Like the upload of a scan of the travel document's biographic page, this process does not pose any technical infeasibilities. Both options should be included as some documents may not be available in an electronic format, and must thus be scanned.

However, during a workshop with the Schengen countries representatives, it became clear that the third-party gateway solution is not feasible from a practical perspective in the foreseeable future. The establishment of such a system would make it necessary to organise and set up agreements between an immense number of parties. For instance, just taking into consideration the retrieval of bank statements would mean that the online application portal would need to interface with all major banks around the world. Furthermore, this would require those external parties to cooperate without being offered a clear incentive for doing so.

Based on the above assessment, the conclusion can be reached that implementing third-party gateways is not feasible in the current landscape. Furthermore, as the provision of supporting documents in paper format must be included regardless, option A2 is clearly preferable.

Collecting biometrics

Although some third countries are enabling applicants to enrol biometrics from any location, for visa processing it makes sense to stick to the status quo for the time being. In fact, the digital option for biometric enrolment is in contradiction with the current requirements of Schengen visa policy. After submitting their applications online, the applicants are required to present themselves at the premises of the consulate or at a visa application centre to carry out the biometric enrolment (fingerprints and facial image). This ensures consulates can observe the physical presence of the individual, their travel document and the biometrics in a controlled environment. Allowing mobile enrolment from a remote area would void the possibility for this 'three-fold observation' and thus increase the risk of identity fraud. According to feedback from national representatives, this 'three-fold observation' needs to stay in place for the foreseeable future.

Some Schengen countries are also providing mobile kit solutions for biometric enrolment for visas.[50] In this case, authorised personnel from consulates and/or visa application centres organise missions throughout the territory of third countries to collect biometrics.

The possibility for applicants of enrolling their biometric identifiers remotely would increase the risk of identity fraud. Therefore, option A2 is clearly preferable from a security perspective.

Declaring that data are accurate and complete

The choice of including a declaration stems from the fact that, legally speaking, an applicant must be required to perform an action, such as a signature or clicking a disclaimer. As the smart implicit declaration does not imply the applicant performing a specific action, it is not feasible without any legal amendments. Therefore, as ticking a tick box is also more transparent for the applicant, (he/she is consciously declaring the data are accurate and complete); the preferred choice would be to implement such a tick box in the online application portal, as proposed by option A2.

[50] Belgium is piloting mobile biometric enrolment in China and will soon do so in India. During interviews it was observed that some ESPs currently offer a similar service (so-called 'added-value' service) to applicants willing to pay a higher service fee.

Paying the visa fee

The 'paying the visa fee' functional block envisages three options:

- a central payment gateway with one account;
- a central payment gateway with multiple accounts;
- multiple payment gateways.

Both option A1 and A2 consider a central payment gateway, but use a single account or multiple accounts respectively.

For the central gateway with a single account, a financial intermediary account would need to be set up which collects all the funds (similar to ETIAS). After a set period, these funds would be distributed appropriately to the Schengen countries. Based on discussions and workshops, it became clear the stakeholders involved were not in favour of any such EU-level account.[51] Therefore, payments should be made directly to the relevant Schengen country.

Both remaining options allow for such an immediate allocation of funds. In the former, the central payment gateway would also have to be set up. However, instead of channelling the visa fees to a single account, the gateway would, by means of automated checks, distribute the fees to the correct Schengen countries immediately, without passing through an intermediate account. This means that an applicant will go through the same payment process, regardless of the country they are applying to. The distribution of funds should be transparent to the user.

The third option, which is not part of either business architecture, does not involve a centralised portal. Instead, the online portal would redirect the applicant to a country-specific payment gateway. This would require the development and maintenance a different payment gateway per Schengen country. Furthermore, this would imply a different payment experience for applicants depending on the country they were applying to. This runs counter to the idea of a uniform Schengen application portal. One benefit of this option would be that Schengen countries have full control of the payment procedure, e.g. by offering specific payment options. However, as the centralised portal with multiple accounts will be able to support the major payment providers, this benefit is minimal.

As only one gateway would need to be developed and maintained for the centralised option, and the central maintenance efforts are comparable in both options,[52] it is clear that the choice to recommend must be the central gateway with multiple accounts.

Based on the assessment above, the conclusion can be drawn that stakeholders do not favour the central gateway with one account and that the multiple gateways would require more effort to develop and maintain across the Schengen Area. Therefore, the central gateway with multiple accounts, part of the 'custom digital' business architecture (option A2), is preferred.

Interacting with the applicant

While technically both option A1 and option A2 provide the same interaction with the applicant, there is a 'sub-option', which needs to be analysed for the appointment management tool.

There are two appointment management possibilities:

- a centralised appointment management tool;
- a decentralised appointment tool offering redirection to national appointment tools.

To assess these two options, the current situation must be analysed. From desk research and discussions, it has become apparent that there is no uniform appointment process for the Schengen Area, i.e. certain busy consulates

[51] Note that this is a viable option for ETIAS as ETIAS collects all ETIAS fees in a central EU account, but those are not redistributed across the Member States.

[52] The central gateway with multiple accounts requires links to be maintained to the correct Schengen country accounts. The multiple gateway option would require links to be maintained to the correct Schengen country's payment gateway.

and ESP operate an online appointment tool, others require an appointment to be scheduled by telephone call, and some do not require appointments to be scheduled and applicants can walk in during opening hours.

The centralised appointment management tool would require the development and maintenance of a new tool, which harmonises the appointment process for all 1,897 consulates and even more ESPs worldwide.[53] To move to this uniform appointment process, the following considerations need to be taken into account.

- A new tool needs to be developed that meets every Schengen country's needs.
- The tool would require configuration by Schengen consulates and ESP to adapt the availabilities of appointment slots on a regular basis, or to cancel appointments, and to provide relevant information to applicants. It would have to send notifications to applicants and provide an overview of appointments to consulates and ESPs.
- As the appointment tool is centralised, issues and questions relating to the tool or appointments need to be addressed at a central level. This would require an expansion of the central governance body.
- Use of the central tool could be optional so that consulates or ESP could choose to maintain their own appointment tools or allow "walk-in" procedure.

While there are challenges in implementing the centralised appointment scheduling tool, it has the key benefit that it can be more easily integrated with the central payment gateway, i.e. it will be easier to guarantee the visa fee has been paid prior to an applicant being able to schedule an appointment, thus avoiding the capturing of appointments by intermediaries and "no-shows". Furthermore, this centralised appointment scheduling tool will allow applicants to undergo an equal appointment scheduling experience, regardless of the consulate they are scheduling an appointment with.

The alternative is a decentralised appointment scheduling tool using a centralised repository providing redirection to the consulate-specific appointment scheduling tool or contact information. For this option, the following considerations need to be taken into account.

- The appointment scheduling tool would also require consulates and ESPs to regularly update the application portal on which an applicant is presented with, or can search for, a specific consulate's appointment process. The repository would need to be configurable to update links/contact information.
- There are no harmonisation requirements across the consulates and ESPs: to start the repository, every consulate and ESP simply needs to provide the link to the consulate appointment website or contact information.
- Since the appointment scheduling itself is not part of the online portal, it will be more difficult to ensure applicants only book an appointment after the visa fee has been collected. This problem could be solved by implementing an external tool, described in more detail in the technical feasibility assessment below. Such a tool would affect the way consulates currently schedule appointments, both from a human and system perspective.
- In the decentralised appointment tool, each consulate and ESP maintains their current appointment scheduling systems and must therefore continue to maintain them (which incurs costs).

Adopting such a decentralised appointment scheduling tool would bring with it the key benefit that each consulate could maintain its current appointment scheduling mechanism. Furthermore, setting up such a centralised repository web page is less complex from a technical perspective.

Based on the assessment above, both options exhibit their own key advantages and disadvantages. The centralised appointment scheduling tool would be a more seamless and integrated solution, at the cost of being more difficult to implement, and being disruptive to the appointment scheduling procedures in existence currently. The alternative is a solution that is simpler to implement, in which consulates can remain working as they are now. However, this solution would not offer the same level of integration with the online portal and uniform application process for the applicant as its alternative.

[53] Data based on the 2018 country-specific Schengen visa statistics; https://statistics.schengenvisainfo.com/ (1897 consulate entries).

Conclusion

Based on the assessments above, the 'custom digital' application business architecture (option A2) is clearly preferable. As currently envisioned, this business architecture could eventually evolve into the more fully digital application portal, whereas some features proposed in the 'fully digital' (option A1) application are not advisable in the current technological, security and legal landscape.

System architecture

This section covers the feasibility assessment of the two recommended options for the online visa application process from a legal, technical, security, data protection, operational and implementation standpoint: the custom digital (option A2) with a centralised architecture (option B1) and the custom digital (option A2) with a hybrid system architecture (option B2). These system architectures have been presented visually in Figure 8.

Legal feasibility

Considering the legal feasibility consists of analysing the current legal instruments and identifying whether they support the proposed solutions. The two tables below display which legal acts require an amendment, along with a rationale for why it is necessary.

Table 5: Amendments to the Schengen Visa Code

Current provision	Suggested amendment
Article 9 Practical modalities for lodging an application	This article should be amended in order to determine that the application has to be lodged in the online application portal.
Article 10(1) General rules for lodging an application	The first paragraph of this article should be amended as some applicant types, i.e. those who have already been issued with a visa, and whose passports and biometrics have not expired, would not be required to appear in person when lodging an application.
Article 10(3) General rules for lodging an application	Paragraph 3 of Article 10 should be adjusted in order to reflect the steps the applicant needs to follow in the online visa application portal, e.g. only first-time applicants or applicants whose biometrics have expired need to provide the travel document.
Article 11 Application form	This article should be amended in order to introduce the online application form that applicants would be required to lodge in the portal. In particular, the reference to the signature on the application form should be deleted (as the application forms would be confirmed via a tick box).
Article 12 Travel document	The different options for submission of the travel document should be reflected in this article. Depending on the type of profile, applicants would have different options available: • physical submission of the travel document (status quo); • scan the travel document's biographic data page (status quo).
Article 14 Supporting documents	This article should be modified in order to introduce the possibility of presenting the supporting documents electronically.
Article 16 Visa fee	As in the case of payment of the visa fee, this article should be amended in order to introduce the possibility that the visa fee will be paid directly from the online application portal to the relevant Schengen countries. The same article should also state that the Commission shall adopt an implementing act on the payment methods and on the technical specification of the direct payment option.
Article 18 Verification of consular competence	This article should be modified in order to explain that a consulate would return an application back to the system if it were not competent to examine it. The same article should also state that the Commission shall adopt an implementing act explaining the procedure in detail.
Article 23 Decision on the application	This article should refer to the notification regarding the decision made on the third country national's visa application via the portal.
Article 32(2) Refusal of a visa	This paragraph should be amended to include the possibility of notifying the applicant via the online portal.

Current provision	Suggested amendment
Article 33 Extension	The article should be amended to include a paragraph stating that the applicant can be informed of the extension via the online portal.
Article 34(6) Annulment and revocation	This paragraph should be amended to include the possibility of notifying the applicant via the online portal.
Article 37(3) Organisation of visa sections	This article should be amended in such a way as to oblige Schengen countries to develop electronic archiving solutions to archive the documents submitted electronically. The possibility of archiving documents in paper format should remain.

Table 6: Amendments needed to the VIS Regulation

Current provision	Suggested amendment
New article	(For option B1): a new article should be included in order to introduce the Application Management System, explaining the data flow with the Visa Information System
New article	A new article should be added to lay down the access rights and functional flows of the interaction with the application tools. In particular, the following tools should be described: • the application checking tool • the visa checking tool • the biometric checking tool • the appointment scheduling tool.
New article	A new article should be laid down that covers the functional flow of the separate read-only database and which data it should extract from VIS. The minimum information this read-only database needs is: • validity of biometric identifiers • the visa status of issued visas • the application status of applications • whether a travel document has already been registered at a consulate.
New article	A new article should be laid down that covers the situations in which an applicant will receive electronic notifications through the notification tool.

All the above-mentioned acts have been adopted through the ordinary legislative procedure (Article 294 TFEU). Therefore, such amendments should be adopted via the same procedure, requiring an agreement between both the European Parliament and the Council.

As indicated in the tables above, the online application process would have several impacts, but mainly on the Schengen Visa Code and the VIS Regulation. In addition, a new regulation might be necessary to establish the online application portal. For the sake of consistency, the study proposes the adoption of a single regulation laying down the new rules and listing the amendments to the current legal acts. The technical specifications of the rules and processes introduced by the regulation will be laid down in implementing and delegated acts.

Technical feasibility

The technical feasibility assessment aims to answer the question of whether the realisation of the recommended options is feasible from a *technical* point of view. In other words, this section aims to answer three questions.

- Can current technology support the realisation of the proposed options?
- If the applicant is expected to use a certain technology, is this technology widespread and readily available enough that this applicant could be expected to use this technology?
- Are there any key differences between the two proposed options that point to a clear preference in favour of one of the options?

To answer this question, the core artefacts of the architectures have been subdivided into three key categories:

1. the online application portal;
2. the storage of application information;
3. the communication links between the different systems.

The following tables analyse the above-mentioned categories and assess the feasibility of their features and capacities, as well as listing other considerations that need to be taken into account from a technical point of view for both system architectures.

1. The online application portal

To analyse the technical feasibility of the online application portal, the seven functional blocks (as identified above) are translated into technical functions that the online application portal needs to fulfil. Table 7 lists these technical features and analyses their technical feasibility. Wherever there is a difference between both system architecture options, the distinction is made and the differences are highlighted. Because the online application portal offers the same features in both system architectures, most technical features are equivalent across the options.

Table 7: Feasibility assessment on the technical functions of the online application portal

Technical function	Centralised system architecture (option B1)	Hybrid system architecture (option B2)
Supported platform (website and/or dedicated application)	Both system architectures consider the online application portal to be a website, accessible online through any supporting device (desktop, laptop, tablet, smartphone). The study does not at this stage suggest the creation of a dedicated smartphone app.[54] Creating a website as such does not require any special technology considerations. It is a widespread technology that should not pose any issues. The website should be designed so it is accessible through mobile devices as well. The limitation of moving to a website only does not restrict the features of the portal, e.g. an applicant will still be able to 'scan the MRZ' by uploading a picture to the application form; the difference is it will be processed centrally instead of on the device itself.	
Support a variety of languages	The online application portal should support at least the EU languages and the most common third country languages, e.g. Arabic, Chinese, and Russian. The creation of a website, which supports multiple languages, is not a technical difficulty and many tools exist to create and maintain a website in multiple languages. The bulk of the effort in creating and maintaining a multi-language website is not typically associated with technical developments, but with user design, e.g. right-to -left languages and the length of languages need to be considered when creating the user interface.	
Offer guidance during the online application process	The portal offers interactive guidance and dynamic instructions during each step of the application process. The tools available to support this guidance (such as chatbots, dynamic pop-ups) are widespread and can be easily adopted by a web service. Additional guidance or 'help' that the portal can offer to the applicant is the automated entry of data in form fields based on an applicant's user account or previous submissions.[55] From a technical point of view, such lookups are trivial and should not pose any challenges.	
Allowing Schengen countries to configure certain elements of the portal	Schengen countries may have specific national rules on the required supporting documents, visa waiver procedures etc. To allow the centralised portal to function effectively and to display the correct information to applicants, it must be able to tailor the portal to each Schengen country's needs. This requirement must be considered from the start of the development in order to ensure the portal is modular and capable of dynamically loading business rules depending on the country an applicant is applying to. Dynamic web pages are widespread and should not cause any technical problems in the creation or performance of the online application portal, on the assumption that the portal has been built from the ground up as a configurable tool. Indeed, implementing the configurable elements (and the associated access rights) after building a static web page could prove to be a cumbersome task. However, even this undertaking should not be considered 'difficult'.	

[54] A smartphone app was not deemed necessary due to the nature of visa applications. Unlike the ETIAS applications, which can be submitted through an app, visa applications always require the attachment of supporting documents. It is typically accepted that the current generation of smartphones are not very suited for the management of digital documents. Therefore, the assessment was made that the number of applications through a smartphone would be very low compared to the number of applications that would be submitted through a web application. Because of this, a smartphone app has not been considered at this stage.

[55] For this, and according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), applicants must consent to their data being retained for future applications. A tool similar to the ETIAS consent tool could be provided for.

Technical function	Centralised system architecture (option B1)	Hybrid system architecture (option B2)
Temporarily storing "draft" applications	To store a "draft" application, the online application portal has a need for a certain storage capacity. This storage capacity could be on eu-LISA's private cloud: the Common Shared Infrastructure. Two considerations need to be taken into account for this temporary storage: • If many applicants abandon their applications halfway or when malicious users intentionally create a large quantity of 'fake' applications, the storage capacity could quickly spiral out of control. To avoid needing excessive storage space for such draft applications, the retention period of such storage must be strictly limited. In addition, a "Captcha" should be included prior to starting an application to prevent the creation of 'fake' applications in the first place. • The temporarily stored applications will contain personal information. Therefore, this information cannot simply be stored on any non-secure servers. Secure temporary storage of these "draft" applications can be guaranteed by adoption of a well-configured Demilitarised Zone (DMZ).[56]	
Filling in the travel document information	To complete their application, an applicant must fill out travel document information in the application form. For this process, two alternatives are proposed. To fill out the application form fields relating to travel document data, the applicant can follow one of two processes: • filling out travel document data in form fields: this is equivalent to filling out any other form field and is thus also covered by simple web services; • the scanning of the Machine Readable Zone (MRZ) in one of two ways: — an applicant should be able to upload a scan of the MRZ to the website, after which the image is processed at a central level and the respective fields are filled out automatically; — if an applicant has a hardware scanner capable of scanning, the website should also support direct scanning of the MRZ. This option will be especially helpful for ESP workers assisting an applicant in filling out their application form. In both cases, there is a limitation in the fact that not all countries currently entitled to the visa requirement offer a MRZ on their travel document. Thus, some countries will not be able to benefit from this option.	
Adding biometric data to the application	As the submission of biometric data remains unchanged from the current operations, there are no special considerations to take into account.	
Adding supporting documents to the application	The uploading of supporting documents consists of three possibilities: • submission of physical supporting documents: this is the status quo – so there are no special considerations for this option; • the submission of scans of supporting documents; • the submission of electronic supporting documents. There are two technical considerations to take into account for the last two bullet points: 1) the uploading of binary files, and 2) the automated quality checks. The former poses no challenges. Multiple tools are available on the market that seamlessly enable the submission of binary files through a web service. This is also the process that will be used for the upload of the travel document's biographic page. The second challenge, the automated quality assurances, ensures that the documents submitted adhere to a minimum data quality level, based on a list of pre-determined configurable parameters, e.g. resolution, format size, readability index, brightness. From a technical point of view, these automated quality checks are complex, but there are currently multiple solutions on the market that can handle these tasks efficiently and at scale.	
Enabling the applicant to declare the submitted data are correct	The proposed 'tick box' solution requires the implementation of a simple checkable box on the online application form. However, this tick box needs to be supported by a rigid logging mechanism as it carries major legal implications. Multiple logging tools are available on the market, and are already widely used across the EU information system architecture.[57]	
Paying the visa fee	The payment of the visa fee needs to ensure three actions occur: • blocking the submission of an application until the payment is processed: this involves implementing a confirmation of whether or not the visa fee has been successfully paid and disabling a 'submit' button until this confirmation has been received. • processing the payment: the secure processing of payments is a very technically complex process (mostly from the technical security angle) but can be completely outsourced to a third party. • distribution of the funds to the correct Schengen country: this process would require some simple checks after which the third party payment gateway would redirect the funds to another destination.	

[56] A Demilitarised Zone is a subnetwork that exposes an organisation's external facing services to an untrusted network. In this case, this DMZ would be on eu-LISA's premises and act as an intermediary between the exposed web services of the online application portal and the highly sensitive EU central IT systems.

[57] The Regulations of the different EU central information systems and interoperability components lay down strict logging rules about data that must be logged by each system/component, e.g. Article 18 of Regulation (EU) 2018/1862 about the SIS logs on central level.

Technical function	Centralised system architecture (option B1) Hybrid system architecture (option B2)
Interacting with the applicant: Appointment scheduling tool	The appointment scheduling tool is in essence a repository of links and/or contact information. This tool should be configurable to allow the consulates to make changes when necessary. As the nature of the information provided through this tool is mostly static in nature, and a consulate will not need to make regular changes, the links and contact information could be manually updated, which does not pose any technical challenges. The challenge with the appointment scheduling tool relates to applicants only being allowed to make an appointment once their visa fee has been paid. As the portal is not integrated with the different consulates' appointment systems, this check needs to be implemented externally. A first safeguard would be to redirect applicants to the link/contact information page only when their visa fee has been paid. This is however not enough, as this would allow applicants, for example, to write down the phone number, and book an extra appointment at a later point in time. To prevent this, consulates should have access to a tool that is able to check whether the payment has already been processed for a specific application. This does not necessarily have to be part of the online application portal, Once an appointment is made, the consulate can then mark the application as 'booked' to ensure an applicant does not book another appointment elsewhere. The process should be: 1. applicant pays the visa fee, 2. visa fee is processed; 3. applicant receives a 'token' associated with their application file (this could be anything as long as the applicant's application file is uniquely identifiable by this token); 4. the applicant is redirected to the appointment scheduling tool; 5. one of the following occurs: a. The consulate operates an online tool: the system has to be adapted so that the applicant also enters the previously received token upon booking the appointment; b. The consulate is accessible by phone call: the applicant gives details of the token when calling the consulate; c. The consulate offers 'walk-in' appointments: the applicant brings the token when going to the consulate; 6. The consulate worker/system verifies whether the token has already been used; 7. The appointment is confirmed and the token is invalidated; 8. Upon cancellation by the applicant, the token is activated again. The process above ensures that it is not possible to book an appointment before paying the visa fee and guarantees that an applicant can only book one appointment per visa fee paid. An alternative to the above process would be the centralised appointment scheduling tool. As the centralised appointment scheduling tool would be part of the online application portal, integration with the payment fee process would be implicit and thus pose fewer challenges than the decentralised alternative. Furthermore, centralised appointment tools are widespread and should pose no technical challenges. However, as described above, a centralised appointment tool would pose major complexity challenges in other domains, such as agreements between central authorities and Schengen counties. Both alternatives are feasible from a technical perspective and either could thus be considered as the solution going forward.
Interacting with the applicant: Status checking tool	The status checking tool allows an applicant to check their application status, visa status and validity of biometrics. To acquire this information, VIS needs to be queried. However, in order not to overload VIS with many concurrent requests, and to enhance security, the requests should not go directly to VIS, but through a secure connection to a separate read-only copy of the VIS database that only stores the data required to provide the requested status data to the applicant. This tool, while implying a significant technical effort, is not complex, and there can be re-use from the EES and/or ETIAS. Furthermore, the ETIAS will already offer a travel authorisation status checking tool and the EES will already offer a 'remaining stay' tool (equivalent to the 'check status of visa' tool). This implies that only the checking of biometric status and the travel document registry are new developments.
Interacting with the applicant: Electronic notification tool	The notification service will offer applicants the possibility of receiving notifications on relevant information, e.g. application status or the need to provide more supporting documents, through email and text messages. Receiving notifications is largely similar to the notification service currently planned for ETIAS. Therefore, no particular challenges are foreseen.

Technical function	Centralised system architecture (option B1)	Hybrid system architecture (option B2)
Submitting the application data	Technically, uploading the application file involves uploading a set of data to another server/database, which does not pose technical challenges. In the central system architecture, the application file simply needs to be uploaded to the AMS. This is equivalent to the applicant uploading supporting documents, biometrics, etc. to the online portal. Therefore, this system architecture offers a very straightforward uploading process.	Technically, uploading the application file simply involves uploading a set of data to another server/database, which does not pose technical challenges. In the hybrid system architecture, the application file needs to be submitted to the correct Schengen country. This decision is of equal complexity to the decision on whom the applicant needs to pay the visa fee to. Technically speaking, this is an easy process, as it should involve detecting some filled out fields in the application and forwarding the file accordingly.

2. The storage of application information

Once the application file has been submitted, it is uploaded to the appropriate database. As described in the table above, this uploading process does not pose any technical challenges.

However, option B1 stores all these application files[58] in one database: the Application Management System (AMS). This AMS stores all submitted application files for one year. In a workshop conducted as part of this study, Schengen countries indicated that such application files are on average 15 MB in size. Given the sheer amount of Schengen visa applications submitted yearly (~16 million), the technical challenges arising from the storage of this amount of information are threefold:

- Given that a single application file is 15 MB, storing 16 million of them for one year would require a storage capacity of ~250 TB. To store data effectively, multiple data redundancy standards need to be applied to ensure data do not get lost or corrupted. Typically, a 200% overhead is used, which leads to an effective storage capacity requirement of 45 MB per application. There could be an impact on this storage space requirement if data are encrypted at storage level. (If that were the case, it would inflate the storage requirements based on the encryption used). Finally, eu-LISA, who would host the AMS, plans to operate with three sites – for disaster recovery purposes. This means that these data would have to be replicated across these three sites. Taking all of these considerations into account, the total amount of storage required would be large (at least 2PB).
- As eu-LISA plans to operate in three sites, the different sites need to be synchronised with one another in order to ensure no data are lost in the event of a disaster. eu-LISA is opting for a self-developed message replication strategy, which, if implemented correctly, would be capable of operating this synchronisation effectively. However, from a technical point of view, it is important to note the high complexity associated with the synchronisation of such large quantities of data across geographically separate sites.
- All Schengen countries would need to access the data stored in the AMS. Clear access control mechanisms would need to be implemented to ensure the countries only have access to the data they should be able to access. Currently, eu-LISA is already operating such forms of access management for other EU information systems (through, for example, logical separation of data), and therefore no considerable challenges are foreseen in this area.

Unlike option B1, option B2 does not operate a central database. As all the application data are distributed across the different Schengen countries, the quantities of data that each Schengen country will have to store is, on average, limited, in comparison to the AMS. In this option, each Schengen country is responsible for the ongoing storage of their own data. Therefore, each Schengen country will have to create or modify one or more national systems to be able to support the increased storage requirements. However, due to the limited storage capacity required for each Schengen country, the technical implications are considerably diminished in the case of the hybrid system architecture.

[58] An application file consists of all data associated with an applicant's application (alphanumeric data, scan of travel document, associated supporting documents, raw biometric data, etc.)

3. The communication links between the systems

The figure below shows the different communication channels involved in each system architecture option. First, the purpose of each communication channel is highlighted:

For option B1, these are the links through which:

1. applicants and ESPs access the online visa application portal and upload/modify any application data;
2. data are uploaded from the online visa application portal to the Application Management System. This process happens when an application is submitted;
3. consulates consult the submitted application files stored in the AMS;
4. Schengen countries create and modify actual VIS data. This link exists already and is thus out of scope for this study;
5. the applicant or ESP can consult the visa status, application status, biometric identifier status and whether a travel document is already registered.

For option B2, these are the links through which:

1. applicants and ESPs access the online visa application portal and upload/modify any application data;
2. data are uploaded from the online visa application portal to the appropriate Schengen country's national system. This process happens when an application is submitted;
3. consulates access the supporting documents stored and archived in the national systems;
4. Schengen countries create and modify actual VIS data. This exists already and is thus out of scope for this study;
5. the applicant or ESP can consult the visa status, application status, biometric identifier status and whether a travel document is already registered.

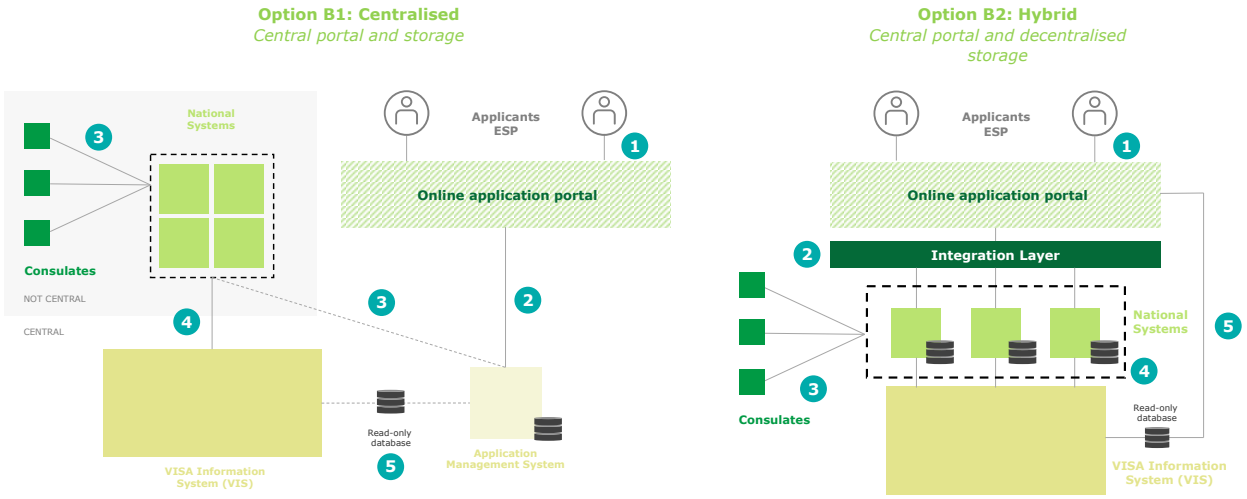

Figure 9: Interfaces of the system architecture options

The table below indicates the technical considerations and challenges associated with the links listed above. As with any communication channel, there is a need to define multiple interfaces between the systems communicating on either end of the channel. These interfaces are recorded in an Interface Control Document (ICD) after agreement with the stakeholders involved.

Table 8: Challenges and considerations of the different interfaces in both system architectures

Link	Challenges and considerations
Option B1: centralised system architecture	
1	This link simply means accessing a web service hosted on the eu-LISA premises. With present-day technology, the realisation of such a link is trivial.
2	Documents are uploaded directly to the AMS through this link. These files are, as previously described, around 15 MB each. Considering the number of applications per year, this link would require a network bandwidth of, on average, 7.5 MB/s.[59] This bandwidth would need to be expanded to support peak loads. However, this remains a negligible amount of bandwidth for eu-LISA and therefore no specific challenges are foreseen for this link. This link also needs to relay the status information requests from applicants (visa application status, visa status, biometric status and whether a travel document has been registered). However, these requests are small in terms of bandwidth demand, so here as well no specific technical considerations are expected.
3	The interface between Schengen countries and the AMS could reuse the Testa-ng but will need to be considerably enlarged given 1) the number of concurrent users accessing it and 2) the large amount of data that need to be retrieved/accessed through the same communication channel. In this case, there are two possible options for retrieving data: downloading information and streaming information. The first requires higher network capacity (bandwidth), whereas the second requires a faster network. Both cases require expansion of the network. The enlargement of the network has two components: a central one implemented under Testa-ng and a national one for which the Schengen countries need to adapt their national network capacity to share supporting documents with their consulates. Therefore, it is likely that Schengen countries will need to invest in network infrastructure. Furthermore, since this channel represents a communication from each Schengen country to a central eu-LISA system (the AMS), the National Uniform Interface (NUI) could be reused to facilitate this communication. This would promote the reuse principle of eu-LISA and lower the technical challenges associated with setting up new communication channels with each Schengen country.
4	The channel between Schengen countries and VIS exists already, but will need to be expanded in accordance with the VIS Revision. It is implemented under Testa-ng. As this channel already exists, no technical challenges associated with this channel are foreseen.
5	From a communication channel perspective, this link involves transmitting simple alphanumeric messages. Therefore, there is no need for large bandwidth.
Option B2: hybrid system architecture	
1	This link simply means accessing a web service hosted on eu-LISA premises. With present-day technology, the realisation of such a link is trivial.
2	In order to distribute the application data to the appropriate Schengen country, an integration layer is needed to facilitate the forwarding process. This integration layer will need to be configured in agreement with all participating Schengen countries. This process will require effort to agree on the specifications of the interfaces and the format of the message exchanges. Furthermore, synergies with the upcoming NUI have been identified. The integration layer could reuse the NUI in order to realise the communication channel between Schengen countries and the central portal.
3	As most Schengen countries do not store and archive application data electronically, it is likely that the Schengen countries will need to adapt their network infrastructures to share these application data with their application examiners across the world. Therefore, it is likely that Schengen countries will need to invest in network infrastructure.
4	The channel between Schengen countries and VIS exists already, but will need to be expanded in accordance with the VIS Revision. It is implemented under Testa-ng. As this channel already exists, no technical challenges associated with this channel are foreseen.
5	From a communication channel perspective, this link involves transmitting simple alphanumeric messages. Therefore, there is no need for large bandwidth.

Security feasibility

The online visa application process involves the processing and storage of personal data. Therefore, secure access to, transfer of and storage of these data are of the utmost importance. This section lists the most crucial security considerations that need to be taken into account for both system architectures.

From a security point of view, both system architectures need to be certain to incorporate at least the following security measures.

1. **Authorisation and authentication**: ensuring users of the online visa application process are whom they claim they are *and* ensuring they only have access to the data and functions, they are allowed to have access to. This

[59] 16.000.000 applications / year * 15MB / application / (31536000 seconds / year)

security function will ensure that the different parties, e.g. the applicants or consulate employees can have access to different features.

2. **Message confidentiality**: ensuring the messages exchanged cannot be intercepted and read by unauthorised users. This principle should, of course, also be extended to include message integrity and non-repudiation. These principles can be guaranteed by applying the proper encryption algorithms to the communication channels between the different systems.
3. **Availability and incident management**: ensuring the solution is up and running, and, if it is not, ensuring the proper protocols, Service level Agreements (SLAs), business continuity and disaster management procedures are in place to resume the business processes as soon as possible.
4. **Business Monitoring**: ensuring the necessary logging and monitoring capabilities are in place. These processes will facilitate troubleshooting and traceability, and provide a high-level view of the operations of the involved systems.

The principles listed above are typically widely available from various market solutions. Furthermore, these principles should already be in place across the different eu-LISA and national systems currently in operation. Therefore, it is not expected that most Schengen countries will encounter any major challenges in the adoption of these security principles. However, those countries whose infrastructure is not ready will need to make a bigger effort to comply with these principles.

Some distinctions need to be made in these core principles for each system architecture.

- While authorisation and authentication needs to be implemented in all data accesses in both system architectures, a special case of access management needs to be considered for the Application Management System. As previously described, the AMS would need to support access management protocols to ensure Schengen countries accessing application files only have access to the data they are entitled to have access to. In the second architecture option, as data are stored and archived at national level, each Schengen country has full control over configuring and enforcing their own authorisation and authentication rules.
- For availability and incident management, the following considerations need to be taken into account:
    - If the online application portal is unavailable, all stakeholders are impacted in both system architectures;
    - As the AMS is the central source for accessing supporting documents, if it is unavailable, all stakeholders are impacted. However, in the hybrid system architecture, if one Schengen country's infrastructure is unavailable, only that country's applicants and consulates are impacted.
- In terms of monitoring, the hybrid system architecture will not allow one single party to have a full view on all systems involved during the application process.[60] Therefore, the central system architecture will enable for a more global view of the online application process for monitoring purposes.

Data protection feasibility

The data protection feasibility assessment mostly relates to the strict data processing rules laid down by Regulation (EU) 2016/679[61] and Regulation (EU) 2018/1725.[62] These regulations lay down provisions and requirements pertaining to the processing of personal data of individuals (in this case, applicants).

Both eu-LISA and the Schengen countries should be familiar with the requirements mandated by these regulations and have adopted them throughout their personal data processing applications. Therefore, no difficulties are foreseen in the data protection domain. However, certain aspects of the data protection principles need to be highlighted in relation to the options.

60 While eu-LISA will know the total number of submitted applications, it will, for example, not know how many times a specific supporting document was accessed by one Schengen country.

61 European Commission; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); https://eur-lex.europa.eu/eli/reg/2016/679/oj

62 European Commission; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

- Both system architectures **collect no more personal data** than are currently being collected in the status quo. The difference lies in the format in which applications and associated files are stored and archived. The impact of this must be considered in a future Data Protection Impact Assessment.
- In option B1, the visa status checking tool needs to consult the read-only replicated VIS database. This database should **only contain the minimal data required to facilitate the visa status check**.
- In both system architectures, the **Schengen countries retain full ownership of the application files assigned to them.** In the hybrid system architecture, this is implicitly the case because application files are stored at national level. However, in the central system architecture this means that, even though the AMS is hosted by eu-LISA, the Schengen countries retain the ownership of the data stored in the AMS. In this case, application files should be logically separated. With the proper access control mechanisms, the Schengen countries will then have seamless access to only those application files of interest to them.
- **Consulates should only have access to the application files they are entitled to access**. In option B2, this is implicitly the case because consulates communicate with their national systems and thus can only have access to the application files stored in them. However, in option B1, consulates (and Schengen countries) should be restricted from consulting application files not assigned to them.[63] A more complex access management system would need to be established.
- Applicants using the online application portal should be **informed** of the privacy regulations and the data being collected by the online portal (such as cookies – see Annex D for a more detailed description of the core data protection aspects). Furthermore, the portal should give the applicants the **option to delete all their personal data stored in temporary storage**.
- The online application portal offers a feature for automated data quality checks. Data protection regulations mandate that, when processing the documents, this automated quality check **should only process the data required to fulfil the data quality checks**, i.e. when checking the clarity of a bank statement, only characteristics such as luminescence and contract should be taken into account. The automated data quality tool should, in this example, not try to extract the monetary value displayed on the bank statement.
- Throughout this report, the notion of a **private cloud** is used and refers to the Common Shared Infrastructure (CSI) hosted by eu-LISA, which would be a scalable, private, infrastructure on which (eventually) all eu-LISA systems will be hosted. As these are hosted by eu-LISA, which also hosts other information systems with personal data, the data protection considerations need to be taken into account, but should not pose any issues.
- From a data protection point of view the centralisation of data could be dangerous. There needs to be assurance that all **data stored on a central level are only used for their intended purposes**. Over time, it might become clear that applicants' application files could be used for purposes other than those for which they were intended. Strict rules need to be laid down in order to ensure that this does not happen.
- **Applicants do not necessarily need to provide their consent** for the processing of their data for visa purposes, as long as this is carried out on a legal basis. However, it is likely that a consent checkbox would need to be implemented for the temporary storage.
- The processing of notifications by means of email or text messages introduces additional data processing processes, which also need to be considered as the **collection of personal information (email and phone number)**. These are data, which are already collected today by the visa application form.
- The proposed options introduce new connections with VIS, e.g. the AMS, the read-only database connection. Therefore, **the data protection impact of these new connections on VIS must also be analysed and considered**.[64]

Operational and implementation feasibility

From an operational point of view, both system architectures require a complex governance model for correct management and operations of the online application portal, the national systems and the AMS (option B1) while maintaining the possibility for Schengen countries to configure the online application portal in accordance with their national rules.[65] It is worth mentioning that these changes will have an impact on the following:

---

63 An exception could be allowed where a Schengen country gives another Schengen country (temporary) access to an application file (a process currently facilitated with VIS MAIL).

64 All the above findings were confirmed in an interview with the European Data Protection Supervisor (EDPS).

65 Note that the Visa Code only lays down the minimal requirements for an applicant to travel to the Schengen Area. Many Schengen countries have specific requirements for applicants.

- Schengen countries need to configure the portal according to their specific national rules and need to coordinate with eu-LISA (AMS management) to make the requisite adaptations to their infrastructure (database schemas, storage, network);
- the applicant, since different documentation will be required to obtain the Schengen visa, depending on the country the person is applying to, and information needs to be provided seamlessly to draw attention to the customised requirements;
- eu-LISA as the portal management Agency that will need to adapt the underlying infrastructure, back-up processes, synchronisation mechanisms, potential network requirements, etc. to successfully adapt to the new policy needs.

In addition, having a central online application portal implies a need for a 'central capability' that can manage all the evolutionary and corrective maintenance, incidents or problems relating to the portal and its underlying features. (Everything that has to do with decision-making or the application/examination process will continue to be managed at Schengen country level). This will result in the need for the online application portal to offer first-line support for third country nationals that is operational 24/7.

Furthermore, option B2 consists of an integration layer that orchestrates the business rules for correct transfer of data from the temporary central storage to the national systems. Given that this integration layer will connect systems with a very different level of digitalisation, it is of utmost importance that the Interface Control Document (ICD) that defines all the interfaces and states how they should be interconnected be up-to-date. The responsibility for this lies with both the Schengen countries and eu-LISA.

Finally, it goes without saying that, in order to guarantee connectivity between the different Schengen countries and the central systems, the current governance should be applied to all existing interfaces (e.g. those between Schengen countries and VIS) and those that can be built using the same infrastructure (e.g. between the Schengen countries and the AMS for option B1).

In terms of implementation, *timing* is of considerable importance. The current EU IT landscape is currently undergoing major changes with the introduction of multiple information systems and the recasting of existing systems. Therefore, the major difficulty for the implementation of the online application process will be to fit this initiative into eu-LISA's already busy timeline. Therefore, it would be appropriate to have the full implementation of the online visa application process after 2023, when the rollout of EES, ETIAS and interoperability is finished.

Option B2 offers a major benefit in terms of the implementation timing mentioned above, i.e. it would mean that a situation could be avoided where all Schengen countries have to move to the online application portal simultaneously.[66] This may indeed be relevant, as many Schengen countries have invested considerably in building their own online application portals. This gradual 'opt-in' approach may lower the financial burden for Schengen countries that are currently already operating a national portal. Furthermore, an expansion of the hybrid system architecture could be envisaged where national portals and the Schengen portal co-exist through added integration with the integration layer.

3.2. Digital visa

3.2.1. Proposed options

As is the case for the visa application process, digital technologies could be applied to the current visa sticker. The introduction of a digital visa would:

- help address the challenges of and burdens arising from the current paper-based visa sticker;
- contribute to improving the security of the Schengen Area and improving the management of the Schengen external borders.

[66] The centralised system architecture also offers the possibility of a gradual opt-in by Schengen countries. However, from an infrastructure point of view, the hybrid system architecture offers an easier gradual transformation. In the centralised system architecture, upon opt-in of a new Schengen country, the AMS, the portal and the link from the AMS to the national systems would have to be scaled up. In the case of the hybrid system architecture, only the portal needs to be scaled up. An option would be to scale the AMS and its link to the national systems to the maximum required capacity from the start. However, this would require large infrastructure investments for infrastructure that will possibly not be used for many years.

This section presents the options for digitalising the visa sticker and the associated procedures. The study has identified two categories of options for the "digital visa" stream.

First, the study identified two options for the visa itself, namely:

- The digital visa
- The visa sticker (status quo).

Second, the study identified three options for verifying the digital visa offline in certain circumstances and by certain stakeholders (see below), namely:

- Option C1: Offline fallback solution 1 (visa issuance notification);
- Option C2: Offline fallback solution 2 (visa issuance notification and non-signed 2D barcode),
- Option C3: Offline fallback solution 3 (visa issuance notification and digitally signed 2D barcode).

Please refer to Annex F for a more comprehensive description of these options.

Preliminary concepts

The core idea behind the concept of a digital visa for short stays in the Schengen Area is to issue a paperless travel authorisation to be verified by the duly authorised authorities directly in one of the EU border management information systems.

At the outset, it is important to clarify the meaning of the term "digital visa" in this context, as similar terms, e.g. 'e-visa', are widely used to refer to a diverse group of electronic travel authorisations issued by certain third countries. The term 'digital visa' should be understood as follows:

1) the term refers only to the travel authorisation itself, and has nothing to do with the way the visa application process unfolds;[67]
2) the digital visa is to be thought of as an electronic or paperless authorisation to stay in the Schengen Area for a specific period of time and which is linked to the third country national's travel document.

It is relative to these two points that the digital visa would build on the current technical solutions.

Indeed, the digital visa would consist of the set of alphanumeric data and biometric identifiers recorded in VIS (as at present). The Schengen visa is already partially 'virtual' as the current sticker needs to be checked against an electronic file that includes all the necessary visa information about third country nationals.[68]

In addition, the digital visa option needs to be explored within the context of the future EES. Pursuant to the EES Regulation, the EES will keep track of every time a third country national enters and exits the Schengen Area. At the border crossing points, border control authorities will be able to query VIS from EES in order to verify the traveller's identity and the validity of the visa.[69] As emerged in the Visa Working Party discussion on the digital visa, the introduction of EES will result in the physical visa sticker becoming less relevant as the EES checks will be based on the traveller's fingerprints and travel document.[70]

The reader is referred to Annex F for a complete explanation of the rationale for adopting a digital visa and the criteria behind the selection of the most suitable option.

---

67 This clarification is justified by the fact that in some third countries, e.g. Iran, Cambodia) the term "e-visa" also refers to the electronic application process, and not specifically to the travel authorisation issued thereafter.

68 Note of 4 September 2017 from the Presidency of the Council – Visa Working Party / Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein) – e-visa: improving the current visa processing with digital visa.

69 Article 14(3) of EES Regulation.

70 The description above outlines the digital visa in a similar fashion to certain third countries, such as Australia. Australian authorities issue tourist visas (subclass 600) and work/study visas (subclass 462) to third country nationals intending to visit Australia for tourism and work/study purposes. The visa is linked electronically to the traveller's passport or other travel document and requires no physical label or sticker. Official information about this travel product can be found at: https://immi.homeaffairs.gov.au/visas/getting-a-visa/visa-listing/visitor-600/tourist-stream-overseas#About ("Visa label" at the bottom of the page) and: https://immi.homeaffairs.gov.au/visas/getting-a-visa/visa-listing/work-holiday-462/first-work-holiday-462#About.

Digital visa

The digital visa would consist of the set of alphanumeric and biometric identifiers recorded in VIS confirming the travel authorisation itself (as at present). The digital visa envisions the following:

- After the submission of the application, the consulate and/or the competent authority of the Schengen country would carry out the risk assessment and examination of the application. If the applicant poses no risks, then the authorities take the decision to issue a visa and notify that decision to the applicant.[71]
- Consulates would not issue a visa sticker. They would simply send a visa issuance notification to the applicant's email address. This would either be done via a mobile application that can use the email address as a means to confirm the user's identity or an email account accessible from different devices (laptop, tablet, smartphone, etc. or, if the online application portal is implemented, it would go to the account of the third country national. The visa holder would then travel with his/her travel document.
- The authorities responsible for checks at the Schengen external borders and within the territory of the Schengen Area would use the travel document and biometric identifiers to query VIS for verification purposes, as is already the case. In other words, border guards would adopt the same procedures that are presently mandatory to verify that the biometric data stored in VIS belong to the person who is about to cross the border.
- Carriers would use the travel document to query the read-only database through the carrier gateway prior to the third country national boarding as provided for in Article 45b of the future revised VIS Regulation. Carriers would read an "OK" answer if the information on the third country national's travel document matched all the data stored in the read-only database, i.e. the data extracted from VIS. They would receive a "NOT OK" answer, on the other hand, if the third country national does not hold a valid visa or a mismatch is detected.
- Moreover, certain third parties, e.g. accommodation service providers, financial institutions, employers, might be authorised, or required by national law, to check whether a third country national holds a valid visa. For that, third parties would use one of the options explained in the section below on offline fallback solutions.
- Finally, the border control authorities of those third countries bound by agreements with certain Schengen countries would also need to verify that outgoing travellers were in possession of a valid visa (see below). In theory, the same concept developed for third parties could be reused to let third country authorities verify the validity of visas. However, this solution has pros and cons that are assessed below in the section on security and data protection feasibility.

Offline fallback solutions

This proposed option for verifying the visa relies on 24/7 availability of the central systems/databases. The technical and security feasibility assessments carried out below show that the digital visa is a sufficiently reliable option in itself without the need for emergency solutions.

However, technical circumstances may compromise accessibility to systems. Although EU border management IT infrastructure guarantees a very high reliability and availability rate, the overall security of the digital visa option could be enhanced by way of options for verifying visa in an offline environment (offline fallback solutions). It is up to the Schengen countries to discuss whether it is worth venturing into any such solutions. The paragraphs below explain the reasons why such solutions might be considered.

Central VIS downtime

The central VIS database may run into a downtime period for technical reasons. Such an issue would be likely to have Schengen Area-wide consequences, since a system failure at central level would prevent any authorised authority from accessing VIS data.

This is an extremely unlikely event. The table below lists the VIS availability statistics of 2016-2018. eu-LISA is also following an approach targeting 100% availability by improving the system continuously.

[71] The authorities would also notify the applicant if the visa applied for had been rejected.

Table 9: Analysis of the uptime/downtime of VIS

Year	Availability rate
2016	99.48%
2017	99.83%
2018	99.93%

Moreover, the VIS architecture is built in such a way as to keep unavailability risks to a minimum. Should the VIS database not be accessible because of a technical issue involving the primary data centre, a backup data centre would become operational, ensuring full access to the VIS database. Along these lines, eu-LISA is already working towards an active-active configuration of the data centre, which would increase the availability of VIS. Therefore, in the future scenario, access to VIS would be ensured continuously with no switching period. It would only be technically impossible access VIS because of a VIS-specific failure if both data centres experienced technical problems at the same time, which is an extremely unlikely event.

Breakdown of Local Area Network (LAN)

If VIS were operating normally, it might become technically impossible to access VIS because of a problem in the local area network (which is not an area of responsibility of eu-LISA). Thus, central authorities need to guarantee that there are no downtimes for this reason (redundancy of lines, inadequate bandwidth, etc.).

There is nevertheless still a wide variety of technical problems, which could leave a particular area disconnected from the internet. The network may be off in an airport or seaport as well as in a (remote) land region, either along the external border or inside the territory. Interviews conducted with Schengen country authorities confirmed the need to take into account the risk of border crossing points and immigration authorities being unable to connect to VIS. However, technical improvements will arguably make such risks less and less likely over time.

Ordinary use cases for certain stakeholders

The two technical challenges mentioned above refer to the use of offline solutions in very exceptional circumstances. Nonetheless, with the abolition of the paper visa sticker, the offline fallback solution may turn out to be very useful to allow the following stakeholders to check visas in *ordinary* circumstances:

- Schengen country immigration authorities: Authorities such as police patrol officers are amongst those stakeholders who need a quick and reliable solution for verifying visas. As they may have trouble accessing VIS directly while checking a TCN in the streets, they may be forced to contact their headquarters to have the TCN's visa checked remotely. An offline solution could allow police officers to verify the visa right away;
- Third parties allowed to check visas by the national law of certain Schengen countries: An offline proof would allow entities, such as financial institutions and employers, to verify the visa of a TCN they may enter into contract with;
- Third country border control authorities: Certain third countries are bound by agreements with individual Schengen countries to carry out preliminary checks on TCNs about to enter the Schengen Area. Having worked with visa stickers so far, such third country authorities may benefit from the offline proof to keep checking travellers using the same procedures as today.

The study considered the following three options for an offline fallback solution, should the European Commission and the Schengen countries endorse the concept:

- Option C1 – visa issuance notification;
- Option C2 – visa issuance notification with non-signed 2D barcode;
- Option C3 – visa issuance notification with digitally signed 2D barcode.

Option C1 consists of a notification sent by the consulate to the third country national to confirm the issuance of the visa. Although the notification would be sent over a secure email address, the message would contain no safeguards to prevent fraud or counterfeiting. The notification would display the following information:

1. the number of the notification / visa reference number (replacing the visa sticker number);
2. the name and surname of the visa holder;

3. a "valid for" heading, indicating the territory in which the visa holder is entitled to travel;
4. a "from - to" heading, indicating the period of validity of the visa;
5. a "number of entries" heading, indicating how many times the visa holder is entitled to cross the Schengen border with the visa;
6. a "duration of visit" heading, indicating the maximum number of days allowed per visit;
7. the date and place of issuance of the visa;
8. the number of the passport with which the visa is linked;
9. the type of visa using letters A and C;
10. the Schengen country and the authority issuing the visa;
11. the mandatory or national entries of the issuing Schengen country or other information about the visa holder, e.g. whether the person is a member of the family of a EU citizen, a minor, etc.;
12. the facial image of the visa holder;

Option C2 would consist of the same visa issuance notification described in option C1 plus a 2D barcode in which the consulate staff would have encoded the visa information listed in the fields above (1-11). The consulate staff would base the barcode on publicly available software. No authority would add any official signature to the barcode.

Option C3 would still rely on the notification sent by the consulate, but would consist of a 2D barcode signed with a key (digital seal) issued by designated authorities of the Schengen countries – called Country Signing Certificate Authorities (CSCAs). In addition to the information that would be included in the simple barcode, the signed 2D barcode could also host the traveller's facial image. This 2D barcode would be generated automatically by software integrated in the national system(s) of the issuing Schengen country and then be signed digitally through a cryptographic key provided by the same country's CSCA (see the technical feasibility below for further details).

The use or not of a digitally signed barcode will depend on the results of ongoing discussions between European Commission and representatives of the Schengen countries within the Article 6 Committee[72] with regard to a 2D barcode to be printed on the visa sticker.[73] The barcode would include the same data and information currently provided by the sticker (except the holder's facial image as that would make the barcode too big to be printed on the sticker) and are intended to mark a transition from the current sticker-based verification to a barcode without sticker (and, potentially, to the fully digital visa).

Furthermore, option C3 could leverage the work currently being carried out by the Article 6 Committee[74], but would differ in two main respects: first, the barcode would be sent electronically to the visa holder and not printed on any sticker; second, as a consequence, the barcode would include the facial image, as there would no longer be any space constraints for printing.

The figure below illustrates the different processes involved in the proposed options.

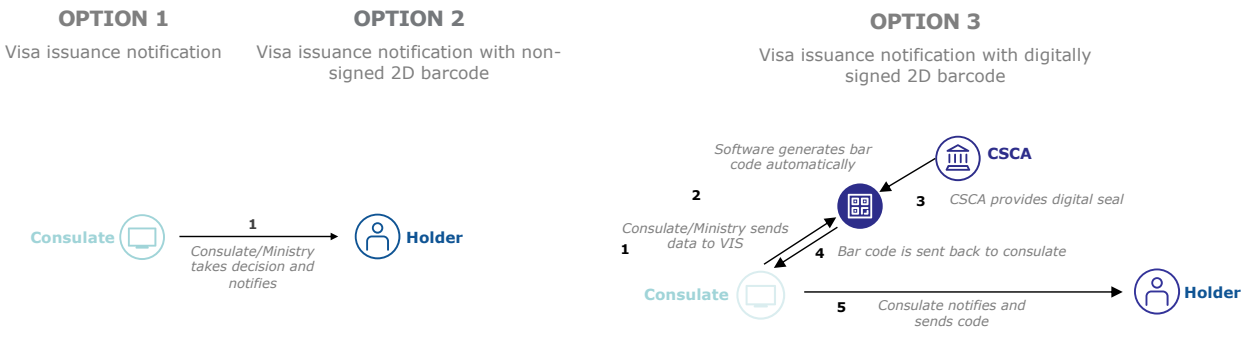

Figure 10: Digital visa offline fallback options

[72] Committee of experts from the Schengen countries established pursuant to Article 6 of Regulation 1683/95. The Committee assists the Commission in the discussion of measures to strengthen the security features of the visa sticker.

[73] To that end, the Commission has recently approved a new Regulation on the standard format of the visa sticker. The new sticker, which is currently being purchased by certain Member States, includes a space for hosting a barcode.

[74] The Article 6 Committee is considering to enhance the current visa sticker with a digitally signed barcode.

The aim of the next section is to carry out a feasibility assessment from the legal, technical, security, data protection, and operational/implementation points of view of:

- the digital visa option as such, vis-à-vis the current visa sticker;
- the three offline fallback solutions vis-à-vis one another.

3.2.2. Feasibility assessment

Legal feasibility

The legal feasibility analysis assesses the impacts that the options would have on the legal acts currently in force or expected to be soon in force at EU and national level. This exercise will evaluate whether the proposed options would comply with existing and future regulation, and will assess the nature and extent of the amendments necessary to current legislation.

The present study does not cover the abolition of the sticker for national visas issued by Schengen countries. However, should the sticker be abolished for such visas as well, the amendments to Regulation 1683/95 would arguably be more extensive, probably leading to a repeal of the Regulation itself.

All the below mentioned acts have been adopted pursuant to the ordinary legislative procedure laid down in Article 294 TFEU.

Legislative amendments

As mentioned in Chapter 2, the visa sticker life cycle affects stakeholders throughout the whole visa processing procedure. As the digital visa option will result in the abolition of the sticker, the digital visa will also have an impact on the legislation binding those stakeholders.

The section discusses the legal amendments needed at each level in the following tables. The tables deal with the relevant articles by content in the left-hand columns, and provide the rationale for the amendment and some suggestions as to the new text to be adopted in the right-hand columns.

EU legal framework

Table 10: Amendments to the Schengen Visa Code

Current provision	Suggested amendment
Article 2(6) – Definition of visa sticker	The paragraph should be deleted. New paragraphs should be added with the definition of a 'digital visa', the digital visa reference number (generated by VIS), and the offline fallback solution chosen (if any).
Articles 27 – Filling in the visa sticker	Article 27 should be amended in such a way as to delete any reference to the sticker, while outlining the procedure for inserting the same visa information in the email notification. Implementing acts should lay down the procedure for sending the visa issuance notification to the visa holder, as well as for generating the non-signed barcode or the digitally signed barcode, if either is chosen.
Article 28 – Invalidation of visa sticker	Article 28 should be replaced. The new article should explain that, in the event of an error, the digital visa and the offline fallback solution, if any (whether a visa issuance notification, a 2D barcode or a 2D digitally signed barcode), should be invalidated and a new digital visa with offline fallback solution, if any, should be issued with the correct information. The technical procedures for invalidation should be laid down in implementing acts.
Article 29 – Affixing a visa sticker	Article 29 should be replaced by an article outlining the procedure for sending the email notification and the 2D barcode to the third country national.
Article 32 – Notification of a refusal	Article 32 should be amended in order to mention that, in the event of refusal, the consulate will notify the applicant by email.
Article 33(6) – Extension of the visa	This paragraph should be replaced by a paragraph explaining that the visa extension would be dealt with in a new notification, which is sent to the third country national, together with the new non-signed barcode or digitally signed barcode, if either is chosen.
Article 34 – Annulment and revocation	Article 34 should be amended in such a way as to provide the means how the third country national will be notified by email of the annulment or revocation of the visa.
Articles 37(2) - Organisation of visa sections (for storage of stickers)	The references to the visa sticker should be deleted.

Current provision	Suggested amendment
Article 43(4) – Cooperation with ESPs	The references to the visa sticker should be deleted. The paragraph should be amended to explain that the procedures relating to notifying the visa holder/applicant of the issued/refused visa, and to sending the non-signed barcode or the 2D digitally signed barcode, if any, are the exclusive responsibility of the consulate.
Article 53(1)(f) – Notification by Member States to the Commission	The word 'sticker' in this sub-paragraph should be replaced by the words 'visa issuance notification'.

Table 11: Amendments needed to the Schengen Borders Code

Current provision	Suggested amendment
Article 6(1)(b) – Entry conditions for TCNs	This sub-paragraph should be amended to include an obligation for visa holders always to carry proof of notification (either a printout or a proof accessible on a mobile device).
Article 6(5)(b) – Entry conditions for TCNs: visas issued at the border	The reference to 'affix a visa in the document' should be replaced by a sentence that takes into account the abolition of the visa sticker.
Article 8(3)(a)(i), (b) and (h)(i) – Additional border checks for visa holders	These sub-paragraphs should be amended with a sentence indicating that, in the event that it is technically impossible to access VIS at the border, the visa should be verified by checking the visa issuance notification and the non-signed barcode or the digitally signed barcode, if either is chosen.

Table 12: Amendments needed to the VIS Regulation

Current provision	Suggested amendment
Article 4(2) – Definition of visa sticker	This paragraph should be replaced with a paragraph including the definition of a 'digital visa', amended to define the digital visa reference number (generated by VIS), and the offline fallback solution chosen (if any).
Article 10(1)(e) – Data to be added for visa issued	Article 10(1)(e): The reference to the visa sticker should be deleted. A new paragraph should be inserted indicating the visa reference number (created by VIS) and that the data set shall include the certificate number of the barcode (in the event the signed barcode fallback solution is selected).
Article 14 – Data to be added for a visa extended	Article 14(1)(d) (data to be added for extension): The reference to the visa sticker should be deleted.
Article 15 – Use of VIS for examining applications	The reference to the visa sticker should be deleted and replaced with a sentence referring to the visa reference number.
Article 18 – Access to data for verification at external border crossing points	Article 18 (verification at the border, as amended by the EES Regulation): — In paragraph (1) the reference to the visa sticker number should be replaced by the visa reference number. The procedure for launching a VIS search would not change; — A new paragraph should be added providing that, in the event that is technically impossible to access VIS, the competent authorities should verify the identity of the third country nationals with the visa issuance notification and the data included in the non-signed barcode or the digitally signed barcode, if either is chosen.
Article 19 – Access to data for verification within the territory of the Member States	Article 19 (verification within the Schengen territory, as amended by the EES Regulation): • Paragraph (1) should be amended by replacing the reference to the visa sticker number with the visa reference number. • A new paragraph should be added providing that, in the event that is technically impossible to access VIS, the competent authorities should verify the identity of the third country nationals with the visa issuance notification and the data included in the non-signed barcode or the digitally signed barcode, if either is chosen.
Article 45c (future) – Technical impossibility of accessing VIS	If an offline fallback solution is chosen, paragraph (1) should be amended to allow carriers to use the visa issuance notification and the non-signed barcode or the digitally signed barcode, if either is chosen, when it is technically impossible for them to query the carrier gateway for any reasons beyond their control, but specify that they are not exempt in these circumstances from verifying that the third country national is in possession of a valid visa.

Table 13: Amendments needed to the EES Regulation

Current provision	Suggested amendment
Article 16(2) - Personal data of third country nationals subject to a visa requirement	Subparagraph (d): this subparagraph should be deleted and replaced by a subparagraph indicating the visa reference number. Subparagraph (e): the reference to the visa sticker should be deleted and replace with "as indicated in VIS".
Article 19 - Data to be added where an authorisation for short stay is revoked, annulled or extended	Paragraph (d): the reference to the visa sticker should be deleted and replaced by a sentence referring to the visa reference number.
Article 24(2) - Use of the EES for examining and deciding on visas	Subparagraph (b): this subparagraph should be amended and refer to the visa reference number.
Article 32(5) - Conditions for access to EES data by designated authorities	Subparagraph (c): the reference to the visa sticker should be deleted and the sub-paragraph amended to refer to the visa reference number.

Table 14: Amendments needed to Regulation 1683/95

Current provision	Suggested amendment
Article 5 – Concept of 'visa'	This article should be amended to explain that the 'visas' referred to in the Regulation are only the national visas issued by the Schengen countries.

As outlined in the tables above, the abolition of the sticker would not imply major legal amendments to the current EU legal framework.

Nonetheless, input by national experts indicated that the visa sticker has for several years been the customary proof for verifying the validity of a visa for the Schengen central authorities, consulates and border control authorities, as well as for authorities of third countries committed to carrying out checks on outgoing travellers. Against this backdrop, it is up to the Schengen countries to consider whether the implementation of an offline fallback solution would make the transition to a digital visa easier.

Option C3 for offline fallback verification is clearly the most feasible for two reasons. First, it would guarantee a very high reliability standard – even higher than that of the sticker. Second, it could carry over the progress made by the Article 6 Committee on the inclusion of a signed 2D barcode in the current format of the visa sticker. As will be explained below in the technical and security feasibility assessment, neither option C1 nor option C2 would attain such objectives. As mentioned previously, the barcode currently under discussion by the European Commission and the Schengen countries in the Article 6 Committee would include the same data and information currently included on the sticker (except for the facial image). This barcode is intended to mark a transition from the current sticker-based verification to the use of the barcode without sticker.

The barcode envisaged by the Article 6 Committee would be produced and signed using the same procedures and safeguards as option C3 profiled in this study. Therefore, if the Article 6 Committee discussions lead to a formal proposal, it will be submitted to the Council for approval. This might pave the way for a future legislative reform adopting the same model of barcode without any sticker, i.e. fallback proof for the digital visa option.

However, the digital visa can be pursued as an option in itself, and there are no clear impediments from the legal standpoint to the implementation of the digital visa as such without any offline fallback solution.

Bilateral international agreements

In order to enforce and improve the effectiveness of the Schengen visa policy, certain Schengen countries have concluded agreements with certain third countries with a view to having travellers checked at a first stage before their arrival at the Schengen border. The Schengen countries have been making efforts to have third country authorities check the departing traveller's identity consistently. Such efforts include political cooperation as well as the deployment of liaison officers assisting local authorities in carrying out identity checks at departure. As a result, third country authorities are increasingly accustomed to verifying the traveller's identity by means of the

visa sticker, even though they have neither the same tools nor the authority to carry out border checks that the Schengen authorities have.

Therefore, with the abolition of the sticker, certain Schengen countries may consider that third country authorities need another means of carrying out exit checks on a consistent basis. This consideration may open up an 'ordinary' use case for an offline fallback solution, i.e. a use case not mandated by any technical failure in VIS or in the local area network. This finding was confirmed in interviews with the Schengen country authorities and validated in a workshop with experts from the Schengen countries, the European Border and Coast Guard Agency (EBCGA).

However, these bilateral international agreements have been implemented in the national law of only a narrow minority of Schengen countries. New EU law provisions would supersede them pursuant to the principle of primacy of EU law.[75]

Technical feasibility

The digital visa option introduces the possibility for visa-required third country nationals to use a paperless travel authorisation to enter the Schengen Area. This section describes the technical impacts, requirements and implications of moving forward to a digital replacement of the visa sticker.

Digital visa

By comparison with the current system landscape in which the visa sticker is used, the digital visa option would not require any complex architecture reforms, as it would largely reuse the system architecture planned by current and upcoming EU IT systems for border management.

The table below summarises the synergies with the key components of the EU landscape for border management.

Table 15: Technical synergies between digital visa and EU IT systems

Technical component	Logic for the synergy
VIS	The digital visa consists of the third country national's **record file** currently uploaded to VIS (alphanumeric and biometric information). The VIS Revision will already make the digital visa more reliable and secure thanks to the automatic pre-examination checks that will allow a Schengen Area-wide query of all EU interoperable systems for border management.
ETIAS[76]	The **carrier gateway** (already laid down in the VIS Revision) – in parallel with the EES and ETIAS – will be used by carriers to verify the validity of the third country national's visa before departure, without the need for any sticker.
EES	As the EES will be the main system for verifying the entry and the exit of third country nationals in the Schengen Area, border control authorities will retrieve VIS data from the EES for verification purposes.

The synergies above will allow the technical requirements for the digital visa to be met smoothly. The figure below displays the type of access that each stakeholder will have to the digital visa.

[75] See the landmark cases C-6/64 Costa v ENEL [1964] and C-106/77 Simmenthal [1978] by the Court of Justice of the EU (CJEU).

[76] Another synergy with the gateway that can be envisaged would be to develop a permissions gateway allowing banks, hotels, employers, etc. to verify visas without stickers. Third parties would launch a query based on the visa number on the visa issuance notification, and the gateway would only reply with an 'OK/NOT OK' answer. However, if an offline fallback solution is adopted, it would be a much cheaper solution than developing a new technical component, albeit based on the carrier gateway.

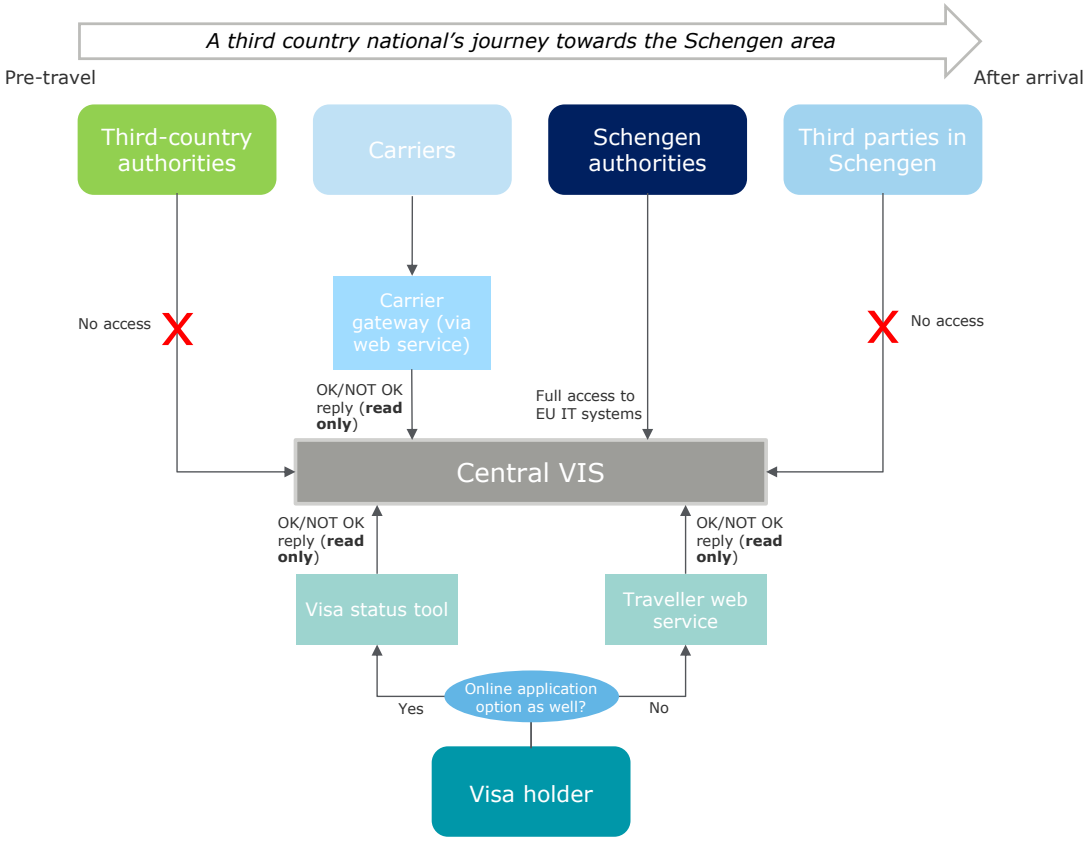

Figure 11: Mapping of access to VIS by the stakeholders involved after the issuance of the visa

However, certain adjustments need to be taken into account.

- VIS – in combination with the EES – needs to be available on a 24/7 basis. To that end, the infrastructure should be made less and less prone to failures in order to maintain and improve the availability rate recorded in past years. The upcoming active-active configuration of VIS will certainly help in that regard.
- Enlarge the network capacity of VIS *in addition* to what is already needed in order to make VIS interoperable with the EES at the border. This is because, whilst, on average, only about 50% of visa-required TCNs are currently checked against VIS at the border,[77] a rise in the queries made to VIS and the EES are to be expected because of the abolition of the sticker in conjunction with the rollout of the EES. Moreover, queries involving biometric data are costlier in terms of resources than alphanumeric queries; therefore, infrastructure and communication channels in VIS need to be reinforced to handle this increase in the processing load.
- The Schengen countries' network should be made more reliable and failure-proof, especially along land borders far away from major cities and airports. The rapid rise in 4G uptake in the EU, and the upcoming availability of 5G, should help make the entire Schengen external border better connected overall.
- Finally, in the event that the digital visa is implemented before and/or without any online application option, third country nationals would not be able to use the visa status tool to receive notifications and check their visa information. Therefore, in this case a new web service would need to be developed enabling communications between consulates and third country nationals regardless of any online portal. The traveller web service would consist of a communication gateway enabling to send automatic notifications to the email account of the third country national. To achieve this, the traveller web service would include a read-only link to the central VIS database and forward an automatic notification to the third country national. The traveller web service would also allow the third country national to check the status of his/her visa through the same connection by logging in and receiving an "OK/NOT OK" answer.

[77] Statement confirmed by statistics communicated by eu-LISA and validated by DG HOME.

Offline fallback solutions

The digital visa relies on the connection and 24/7 availability of the systems managed by the central authorities and on the EU systems. As explained at the beginning of this chapter, if any of the systems involved is not accessible, an offline fallback solution must come into play because border control authorities need to prove the identity of a third country national and the validity of their visa in any circumstances. Moreover, the Schengen countries may consider that the Schengen immigration authorities and third country authorities need to have recourse to a replacement for the sticker.

Option C1: visa issuance notification

From a technical standpoint, the development of option C1 would require no technical adjustments beyond those expected for the online application portal (if an online application option is chosen), or for the abovementioned traveller web service (should the digital visa be implemented before and/or without the online application portal).

In both cases, the notification would be sent through one of the embedded features. Once the visa has been issued, VIS would automatically send an official notification to the third country national. In both scenarios, this option is the easiest as no technical component would need to be developed other than those implied by the Schengen online application portal or the digital visa as such.

Option C2: visa issuance notification with non-signed 2D barcode

In addition to providing the visa issuance notification, option C2 would include a simple 2D barcode in which the consulate staff would have encoded the same information provided in writing.

Furthermore, option C2 would not require the development of new IT infrastructure components. However, it would be slightly more complex compared to option C1 to the extent that software for generating codes on a daily basis would need to be integrated in the national system. The Schengen countries would procure contracts with third parties for the provision and regular update of such software. In conclusion, from the technical point of view, option C2 requires more effort than option C1.

The Schengen countries would need to update national systems in such a way that the data recorded in VIS – except the biometric identifiers – would be automatically transferred on a barcode through the barcode-generating software.

Nonetheless, option C2 shows a very high degree of feasibility from the technical point of view.

Option C3: barcode signed with a digital seal (cryptographic key)

Option C3 would retain the visa issuance notification but would include a secure 2D barcode signed by the Schengen country's duly designated authority (CSCA). The 2D barcode would need to be readable by scanning equipment and devices. Moreover, amongst the barcode formats available, only those barcodes whose symbology is certified by the International Organization for Standardization (ISO) should be used.[78]

Option C3 would be more complex than options C1 and C2 for two reasons:

- First, option C3 would need to be based on technical infrastructure and communication channels that make it possible to sign documents digitally and that, for this reason, go beyond the barcode solution envisaged in option C2.
- Second, in option C3 the 2D barcode would include the facial image of the third country national. This would require the Schengen countries to adapt their national systems in such a way that not only alphanumeric data from VIS, but also the digital facial image, were automatically retrieved for the purposes of generating the barcode at a later stage. The inclusion of the facial image requires significant storage capacity in the barcode when

[78] See the 2018 Report by ICAO on visible digital seals for non-electronic documents, p. 9, available at: https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Visible%20Digital%20Seals%20for%20Non-Electronic%20Documents%20V1.7.pdf. Examples of such barcode formats include: DataMatrix [ISO/IEC 16022], Aztec Codes [ISO/IEC 24778], and QR Codes [ISO/IEC 18004].

compared to alphanumeric data. For this reason, option C3 could opt to use a coloured 2D barcode, which uses colour information to increase the data storage without affecting the barcode size.[79]

The process envisaged for generating a barcode with a digital signature is explained below in order to highlight the technical infrastructure and communication channels involved, as Option C3 relies heavily on technological solutions and governance structures that already exist in all Schengen countries for signing passports and other documents cryptographically.

This infrastructure, known as Public Key Infrastructure (PKI), involves having recourse to a specifically designated authority charged with placing a digital seal, i.e. a cryptographic signature, on the documents concerned. Such authorities are known as Country Signing Certificate Authorities (CSCAs). Through this infrastructure, CSCAs authenticate documents following a procedure that is fully compliant with the technical specifications set out by the International Civil Aviation Organization (ICAO) on visible digital seals for non-electronic documents.[80]

The process for option C3 would be as follows (in line with Figure 10).

1. The consulate staff receives the data from the third country national's application and runs the necessary checks against VIS and the other EU information systems according to the future revised VIS Regulation.
2. After carrying out the examination and deciding to issue a visa, the consulate staff pushes the new information into VIS. At the same time, the visa information is pushed automatically to software installed in the issuing country's national system, which encodes the data in a 2D barcode.
3. The CSCA provides a cryptographic seal (so-called 'visible digital seal') that certifies the authenticity of the data encoded in the barcode.
4. The digitally signed barcode is created in a format commonly used for pictures, e.g. jpeg;
5. The consulate includes it in the visa issuance notification and sends the notification and the 2D barcode to the third country national (via email and/or secure account, depending on whether the online application is implemented).

The possibility of re-using the PKI is already up and running, as are the secure communication channels connecting the consulates and central authorities. This means the Schengen countries could build option C3 without the need for new infrastructure and communication channels.[81] This improves technical feasibility. A few Schengen countries are already using 2D barcodes to enable authorities in the field to check the identity of individuals and the validity of their documents. For instance, the German Ministry of Interior is currently digitally signing the documents provided by the German authorities to international refugees on their arrival.[82] Third country nationals are issued with a document featuring a barcode that can be checked offline by German authorities (see also operational and implementation feasibility below).

However, whilst all the Schengen countries have a CSCA in charge of digitally signing certain categories of document, they would all need to introduce visa barcodes to the list of items to be signed and maintained through the PKI. As it is up to each Schengen country to determine the amount and the nature of the items covered by its PKI, not all Schengen countries may be ready to the same extent to introduce visa barcodes. Therefore, depending on which and how many documents are signed digitally, the Schengen countries may need varying adjustments to the software and technical components currently in use. This means that option C3 would run on more technically complex components than the other two options. Nonetheless, since the backbone of the infrastructure is up and running and the most invasive technical efforts have already been made, option C3 would still score high in terms of technical feasibility.

---

79 This technical adjustment would be in line with the guidelines published by the German Federal Office for Information Security. See for more information: BSI TR 03137 – Part 2: JAB Code (Just Another Barcode) – Color Barcode Symbology Specification, available at: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03137/BSITR03137.html.

80 For the technical specification see the 2018 Report by the ICAO on visible digital seals for non-electronic documents.
https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Visible%20Digital%20Seals%20for%20Non-Electronic%20Documents%20V1.7.pdf.

81 Interviews with DG HOME B.2 officials.

82 For more information on the German Proof of Arrival for international refugees see e.g.: https://www.bamf.de/SharedDocs/Anlagen/EN/Downloads/Infothek/Asyl/faq-ankunftsnachweis-asylsuchende.pdf?__blob=publicationFile.

Security feasibility

This section performs a security analysis on the proposed digital visa option and the three offline fallback solutions. The following security criteria are used to assess the options: data security, risk of forgery/counterfeiting, and availability of IT systems. At the same time, the security measures that need to be taken to deal with the security challenges of each option are explained.

Digital visa

This section covers the security feasibility assessment for the different criteria relating to the digital visa as such.

Data security

Because of its electronic nature, the digital visa has a number of clear advantages in terms of the security of the traveller's data.

1. There is zero risk of the digital visa being physically lost or stolen. It will no longer be possible for a potential impostor to steal a (used) visa sticker and use it to impersonate the rightful owner of the visa.
2. Electronic documents and digital identities, such as the digital visa, offer a better potential for protecting against security incidents compared to visa stickers. For example, blank visa stickers can be lost or misfiled, while there is no such risk with electronic documents. Furthermore, travel documents can be easily tampered with, for example by removing pages (and/or adding counterfeit elements).
3. Electronic documents can be better protected against inappropriate access inasmuch as they can be encrypted, and in the event of theft, the information remains protected.

Risk of forgery/counterfeiting

The electronic nature of the digital visa lowers the risks of forgery and counterfeiting for the following reasons.

1. A paper-based document runs the risk of being counterfeited despite the enhanced security of the new sticker format and despite the need for special technical expertise. The fully digital visa would remove the need for paper and therefore would make counterfeiting strategies useless.
2. The training and experience of border guards is indispensable in identifying whether the document is genuine or not. Despite the extensive experience of border authorities, such checks are prone to false decisions, i.e. letting travellers through with counterfeit stickers. In the case of a digital visa, a machine carries out the check. This guarantees higher reliability per se and because this solution would not suffer from the typical shortcomings of human labour, e.g. fatigue. With the paper document, there is currently a risk that border guards will only use the physical visa document as the only verification of proof for determining if the individual is allowed to enter the country or not.
3. A visa can be revoked during the traveller's stay or during travel. If the visa is checked against VIS, the competent authority will instantly know if the visa is no longer valid. This is not the case if border guards only check the paper-based alternative.

Availability of systems

It is clear that a digital visa will rely on 24/7 availability of the central systems/databases, i.e. VIS and the carrier gateway, including the architecture behind it. Therefore, if the digital visa is implemented and enforced, there is a risk of carriers and the Schengen authorities being unable to verify visas if ever the information systems and gateways are inaccessible for technical reasons.

As showed in Table 9 above, the VIS is already characterised by high availability. The impact of VIS downtime is minimal, and the portrayed availabilities are likely to increase in the future. A more problematic event for availability would be the lack of internet connection. This is because, even were VIS operating normally, the local area network might be the source of the technical impossibility of accessing VIS. This is not an area of responsibility of eu-LISA). This might happen in either the Schengen Area or the third country. The network may be unavailable in a major airport or seaport as well as in (remote) land region, either along the external border or inside the territory.

Arguably, the impact of network failure in the third country on border security would be lower than the impact of a network failure at the Schengen border. If there were a network failure in the country of departure, i.e. if carriers and – if applicable – third country authorities were not able to verify the traveller's visa prior to departure (via

permissions gateways), the traveller would still be checked upon arrival at a Schengen border crossing point. It is extremely unlikely that both the third country and the Schengen border crossing point would both experience a lack of connectivity.

It is therefore clear that there are security risks stemming from possible (albeit rather unlikely) technical failures. This means that an offline fallback option should be considered, even though it is reasonable to expect that it would be used only in very limited circumstances.[83]

Offline fallback solutions

This section presents a comprehensive analysis of the three offline fallback solutions, identifying the security risks and benefits of each. There are two provisos in this connection.

- Since all options include a notification, they are all subject to data security risks inherent in the notification, e.g. being easy to forge or provided to a potentially vulnerable email account;
- None of the options discussed would enable the authorities to detect in an offline scenario that the third country national's visa had been revoked or annulled after issuance. However, the event of a third country national arriving at the border with a revoked/annulled visa at the same time as VIS is inaccessible is extremely unlikely.

Table 16: Overview of the different security risks and benefits of the different offline fallback solutions

Fallback solutions	Data security	Risk of forgery/counterfeiting	Accessibility of systems
Option C1: Email notification	Very low level of data security if notification is printed: the notification can be stolen as it is a physical paper-based document. Although they can be sent through secure (email) accounts, notifications cannot be encrypted to protect against unauthorised access to data.	High risk of counterfeiting: it is very easy for most people to counterfeit an email or paper document.	Would enable verification offline, but because of its limited security features, border guards may be less ready to rely on it.
Option C2: Email notification with a non-signed barcode	The information in the barcode can easily be tampered with and is not protected against unauthorised access.	High risk of counterfeiting: to forge a barcode with information does require specialised technical expertise, but is possible.	Would enable verification offline, but because of the limited security, border guards may be less ready to rely on it.
Option C3: Email notification with digitally signed barcode	The information in the barcode is very well protected against unauthorised access.	Very limited risk of counterfeiting: the digital seal applied by CSCAs is highly reliable and extremely hard to counterfeit.	More secure inasmuch as it can include biometric information data in the barcode (facial image) and increase the accuracy of a non-biometric check.

The overview provided in the table above clearly shows that option C3 is preferable from a security point of view, even though none of the three options would allow the authorities to find out during a technical downtime whether the visa had been revoked or annulled after issuance.

- Option C1 is not secure enough under any criteria, as it carries the same paper-related weaknesses as the sticker, and poses higher risks of counterfeiting/forgery.
- Option C2 improves the situation, as it is slightly more difficult to unduly access and/or counterfeit data through a barcode. However, the enhanced security compared to option C2 lies merely in the technical expertise needed to forge a barcode. In other words, there is no specific security feature guaranteeing the reliability of such barcodes.
- Option C3 would use the digital seal to protect against unauthorised access and would be practically immune from counterfeiting/forgery attempts thanks to the unique cryptographic key issued by the CSCAs.

Data protection feasibility

As is the case for the online visa application portal, the digital visa option as such does not modify the nature or amount of personal data collected from third country nationals. In fact, by abolishing the visa sticker, the digital visa option would repeal one of the existing physical supports that involves processing of personal data, i.e. the

[83] Such circumstances do not refer to the ordinary use of the fallback solution by third country authorities and Schengen immigration authorities carrying out immigration checks in the territory.

visa sticker. All data included in the digital visa will be the data collected from third country nationals in accordance with current legislation and to the revised VIS Regulation.

Therefore, the data protection requirements applying to the current Schengen visa remain applicable to the digital visa option. This means that, in general, the digital visa would be fully compliant with EU data protection law, as the 'virtual' part of the visa exists already today.

In principle, the same reasoning is applicable to the offline fallback solutions. None of these solutions adds to the type and quantity of data currently collected, processed and shown on the visa sticker. Options C1 and C2 would carry exactly the same alphanumerical data, whilst in option C3 the digitally signed barcode would also include the facial image (which is currently included on the sticker).

However, option C3 would entail the automatic generation of a barcode by a software integrated in the national system of the issuing Schengen country. This step has data protection implications insofar as, although neither the consulate nor the CSCA encode the data manually, the generation of the barcode by the software equates to new processing of personal data.[84] Therefore, there needs to be assurance that the authority responsible for managing the national system complies with the relevant provisions on lawful processing laid down in the General Data Protection Regulation (GDPR).[85] In particular, the authority has to comply with Article 6(e) relating to processing in the public interest.[86]

Finally, it is worth making a remark concerning data privacy. In each of the three fallback solutions, personal information is sent to the applicant through a secure email address. However, this implies that unauthorised individuals could access the data if the email address is compromised ("hacked"). Moreover, the data could be sent to the wrong person if the applicant made a mistake while entering their email address. Therefore, a privacy statement should be included in the notification, letting the reader know that its content is only intended for the use of the addressee and should not be shared with unauthorised individuals.

For options C2 and C3 (non-, and digitally signed barcode) the same principles would apply. However, in the light of the result of the security feasibility assessment, it would be somewhat harder to obtain personal data from the non-signed barcode (although it would not require specialised expertise), and nearly impossible from the signed barcode.

Operational and implementation feasibility

This section describes the operational and implementation impacts, requirements and implications inherent in the different digital visa options when moving forward to a digital replacement of the visa sticker. Whereas the technical feasibility dealt with the requirements and measures relating to IT infrastructure, this section deals with the measures needed to get the options up and running, and usable on a daily basis.

Digital visa

As all core IT systems for border management are up and running or planned, the implementation and operational functioning of the digital visa option would benefit from measures already taken to implement those systems. However, as mentioned earlier in the technical feasibility assessment, if no online application option is chosen, then an independent traveller web service would have to be developed based on the EES web service.

In particular, by the time the digital visa option is rolled out, the revised VIS and EES will have already implemented the necessary measures – namely, equipping border crossing points with scanners capable of reading fingerprints and facial images, and launching a query to the EES and VIS. Therefore, if the current situation – including the

[84] This finding was confirmed in an interview with the European Data Protection Supervisor (EDPS).

[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); https://eur-lex.europa.eu/eli/reg/2016/679/oj

[86] Article 6(e) GDPR reads: "Processing shall be lawful only if and to the extent that [...] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

measures to implement the upcoming systems – were considered the baseline, the digital visa option would be extremely feasible from the operational and implementation perspective.

Offline fallback solutions

No specific implementation measures would be needed for option C1, if any of the online application options were chosen, as it would rely exclusively on the measures implemented to have the online application portal up and running. Conversely, if the digital visa were implemented before and/or without any online application portal, then consulates would use the new web service developed for this purpose to ensure communications with third country nationals (see the technical feasibility above).

Options C2 and C3 would need certain implementation measures in order to verify the barcode.

Border crossing points and Schengen immigration authorities will need to be equipped with appropriate mobile phones to read the barcodes. As the authorities in most Schengen countries have already issued or are issuing border control, immigration and police authorities with such devices, only a minor additional effort by certain Schengen countries would be necessary to enable all stakeholders to access the visa information included in the barcode.

For options C2 and C3, border control and police authority smartphones will have to host a mobile application capable of reading the data in the barcodes. Mobile applications for reading both types of barcodes are publicly available on the market, but they are fundamentally different.

- Applications for reading non-signed barcodes (option C2) are mostly free or low-budget applications enabling the user to scan a barcode and immediately read the encoded data.
- Applications for reading digitally signed barcodes (option C3) are capable of recognising the digital seal added to the barcode (by scanning the corresponding pixels on the barcode's surface) and informing the user that the barcode is authentic. Then the application would go on to decode the third country national's data encoded in the barcode. Amongst the applications available on the market, SealVer[87] is a publicly available software currently used by German authorities carrying out checks on refugees' documents of arrival authenticated through a digital seal (see also technical feasibility above).

In both cases, the software developer is in charge of constantly updating the applications and fixing possible bugs. From the analysis above, it follows that option C1 is clearly the most feasible from an operational and implementation perspective. However, options C2 and C3 would be able to rely on the ongoing deployment of appropriate mobile phones and on publicly available software to scan barcodes. Therefore, their implementation would not require massive efforts by the Schengen authorities.

Moreover, additional synergies are possible with the barcode solution proposed within the Article 6 Committee. If the solution becomes operational, then the Schengen countries will already have issued such devices to national authorities as part of the implementation of this solution. The Schengen Area could then transit to a fully digital visa by relying on those efforts and investment.

[87] See a gateway for download: https://play.google.com/store/apps/details?id=de.tsenger.sealver.

4. Cost-benefit analysis

The cost-benefit analysis (CBA) of the online application process estimates the costs that the Schengen countries would incur if there were no Schengen-wide online application portal. In addition, the chapter estimates the costs associated with both system architectures of an online application portal as described in Section 3.1. Obtaining these two costs makes it possible to estimate the potential savings across the Schengen countries as a result of adopting one or other system architecture. The analysis also explores other cost savings, and calculates efficiency gains and other qualitative and quantitative benefits for third country nationals, Schengen countries and the European Union.

The CBA of the digital visa follows a similar approach. After estimating the cost of introducing a digital visa and the options for the offline fallback solution, the chapter compares these costs with the costs currently flowing from the use of paper stickers. It also estimates the cost savings and efficiency gains for the applicants and the Schengen countries.

This chapter presents the results of a more detailed cost-benefit analysis presented in Annex A. The results presented in this chapter are purely indicative and based on readily available data, data obtained through questionnaires, interviews and studies conducted previously. The level of detail currently available and within the scope of this study means that a detailed cost analysis is not possible. Therefore, the results should be considered only as an initial, indicative estimate.

4.1. Online application

This section presents the results of the cost-benefit analysis for the online application process. To perform the cost analysis, two scenarios are considered:

- **the baseline scenario** where no Schengen online application portal is set up;
- **the solution scenario** where a Schengen-wide online application portal is set up to be shared with all Schengen countries. This analysis considers both system architecture options.

The first subsection estimates the costs associated with each scenario. Estimating the costs for both scenarios enables the comparison of two aspects:

- the comparison of the system architectures makes it possible to show the relative financial effort required for each; and
- the comparison of the system architectures to the baseline scenario makes it possible to calculate the potential cost savings as a result of transitioning to a Schengen online application portal.

The second subsection shows the benefits obtained by adopting one or other system architecture. These benefits are split between in quantitative benefits, which were estimated based on questionnaires to Schengen countries who already have some form of online application portal, and qualitative benefits, which are based on the online application portal's core features, and the proven experience of certain Schengen and non-Schengen countries, e.g. the United Kingdom.

Furthermore, because of the level of detail available in this study is limited, a 30% uncertainty interval is applied to the estimations. Therefore, all estimated costs are presented in ranges, e.g. EUR 1-2 million.

4.1.1. Costs

The baseline scenario

The baseline scenario covers the scenario where there is no Schengen-wide online application portal. In this scenario, it is likely that the Schengen countries' national systems will continue to evolve as they are now: each Schengen country would eventually set up their own national online visa application portal. Therefore, the baseline scenario considered in this CBA is not the situation of the current as-is, where only a handful of countries are investing considerably in their national application portal, but the continuation of this trend into the future.

For this exercise, the actual cost of a fully-fledged online application portal at a *national* level, with the same features as the Schengen online application portal, was estimated. This estimate was based on information provided by eight Schengen countries through a questionnaire[88] and expert knowledge. From there, the 29[89] Schengen and obliged to eventually join the Schengen Area countries were subdivided into three groups, based on their current national application portal's maturity level.

Knowing the cost of the fully-fledged online visa application portal, and knowing the average current investments per group, a cost can be assigned per Schengen country. This cost represents the need for investment in the national application portals. Aggregating all these costs leads to the final result, which represents the investments needed, across all Schengen countries, to transition to a scenario where all Schengen countries operate their own national online visa application portal.

The result of the cost exercise described above is an estimate that setting up a national online visa application portal, from scratch, requires an initial investment of **EUR 3-5.7 million**.[90] Countries without an online visa application portal would therefore need to invest 100% of this figure to reach the target state. For the other groups, the assumption is made that countries with a moderately advanced online visa application portal would have to invest 66% of this sum to reach the target state. Countries with an advanced visa application portal would need to invest 33% of this sum to reach the target state.

The table below shows the distribution of the Schengen countries per level of technological maturity, along with the percentage of further investment needed relative to the cost of starting from scratch.

Table 17: Classification of Schengen countries by levels of technological maturity of their national portal and further investment needed

	No national portal	Moderately advanced national portal	Advanced national portal
Countries in category	15	10	4
Investment needed (% of cost of totally new portal)	100%	66%	33%

After the national application portals have been set up, they also need to be maintained. Since, in the hypothetical future baseline scenario, all Schengen countries operate 'the same' fully fledged online visa application portal, the operations and maintenance costs associated with these national portals can be considered as equal. This operations and maintenance cost in IT systems is typically equal to 20% annually of the total investment in the initiative.

The table below summarises these estimates.[91] The investment costs (row 3) clearly differ per Schengen country category. A country with no national portal yet will have to invest more than a country that is already operating portal with a more advanced maturity level.

88 The questionnaire asked Schengen countries to provide information on the costs related to their current investments in their national online application portal. Furthermore, the questionnaire asked for the maintenance and operational costs, and the features supported by the national portals. Based on this and expert knowledge, it was possible to extrapolate the costs of the proposed EU application portal.

89 Costs for Liechtenstein are not considered as the country does not issue its own visas.

90 This cost includes the procurement, design, development, testing, deployment and any infrastructure costs associated with the portal.

91 The delivery period has been estimated to last three years. Furthermore, the operational and maintenance period has been assumed to be 5 years as the technological costs cannot be estimated further ahead. The table presents the costs, per year, over this eight-year period.

As explained above, the operation and maintenance costs are equal for all categories, so that, even though the Schengen countries might have different investment costs, they will, in the end, all be operating their own equally advanced national portal.

Table 18: Summary of national online application costs per Schengen country maturity level

Cost category	No national portal (million EUR)	Moderately advanced national portal (million EUR)	Advanced national portal (million EUR)	Total (all countries) (million EUR)
Yearly delivery costs	1.0-1.9	0.67-1.3	0.33- 0.63	23.0-44.0
Total delivery costs (3 years)	3.0-5.7	2.0-3.9	1.0-1.90	69.0- 132.0
Yearly operations and maintenance costs	0.60-1.1	0.60-1.1	0.60-1.10	17.4- 31.9
Total operations and maintenance costs (5 years)	3.0-5.5	3.0-5.5	3.0-5.50	87- 159.5
Total costs (8 year period)	**6.0-11.2**	**5.0-9.4**	**4.0-7.4**	**156.0- 292.0**

The solution scenario

The solution scenario is the scenario where a Schengen online application portal is set up. Similar to the estimate presented in the previous section, this initiative consists of initial investments, during which the portal is delivered, and a period of operations and maintenance.

Because the Schengen online application portal consists of central systems (hosted by eu-LISA) and national systems, the costs have been subdivided into these two categories. The table below summarises the costs for the online application portal. Please refer to Annex A for the details on which these estimates are based. The EU centralised application portal has been estimated to take three years. Furthermore, the operation and maintenance period is only forecast for five years as technology costs cannot be estimated accurately further ahead.

Table 19: Summary of the costs for the online application portal

	Centralised system architecture (option B1) (million EUR)		Hybrid system architecture (option B2) (million EUR)	
	Central System	National System	Central System	National System
Yearly delivery costs	4.1-7.6	0.14- 0.26	2.2- 4.2	0.35- 0.66
Total delivery costs (3 years)	12.3-22.9	0.42- 0.78	6.7- 12.5	1.1- 2.0
Yearly operations and maintenance costs	2.50-4.6	0.085-0.16	1.3- 2.5	0.21- 0.40
Total operations and maintenance costs (5 years)	12.3-22.9	0.42- 0.78	6.7- 12.5	1.1- 2.0
Total costs (8 years)	**24.6-45.8**[92]	**0.8- 1.6**[93]	**13.4- 25.0**[94]	**2.20- 4.0**[95]
Total option cost (8 years)	**49.0-91.0**[96]		**75.1- 139.6**[97]	

[92] EUR 3.1million – EUR 5.7million average annual costs
[93] EUR 105K – EUR 200K average annual costs
[94] EUR 1.7million – EUR 3.1million average annual costs
[95] EUR 275.000 – EUR 500.000 average annual costs
[96] EUR 6.1million – EUR 11.4million average annual costs
[97] EUR 9.4million – EUR 17.5million average annual costs

There are two key observations to make about the table above:

- First, for option B1, the central system costs are higher than in option B2. Conversely, the national system costs are lower than in the hybrid architecture option. This is because both system architectures perform the same process, but the application files are stored in different locations. In option B1, the AMS is situated at a central level, which shifts the focus to the central systems. In option B2, the national systems need to store the application files, which shifts the focus to the national systems.
- Second, although both system architectures perform the same process, option B2 is considerably more expensive. This is because in option B1 only one single system storing all application files needs to be developed and maintained, i.e. the AMS. In option B2, 29 such systems need to be developed and maintained. While the complexity of these systems is lower than the effort required for the AMS, this does not outweigh the efficiency of creating a central system.

Scenario comparison

This subsection compares the cost of the proposed system architectures to the likely baseline scenario, described above.

The delivery period of the Schengen online application portal, during which the accompanying systems are procured, designed, developed, tested and deployed is estimated to be three years. Therefore, the costs presented in Table 19 can be spread across three years. Furthermore, yearly operations and maintenance costs are typically estimated for a five-year period. Estimating these costs further ahead would lead to inaccurate predictions as it is not possible to assess technological costs accurately more than five years into the future. Therefore, for the yearly operation and maintenance cost, 20% of the total investment costs are incurred every year for five years.

It is not feasible to estimate the delivery period of the national online application portals, as all countries are free to start and end the development of their national systems at their discretion. However, to allow a comparison, the costs presented in the table above are spread across the same delivery period as the Schengen online application portal. Finally, the operation and maintenance costs are also estimated for a five-year period after the delivery of the national portals.

The table below summarises the different costs associated with the three to-be scenarios considered (baseline, centralised architecture and hybrid architecture) presented in the earlier tables. The costs are presented as an aggregated result (central system costs + 29 times the national system costs).

Table 20: Total costs per year for each to-be scenario considered

Year	Baseline scenario (million EUR)	Option B1 (million EUR)	Option B2 (million EUR)
Yearly delivery costs	23.0- 44.0	8.2-15.2	12.5- 23.3
Total delivery costs (3 years)	69.0-132.0	24.5-45.5	37.6- 69.8
Yearly operations and maintenance costs	17.4-31.9	4.9-9.1	7.5-14.0
Total operations and maintenance costs (5 years)	87.0-159.5	24.5-45.5	37.6- 69.8
Total costs (8 year period)	**156.0-292.0**	**49.0- 91.0**	**75.2- 139.6**

The figure below illustrates visually by means of a graph the yearly costs associated with the scenarios. The ranges are presented as a coloured box indicated with an 'uncertainty interval' indicator. Furthermore, the costs are stacked on top of the blue (the lowest) line in order to illustrate the operations and maintenance costs that Schengen countries are currently incurring.[98] The drop after the delivery stage comes from the fact that the online application portal will eliminate some costs that Schengen countries are currently incurring, i.e. the archiving and

[98] These costs were calculated based on questionnaires asking for Schengen countries' costs relating to the operation of the national portals, the archiving of physical documents and their destruction. Responses were received from nine Schengen countries.

subsequent destruction of supporting documents. Not all costs disappear as the Schengen countries could opt to continue to use their current portals for their national visa issuing process[99].

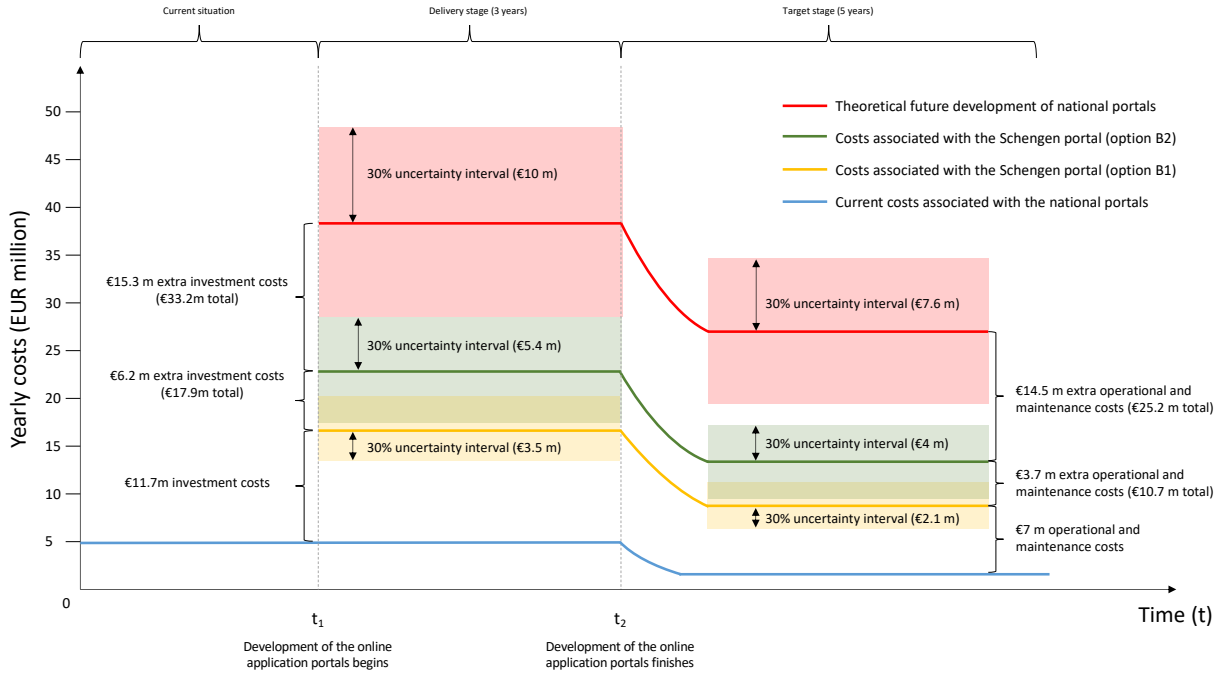

Figure 12: Visualisation of total costs of the baseline and solution scenarios

Figure 12 clearly illustrates the financial benefits that can be obtained by opting for a Schengen online visa application portal instead of different national versions. Indeed, for both system architectures, there are considerable savings to be made. The figures below show the savings obtained per system architecture option. Based on the data in the figure above, the following cost savings are possible (over the total eight-year period):

- For the centralised system architecture (option B1): **EUR 107-201 million**
- For the hybrid system architecture (option B2): **EUR 75-140 million**

4.1.2. Benefits

The development of a Schengen online application portal brings multiple qualitative and/or quantitative benefits that can be identified for 1) third country nationals; 2) the Schengen countries; and 3) the Schengen Area as whole. Both system architecture options enable the same qualitative and quantitative benefits, but as described in the previous section, at a different cost. Please note that this section does not include a calculation on the return on investment as the level of detail available in the study and the length of the online application roll-out does not allow the estimation of an accurate prediction at the time of this writing.

Schengen countries

The creation of a unique online application portal hosting intelligence-driven features will enable the Schengen countries to achieve the following qualitative benefits:

- An increased rate of 'first-time right' applications thanks to automated form-filling technologies and automated quality checks, which will reduce the error rate in the applications submitted and reduce the time it takes to process them. This will in turn enable consulates to save time in pre-screening and processing applications. Based

[99] It has been assumed that 50% of the existing national portals will be depreciated upon the availability of either the Schengen or national online visa application portal.

on data provided by the Schengen countries in response to questionnaires[100], it has been estimated that the Schengen countries will **save 708**[101] **Full-Time Equivalents (FTEs)** ***per year***.[102] This employee time could then be spent on more critical tasks, i.e. examination.

- In the survey, Schengen countries indicated that they have observed a small increase in visa applications with the introduction of national portals (<5%). Therefore, the Schengen online application portal will result in an increase in applications, which will ultimately boost the economy of the participating countries.
- Higher conversion rate, i.e. thanks to advanced guidance tools, more applicants are expected to complete their applications without quitting the process.

Furthermore, both system architecture options display considerable financial benefits as opposed to the hypothetical future evolution of the systems (see Figure 12).

Third country nationals

As the online visa application portal would remove the need for third country nationals to travel to a consulate or an external service provider, there are significant savings in travel costs for those individuals. The average saving in travel costs will be EUR 55 *per application.*[103] This amounts to a total travel cost saving for third country nationals of **EUR 880 million**.

The various features of the online application portal, such as the guidance during the submission, the centralised payment service, the appointment management tool, the notification service, the visa status checking tool and the automated data quality checks improve the TCN's visa application experience and enable a smoother visa application process overall. This is because:

- many applicants would no longer need to travel to the consulate/ESP (except if they need to enrol their biometrics or verify travel document), so they would benefit from substantial time savings;
- compared to a scenario where each Schengen country offers its own application portal, applicants would save time with a common Schengen portal because they would find all the relevant information and guidance in that one place;
- the advanced guidance tools would enable applicants to make fewer mistakes and complete all the steps more efficiently, leading to a better user experience that may translate into more returning applicants (which is in turn a benefit for the Schengen countries);
- applicants would submit more 'first-time right' applications, so fewer applicants would need to spend time correcting data and submitting additional documents;
- the interactive guidance on the online application portal enhances the speed at which applicants can fill out the application forms.

Schengen Area

Finally, from a Schengen Area point of view, the Schengen online visa application portal will present a unified image to all third countries. This will reflect positively on the public image of the Schengen Area.

---

100 In their responses to the questionnaires, three Schengen countries with an online application portal indicated the time gained per application as a result of their national portal.

101 This calculation is based on the questionnaire mentioned in the previous footnote. In addition, the calculation takes into account a 50% increase in the average time saved due to the extra features the online application portal offers. This makes it possible to calculate the total time saved based on the number of applications per Schengen country, and whether the country already has a national portal or not.

102 This equals, on average, 24 FTEs per Schengen country. Similar to the costs, these figures will vary considerably per Schengen country.

103 This cost is based on an average travel cost per application of EUR 110, based on the 2013 Impact assessment study supporting the review of the Union's visa policy to facilitate legitimate travelling (Annex 2- footnote 49). Only 50% of the applicants (first-time applicants + applicants whose biometrics have expired + applicants whose travel document has been renewed) need to present themselves physically at a consulate. Hence the average travel cost is EUR 55.

4.2. Digital visa

This section estimates the costs associated with and the benefits obtained by moving to the digital visa. The following approach has been used:

- first, the section outlines the costs required to implement the digital visa and compares the costs needed to implement the three options for the offline fallback solution;
- second, the section presents the quantitative and qualitative benefits of the digital visa for stakeholders.

Please refer to Annex A for the details of the cost-benefit analysis.

4.2.1. Costs

The introduction of the digital visa will benefit from synergies with current and upcoming EU systems for border management. There will be no additional costs to incur in either developing a new system architecture, as the digital visa will rest on the VIS architecture (including the adjustments to network capacity needed because of the VIS Revision) or equipping border crossing points with devices to carry out biometric verification.

Traveller web service

The digital visa may require additional costs for the web service enabling communications between consulates and third country nationals in the event that no online application option is chosen (and therefore this communication cannot rely on the online portal). The traveller web service would be based on the concept used to develop the EES and ETIAS web services.

This study assessed the costs of the service based on the Software Development Life Cycle (SDLC). Following this methodology, the end-to-end process for building a system is broken down into the following consecutive phases: procurement, design, development, testing and deployment. Each of these phases represents a cost factor corresponding to the cost of the personnel needed (system designers and developers). In addition, infrastructure costs, and operations and maintenance costs need to be taken into account.

In order to assign a cost value to each phase, the methodology starts by assessing the cost of the development phase. Based on assumption B_1, the development effort needs to be established in order to assess the costs. This study envisaged this phase lasting for one year, incurring a cost of EUR 1.1 million. Applying the 30% uncertainty margin mentioned above, this means that the development phase would require an effort ranging from EUR 0,8-1,4 million. Based on this benchmark, the table below summarises the costs of the other phases.

Table 21: One-off costs for the stand-alone traveller web service

Cost factor	Description	Cost (million EUR)
Phase 1: Procurement	The European Commission, eu-LISA, and the Schengen countries agree on common technical components and specifications, such as protocols and interfaces, and select the party responsible for each future phase.	0.25-0.50[104]
Phase 2: Design	In this phase, the traveller web service is designed through to the definition of the interfaces, interactions between components, data models of databases, and the protocols to be used.	0.60-1.10
Phase 3: Development	During this phase, the components will need to be built according to the agreed technical specifications.	0.80-1.40
Phase 4: Testing	Once developed, the infrastructure needs to go through testing procedures to ensure future performance.	0.60-1.10
Phase 5: Deployment	This phase concerns the rollout of the traveller web service so that the consulates and third country nationals can use it on a daily basis.	0.08-0.14
Infrastructure	This category is not a phase. It includes the hardware necessary to run the service and deliver interaction with existing systems (servers, databases, licences, network capacity, routers, etc.)	1.20-2.20
All factors	**All phases for building the traveller web service**	**3.50–6.40**[105]

[104] This cost is not directly linked to the development effort, but is just an estimation of the costs required to negotiate the specifications for the gateway with all stakeholders.

[105] The total figures are rounded to emphasise that they are estimations.

The traveller web service would therefore need a one-off effort costing approximately **EUR 3.5-6.4 million,** plus a **EUR 0.7-1.2 million** yearly effort in operations and maintenance.

The digital visa may open up the possibility of creating a permissions gateway for hotels, banks and other third parties operating within the Schengen Area. It would be based on the carrier gateway and provide an "OK/NOT OK" answer to the query. However, this study found that it is not worth considering due to the associated effort and costs.[106]

These third parties may use one of the offline fallback solutions. This will imply certain additional costs depending on the option selected.

Option C1 – Visa issuance notification

No additional costs are expected if this option is selected. If an online application portal is implemented, the only (very minor) costs associated with option C1 would merely require configuring the online portal's web service connecting the consulates and the applicants. If the digital visa were implemented before and/or without any online application portal, the costs for the independent web service would be accounted for in the implementation of the digital visa (as would also be the case for options C2 and C3).

Option C2 – Non-signed barcode

The encoding of visa information in a simple, non-signed 2D barcode requires the following:

- Software for encoding information in barcodes. This would cost **EUR 1.1-1.9 million** for the whole Schengen Area;
- Equipment for border crossing points and Schengen police authorities with appropriate smartphones for scanning barcodes. It is reasonable, however, to start from the assumption that the authorities in most Schengen countries are already equipped with such devices, and the central authorities in the remaining countries are in the process of deploying them. Therefore, the study does not foresee any new costs for this. However, additional costs might have to be incurred by individual Schengen countries in the event that, when option C2 is implemented, their authorities had not already been provided with such devices.[107]

Option C3 – Barcode signed with digital seal

The generation of a barcode digitally signed by the CSCA would entail the following:

- the acquisition and maintenance of software for signing an additional category of documents digitally, i.e. visas, in addition to those already being signed by each Schengen country's CSCA. Based on the advice of national experts, such adjustments would require a **EUR 0.1-0.2 million** effort per Schengen country, i.e. **EUR 3-6 million** for the whole Schengen Area;
- The same equipment for border crossing points and police authorities as in option C2. The same assumption made above applies also for option C3.

The table below sums up the estimates of the investment needed to implement the digital visa and each of the three offline fallback solutions.

---

106 One can estimate that the project for designing, developing and deploying the permission gateway would last approximately 2 years and require a one-off cost ranging between EUR 4.5 million and EUR 5.6 million. Such costs would cover the whole project for building the gateway, including: procurement, design, development, testing, deployment and infrastructure. Additionally, EUR 500,000-600,000 yearly maintenance costs would have to be allocated.

107 The unit cost of one device would be in the EUR 300-500 range. The EUR 300 estimation is based on the deployment of fingerprint-reading scanners by the UK Home Office. The unit cost of such scanners is less than GBP 300 and they include even more complex features, i.e. biometric scanning, than those necessary for reading barcodes. The estimate is then scaled up to EUR 500 to leave room for more costly devices (depending on the procurement choices of each Schengen country).

Table 22: Investment needed to implement the digital visa and offline fallback solutions

Category	Option C1	Option C2	Option C3
Cost of developing and implementing the digital visa (EU budget costs) (million EUR)			
Development of the web service (*if no online application portal is implemented*)	3.5-6.4 (one-off)		
Operations and maintenance costs for the web service (*if no online application portal is implemented*)	0.7-1.2 (per year)		
Cost of developing and implementing the offline fallback solutions (Schengen countries' costs) [108] ***(million EUR)***			
Software for encoding barcodes	N/A	1.1-1.9	N/A
Adjustments to the Schengen countries' PKI	N/A	N/A	3-6
Barcode-reading devices at the border	N/A	Negligible (*if needed*)	Negligible (*if needed*)
Barcode-reading devices for inland checks	N/A	Negligible (*if needed*)	Negligible (*if needed*)
One-off costs with an online application portal (digital visa plus offline fallback solution)	**zero**	**1.1-1.9**	**3-6**

Category	Option C1	Option C2	Option C3
One-off costs without an online application portal (digital visa plus offline fallback solution)	**3.5- 6.4**	**4.6- 8.3**	**6.5-12.4**
Periodic costs without an online application portal (per year)	**0.7-1.2**	**0.7- 1.2**	**0.7-1.2**

The following can be concluded from the table above.

- Option C1 is by far the least expensive, as it only requires the costs of developing the traveller web service in the event that the digital visa is implemented before and/or without any online application portal. Option C1 would entail **no costs** if it were adopted together with the online application portal, or **EUR 3.5-6.4 million** with no online application portal. However, option C1 is the least feasible option based on all the criteria applied in the feasibility assessment above.
- Option C2 is more costly, especially with regard to the deployment of software for encoding the barcodes in the consulates. It would require an effort of **EUR 1.1-1.9 million** (with an online application portal) or **EUR 4.6-8.3 million** without.
- Option C3 is the most costly. It would require an effort of **EUR 3-6 million** (with an online application portal) or **EUR 6.5-12.4 million** without. The main reason is the effort required from each Schengen country in updating and extending their PKI. The clear differentiating factor, however, is that option C3 scores higher than option C2 under all feasibility criteria.

The discussion in the Article 6 Committee by European Commission and experts from the Schengen countries, which is described previously in this report, as to whether it is advisable to start issuing visa stickers with digitally signed barcodes may help reduce the costs for options C2 and C3, notably in relation to the deployment of appropriate smartphones. If such a solution is adopted in the form of a recommendation, the more Schengen countries decide to make it operational, the more likely it will be that Schengen Area authorities will already have been issued with appropriate smartphones (over and above efforts currently undertaken by the Schengen countries on their own).

[108] The study considered the current 26 countries fully applying the Schengen acquis, plus Bulgaria, Croatia, Cyprus and Romania, which have committed to joining the Schengen Area in the future.

4.2.2. Benefits

As is the case for the online application portal, the digital visa solution will yield both quantitative and qualitative benefits. Such benefits will accrue to 1) the Schengen countries and 2) third country nationals.

Schengen countries

Schengen countries will make significant savings on the current costs for purchasing and filling in visa stickers. Unlike most of the investment costs highlighted above, such cost savings would recur annually every year following the adoption of the digital visa.

The table below displays the costs relating to the sticker. The replies from twelve Schengen countries to the same data collection questionnaire referred to earlier in Chapter 4 are the main source of the data. All costs reported in the middle column ('single sticker') were obtained by averaging the data collected from the countries' replies. Each unit cost, e.g. production cost, was then multiplied by the total number of Schengen visas issued in 2018. This provides an estimation of the total expenses incurred by the Schengen countries.

Table 23: Costs related to the visa sticker

Categories	Single sticker (EUR)	Aggregated cost for the Schengen Area (million EUR)
Production cost	0.64	9.1
Transportation cost	0.19	2.7
Storage cost	0.07	1.0
Filling in cost	0.09	1.0
Total cost	**0.99**	**13.8**
Total number of visas issued (2018)	*14,265,282*	

The table above shows that the Schengen countries currently spend around **EUR 13.8 million** on visa stickers yearly (aggregated costs). However, the cost savings from abolishing the sticker for Schengen visas will be somewhat less for the following reasons.

1. The storage and filling in costs mentioned above relate to assets used by the Schengen countries to issue national *as well as* Schengen visas. Therefore, if national visas continue to be sticker-based, the Schengen countries will still incur in those costs (albeit to a lesser extent).
2. The transportation costs do not correspond to the exact cost of transporting stickers, because stickers are delivered along with other diplomatic material.

It follows that all Schengen countries combined will nevertheless certainly save **EUR 9.1 million per year**, i.e. EUR 0.64 multiplied by the number of visas issued, assuming that this number remains rather constant over time. In addition, they will save something under **EUR 1 million per year** on transportation, storage and filling-in if national visas continue to be based on stickers.

It is now possible to assess the return on investment for the Schengen countries, by comparing the investment with the cost savings. According to Table 23 above, if no offline fallback solution is implemented, the digital visa would require an investment of **EUR 3.5-6.4 million** (for the traveller web service) incurred by the EU budget if no online application portal is adopted.

If the Schengen countries decide to adopt an offline fallback option, the budget of each Schengen country would incur the following investment depending on the option selected. These are, of course, average costs and these will vary widely depending on the Schengen country in question:

- Option C1 would not require any specific investment;
- Option C2 would require an effort of **EUR 0.380-0.660 million**;
- Option C3 would require an effort of **EUR 0.103-0.207 million**.

Based on these estimates, the table below shows the Return on Investment (RoI) that the Schengen countries would achieve, depending on whether or not an online application option is implemented in parallel. It is expressed in months.

Table 24:Return on investment for each offline fallback solution

	Implemented together with an online application portal (months)	Implemented before and/or without an online application portal (months)
Option C1	0	4.4-8
Option C2	1.4-2	5.8-10.4
Option C3	3.8-7.5	8.1-15.5

The rationale for the results above is based on the savings per year due to the abolition of the visa sticker: the Schengen Area would save EUR 10.1 million per year, i.e. around EUR 0.8 million per month. Therefore:

- With option C1, the Schengen countries would achieve a RoI **immediately** (after 0 months) with an online application option; or they would achieve it after **4.4-8 months**[109] without an online application option;
- With option C2, the Schengen countries would achieve a RoI after **1.4-2 months**[110] with an online application option, or after **5.8-10.4 months**[111] without an online application option;
- With option C3, the Schengen countries would achieve a RoI after **3.8-7.5 months**[112] with an online application option, or **8.1-15.5 months**[113] without an online application option.

Moreover, the Schengen countries would experience benefits of a qualitative nature, such as those relating to their personnel. The assessment of these benefits was based on the analysis of data provided by five Schengen countries on the FTEs required to manage sticker-related tasks. The average number based on the data provided by those countries is 21.3 FTEs. This means that the whole Schengen Area would be able to save **between 500 and 800 FTEs**.[114] The range takes into account the fact that the raw data provided by the five Schengen countries includes outliers and therefore may not be totally representative of the situation in all the remaining Schengen countries.

Saved FTEs could be redeployed to more critical tasks, i.e. the examination of applications, thereby potentially increasing the efficiency of the visa application procedure thanks to a higher time-per-application ratio made possible by the savings above in conjunction with the benefits of the digital portal.

Finally, by abolishing the sticker, the Schengen Countries would terminate the negative environmental footprint linked to the sticker business chain, i.e. production from paper to transportation.

Third country nationals

Third country nationals would also experience both quantitative and qualitative benefits from the abolition of the sticker.

The quantitative benefits for visa applicants would come from the savings in the total costs currently incurred to have their travel documents returned at the end of the application process. As set out in detail in Annex A, these costs are the fees charged by the ESPs for the delivery of the travel documents, and can be estimated in a range of **EUR 250-280 million**, i.e. a cost per application of EUR 15.60-17.50. Only service fee costs have been taken into account – and not travel costs to reach the consulate/ESP, because the majority of applicants will typically find it cheaper to use the ESP services rather than buying a train/flight ticket.

[109] EUR 3.5 million investments / EUR 0.8 million savings per month to EUR 6.4 million investments / EUR 0.8 million savings per month
[110] EUR 1.1 million investments / EUR 0.8 million savings per month to EUR 1.9 million investments / EUR 0.8 million savings per month
[111] EUR 4.6 million investments / EUR 0.8 million savings per month to EUR 8.3 million investments / EUR 0.8 million savings per month
[112] EUR 3 million investments / EUR 0.8 million savings per month to EUR 6 million investments / EUR 0.8 million savings per month
[113] EUR 6.5 million investments / EUR 0.8 million savings per month to EUR 12.4 million investments / EUR 0.8 million savings per month
[114] The exact number would be: 21.3 FTEs by 30 Schengen countries = 617 FTEs.

The qualitative benefits from the abolition of the sticker would come from third country nationals being able to retain their travel document throughout the whole visa application procedure. This would translate into enhanced mobility for those applicants who need to travel to other countries and are in possession of no suitable travel document other than their passport.

Finally, the qualitative benefits to the Schengen countries highlighted above (time and efficiency gains) might also result in benefits for third country nationals. Applicants may receive a response to their visa application more quickly than is the case today. Thus, they may get their visa in fewer days or – in the event of refusal – be able to lodge an appeal and/or submit a new application within a shorter period.

5. Recommended option and way forward

In view of the options presented in the feasibility assessment (Chapter 3) and their associated costs and benefits (Chapter 4), the option described in this chapter will offer the most practical and cost-efficient way forward for digitalising the Schengen visa application and the visa itself.

5.1. Online application

For the online application, the following options are recommended:

- Business architecture: The 'custom digital' online application portal (option A2);
- System architecture: The hybrid system architecture (option B2).

5.1.1. The 'custom digital' online application portal (option A2)

The study identified the 'custom digital' online application portal as the preferred way forward. This portal offers a web service to travellers from around the globe who wish to apply for a Schengen visa. This study has concluded that the online application process should support the following features.

- The portal should ensure visa applications are submitted accurately ('first-time-right') by:
    - offering interactive guidance and dynamic instructions during each step of the application process;
    - supporting a public website portal accessible on mobile devices;
    - implementing algorithms and questions in line with the Schengen visa policy to ensure applicants lodge their applications with the competent Schengen country, pay the correct fee, and submit the correct documents;
    - supporting the configuration of the portal by Schengen countries in line with specific national circumstances or requirements, e.g. locations of consulates and ESPs, supporting documents required;
    - facilitating automated form field verifications to assess whether the data inserted complies with data formats;
    - reviewing and amending fields prior to submission to ensure the applicant rechecks the data provided;
    - allowing a user to scan the Machine Readable Zone (MRZ) of his/her travel document to automatically fill out the travel document form fields;
    - temporarily storing "draft" applications so the applicant can resume the application process at a later stage;
    - maintaining a Frequently Asked Questions (FAQ) web page that lists general guidelines on how to resolve the most commonly encountered issues.
    - The submission of travel document information by uploading a scan of the travel document's biographic page.
    - The submission of supporting documents by uploading a scan of supporting documents or by uploading supporting documents in their native format, e.g..pdf,.docx,.xslx,.jpg.
- The declaration by the applicant that the data provided is accurate and complete through a checkable tick box.
- The payment of the visa fee through a third-party central payment gateway that immediately transfers the visa fee to the appropriate Schengen country.
- Access rights management that gives specific profiles access to the features the person requires.
- Interaction with an applicant by:
    - sending custom and static notifications relating to the major milestones in an applicant's application process;
    - the ability of an applicant to check the status of their visa application, the status of their visa and the status of their biometric identifiers; and
    - a centralised appointment scheduling repository that redirects the applicant to the locally organised appointment scheduling tool or contact information of the appropriate consulate or ESP.

Note that because the solution does not offer a digital alternative for the collection of biometric identifiers, the collection of biometric identifiers will remain as it is. Additionally, where required, applicants still need to physically submit their travel document and/or supporting documents.

The 'custom digital' online application portal is recommended because of the following key considerations:

- Due to the need to identify applicants, Schengen country representatives took the view that the physical submission of the travel document should continue to be required for first-time applicants and applicants who have received a new travel document since their latest application.
- Applicants with a lack of technological knowledge or with a lack of access to the required technology should still be able to submit supporting documents in paper format.
- Due to the risks of identity fraud, the remote enrolment of biometric identifiers was not deemed feasible by Schengen country representatives.
- From a legal point of view, explicit action by the applicant remains necessary to declare that the filled-out data are correct. Therefore, a tick box must be included in the online application process.
- Schengen country representatives expressed a desire for direct payment of the visa fee to the Schengen countries as opposed to being collected by an intermediary and then distributed at a later stage.

5.1.2. The hybrid system architecture (option B2)

In order to support the online application process, a supporting system architecture must be designed. For this purpose, the study identified a hybrid system architecture as the preferred way forward. The hybrid system architecture, visualised in the figure below, is constructed around two key characteristics:

- a centralised online application portal through which applicants all over the world can apply for a Schengen visa;
- the principle that application files are stored electronically at the national level, i.e. each Schengen country manages national systems that electronically store the applications for which they are responsible.

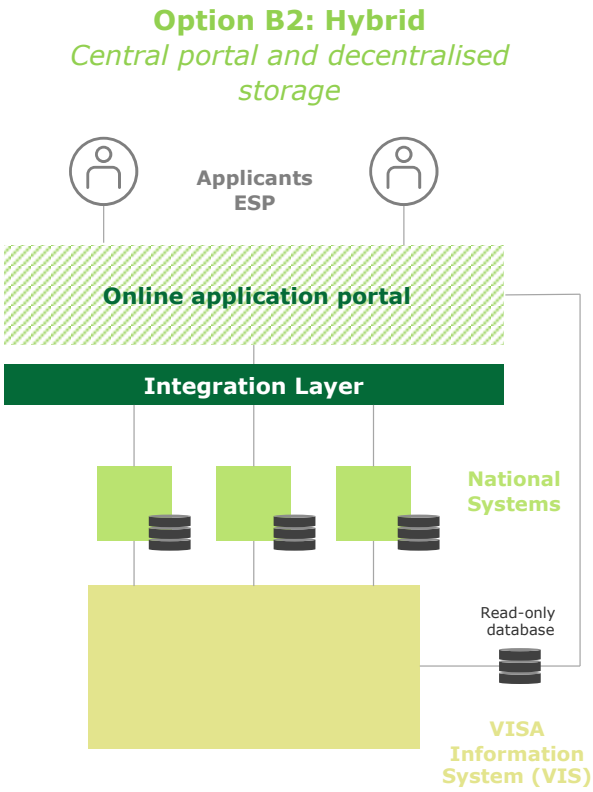

Figure 13: The hybrid system architecture

This hybrid system architecture (option B2) has been selected as the preferred option because:

- Schengen countries only need to access data stored in their national systems. This simplifies the access rights management process across the architecture;
- there is a clearer sense of data ownership and responsibilities, simplifying the governance needs;
- Schengen countries can more easily ensure compliance with specific national rules as they retain full control of their own information systems;
- the approach is less disruptive to the current way of working;
- the option mitigates a long-term risk in which centrally stored data could be used for purposes other than it was initially intended for;
- the consulates are only dependent on the availability of the national systems, i.e. in the other option, if the central storage capacity (AMS) were unavailable due to, for example, an outage, visa officers worldwide would be prevented from executing the examination procedures;
- there will be a lower loss of current investments as national systems could be reused/repurposed or expanded to facilitate the online application process;
- the architecture allows for a clear progressive rollout approach (Schengen countries can opt into the online application portal at the time of their choosing).[115]
- it is easier to guarantee the performance requirements. The hybrid system architecture requires significantly less investment and effort for eu-LISA in both storage and the network;

However, to develop this system architecture successfully, there are many challenges and considerations need to be taken into account:

- the proposed solution requires Schengen countries to invest in national systems that support the online application process and the associated infrastructure, i.e. a considerable investment in the network to share the documents around the world;
- the architecture requires an effort to agree on common specifications for the integration layer and agreements between all Schengen countries;
- as the cost-benefit analysis has pointed out, this hybrid system architecture will involve investment[116] by both the Commission and the Schengen countries at the level of the central systems and the national systems over an eight-year period. Note that the hybrid system architecture was the more expensive solution identified by the study. However, the study has determined that the considerations mentioned above outweigh the extra cost.

5.1.3. Legal and financial considerations

From a legal standpoint, the feasibility assessment of the online application process concluded that there are no major data protection implications as no additional data would be collected and no other actors would manage or process data than is currently the case. A data protection impact assessment would have to be carried out for the digital portal demonstrating the validity of this statement and explaining the data protection measures.

However, transitioning to a more digitally focused application process, e.g. electronic supporting documents instead of physical alternatives, will require specific amendments to some regulations. The required amendments mostly involve allowing the kind of digital transformation described in this report.

Finally, from a cost-benefit perspective, the online application process would require the Schengen countries to make considerable investments. However, as concluded by the cost-benefit analysis, these investments would lead to significant savings in the future.[117]

[115] The centralised system architecture also offers the possibility of gradual opt-in by Schengen countries. However, from an infrastructure point of view, the hybrid system architecture offers an easier gradual transformation. In the centralised system architecture, upon opt-in of a new Schengen country, the AMS, the portal and the link from the AMS to the national systems would have to be scaled up. In the case of the hybrid system architecture, only the portal needs to be scaled up. An option would be to scale the AMS and its link to the national systems to the maximum required capacity from the start. However, this would require large investment in infrastructure that will possibly not be used for multiple years.

[116] Over the eight-year delivery + operational period, the central systems and national systems would incur a cost of EUR 75.2-139.6 million.

[117] The central and national systems would save, over an eight-year period, EUR 75-140 million.

5.2. Digital visa

The digital visa is the option that this study recommends for the issuance of the visa to a third country national. Akin to the objectives driving the option selected for the online visa application portal, the digital visa will help reduce the burdens caused by the current visa sticker and improve the management of the Schengen Area's external borders as well as the security of the Schengen Area.

5.2.1. The main option: the digital visa

The digital visa reflects to a large extent the concept endorsed by the Visa Working Party under the Estonian Council Presidency. The future digital visa will rely on the following elements:

- the abolition of the current visa sticker,
- the record file of the third country national stored in VIS.

The second point makes it clear that the Schengen Area will not need to start from scratch in implementing the digital visa option. Its backbone is the existing EU information system for visa policy, i.e. VIS. Thanks to the VIS architecture, there will be no need for a new system, and consulates will issue visas by simply updating the holder's VIS file. If the online application is also implemented at the same time as the digital visa, consulates will send a notification to the visa holder through the holder's online application account; otherwise, they will do so through a web traveller service connecting authorities and third-country nationals.

From a technical, security and operational standpoint, the other existing and upcoming EU information systems for border management will help in achieving extensive synergies with the digital visa. By relying on the same data and information covered by the revised VIS Regulation, the digital visa will fit perfectly into the future EU interoperability framework for border management.:

1. It will not entail more operational adjustments at border crossing points than those already mandated by the EES, i.e. scanners for reading the traveller's fingerprints and biometric facial image.
2. The EES will require border control authorities to carry out biometric checks on incoming travellers through VIS in order to update the EES file. This, combined with the abolition of the sticker, will prevent border control authorities from clearing travellers based solely on the visa sticker, thereby increasing the reliability of border checks and improving the security of the Schengen Area.

5.2.2. The offline fallback solution: (option C3)

It is recommended that the digital visa be backed up by a notification email including a digitally signed 2D barcode as an 'offline fallback solution' (option C3) to ensure a minimum level of security in case VIS cannot be reached. As concluded by the feasibility assessment, it is the most advisable option from a security standpoint, and is the most advisable in terms of legal, technical, data security and implementation compared to the other two options considered.

This barcode will be signed by the Country Signing Certificate Authority (CSCA) of the issuing Schengen country with a unique cryptographic key by leveraging on the Public Key Infrastructure (PKI) currently used to sign other types of documents digitally. The consulate will then send the visa holder a notification email with the 2D barcode. Either this will be sent through the web service part of online application portal, or through a stand-alone web service, if no online application portal is implemented. The barcode will serve a range of purposes.

1. It will provide third country nationals with a proof that they hold a valid visa – but it will be more user-friendly than the sticker, as they will be free either to print the barcode with the visa issuance notification or simply to show the barcode on an electronic device. They will no longer need to leave their travel document at the consulate throughout the whole application process and pick it up or have it returned by courier at the end.
2. It will enable border control authorities to verify visas at Schengen border crossing points even in the unlikely event of the EU systems not being accessible due to technical difficulties (either VIS unavailability or problems with a local area network). Offline checks will be even more secure than today as the digitally signed barcode is less prone to counterfeiting than the sticker.

3. It will provide a reliable means of verification for a) police authorities carrying out immigration checks on third country nationals within the Schengen Area; and b) third country authorities benefiting from bilateral agreements with the Schengen countries checking the traveller's entry conditions before departure.

The 2D barcode will be readable through mobile devices running a publicly available mobile application. Border crossing points and Schengen police authorities will need to be equipped with appropriate smartphones for scanning and reading barcodes.

5.2.3. Legal and financial considerations

The introduction of the digital visa option will have no major data protection implications, as no additional data would be collected, and no other actors would manage or process data. The abolition of the sticker and the introduction of the 2D barcode will require new EU legislation amending existing regulations. The discussions on the 2D barcode within the Article 6 Committee[118] may lead to easier implementation should the European Commission launch a policy initiative in this area.

Finally, from a cost-benefit perspective, the digital visa will enable the Schengen countries and third country nationals to save most of the costs currently incurred when dealing with the visa sticker. Moreover, synergies with EU information systems will allow the Schengen Area to adopt the digital visa at very little cost. The only investments needed will be for:

- creating and maintaining the web service for travellers should no online application option be selected (budget costs for the EU);
- extending the PKI for digitally signing visa 2D barcodes and installing software for encoding barcodes (budget costs for each Schengen country);
- equipping the authorities with devices and mobile applications for reading barcodes (budget costs for each Schengen country).

The last two items will not be necessary if the 2D barcode being discussed by the Article 6 Committee is eventually implemented.

5.3. Way forward

This section presents the way forward and steps to implement the online application portal and the digital visa solution. In particular, it presents a high-level roadmap and suggests the implementation of a pilot project for the application portal.

5.3.1. High-level roadmap

This subsection presents displays a high-level roadmap for the implementation, including possible timings, of the online application portal and the digital visa. The timeline presented in the figure below is highly indicative and subject to change.

The roadmap is based on the following assumptions.

- A pilot project (relating to the online application portal) could be conducted prior to the preparation of the legislation in order to test the solution beforehand and feed any possible changes to the legal stream. The proposed pilot (and its associated phases) are described in more detail in the next section).
- The legal phase is in two stages: a legislative stage (the preparation and adoption of regulations) and a specifications stage (the preparation and adoption of the secondary legislation, i.e. the delegated and implementing acts).
- An incremental rollout of the online application process and a full deployment of the digital visa will occur only once the contractor develops the solution.

[118] The Article 6 Committee is considering to enhance the visa sticker with a digitally signed barcode

Figure 14 displays the indicative high-level roadmap. A key point to understand is that the roadmap for the online visa application does not depend on the roadmap for the digital visa, or vice-versa. Each solution could be piloted and implemented in an independent manner. In the event of the digital visa being implemented before and/or without an online application portal, then a traveller's web service would be required in order to provide the features of the notification tool and of the visa verification tool.

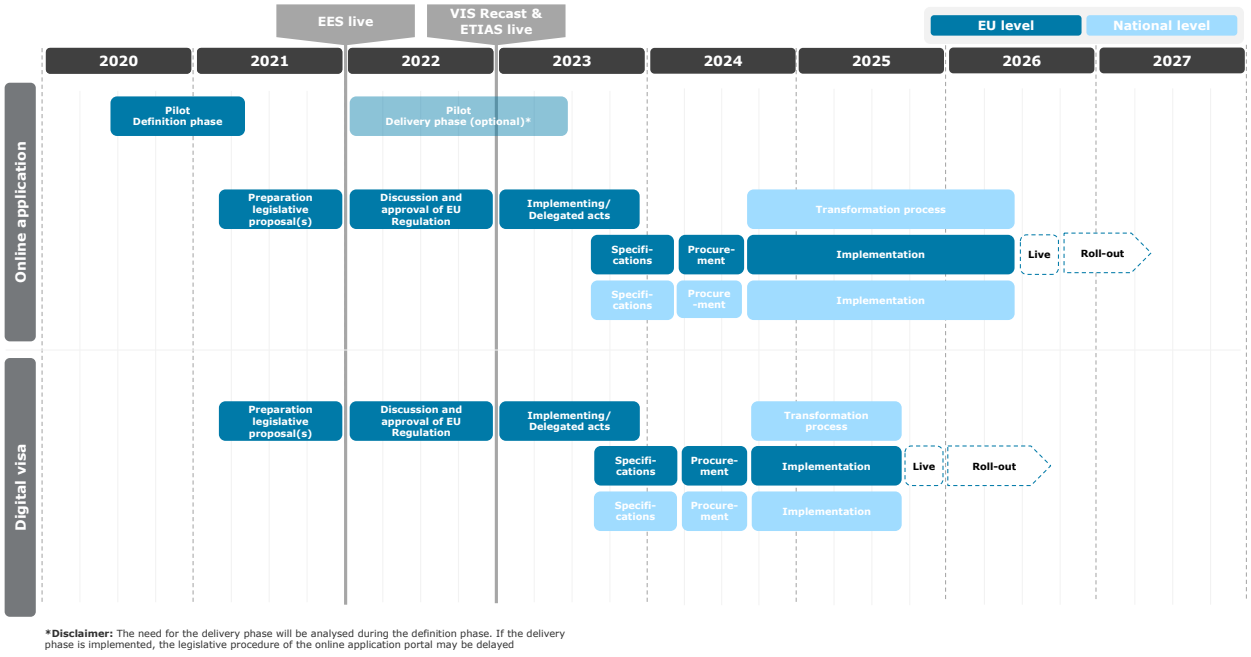

Figure 14: High-level roadmap

As illustrated in the figure above, new legislation would need to be enacted. First, similar to the ETIAS Regulation, a regulation for the online application portal would establish its purpose and scope, as well as the technical requirements (which will be further defined through delegated and implementing acts). This new regulation would amend the Visa Code and the VIS Regulation. Some new provisions would need to be included or modified in the former in order to reflect the changes brought about by the portal. These would mainly concern the lodging of the form (i.e. applicants who have been issued with a visa whose biometrics or passport have not expired would not be required to attend the consulate or VAC in person), the travel document and supporting documents, and the payment of the visa fee.

Second, a new regulation would also be necessary in order to introduce the digital visa and its fallback solution, i.e. a secure barcode. Such a regulation would outline the purpose of the digital visa, defining it and detailing how it should be used. It would amend the Schengen Visa Code, the Schengen Borders Code, the VIS Regulation, the EES Regulation, and possibly other instruments. The amendments would ensure that all references to the visa sticker are removed and replaced by mentions of the digital visa and its fallback solution.

In addition to these two regulations, secondary legislation will be necessary to set out in detail the technical requirements needed. In parallel to this legal phase, as described in more detail below, a pilot project could be conducted on a small scale, e.g. in certain countries. Subsequent to this, the technical specifications would be drafted and published, opening the procurement phase. Once a contract had been awarded, the implementation of the project would start. The contractor would develop the solution based on the technical specifications. When the solution had been sufficiently tested and accepted in a later stage by all stakeholders, it would be rolled out to the remaining Schengen countries.

The figure above shows that the implementation involves the EU and the national level in both streams (online application and digital visa). This is because, for the online application, the Member States would need to adjust their national infrastructure in parallel as the implementation of a common EU portal is being carried out. For the digital visa, the Member States would need to complete the transition from the sticker to the fully digital visa in the central offices and consulates. In parallel, also eu-LISA would also have a major role in implementing and

managing the new landscape, defining the specification for the offline fallback solution and for the web traveller service (if needed: i.e., without an online application solution).

For both the online application and the digital visa, a transformation process phase is included in order to ensure that the ministries and consulates are ready to accommodate the changes brought by the online application process and digital visa. These are the adjustment of their national systems and working processes.

5.3.2. Piloting an online application portal

A pilot project is a small-scale implementation of a full-scale project to evaluate the feasibility, time and cost and to identify any risks and/or issues that were not detected prior to the final release of the portal. The purpose is to have a gradual approach towards a successful outcome with an efficient allocation of effort and money.

This study envisages a pilot project with two major phases:

1. definition
2. delivery.

Please note that phase 2 provides a real-world implementation of the online application process and thus handles real data and integrates with the VIS. Because of this, it could be that this phase of the pilot project must be supported by a legal basis. During the first phase, it should be examined and decided whether the second phase is feasible and necessary. Therefore, this study positions the delivery phase as being optional.

This section briefly covers the key aspects of the proposed pilot project. For a more thorough description of the pilot project, please refer to Annex C.

The definition phase

The goals of the definition phase are to:

- identify and research the pain points for consulates and applicants and their needs;
- identify technological solutions for the identified pain points and needs;
- build a prototype realisation of the online application portal;
- validate a proof of concept;
- prepare the governance and coordination landscape required to deliver the online application portal and the optional delivery phase.

In order to achieve these objectives, this study proposes to bring together a set of Schengen country, European Commission and eu-LISA representatives and together follow design thinking principles to iteratively build a working prototype under the guidance of an independent coordination partner to facilitate the process. Once the prototype has been realised, an initial governance and coordination landscape should be laid down. Regular meetings with the stakeholders involved should be part of the process.

The delivery phase

Upon successful validation of the proof of concept created during the definition phase, the delivery phase aims to roll out an operational portal in multiple releases.

The goals of the delivery phase are to test the more technical aspects relating to the online application portal. In particular, the delivery phase aims to:

- test the digital user journey and its associated features;
- refine the coordination and governance landscape described previously in the definition phase;
- detect integration problems for countries of varying levels of technological maturity;
- detect loopholes and security vulnerabilities;
- better understand storage and network requirements;
- fine-tune cost estimates and budgets.

To achieve these objectives, the study proposes to roll out the delivery phase in at least six Minimum Viable Products (MVPs). These MVPs would gradually offer more features to the online application portal, consequentially allowing the testing of different objectives over time.

The MVPs proposed in this study start off with a simple minimum release to selected applications. At this stage, the portal would only support the minimum required features to submit a basic online application. By the last, sixth, MVP, this minimal pilot project will have been expanded to include all core features of the online application portal to allow the thorough testing of all aspects. For a more detailed description of each MVP, please refer to Annex C.

Note that for security purposes the scope of this delivery phase should be limited to a selected few third-countries and Schengen countries. Furthermore, the pilot project should also limit the material scope of applicants, e.g. only low-risk profiles can participate. For more details on this scoping, please refer to Annex C.

Timeline

The previous section gave a timeline situating the pilot project in the legislative and development context of the online application portal and the digital visa. The figure below zooms in on the pilot project timeline itself and maps the phases described above to this timeline.

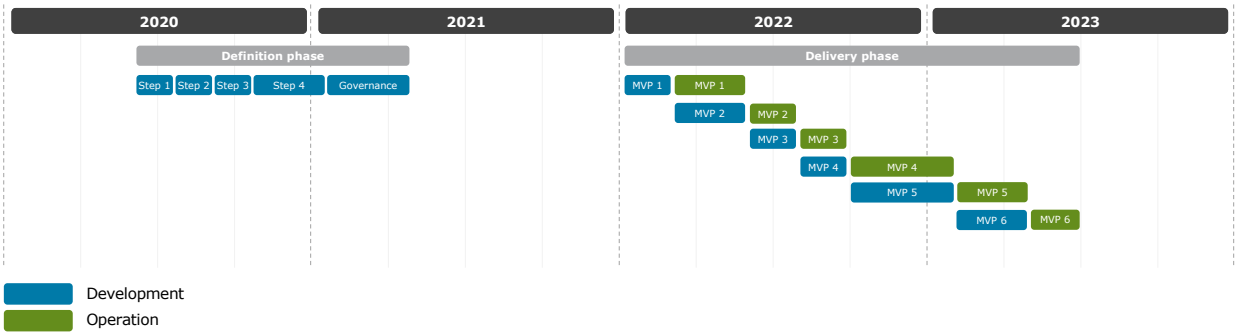

Figure 15: Proposed timeline for the pilot project phases

Cost

In conclusion, the table below presents an estimation of the costs associated with both phases based on the cost-benefit analysis conducted in the previous chapter. These estimates take into account the costs incurred at a central level and the estimated costs that would be incurred by each participating Schengen country. The costs presented are average costs and could vary based on the technological maturity of the participating Schengen country. For more information on how these numbers were arrived at, please refer to Annex C.

Table 25: Costs associated with the pilot project

	Central costs (million EUR)	National costs (per participating Schengen country) (million EUR)
Costs for the definition phase	1-1.9	0.028-0.052
Costs for the delivery phase	4.2-7.8	0.95-1.8
Total	5.2-9.7	1-1.8

6. Conclusions

The assessment of the level of digitalisation across the Schengen countries shows varying degrees of maturity across the countries. While a few Schengen countries are already aiming for full digitalisation of their visa processes, others still rely on paper-based visa processing. In the case of the latter, stakeholders are carrying a significant burden that digital options applied to the different steps of the visa processing could relieve.

6.1. Options available for the digitalisation of visa processing

This report has identified a broad spectrum of options, from the more conservative, i.e. closer to the current situation, to the more far-reaching. However, the feasibility assessment has proved that not all are practicable.

Based on the analysis in this report, the two solutions identified for the business architecture are the 'fully digital (option A1), and the 'custom digital' (option A2). While the former aggregates the most digital and far-reaching options, the latter encompasses a mix of digital option and the status quo.

Taking into account the findings of the feasibility assessment, this report recommends the business architecture solution for the online application process, which consists of a mix of options and the status quo, i.e. option A2. This option introduces new technical solution, such as the filling in of the visa application online, while retaining some steps of the current situation, for security purposes. These steps mainly refer to the verification of the travel document, the submission of the supporting documents, and the enrolment of the biometrics.

As for the architecture lying behind this business architecture, this report identifies two options. On the one hand, a centralised architecture (option B1), consisting of a central application portal and a centralised application file database, and on the other hand, a hybrid architecture (option B2) also composed of a central application portal but storing the application files at national level.

This report suggests that this solution across the Schengen countries relies on the hybrid system architecture (option B2). The preferred/recommended solution leverages the reuse of existing and upcoming systems to the full extent possible, while respecting the current limitations of technology and the current investments made by Schengen countries in their own national systems.

The analysis carried out in this report also shows that the current paper visa sticker entails costs and administrative burdens for all stakeholders (both before and after the issuance of a visa), and does not have any security features such to make it indispensable for visa policy.

Therefore, the study suggests abolition of the sticker in the Schengen Area and adoption of a digital visa. The digital visa would rely on the existing and upcoming EU system architecture for border management, without the need to spend resources and time on the development of a brand new system. It would consist of the visa holder's record file stored in VIS (taking into account the reforms brought in by the new VIS Regulation), to be verified biometrically by the Schengen authorities through access to the entire IT framework for border management, e.g. through an EES check at the border.

In some circumstances, it will not be possible to verify the digital visa, e.g. during VIS downtime or lack of network connectivity. Therefore, for security reasons, a fallback solution is needed. This report presents three options: visa issuance notification (option C1), visa issuance notification with non-signed 2D barcode (option C2), and visa issuance notification with digitally signed 2D barcode (option C3).

The abolition of the sticker, and the introduction of the digital visa with a fallback solution (a 2D barcode), would require specific amendments to the current legislation, with a new EU regulation amending the relevant EU legislation accordingly. It would also require a solution for Schengen authorities performing inland checks and for third country authorities bound by bilateral cooperation agreements with the Schengen countries. The solution would be a barcode signed digitally by the central authority of the issuing Schengen country and sent to the visa

holder. This barcode would guarantee higher security and reliability than the sticker. It would also enable offline checks on visas in the unlikely event of VIS being inaccessible.

6.2. Cost-benefit analysis

The analysis of the costs and benefits of the different options for both the application process and the digital visa has enabled a quantitative comparison between them, leading to the preferred/recommended option.

For the application process, the analysis has found that setting up a Schengen visa application portal is actually less expensive than the current baseline scenario in the long run. The current baseline involves each Schengen country operating and maintaining its own national portal, or developing one. A total investment (across all Schengen countries) of between EUR 156 million and EUR 292 million would be needed if all Schengen countries were to transition to operating their own national application portal.

As mentioned above, the study identified two possibilities, a centralised (option B1) and a hybrid (option B2) system architecture. The preferred option B2 comes at a total cost of EUR 75-140 million over an eight-year period. Of this, EUR 13.4-25 million would be for central systems while each Schengen country's national systems would incur a cost of EUR 2.2-4 million, both over the same period.

The option B1 would come at a total cost of EUR 49-91 million over an eight-year period. Of this, EUR 24.6-45.8 million would be for central systems while each Schengen country's national systems would incur a cost of EUR 0.84-1.6 million, both over the same period.

In terms of benefits, this report found that both system architectures enable the same benefits: the online application portal would save a total of EUR 880 million in travel cost for TCNs and overall save 708 Full-Time Equivalents (FTEs) *per year* for Schengen countries, and increase the number of applications slightly.

From a purely cost-benefit perspective, the centralised architecture would be the recommended way forward. However, this report identified this option to be less feasible in the legal, technical, security, data protection, operational and implementation domains.

The implementation costs for the digital visa mainly depend on options of the fallback solution selected. The cost-benefit analysis concluded that the option C1 is the less expensive solution. It is also the least technologically advanced. The option C3 is estimated to be the most expensive: EUR 100,000-200,000 per Schengen country for a total of EUR 3-6 million. However, it is also the most secure.

Moreover, the digital visa could bring significant benefits for the Schengen countries: up to EUR 10 million could be saved yearly in production, transportation and storage of the visa stickers, as well as some 554 FTEs. It would also reduce their environmental footprint. The digital visa would also remove some of the costs for third country nationals, such as the travel document transportation fee: between EUR 15.60 and EUR 17.50 per applicant.

Based on this assessment, this report suggests implementing the digital visa with an offline fallback solution for security reasons. Of the three fallback options, this report recommends considering the option C3 as it is the most complete and will contribute more to the security of the Schengen Area.

6.3. Way forward and roadmap

For the way forward, this report suggests launching a two-phase pilot project to test the visa application portal. The phases would be a definition phase (EUR 1-1.9 million in central costs; EUR 28,000-55,000 per participating Schengen country) and a delivery phase (EUR 4.2-7.8 million in central costs; EUR 0.95-1.8 million per participating Schengen country). In parallel with the pilot, adoption of the relevant legal framework should accommodate the changes that the online application portal and the digital visa will bring to the new visa process.

Annex A. Cost-benefit analysis

This Annex elaborates on the Cost-benefit analysis presented in Chapter 4 of this report.

1.1. Online application

This section covers the cost-benefit analysis relating to the online application process. The following sections analyse the costs associated with, and the benefits obtained by, rolling out a Schengen online application portal. The analysis will be conducted for both system architecture options.

The results presented in this section are based on multiple questionnaires and interviews with stakeholders and Schengen countries. Furthermore, studies conducted previously and public reports on Schengen (visa) operations were taken into account over the course of the cost-benefit analysis. Finally, as the online application process contains many similarities to the ETIAS application process, these similarities were leveraged in order to refine the estimations.

1.1.1. General Approach

This section elaborates on the general approach followed for the online application cost-benefit analysis, henceforth called the CBA.

The CBA considers three categories of costs.

- **The current costs** associated with current national portals (and their future evolution);
- **The baseline costs** where no Schengen online application portal is set up; and
- **The solution costs** where a Schengen-wide online application portal is set up to be shared with all Schengen countries. This analysis considers both system architecture options:
    - the centralised system architecture (option B1);
    - the hybrid system architecture (option B2).

Each of these categories of costs are estimated in three time periods:

1) **the current situation**: this reflects the as-is context;
2) **the delivery stage**: this indicates the time during which the scenarios evolve to their target stage;
3) **the target stage**: this predicts the future *stable* situation where the scenarios have been fully implemented.

This CBA analyses, visualises and compares the costs associated with each category, for each time period (where applicable, e.g. the current situation period can only include the current costs). The following sections briefly explain each cost category.

Because of the level of detail available in this study, a 30% uncertainty interval is applied to the estimations. Therefore, all estimated costs are presented in ranges, e.g. if a cost of EUR 1.5 million was estimated, a range of EUR 1-2 million will be presented.[119]

The current costs

The current costs category analyses the costs currently incurred by the Schengen countries to operate and maintain their national portals. These portals can, depending on the Schengen country, be used for both Schengen visas and national visas.

[119] Arithmetically, this is EUR 1.05-19.5 million, but, such values have been rounded appropriately.

This category fully represents the costs of the 'current situation'. Furthermore, the current operation and maintenance costs extend into the 'delivery stage', as the Schengen countries will need to continue operating and maintaining their existing portals until a replacement solution is in place. Finally, in the 'target stage', the current costs must still be considered after the delivery of a replacement solution, as certain countries might opt to keep their old systems operational to handle national visas. Therefore, the operational cost of the current situation does not completely disappear.[120]

The implication is therefore that the future incurred costs, both during the delivery stage and the target stage, will be stacked on top of the current costs (as visualised in Figure 16).

The baseline costs

To present the costs and benefits associated with the adoption of either system architecture option, the solution scenarios are compared to the baseline scenario, in which no Schengen-wide online application portal is set up. Therefore, it is important to define a baseline scenario, which will allow an accurate analysis and comparison of the costs incurred.

At first glance, the baseline scenario would be to analyse the costs associated with the current as-is situation, i.e. certain Schengen countries operate a national online application portal, while others do not. Furthermore, the features offered by each national portal vary per country as well. Thus, these countries' total investments, and their current recurring costs, could be compared to an estimation of the investment needs and future operating costs of the two system architectures.

This approach would, however, contain a major flaw: the comparison of the system architectures, which will be developed in the future, should not be compared to something that is currently undergoing major changes (indeed, Schengen countries are investing considerably in their national online application portals). Therefore, the approach of the CBA should not be to make a comparison with the costs incurred by the Schengen-wide online application portal, but to compare these costs to a hypothetical but likely scenario in which all Schengen countries continue investing in their own, separate national online application portals.

To summarise, this CBA will compare the costs incurred by both proposed system architecture options with the costs that it is predicted **would arise in the future** if a centralised online application portal for the Schengen countries were not built. Indeed, it is easy to see that in such a scenario, the current trend of investing in separate national application portals will continue as it is now.

The solution costs

The solution costs are the estimations of the costs that will be incurred by both system architecture options, both from a delivery, i.e. procurement, design, development, testing and deployment, and an operations and maintenance standpoint.

Summary

Figure 16 visualises the aforementioned approach *conceptually*. Please note that the lines are drawn purely arbitrarily. The ratio of increases and decreases, as well as the relationship between the 'before and after' are visualised conceptually and do not aim to reflect the actual results. The image purely aims to visualise the different aspects of the CBA. An accurate representation of the results is shown in a summary section later in the analysis.

Note that, using this approach, the difference between the baseline costs and the solution costs can be interpreted as savings, i.e. if nothing happens, the baseline (green) costs will be incurred. By adopting a Schengen online application portal solution, the yellow costs will be incurred.

[120] It has been assumed that 50% of the existing national portals will be deprecated upon the availability of either the Schengen or national online visa application portal.

This visualisation makes it easy to see that the gap between the green and yellow lines represents the actual cost savings of going forward with the online application initiative (if yellow does not happen -> green happens).

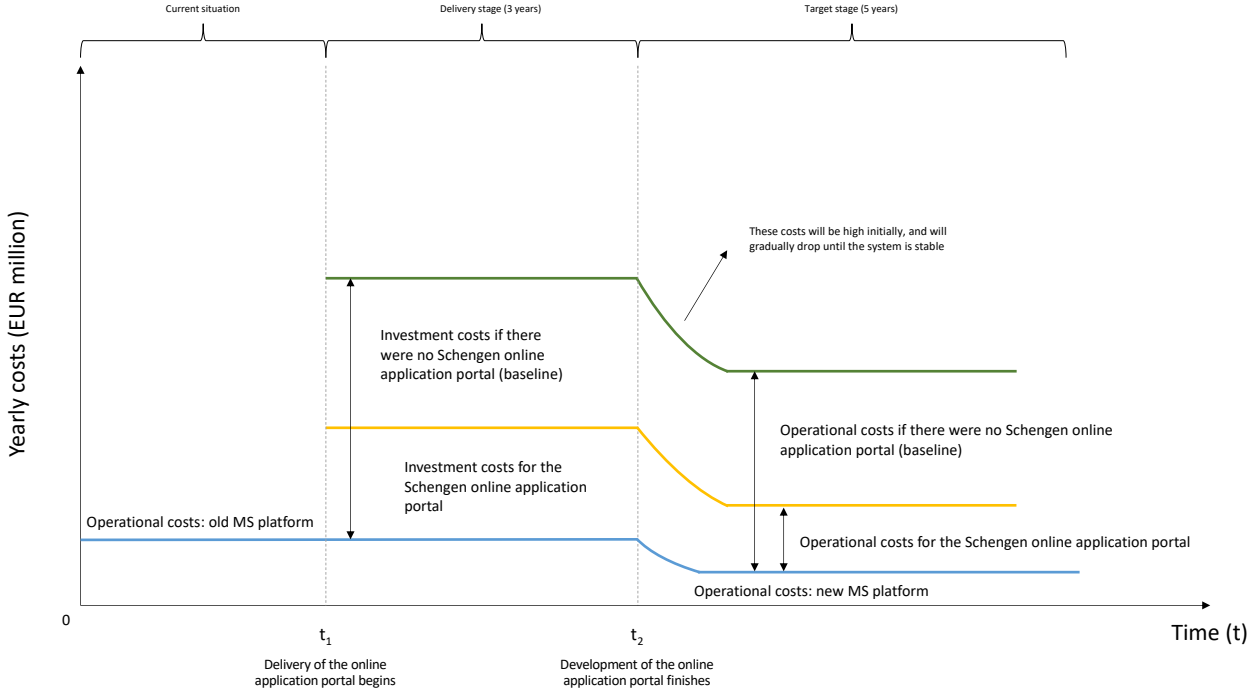

Figure 16: Conceptual representation of the online application CBA

1.1.2. Assumptions

Because of the level of detail in scope of this study, multiple assumptions had to be made to allow certain aspects of the CBA to be estimated. The purpose of this section is to list all the assumptions on which the online application CBA is based. The assumptions have received unique identifiers to allow them to be references in the rest of the Annex. The table below lists these assumptions.

Table 26: List of assumptions for the online application CBA

ID	Assumption
A_1	If there were no centralised Schengen online application portal, Schengen countries would, individually and gradually, evolve towards enhancing their own national systems to support a national online application portal (the rationale for the baseline architecture).
A_2	The costs associated with VIS (including the VIS Revision) and national systems for processing applications are not included in the costs. Only the currently recurring costs for Schengen countries' application portals, the archiving of documents and the destruction of documents are included in these current costs.
A_3	"Operations and Maintenance costs" include evolutionary maintenance, corrective maintenance and system operations costs.
A_4	Many of the data presented in this chapter are based on responses to questionnaires.[121] As with any questionnaire, outliers have been detected. These have been discarded based on a common sense approach.
A_5	The CBA considers 30 countries in the Schengen Area. While the Schengen Area only consists of 26 European Countries, Bulgaria, Croatia, Cyprus and Romania have also been included as they are currently in the process of fully implementing the Schengen acquis.
A_6	Costs for Liechtenstein are not considered as the country does not issue its own visas.[122] They have therefore been excluded from any average calculations.

[121] The questionnaires were shared with all Schengen countries and 14 responses were received. Not all questionnaires included usable information on all domains. On average, seven responses were considered for calculations. The questionnaire was built in such a way that the format of responses would be comparable.

[122] The official Visa statistics for consulates, 2018, does not mention any visa applications for Liechtenstein. Therefore, Liechtenstein is assumed not to process their own visa applications. https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy_en#stats

ID	Assumption
A_7	In the questionnaires, some Schengen countries provided detailed information on investments in their national portals when the portal in question is not yet in operation. These answers have been included in the data. However, as these portals are not yet operational, those countries have been classified as not having a portal yet.
A_8	Travel costs have been estimated at EUR 110 per application. This number was estimated by *PEARLE in a previous study[123] and has been adjusted for inflation.
A_9	In 50% of visa applications, the TCN will have to travel physically to the nearest consulate. This is the case for first-time applicants, TCNs with a renewed travel document and TCNs whose biometrics have expired (and thus need to be resubmitted every 5 years).
A_10	100% of the applications will be submitted through the online application portal.
A_11	The yearly operations and maintenance costs (for the future) are equal to 20% of the one-off investment costs of the system. This estimation holds good for a five-year period.
A_12	As some Schengen countries use their national portal for both national visas and Schengen visas, the portal would not be completely decommissioned after the launch of the online application portal. Therefore, the assumption is made that, for countries that currently have a portal, the operations and maintenance costs will remain at 50% of their current values.
A_13	Based on questionnaire responses from the Schengen countries with the greatest technological maturity, this delivers an increase in the efficiency of the visa application process. As the current national portals do not contain the full set of features proposed by the centralised application portal, it is assumed that the EU online application portal will increase the efficiency of the visa process by another 50%.
A_14	The delivery (from the start of procurement until the go-live) of the online application portal will take three years.

1.1.3. The current costs

This section covers the costs associated with the first category: the current costs (and the evolution thereof).

Current situation

The current costs reflect the current costs incurred yearly by countries in the Schengen Area. From stakeholder interviews, three different categories of non-negligible costs[124] were identified: *Operations and Maintenance*, *Archiving of documents* and *Destruction of documents* costs. Technically the visa-sticker related costs are also a yearly burden on the Schengen countries. However, as these costs do not relate to the application process, they are considered in Section 1.2, where the digital visa CBA is covered.

All current operations costs are based on replies to the CBA questionnaire shared with all Schengen Area countries (and the envisioned new-joiners). Based on the replies, the average cost per Schengen country is calculated for each aforementioned category to enable calculation of the inferred aggregate cost for the entire Schengen Area.

Operations and maintenance

The operations and maintenance costs relate to the costs associated with the operation and maintenance of the national online application portals in existence now. Based on the surveys, 20 Schengen countries currently operate a national application portal to some extent. Therefore, the average cost resulting from the questionnaire replies could not simply be multiplied by 29 (as per A_5 and A_6). This discrepancy between countries has been taken into account when calculating the aggregate cost estimation by only multiplying the observed average cost by 20 instead of 29.

Archiving of documents

The bulk of a visa application consists of the supporting documents attached. These documents need to be archived for a period of time according to the Visa Code. These documents are currently provided in a paper format and need to be stored physically in an archive. As the number of applications can reach very high numbers, these archives

[123] European Commission; Impact Assessment study supporting the review of the Union's visa policy to facilitate legitimate travelling; 2013 Impact assessment on EU visa policy.pdf

[124] Of course, employees on a payroll also give rise to a considerable yearly cost. However, as the number of these employees will remain the same between the current situation and the future operations time period, they are omitted from the analysis.

can take up considerable physical space. This has an associated cost.[125] Based on the surveys, an average yearly cost for this archiving was calculated. Unlike the operations and maintenance costs, the archiving of documents applies to all countries and can thus be multiplied by the total number of Schengen countries to reach an estimate of the aggregate cost for the Schengen Area.[126]

Destruction of documents

The destruction of documents is closely related to the archiving of documents described above. As supporting documents cannot be (physically) archived indefinitely, they need to be destroyed after the end of the retention period. In the answers to the surveys, most respondents indicated that they use a third party to destroy these documents.

Table 27 illustrates the findings on the current yearly recurring costs, i.e. a total per country of EUR 230,000 on average and an aggregate cost for the Schengen Area of EUR 5 million. These numbers are not provided in ranges, as they are calculated directly from questionnaire data.

Table 27: Summary of the current situation for the *current costs* category

	Average per country (million EUR)	Aggregate cost for the Schengen Area (million EUR)
Operations and maintenance	0.178	3.60
Archiving of documents	0.032	0.92
Destruction of documents	0.020	0.57
Total	**0.230**	**5.00**

The delivery stage

As previously explained, the aforementioned costs continue to be incurred during the entire delivery stage. Indeed, the Schengen countries need to maintain their current way of working until an alternative solution is deployed. Therefore, Table 27 also represents the costs incurred during the delivery stage.

The target stage

In the target stage, an alternative to the current national portals is available, whether it be the hypothetical evolution to the baseline, or the implementation of a Schengen-wide online application portal. In both these cases, the costs of *Archiving of documents* and the *Destruction of documents* no longer need to be incurred, since all documents are submitted through the online application portal, which stores documents electronically (see A_10).

Unlike these two costs, the operations and maintenance of the online application portals do not completely disappear: as mentioned before (see A_12), these portals could still be maintained for national visa purposes. To consider this, the costs for operations and maintenance presented in Table 27 have been halved.

Summary of the current situation costs

The costs represented by the blue line in Figure 16 are listed in Table 28. Depending on multiple factors, these costs could vary considerably per Schengen country.

[125] Note that some respondents indicated the cost is effectively 0, because it is included in the premises costs. However, other respondents indicated a price tag associated with these premises costs. Those responses have been considered when calculating the average cost.

[126] Some countries are currently starting initiatives to store supporting documents electronically. However, since the number of electronically stored applications is negligible compared to the physically archived applications, this minority is disregarded for the calculations.

Table 28: Summary of the *current costs* category

	Observed yearly cost for the Schengen Area (million EUR)
Current situation	5.0
Delivery stage	5.0
Target stage	1.8

1.1.4. The baseline costs

For this exercise, the actual cost of a fully-fledged *national* online application portal, with the same features as the Schengen online application portal, was estimated based on answers to questionnaires with the Schengen countries and expert knowledge. From there, the 29[127] Schengen countries were subdivided into three groups, based on their current national application portal's maturity level.

Knowing the cost of the fully-fledged online visa application portal, and knowing the average current investments per group, a cost can be assigned per Schengen country. This cost represents the investment needs of national application portals. Aggregating these costs leads to the final result, which represents the investments needed, across all Schengen countries, to transition to a scenario where all Schengen countries operate their own, separate national online visa application portal.

The result of the cost exercise is an estimate that setting up a national online visa application portal from scratch requires an initial investment of **EUR 3-5.7 million.**[128] Countries without an online visa application portal would therefore need to invest 100% of this figure to reach the target state. For the other groups, the assumption is made that countries with a moderately advanced online visa application portal would have to invest 66% of this sum to reach the target state. Countries with an advanced national visa application portal would need to invest 33% of this sum to reach the target state.

Table 29: Classification of Schengen countries in levels of technological maturity and their further investments needed

	No national portal	Moderately advanced national portal	Advanced national portal
Countries in category	15	10	4
% of investments needed	100%	66%	33%

After the national application portals have been set up, they also need to be maintained. Since, in the hypothetical future baseline scenario, all Schengen countries operate the 'same' fully fledged online visa application portal, the operations and maintenance costs associated with these national portals can be considered equal. In IT systems, this operations and maintenance cost is typically equal to 20% each year of the total investment for the initiative (see A_11).

The table below summarises these estimations.[129] The investment costs (row 3) clearly differ per Schengen country category. Indeed, a country that has no national portal yet will have to invest more than a country that is already operating a portal with an advanced maturity level. Furthermore, as explained above, the operations and maintenance costs are equal for all categories. Thus, even if Schengen countries might have different investment costs, in the end they will all operate their own, equally advanced, national portal.

127 Costs for Liechtenstein are not considered per A_5 and A_6.

128 This cost includes the design, development, testing, deployment and any infrastructure costs associated with the portal.

129 The delivery period has been estimated to last three years. The operations and maintenance period has been assumed to be five years as the technological costs cannot be estimated further ahead. The table presents the costs, per year over this eight-year period.

Table 30: Summary of the baseline costs category

Cost category	No national portal (million EUR)	Moderately advanced national portal (million EUR)	Advanced national portal (million EUR)	Total (all countries) (million EUR)
Yearly delivery costs	1.0-1.9	0.67-1.3	0.333-0.630	23.0-44.0
Total delivery costs (3 years)	3.0-5.7	2.0-3.9	1.0-1.9	69.0-132.0
Yearly operations and maintenance costs	0.6-1.1	0.60-1.1	0.600-1.1	17.4-31.9
Total operations and maintenance costs (5 years)	3.0-5.5	3.0-5.5	3.0-5.5	87.0-159.5
Total costs (8 year period)	**6.0-11.2**	**5.0-9.4**	**4.0-7.4**	**156.0-292.0**

1.1.5. The solution costs

This section covers the one-off investment costs (during the delivery stage) and the recurring operations and maintenance costs (during the target stage) of both system architecture options. This category does not incur any costs in the 'current operations' time period, as that period ends with the start of the development of the solutions.

Delivery stage

This section estimates the costs associated with the second time period, during which the online application portal is procured and developed. The estimates for this time period relate to the total cost of all phases of the Software Development Life Cycle (SDLC) and all infrastructure-related costs.[130] Operations and maintenance costs are not included for this time period. The next section covers both architecture options.

The investment estimate for both architecture options involves sub-dividing the architectures into their key systems and connections. For each of the systems and connections, a *relative* score is associated with both the SDLC phases and the infrastructure effort required to deliver the system or connection in question. These scores are scaled linearly, i.e. a system that receives a score of '2', requires twice as much effort as a system with an associated score of '1'. By subsequently assigning a monetary value to one of the scores, all other costs can be inferred because of the linearity of the effort scale. Annex B contains a more detailed description of the model.

For this exercise, multiple architects have analysed the architectures and, based on their expert knowledge, assigned a relative effort to all systems and connections. Afterwards, a separate group of people analysed the key systems and assigned a monetary value to one of them.[131] The total cost for both architectures was then inferred.

Table 31 illustrates the findings of the investment cost exercise. The costs have been split into central system costs and national system costs. These costs were defined to reflect the costs at a central level (at the eu-LISA premises) and at a national level (for each Schengen country).

Table 31: Summary of delivery costs of the *solution costs* category

	Option B1: Centralised system architecture (million EUR)		Option B2: Hybrid system architecture (million EUR)	
	Central system	**National system**	**Central system**	**National system**
SDLC costs	9.0-16.6	0.28-0.52	4.5-8.3	0.84-1.6
Infrastructure costs	3.4-6.2	0.14-0.26	2.2-4.2	0.22-0.42

[130] The phases of the SDLC involve creating the logic under which an application behaves. In other words, these costs are related to delivering the software of the architecture. These costs also include any costs associated with reaching an agreement between the various Schengen countries. On the other hand, the infrastructure-related costs are the costs associated with physical machines, such as servers and databases. In other words, these costs are related to delivering the hardware of the architecture.

[131] By considering the similarities to ETIAS for, for example, the digital application portal, a more accurate estimation was obtained.

The costs are higher overall for option B2. This was to be expected as the logic is distributed across the Schengen countries, each of which has to make considerable changes to their national systems. The central system costs are significantly lower for architecture option B2. This relates to the decentralised nature of option B2 (the central costs only include the costs associated with the centralised systems at eu-LISA premises).

There are two interesting metrics to derive from the results presented in Table 31:

1) the yearly costs incurred over the three-year delivery period;
2) the total delivery costs per system architecture option.

The following sections briefly cover these metrics.

Yearly incurred cost

As mentioned in the introduction to this section, a period of three years is estimated for the delivery of the online application portal. Therefore, to calculate the costs incurred yearly over these three years, the total investment costs are simply split across these three years. The table below lists those yearly costs (during the delivery stage).

Table 32: Costs incurred yearly for the Commission and Schengen countries during the delivery stage of the *solution costs* category

	Option B1: Centralised system architecture (million EUR)		Option B2: Hybrid system architecture (million EUR)	
	Central System	National system	Central system	National system
Yearly costs	4.1-7.6	0.14-0.26	2.2-4.2	0.35-0.66

The total delivery costs per system architecture option

An immediate concern of the system architecture option comparison is the immediate cost difference between them. The table below lists the total costs of both system architecture options for the delivery period. The costs displayed include the central system costs as well as the costs for the national systems combined.

Table 33: Total delivery costs for both system architectures

	Option B1: Centralised system architecture (million EUR)	Option B2: Hybrid system architecture (million EUR)
Total delivery costs (over 3 years)[132]	24.5-45.5	37.6-69.8

Target stage

This section covers the future recurring costs for both system architectures in the third time period, which occurs after the delivery of the online application portal.

These costs, the new costs associated with the operation and maintenance of the new online application portal, can be directly inferred from the results obtained previously. Typically, a large-scale IT system requires on average 20% of its initial delivery costs for the operations and maintenance phase after the deployment of the system. This is defined by assumption A_11, which states that the yearly recurring costs are 20% of the total investment costs of the Schengen online application portal.

Table 34 shows the results of the future operations and maintenance calculations. The recurring costs for the national systems in option B2 are once again higher than in option B1. This is because option B2 will require the maintenance and operation of multiple decentralised systems as opposed to one single centralised system.

[132] Calculation: 3 * (yearly central system delivery costs + 29 * yearly national system costs)

Table 34: Summary of the target stage costs of the *solution costs* category

	Option B1: Centralised system architecture (million EUR)		Option B2: Hybrid system architecture (million EUR)	
	Central system	National system	Central system	National system
Yearly operations and maintenance costs	2.5-4.6	0.085-0.160	1.3-2.5	0.210-0.400

Similar to the delivery stage, it is interesting to look at the total costs associated with the target stage period (five years).

Table 35: Total operations and maintenance costs for both system architectures

	Option B1: Centralised system architecture (million EUR)	Option B2: Hybrid system architecture (million EUR)
Total operations and maintenance costs cost (over 5 years)[133]	24.5-45.5	37.6-69.8

The attentive reader might notice that the values displayed in the table above are the same as those for the delivery stage presented in Table 33. This was to be expected, as the operations and maintenance costs are 20% of the total investment costs incurred every year for five years. The difference is that these costs are spread over a five-year period, while the delivery stage costs are spread over a three-year period.

Summary of the solution costs

To summarise the solution costs category, Table 36 presents the costs for each time period, similar to the current costs and baseline costs category summary. These figures represent the yellow line of Figure 16.

Table 36: Summary of the *solutions costs* category

	Centralised system architecture (option B1) (million EUR)		Hybrid system architecture (option B2) (million EUR)	
	Central System	National System	Central System	National System
Yearly delivery costs	4.1-7.6	0.14-0.26	2.2-4.2	0.35-0.66
Total delivery costs (3 years)	12.3-22.9	0.42-0.78	6.7-12.5	1.1-2.0
Yearly operations and maintenance costs	2.5-4.6	0.085-0.160	1.3-2.5	0.21-0.40
Total operations costs (5 years)	12.3-22.9	0.42-0.78	6.7-12.5	1.1-2.0
Total costs (8 years)	**24.6-45.8**[134]	**0.84-1.6**[135]	**13.4-25.0**[136]	**2.2--4.0**[137]
Total option cost (8 years)	**49-91**[138]		**75.1-139.6**[139]	

[133] Calculation: 5* (yearly central system operations and maintenance cost + 29 * yearly national system operations and maintenance cost)
[134] EUR 3.1 million – EUR 5.7 million average annual costs
[135] EUR 105K – EUR 200K average annual costs
[136] EUR 1.7 million – EUR 3.1 million average annual costs
[137] EUR 275K – EUR 500K average annual costs
[138] EUR 6.1 million – EUR 11.4 million average annual costs
[139] EUR 9.4 million – EUR 17.5 million average annual costs

1.1.6. Scenario comparison

By defining the likely baseline scenario, it becomes possible to compare the cost savings obtained by adopting the Schengen online application portal.

The delivery period of the Schengen online application portal, during which the accompanying systems are procured, designed, developed, tested and deployed is estimated to last three years. Therefore, the costs presented in Table 33 can be spread across three years. Furthermore, operations and maintenance costs are typically estimated for a five-year period. Estimating these costs further ahead would lead to more and more inaccurate predictions. Because of this, a five-year time frame is used as a basis for the comparison. Therefore, 20% of the total investment costs are incurred on operations and maintenance costs every year for five years.

It is not feasible to estimate the delivery period of the national online application portals, as all countries are free to start and end the development of their national systems at their discretion. However, to make a comparison possible, the costs presented in the table above are spread across the same delivery period as the Schengen online application portal. Finally, the operations and maintenance costs are also estimated for a five-year period after the delivery of the national portals.

The table below summarises the different costs associated with the three to-be-considered scenarios (baseline, option B1 and option B2) presented earlier in the tables above. The costs are presented as an aggregated result of the values presented in Table 30 and Table 36 (central system costs + 29 times the national systems costs.

Table 37: Total costs per year for each to-be considered scenario

Year	Baseline scenario (million EUR)	Option B1: Centralised system architecture (million EUR)	Option B2: Hybrid system architecture (million EUR)
Yearly delivery costs	23.0-44.0	8.2-15.2	12.5-23.3
Total delivery costs (3 years)	69.0-132.0	24.5-45.5	37.6-69.8
Yearly operations and maintenance costs	17.4-31.9	4.9-9.1	7.5-14.0
Total operations and maintenance costs (5 years)	87.0-159.5	24.5-45.5	37.6-69.8
Total costs (8 year period)	**156.0-292.0**	**49.0-91.0**	**75.2-139.6**

The figure below visually illustrates the yearly costs associated with the scenarios on a graph. Note that the ranges are presented as a coloured box indicated with an 'uncertainty interval' indicator.[140] The costs are stacked on top of the blue (the lowest) line in order to illustrate the operations and maintenance costs that Schengen countries are currently incurring.[141] The drop after the delivery stage comes because the online application portal will eliminate some costs that Schengen countries are currently incurring, i.e. the archiving and subsequent destruction of supporting documents. Not all costs disappear, as the Schengen countries could opt to continue to use their current portals for their national visa issuing process.[142]

The figure below illustrates both scenarios by plotting the yearly costs (aggregated across the central and national systems) in function of the time. The values on which this figure is based can be found in Table 37.

[140] As mentioned at the start of the chapter, the CBA estimates a value, after which a 30% range is applied around the value because of the level of detail currently available in the study.

[141] These costs were calculated based on questionnaires asking for Schengen countries' costs related to the operation of the national portals, the archiving of physical documents and their destruction. Responses were received from nine Schengen countries. The values on which this line is based can be found in Table 28.

[142] It has been assumed that 50% of the existing national portals will be deprecated upon the availability of either the Schengen or national online visa application portal.

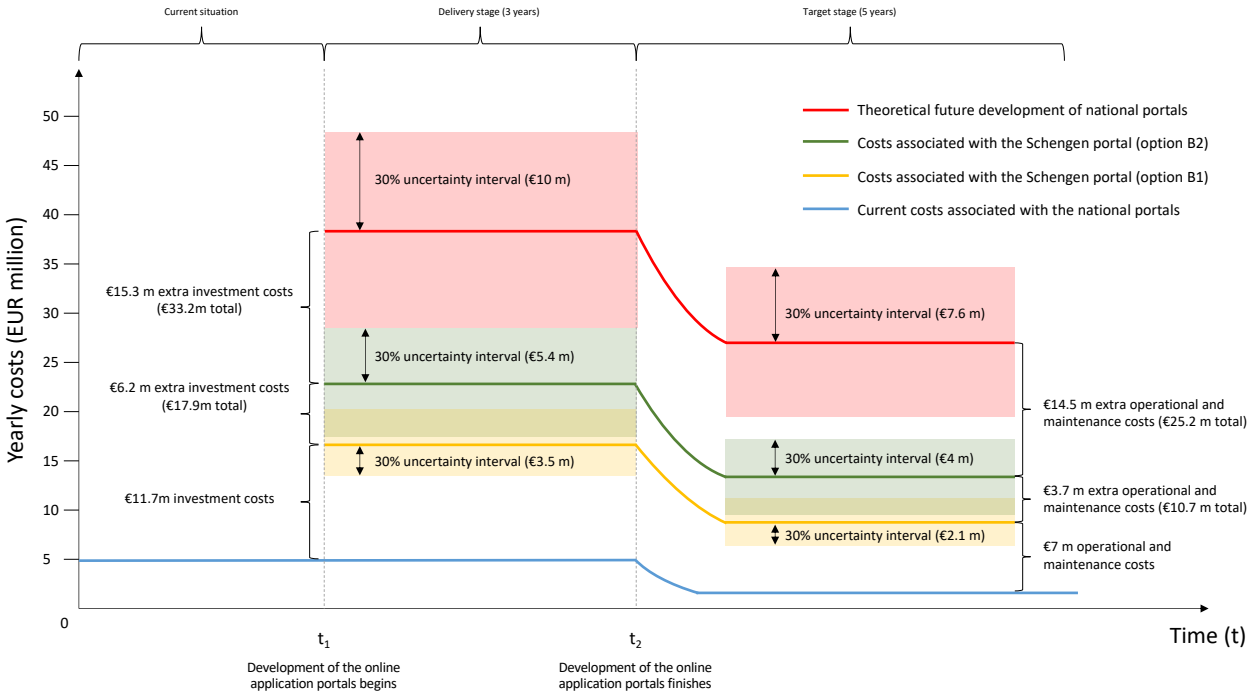

Figure 17: Total cost visualisation of the baseline and solution scenario

Figure 17 clearly illustrates the financial benefits that can be obtained by opting for a Schengen online visa application portal instead of different national versions. Indeed, considerable savings can be observed for both system architectures. The table below shows the savings obtained per system architecture option. In particular, based on the figures in the table above, the following cost savings can be observed (over the total eight-year period):

- for option B1: **EUR 107-201 million**
- for option B2: **EUR 75-140 million.**

1.1.7. Benefits

The previous sections covered the costs associated with the one-off and recurring costs of the online visa application portal. This section details the benefits that can be achieved as a result of going forward with this initiative. This section covers all the benefits identified for TCNs, participating countries and the Schengen Area. As previously mentioned, not all benefits can be quantified. Therefore, some benefits will have to be described textually. This section does not include a calculation on the return on investment as the level of detail available in the study and the length of time needed for the online application roll-out mean it is not possible to make an accurate prediction at the time of writing.

Benefits for the TCNs

The online application portal offers one quantifiable benefit for TCNs: travel savings. Based on assumptions A_8 through A_10, the average savings in travel costs per application are **EUR 55.** From there, by multiplying this average saving by the total number of applications, the total savings for all TCNs can be calculated. Due to the introduction of an online visa application process, the estimated total travel savings are roughly equal to **EUR 880 million.**

Aside from this quantifiable benefit, the introduction of an online visa application process would enable many qualitative benefits for TCNs. The table below lists the qualitative benefits identified.

Table 38: List of qualitative benefits for TCNs

	Benefit
1.	The online application process would guide TCNs through the application process, step-by-step. This guidance smooths the application process for TCNs, which lowers the barrier to applying, ultimately leading to a higher quality of life (easier to travel, visit friends, study abroad, etc.)
2.	The online application portal offers a centralised payment service. Over time, the payment options can be expanded, which eases the payment process for the applicant.
3.	The online application portal includes an appointment management tool. By having this centralised tool, which can redirect applicants to the correct source of information regarding appointments, the appointment-making process will be made seamless.
4.	The online application process makes the entire application process more transparent for TCNs by sending notifications. These notifications could show major milestones in the applicant's application process, e.g. processing of application started, application accepted, application denied, etc., or they could specify other relevant information, such as appointment reminders and/or biometric data expiry indications.
5.	Currently, individuals who have been granted a visa are expected to keep track of the allowed remainder of their stay themselves. The online application process adds a feature through which travellers could check the remainder of their stay digitally. This lessens the burden on TCNs during their travel.
6.	The automated data quality checks implemented in the online application portal ensure that the data submitted by applicants are more likely to be correct on the first submission (an increase in the 'first-time right submission' rate). This ultimately leads to a more efficient application process, which saves time for applicants.

Benefits for Schengen countries

From the surveys conducted during this study, it became clear that a major benefit of a national application portal is the increase in efficiency of the application process. Based on data provided by the Schengen countries, it can be inferred that those countries are experiencing, on average, **6 minutes and 20 seconds** time saved per application. However, the portals currently in operations often contain fewer features than the proposed online application portal, so it is assumed that the actual time saved per application will be 50% higher than the so it is assumed that increase in efficiency identified (see A_13).

The calculation below takes only the **additional** time saved by introducing the online application portal into account. In other words, countries indicating that they already have a national application portal are only attributed 50% of the above-mentioned 6 minutes and 20 seconds. Schengen countries without an online application portal will be attributed 150% of these 6 minutes and 20 seconds (9 minutes and 30 seconds) per application.

In the light of this and taking the total visa number of applications per Schengen country, the estimated total additional time saved is equal to **708 FTEs** (full-time equivalents). This corresponds to over one million hours of employee time that could be spent on other critical tasks.

A second quantifiable benefit for the participating countries would be the costs avoided due to the implementation of the Schengen online application portal. This is an indirect benefit based on the reasoning that countries that currently do not have a digital solution would eventually need to invest in creating their own national application portal if there were no Schengen online application portal. As illustrated above these savings would be roughly equal to (over the complete eight-year period):

- for option B1: **EUR 107-201 million**;
- for option B2: **EUR 75-140 million.**

The key benefit for participating countries is the time saved during visa application processing. However, other additional qualitative benefits have also been identified. Table 39 lists the qualitative benefits identified.

Table 39: List of qualitative benefits for the Schengen countries

	Benefit
1.	For option B1, the centralisation of the supporting documents in the Application Management System allows for an easier information exchange between Schengen countries. Access can be granted through simple permission requests as opposed to having to use the VIS Mail process.
2.	In the survey, Schengen countries indicated that they had observed a small increase in visa applications as a result of having national portals (<5%). Therefore, the Schengen online application portal will result in an increase in applications. This leads to an increase in the visa fees collected and a higher number of Schengen Area visitors, which ultimately boosts the economy of the participating countries.

Benefits for the Schengen Area

All benefits experienced by the Schengen countries are also considered benefits to the Schengen Area as a whole. Furthermore, one key qualitative benefit has been identified for the Schengen Area. Table 40 lists this additional benefit.

Table 40: List of qualitative benefits for the Schengen Area

	Benefit
1.	Having a unified online application portal that is identical for the entire Schengen Area portrays a unified image to other countries. This will reflect positively on the public image of the Schengen Area.

1.1.8. Conclusion

This section lists the conclusions that can be drawn about the two system architecture options *from a cost-benefit* point of view.

From the assessment above, it is clear that both system architecture options enable nearly identical benefits. This is normal, as both system architectures support the same business objectives. As Table 36 has shown, the centralised system architecture option is cheaper than the hybrid architecture options.

Therefore, from a cost-benefit analysis perspective, **the central system architecture is the preferred choice.**

1.2. Digital visa cost-benefit analysis

This section estimates the main costs and benefits inherent in the implementation of the digital visa option as such and the three offline fallback solutions.

- The digital visa option: The goal is to compare the costs and benefits of this option against the costs incurred by stakeholders in using the current visa verification mechanism, i.e. the visa sticker.
- The three offline fallback solutions backing up the digital visa: The goal here is to compare the investment and maintenance costs inherent in the three solutions profiled. This comparison will then be factored into the overall cost-benefit analysis for the digital visa option.

This section outlines the general approach followed to carry out the CBA for the digital visa. As in the case of the CBA on the online application portal, quantitative and qualitative data were collected mainly from a data collection questionnaire sent to the Schengen countries, as well as from interviews, and studies and reports conducted in the past. Replies from twelve Schengen countries contained data relating to the visa sticker.

The nature of the data points used in the digital visa CBA and the data availability lead to some additional methodological considerations. Three main types of data can be distinguished.

- Data on the sticker price and the number of stickers. Even though replies were received from only twelve Schengen countries, these data are very precise, with no significant outliers, and can be combined with official statistics on the number of visa applications submitted and of visas issued.
- Data on other costs in the visa sticker process, i.e. transportation, storage and filling in. For this type of data, fewer responses were received and the analysis was confronted with significant outliers.
- Data on costs in terms of workforce (FTEs). These data also suffer from a lack of replies, and they are different in nature to those covered by the previous two bullet points, as they do not relate to monetary values.

In light of the above considerations, the study could not provide the same level of precision throughout the whole digital visa CBA. The costs and benefits derived directly from the data on the sticker prices and the volume of stickers are very precise; the same goes for data about the prices charged by the ESPs for returning travel documents. However, the costs and benefits derived from the remaining data points are to be considered as indicative estimations.

1.2.1. General approach

Similar to the CBA conducted for the online application portal, a three-fold approach was followed for the digital visa CBA. The quantitative and qualitative data estimations are grouped into the following three categories.

- Current costs relating to the visa sticker. This category is limited to the status quo. The analysis presents all the available data relating to the financial burdens on the Schengen countries and third country nationals attributable to the visa stickers. This section sets the baseline for comparing future costs and benefits.
- Investments for the digital visa option. This category moves away from the status quo and looks into future potential costs linked to the implementation of the digital visa option and the fallback solutions.
- Benefits of the digital visa option. This category outlines the cost savings and the qualitative advantages attainable by developing the digital visa.

The three-fold structure described above does *not* correspond to the timeline outlined in the CBA of the online visa applications. It is possible to roll out and implement the digital visa option independently of the online application portal.

Furthermore, given the level of detail available to this study, a 30% uncertainty interval is applied to the estimations when assessing costs. Therefore, all estimated costs are presented in ranges, e.g. EUR 1-2 million.

1.2.2. Assumptions

As was the case for the cost-benefit analysis carried out for the online application, the analysis of the digital visa option also rests on a number of assumptions highlighted in the table below:

Table 41: Assumptions underpinning the digital visa CBA

ID	Assumption
B_1	When estimating the costs required to build the traveller web service (in the event the digital visa is implemented before and/or without any online application option) the following method is used. The analysis has been based on the Software Development Life Cycle (SDLC) process typically used to develop hardware and software solutions The approach includes the following phases (with the addition of procurement): • Phase 1: Procurement • Phase 2: Design • Phase 3: Development • Phase 4: Testing • Phase 5: Deployment. The economic efforts required to perform these phases are all one-off efforts relating to the cost of the team of developers hired to complete the work. In addition to these one-off costs, the following also need to be allocated: • operations and maintenance costs (per year); • infrastructure costs (per year). Estimating the total costs starts from the development phase as the unit of measure for the other phases. It is assumed that the development phase makes up 40% of the effort required for design, development and testing combined. Design and testing require 30% of the effort each. Then: • deployment requires 10% of the development costs; • operations and maintenance each require 20% of the costs for design, development and testing; • infrastructure costs are 60% of all phases, excluding procurement costs, and operations and maintenance costs.
B_2	To estimate the costs incurred by third country applicants to have their travel document returned by courier, the analysis was based on the service fee charged by the ESPs to applicants applying for a Schengen visa issued by France, and assuming that the fees charged for other countries of arrival do not vary considerably.
B_3	To estimate the costs needed to equip all border crossing points with barcode readers, the analysis was based on the total number of Schengen border crossing points combined with official eu-LISA statistics about the number of queries launched in VIS at those border crossing points.
B_4	To estimate the costs needed to equip immigration authorities in the Schengen countries with barcode readers, the analysis was based on the overall police workforce active in all Schengen countries and deemed that 1 in 10 officers should be equipped with a reader (to take into account the more limited number of patrol officers and the number of officers already equipped).
B_5	The maximum quantitative benefits for the Schengen countries will be attained if the stickers are also abolished for national visas.
B_6	The costs referred to in option C3 (digital visa + signed barcode) are considered as costs to be incurred by the Schengen countries. This is because the barcode sticker discussed by the Article 6 Committee, which may imply the same costs, may just be optional.

1.2.3. Current costs relating to the visa sticker

The current sticker entails costs for the Schengen countries and for third country nationals. This subsection presents the costs driven by the visa sticker and incurred by both stakeholder groups.

Costs for the Schengen countries

The table below provides an overview of the main cost factors relating to the visa sticker.

Table 42: Costs relating to the visa sticker

Categories	Single sticker (EUR)	Aggregated cost for the Schengen Area (million EUR)
Production cost	0.64	9.1
Transportation cost	0.19	2.7
Storage cost	0.07	1.0
Filling in cost	0.09	1.0
Total cost	**0.99**	**13.8**
Total number of visas issued (2018)	*14 265 282*	

The data provided in the "single sticker" column are average costs obtained from data provided by 12 Schengen countries. As mentioned earlier, the average cost for production (unit price paid by the central authorities) of a single sticker is highly reliable as the unit price does not vary considerably across the Schengen countries that replied to the survey. The data provided in the right-hand column are the results of multiplying the average cost per sticker by the total number of Schengen visas issued in 2018. As a result, one can estimate that the whole Schengen Area spends roughly **EUR 13.8 million** on stickers and related equipment and procedures.

The above cost data do not include the salary paid by the Schengen countries to posted or local staff tasked with filling in and affixing the stickers to the travel documents. This is because the organisational structure of the Schengen countries' public administrations and the nature of the tasks performed by posted and local staff is of a nature such that it is not possible to single out expenditure on salaries related only to the filling in and affixing of the stickers.

Therefore, the analysis was based on data provided by some Schengen countries in relation to the FTEs currently required to fill in and affix visa stickers at the consulate. The estimate is that this accounts for 21.3 FTEs per Schengen country, which leads to a total of **554.7 FTEs** for the whole Schengen Area. Although this is the most precise figure possible in the current analysis, it is the result of an average based on data provided by only three Schengen countries. Therefore, it is representative only to a limited extent.

Costs for the TCNs

Visa applicants incur some costs at the end of the visa application procedure, as they have to collect their travel document from the consulate/ESP at the end of the process.[143]

In principle, third country nationals would return to the consulate and incur the same costs incurred a few days earlier (if required to).[144] However, most Schengen countries have cooperation agreements with ESPs in most third countries. ESPs usually provide a delivery service to third country nationals: the applicant can ask for his/her travel document to be returned at a selected location and does not need to travel for a second time. Such delivery services are added-value services for which ESPs charge a service fee to third country nationals, service fees that are likely to be much less expensive than a train or flight ticket from where the TCN lives to the consulate premises.

[143] For an explanation of the main pain points faced by visa applicants, please refer to Chapter 2.
[144] i.e. when travelling to the consulate/ESP for identification, see also Chapter 2.

The table below displays the fees charged by major ESPs to third country nationals for returning the travel document when applying for a Schengen visa in France, with the exception of the data for Russia, which is based on the fee for applications submitted in Belgium, and for Belarus, which is based on the fee for applications submitted in Denmark. The ten third countries accounting for the highest number of visa applications in 2018 were selected.[145]

Table 43: Service fees for the return of the travel document in ten third countries

Third country	Service fee for returning travel document (EUR)
Russia	30.00
China	Starting from 7.70
India	5.70
Turkey	10.0
Algeria	8.90
Belarus	5.10-6.00
Morocco	24.90
Saudi Arabia	9.90
Thailand	45.10
Iran	10.00

It is reasonable to assume that the fees for third country nationals applying in other Schengen countries do not differ significantly from the figures above. In fact, it is the applicant's country of origin that dictates whether differences are significant. The table below displays the aggregate costs for collecting the travel document at the end of the application procedure.

The data below assume that all third country nationals who submitted an application in 2018 from those ten countries used the added-value service provided by the ESP. In practice, there will be those instances where applicants found it cheaper to travel to the consulate/ESP, e.g. because they live relatively close to it. Nevertheless, it is more realistic to estimate the aggregate costs based on the service fee than on train/flight tickets. This is because the price of a relatively few, very expensive tickets risks being overrepresented and the large amount of third country nationals opting for the delivery service being underestimated.

Table 44: Aggregate costs for the return of the travel document (10 busiest third countries)

Third country	Visa applications in 2018	Aggregate costs for applicants for collecting the travel document (million EUR)
Russia	3 695 671	110.90
China	2 823 252	21.7
India	1 081 359	6.20
Turkey	879 240	8.80
Algeria	713 255	6.30
Belarus	681 106	3.70
Morocco	662 585	16.50
Saudi Arabia	360 287	3.60
Thailand	332 269	15.00
Iran	273 580	2.70
Total (top 10)	**11 502 604**	**195.40**

[145] Iran (11th place) is considered instead of the United Kingdom (10th place).

The estimation above is not complete as it misses the costs incurred by third country nationals applying from those third countries excluded from the top 10. As not all ESPs provide added-value services – and specifically: return of travel documents – in all the remaining third countries, it is not possible to make a reliable estimation for all countries individually.[146] Therefore, the average cost is calculated for the passport delivery service (based on the table above), i.e. EUR 15.77, and multiplied by the amount of remaining applications. The table below provides the figure.

Table 45: Aggregate costs for the return of the travel document

Category	Visa applications in 2018	Aggregate costs for applicants (million EUR)
Applications from third countries other than the 10 busiest	4 513 995	71.2
Applications from the 10 busiest third countries	11 502 604	195.4
Total visa applications	**16 016 599**	**266.6**

Certain applications (roughly 5% worldwide[147]) are processed in third countries other than the applicant's country of origin, for instance because the Schengen country of arrival does not have an official representation in that country. Cross-border transportation of travel documents is likely to mean the overall return costs are higher.

In light of the foregoing caveats, the above estimate should be understood as a guideline. It reasonable to use a total figure for the total cost incurred by third country nationals to collect their travel documents ranging between **EUR 250 million** and **EUR 280 million** per year.

1.2.4. Investments for the digital visa option

In this section, the costs needed to implement the digital visa option are estimated, including the three offline fallback solutions.

No additional costs needed to be allocated for the system architecture of the digital visa as such because, as pointed out earlier in this report, the digital visa already exists de facto and is an integral part of the EU framework for border management. Therefore, consulates and/or central Schengen country authorities will simply keep creating visa file records in VIS. No costs will be necessary to improve and update the EU core systems apart from those already envisaged as part of other initiatives, i.e. VIS Revision, EES rollout.

As far as implementation is concerned, the costs for equipping the border crossing points at the external borders with the biometric scanners are already taken into account in the context of the VIS Regulation and of the imminent rollout of the EES.

However, opting for a digital visa may include the creation of an independent traveller web service, based on the EES web service,[148] enabling communication between consulate and third country nationals, and allowing the latter to check the status of their visa. Such a solution will be proposed in the event that the digital visa is implemented before and/or without any online application option.

The traveller web service would consist of a communication gateway complemented by a read-only link to the central VIS. This link would enable the web service to send the third country national a notification about the issuance/refusal of the visa automatically, and would allow the third country nationals to check the status of their visa by logging on and receiving an "OK/NOT OK" answer.

[146] For example, ESPs provide the passport delivery services in certain third countries, but only to citizens applying to Schengen countries other than France (that has been chosen as the benchmark in this case because it covers most third countries in the top 10).

[147] Figure obtained during interviews with DG HOME B.2 officials.

[148] Article 13 of the EES Regulation.

Despite being based on the EES web service, the traveller web service would need to be designed, developed, tested and maintained. The study plans for two major periods.

1. Implementation. This period would run for two years and would include all the phases mentioned in assumption B_1 above;
2. Operations and maintenance. This phase would run once the implementation had been completed and would include the effort to solve malfunctions and upgrade the system.

In order to assess the costs and based on assumption B_1 above, there is a need to estimate the efforts required to build the required system(s). The study envisages that this phase would require a five-person team of developers be engaged for 220 working days at EUR 1,000 per day per person. The development phase would run for half the project, i.e. one year, which would result in a cost of EUR 1.1 million Applying the 30% uncertainty margin mentioned above, this means that the development phase would require an effort ranging from EUR 0.8-1.4 million. Based on this benchmark, the table below summarises the costs of the other phases.

Table 46: One-off costs for the independent traveller web service

Cost factor	Description	Cost (million EUR)
Phase 1: Procurement	The European Commission, eu-LISA, and the Schengen countries agree on common technical components and specifications, such as protocols and interfaces and select the party responsible for each future phase.	0.25-0.50[149]
Phase 2: Design	In this phase, the traveller web service is designed through to the definition of the interfaces, interactions between components, data models of databases, and the protocols to be used.	0.60-1.10
Phase 3: Development	During this phase, the components will need to be built according to the agreed technical specifications.	0.80-1.40
Phase 4: Testing	Once developed, the infrastructure needs to go through testing procedures to ensure future performance.	0.60-1.10
Phase 5: Deployment	This phase covers the rollout of the traveller web service so that the consulates and third country nationals can use it on a daily basis.	0.08-0.14
Infrastructure	This category is not a phase. It includes the hardware necessary to run the service and deliver interaction with existing systems (servers, databases, licences, network capacity, routers, etc.)	1.20-2.20
All factors	All phases for building the traveller web service.	3.50-6.40[150]

Table 47: Periodic costs for the traveller web service

Cost factor	Description	Cost (million EUR)
Operations and maintenance	Activities relating to ordinary maintenance and bug-fixing	0.7-1.2 (per year)

The traveller web service gateway would therefore need a one-off effort of approximately **EUR 3.5-6.4 million**, plus a **EUR 0.7-1.2 million** yearly effort in operations and maintenance.

Apart from the costs relating to the traveller web service, as the digital visa option would not include any additional data to be biometrically checked against VIS, there is no need to equip border control authorities with visa-specific tools. Finally, as mentioned in the CBA of the online application portal, this study assumes that none of the costs linked to developing and improving existing systems should be taken into account, as they would arise regardless of whether the digital visa option is implemented. For all those reasons, the focus below is on the investments for the offline fallback solutions.

149 This cost is not directly linked to development efforts, but is just an estimation of the costs required to negotiate the specifications for the gateway with all stakeholders.

150 The total figures are rounded to emphasise that they are estimates.

Option C1 – Visa issuance notification

As mentioned in Chapter 3, option C1 consists of sending the visa issuance notification to the third country national's email and user account, including the information currently displayed on the visa sticker. The costs to be incurred by consulates in gathering such information and notifying the applicant are negligible, regardless of whether any option is selected for the online application. If one such option is selected, the costs are fully covered by the features offered by the Schengen online application portal; if no option is selected, then the traveller web service will be used to send the notification. Therefore, such – arguably negligible – costs are already accounted for and do not represent a cost factor to be added in the cost-benefit analysis.

As far as the visa verification phase is concerned, all the stakeholders entitled to check visas, i.e. third country authorities, carriers, Schengen authorities and third parties in the Schengen Area, would simply read the information written on the notification. Therefore, no additional costs are expected in this respect.

Option C2 – Non-signed barcode

As explained in Chapter 3, option C2 consists of the visa issuance notification displaying visa information in writing as well as the same information encoded in a non-signed barcode. Personnel at consulates and embassies would be using publicly available barcode technology to encode the visa information and include it in the visa issuance notification. This new procedure requires an assessment of which new assets consulates would need.

The encoding of visa information in a barcode requires the software for encoding information in barcodes on a very large scale. The special printers are not included amongst the cost factors. This is because, differently from the current barcode sticker under discussion in the Article 6 Committee, the barcode would not need to be printed on any paper support. The consulate would simply send it to the third country national electronically.

Software for encoding information in barcodes is currently available on the market at varying prices. A high-level market analysis showed that the price for comprehensive barcode-generating software for industrial use is around EUR 800.[151]

The consulates of some Schengen countries are already accustomed to using to barcode technology in the application phase. A few Schengen countries[152] enable visa applicants to complete application forms online and then submit the forms to the consulate or ESP with a barcode including all the information provided in the application.[153] However, whilst Schengen countries such as Germany could reuse existing software to generate the option C2 visa barcodes, it is safe to assume that they would still need to scale up their equipment in order to be able to generate an amount of barcodes as large as the number of visas issued by their consulates. Moreover, several Schengen countries would still need to acquire such technology and distribute it to their consular posts all over the world (1,897 consulates).[154] Multiplying EUR 800 per software licence by the number of consulates gives a figure of EUR 1.5 million, i.e. a range between EUR 1.1 million and EUR 1.9 million.[155]

As far as the visa verification phase is concerned, all stakeholders need to be enabled to read barcodes. As the equipment for third country authorities is a burden on third countries, the focus here is on the costs for EU stakeholders. Such costs include professional devices and barcode-reading applications. A high-level market analysis resulted in prices for such devices ranging between EUR 300 and EUR 500.[156] Conversely, applications for reading simple barcodes are generally available in the mobile application market, e.g. Google Play Store.

However, as mentioned in the assumptions above, most Schengen countries have already issued or are in the process of issuing such authorities with professional mobile phones suitable for hosting barcode-scanning applications.

---

151 A detailed description of such a software can be found here: https://www.tec-it.com/en/software/barcode-software/barcode-linux-unix-mac-os-x/overview/Default.aspx.

152 See the official Videx website: https://videx.diplo.de/videx/desktop/index.html.

153 See section above.

154 Data based on the 2018 country-specific Schengen visa statistics; https://statistics.schengenvisainfo.com/ (1897 consulate entries).

155 The Schengen countries may benefit from rebates based on the amount of software packages purchased. Therefore, this number may be an overestimate.

156 The EUR 300 estimation is based on the deployment of fingerprint-reading scanners by the UK Home Office. The unit cost of such scanners is less than GBP 300 and they include even more complex features, i.e. biometric scanning, than those necessary for reading barcodes. The estimation is then scaled up to EUR 500 to leave room for more costly devices (depending on the procurement choices of each Schengen country).

Therefore, the study starts from the assumption that it is not necessary to compute and assess such costs as they form part of the baseline.

If a few Schengen countries have not yet issued appropriate smartphones to their national authorities by the time the digital visa is implemented, then such countries will have to make an additional economic effort based on the above-mentioned figures (EUR 300-500 per device).

The table below sums up the estimations of the investment needed to implement option C2. The 'aggregate cost estimation' column refers to the overall cost estimated for the Schengen Area.

Table 48: Investment needed to implement option C2

Investment factor	Unit cost estimation (EUR)	Aggregate cost estimation (million EUR)
Traveller web service *(only if no online application option is chosen)*	3.5-6.4	
Operations and maintenance of the traveller web service	0.7-1.2 (per year)	
Software for encoding barcodes	800	1.1-1.9
Barcode-reading devices at the border	300-500	Negligible (if needed)
Barcode-reading devices for inland checks	300-500	Negligible (if needed)
Total one-off costs without online application option		**4.6-8.3**
Total one-off costs with online application option		**1.1-1.9**
Total periodic costs		**(per year) 0.7-1.2**

Because of the latest developments in the discussions within the Article 6 Committee, the proposal for a barcode sticker has been endorsed by the Schengen countries and is likely to be adopted by those countries on a voluntary basis. Therefore, the costs estimated above for the barcode-reading devices will be incurred only if no Schengen country eventually introduces the barcode sticker. If all Schengen countries do introduce it, then the above costs will be linked to this policy development and not directly to the digital visa option C3 assessed here.

Option C3 – Barcode signed with digital seal

Option C3 consists of the visa issuance notification displaying visa information in writing as well as the same information encoded in a barcode signed by the Country Signing Certificate Authority (CSCA) of the issuing Schengen country.

Option C3 relies heavily on the Public Key Infrastructure (PKI) currently in place in the Schengen countries for signing several categories of documents with a digital seal in the form of a cryptographic key. All Schengen countries have already developed and are currently operating such PKIs; moreover, consulates would be transmitting visa data through the existing secure communication channels established between the consulates and the central authorities. Therefore, no additional costs relating to the core infrastructure are envisioned.

The only cost factors to be added are the following:

- the acquisition and maintenance of software for digital signing of an additional category of documents, i.e. visas, on top of those already being signed by each Schengen country's CSCA; and
- costs for barcode-reading devices at the border and within the Schengen Area.

The extent of the necessary economic effort depends on several factors, such as the readiness of existing PKIs in the Schengen countries, and on the level of maturity of the software used by the Schengen consulates. Thanks to interviews with public officials from certain Schengen countries, an estimation could be made of EUR 100,000-200,000 per Schengen country.

As far as the visa verification phase is concerned, the costs for option C3 would be largely similar to the costs for option C2, as both require authorities and third parties to be able to scan and read the barcode. As mentioned in Chapter 3, the German authorities are equipped with devices for reading barcodes printed on each refugee's proof of arrival. The application used by the German authorities to scan and read such barcodes is called SealVer and is publicly available for free on Google Play.[157]

The table below sums up the estimations of the investment needed to implement option C3.

Table 49: Investment needed to implement option C3

Investment factor	Unit cost estimation	Aggregate cost estimation
Traveller web service (*only if no online application option is chosen*)	EUR 3.5-6.4 million	
Operations and maintenance of the traveller web service (*only if no online application option is chosen*)	EUR 0.7-1.2 million (per year)	
Adjustments to the PKI of the Schengen countries	EUR 0.10-0.20 million (per Schengen country)	EUR 3.0-6.0 million
Barcode-reading devices at the border	EUR 300-500	Negligible (*if needed*)
Barcode-reading devices for inland checks	EUR 300-500	Negligible (*if needed*)
Total one-off costs without online application option		**EUR 6.5-12.4 million**
Total one-off costs with online application option		**EUR 3.0-6.0 million**
Total periodic costs		**EUR 0.5-0.6 million (per year)**

1.2.5. Benefits of the digital visa option

The goal of this subsection is to look at the benefits of the digital visa option. As with the online application, two types of benefits can be considered: quantitative benefits (either in monetary or non-monetary terms) and qualitative benefits. With regard to qualitative benefits, a comparison is made with the investments needed to implement the offline fallback solutions.

Benefits for the Schengen countries

The Schengen countries would experience two main types of benefit: quantitative and qualitative.

Quantitative benefits

In terms of quantitative benefits, the Schengen countries would experience cost savings relating to the abolition of the visa sticker.

It is worth bearing in mind that the abolition of the sticker discussed by this study is confined to the Schengen visa sticker, as the process for national visas is out of scope. It follows that the benefits stemming from the abolition of the sticker, as understood in the context of this study, will depend on whether the Schengen countries will at some point stop using stickers for national visas as well. In that case, the sticker costs outlined above would correspond exactly to the future benefits; otherwise, the extent of the benefits would necessarily be lower than the above costs.

In the event the sticker is abolished only for Schengen visas, it is useful to look at the cost breakdown provided above in order to pinpoint which cost factors would translate into equivalent benefits, and to what extent.

- Sticker purchasing costs. It is rather straightforward to see that, of the total costs incurred by the Schengen Area for purchasing stickers, the Schengen countries would save up to the amount of the costs linked to those stickers used for Schengen visas.

[157] For more information on SealVer, see the following link: https://apkpure.com/sealver/de.tsenger.sealver.

- Costs for transporting, storing and filling in stickers. These costs are unlikely to decrease or increase linearly with the decrease or increase in stickers that consulates deal with. This is because consulates in any event need some form of transportation (that includes other diplomatic dispatches), storage space, printing equipment and personnel regardless of the amount of stickers. Therefore, if the Schengen countries kept using stickers for national visas, they would probably still incur most of the costs relating to transportation, storage and filling in. Nonetheless, these are not the most significant in the overall model drawn above.

With regard to the offline fallback solutions, option C3 would be the most expensive of the three, although the costs would be still limited to the same order of magnitude as option C2. The table below provides the cost-benefit figures for the digital visa and the three offline fallback solutions. Table 50 refers to the scenario in which the digital visa and one online application portal are implemented in parallel; Table 51 refers to the scenario in which only the digital visa is implemented. All available figures have been rounded up to reflect the indicative nature of the estimates.

Table 50:Cost-benefit of the digital visa and the offline fallback solutions implemented in parallel with an online application option

Cost/benefit	Digital visa and option C1	Digital visa and option C2	Digital visa and option C3
		Costs (million EUR)	
Hardware and software	0	1.1-1.9[158]	3.0-6.0 [159]
Barcode-reading devices	0	Negligible (if needed)	Negligible (if needed)
Total costs	0	1.1-1.9	3.0-6.0
		Benefits (per year)	
Cost savings on stickers	10.1	10.1	10.1
		Total (in the rollout year)	
Total savings	10.1	8.2-9.0	4.1-7.1

Table 51:Cost-benefit of the digital visa and the offline fallback solutions implemented without any online application option

Cost/benefit	Option C1	Option C2	Option C3
		Costs (million EUR)	
Traveller web service (EU budget costs)		3.5-6.4	
Hardware and software	0	1.1- 1.9	3.0-6.0
Barcode-reading devices	0	Negligible (*if needed*)	Negligible (*if needed*)
Total costs	3.5-6.4	4.6-8.3	6.5-12.4
		Benefits (per year)	
Cost savings on stickers	10.1	10.1	10.1
		Total (in the rollout year)	
Total savings	3.7-6.6	1.8-5.5	2.3-3.6

Even though the digital visa option C3 would result in higher costs than the other options, such costs would be of the same order of magnitude as those for option C2. Moreover, as the above figures merely represent a one-time monetary effort, no final conclusions should be drawn as to the feasibility of the options based exclusively on those figures. Rather, account should be taken of the results of the feasibility assessment made based on all criteria. This shows the clear advantages of option C3.

[158] This includes the software for encoding barcodes.
[159] This includes the costs for extending the PKI in the Schengen countries.

It is also essential to stress that the costs considered in the above tables are one-off costs, i.e. they would only be incurred once. On the other hand, the costs incurred from using the visa sticker are periodic costs charged on the Schengen countries' budget on a yearly basis.

With option C1, the Schengen countries would achieve an immediate return on investment, but would miss all the security improvements made possible by option C3. The following table outlines the likely return on investment for options C1, C2 and C3, distinguishing between a scenario with an online visa application option and a scenario without a visa application option.

Table 52: Return on investment

	Implemented together with an online application option	Implemented before and/or without an online application option
Option C1	0 months	4.4 to 8 months
Option C2	1.4 to 2 months	5.8 to 10.4 months
Option C3	3.8 to 7.5 months	8.1 to 15.5 months

The rationale for the results above is that the savings per year due to the abolition of the visa sticker would be EUR 10.1 million per year, i.e. around EUR 0.8 million per month. The RoI would therefore be achieved in the following time frames:

- with option C1, the Schengen countries would achieve their RoI **immediately** (after 0 months) with an online application option; they would achieve it in **4.4 to 8 months**[160] without an online application option;
- with option C2, the Schengen countries would achieve their RoI after **1.4 to 2 months**[161] with an online application option, or after **5.8 to 10.4 months**[162] without an online application option;
- With option C3, the Schengen countries would achieve their RoI after **3.8 to 7.5 months**[163] with an online application option, or **8.1 to 15.5 months**[164] without an online application option.

As shown in the table, option C3 would not require a significantly higher cost recovery time. Combined with the qualitative benefits highlighted below, it is clear that **option C3 is to be preferred**.

Qualitative benefits

As for qualitative benefits, the Schengen countries would be able to achieve certain efficiency gains in the management of the administrative machinery. Each Schengen country deploys on average 21.5 FTEs for the operational tasks relating to the visa sticker. The extent to which such a figure can translate into a benefit depends, once again, on whether the Schengen countries keep using stickers for national visas or not. If no stickers at all were being issued, then the Schengen countries would save all those 21.5 FTEs and would be able to reallocate to other tasks the posted and/or local staff corresponding to those FTEs.

The efficiency and consistency of the visa application procedure would also increase. The FTEs saved could be redeployed to added-value tasks, such as the examination of visa applications. Consulates would be able to reduce the time currently needed per application (a benefit to be read in conjunction with the concomitant benefit relating to the online application portal, see above). They may also be able to carry out a better and more thorough examination, with more staff available to check supporting documents, exchange information with other Schengen countries, and run the risk assessment.

Finally, as sketched out in Chapter 2, the sticker life cycle has a negative impact on the environment. The paper used to produce stickers is the product of a value chain associated with deforestation practices, even though it is very hard to estimate the exact share of the damage caused by the industrial processes linked to the sticker. Secure transportation and the return of travel documents after the issuance of the visa increase the negative environmental

[160] EUR 3.5 million investments / EUR 0.8 million savings per month to EUR 6.4 million investments / EUR 0.8 million savings per month
[161] EUR 1.1 million investments / EUR 0.8 million savings per month to EUR 1.9 million investments / EUR 0.8 million savings per month
[162] EUR 4.6 million investments / EUR 0.8 million savings per month to EUR 8.3 million investments / EUR 0.8 million savings per month
[163] EUR 3 million investments / EUR 0.8 million savings per month to EUR 6 million investments / EUR 0.8 million savings per month
[164] EUR 6.5 million investments / EUR 0.8 million savings per month to EUR 12.4 million investments / EUR 0.8 million savings per month

footprint of the sticker. By abolishing the sticker, the Schengen countries would overall make a positive contribution to the environment and, in turn, experience a benefit (albeit of limited scope), as remediation of environmental damage requires policy and economic efforts *inter alia* from such countries' governments.

Benefits for the TCNs

Third country nationals would also experience both quantitative and qualitative benefits from the abolition of the sticker.

With regard to the quantitative benefits, the above estimations show that, by abolishing the visa sticker and implementing the digital visa option, visa applicants would save between **EUR 250 million** and **EUR 280 million**, i.e. on average EUR 15.60-EUR 17.50 per applicant. To be sure, this amount of money cannot be expected to have a major impact on a third country national's decision to apply. However, it is a welcome cost saving from making it unnecessary to leave the travel document at the consular premises.

With regard to qualitative benefits, the abolition of the sticker would enable third country nationals to retain their travel document throughout the whole visa application procedure. This would translate into enhanced mobility for those applicants who need to travel to other countries and are in possession of no suitable travel document other than their passport. If they have to do so before a decision on the application has been taken, i.e. before they can collect their travel document in the current situation, then the retention of the travel document can result in greater flexibility.

Finally, the qualitative benefits the Schengen countries highlighted above (time and efficiency gains) may also result in benefits for third country nationals. Applicants may receive a response to their visa application more quickly than is the case today. Thus, they may get their visa in fewer days or – in the event of refusal – be able to lodge an appeal and/or submit a new application within a shorter period.

1.2.6. Conclusions

The goal of this section is to draw the conclusions from of the cost-benefit analysis carried out on the digital visa option. For an aggregate conclusion that takes into account the results of the feasibility assessment, please refer to Chapter 6.

In the current situation the Schengen countries incur total costs of around EUR 13.8 million for maintaining the sticker life cycle; they also deploy on average 21.5 FTEs to the activities relating to fill in and affixing the sticker to the travel documents, thus failing to reallocate to added-value tasks those employees corresponding to that time. Assuming that stickers will also be abolished for national visas, the Schengen countries would experience a cost benefit equal to the above-mentioned expenditure. The implementation of the digital visa, would, however, require the Schengen countries to invest to implement the offline fallback solution. Option C3 is in the end-analysis the most expensive, but the costs and RoI are within the same order of magnitude as option C2 (whilst this options brings more advantages, especially in terms of security).

In the event of no online application option being selected, the EU budget should be used to develop the independent traveller web service to enable third country nationals to receive visa notifications and check the status of their visas (as such features would not be provided otherwise).

Moreover, the Schengen countries would be able to redistribute staff to added-value activities, thereby improving the effectiveness and efficiency of the visa application process. Finally, the Schengen countries would reduce the environmental footprint of the visa application process.

In the status quo, third country nationals incur the costs of collecting their travel document, which are in a range between **EUR 250 million** and **EUR 280 million**. With the abolition of the sticker, such costs would drop to zero because third country nationals would simply keep their travel document throughout the whole application phase. Besides saving money, applicants would also enjoy enhanced international mobility, and benefit, in general, from a more efficient and quicker service provided by the consulates.

Annex B. The cost model

This Annex presents the mathematical model from which the estimations for the system architecture options and the baseline costs are derived.

The model considers two cost categories that need to be estimated:

1. The delivery costs – these cover the SDLC phases from the design up to and including the deployment); and
2. The infrastructure costs – these cover hardware related costs such as servers, network, storage etc.

For each of these cost categories, the model requires the relative cost[165] of each component, the hardware they run on and the communication requirements. This is the goal of the first estimation exercise. More specifically, each component and connection is assigned an 'effort score' that signifies its relative cost for both the delivery and infrastructure. These estimations are made by a team of experts in order to promote collaboration and exchange ideas. This exercise is also an iterative one to ensure accurate scores are estimated. It is important these scores be estimated accurately as the costs will follow from there.

The figure below shows the components and connections that are considered for both system architectures, along with a unique number for reference purposes. For clarity purposes, components are indicated with a blue circle and communication links are indicated with a green circle.

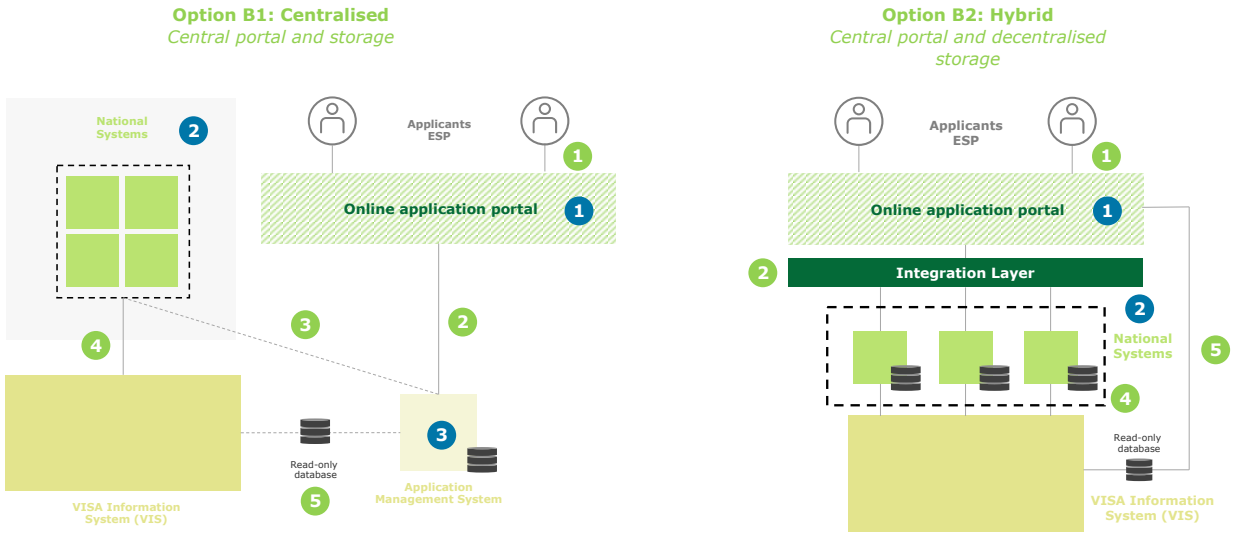

Figure 18: Identification of components and communication links

In both system architectures component number '2' includes all costs at a national level (including the communications required with the consulates) which are omitted from this figure.

As the figure above implies, the model requires the following table to be filled out with relative effort values. It is very important that all these efforts are relative to each other, e.g. a '1' for option B1 has the same weight as a '1' for option B2.

[165] E.g. if a specific component were assigned a score of '1', and the assessment was made that another component would be three times as costly to deliver, the second component would receive a score of '3'.

Table 53: Template for relative effort scoring

ID	Option B1		Option B2	
	Delivery effort	Infrastructure effort	Delivery effort	Infrastructure effort
Components				
1				
2[166]				
3			N/A	N/A
Communication channels				
1[167]	0	0	0	0
2				
3			N/A	N/A
4[168]	0	0	0	0
5				

The second part of the exercise, ideally conducted with a separate team, involves estimating two of the above cells in monetary values, i.e. a team of experts estimates how much the delivery of a portal would cost. This should be a standalone exercise to ensure these estimates are not biased by the previously estimated relative scores.

Once such values have been estimated, the monetary value of a relative effort score of '1' can be inferred from the estimated monetary values and the filled out table. Once the monetary value of a score of '1' is calculated, the monetary value of all components and communications can be calculated, as they are all relative to each other.

An example is provided to summarise and illustrate the above approach.

Consider an architecture that requires the development of two components (a client and server application for internal use), connected with each other through one communication link. Because more context is required to make some form of relative estimation, a simple background story is described below. During a real exercise, many more details are actually considered.

The architecture involves a server application that has to carry out very simple operations, but performance is of the highest importance. On the other hand, the client application needs to be able to access these results quickly, and apply complex, yet not performance-critical, algorithms to them. Because performance is of the highest importance, the latency of the communication link should be minimised as well.

The first step of the process would be to map the required estimations that need to be made for such an architecture:

- delivery of the client component;
- infrastructure of the client component;
- delivery of the server component;
- infrastructure of the server component;
- delivery of the communication link;
- infrastructure of the communication link.

166 This is the cost incurred per Schengen country

167 This link represents web access by the applicant/consulate worker. Therefore, this does not incur any costs for the central systems or the national systems.

168 This link represents the pushing of data to the VIS through the national systems. This link exists already and remains unchanged with the proposed options.

The second step involves estimating the relative effort of each of the above items. As a result of this exercise, the table below is obtained. Example rationales for the scores have been included in the table to facilitate understanding of this estimation step.

Table 54:Example of the relative estimation scores

Item	Score	Rationale
Delivery of client component	3	From the requirements, it is apparent that the client component will require a major delivery effort as the implementation and testing of complex algorithms takes a long time.
Infrastructure of client component	1	From the requirements, it is clear that the performance of this client component is not critical. Therefore, no difficult hardware needs to be provided.
Delivery of server component	1	The server does not need to carry out complex operations, and is thus easy to implement.
Infrastructure of server component	4	Performance is critical for the server application, so high infrastructure investments would need to be made to ensure the server has enough processing power.
Delivery of communication link	0	This specific communication link does not contain any logic and thus no delivery effort is required.
Infrastructure of communication link	2	The communication link's latency is of high importance and has been estimated to take roughly half the effort of the infrastructure of the server component.

Once the above values have been estimated, a separate team selects one or two items that can be accurately assessed in monetary terms with the available information. In this case, for example, this could be the infrastructure of the communication link and the delivery of the server component.

As a subsequent step, this team of experts sits together and estimates these two items as accurately as possible, considering all the information available and their previous experience. For illustrative purposes, assume that this team arrives at a cost of EUR 100,000 for the infrastructure of the communication link and EUR 40,000 for the delivery of the server component.

To calculate the monetary value of a score of '1', these two values are added together, and then divided by the sum of their relative efforts: (EUR 100,000 + EUR 40,000) / 3 = EUR 46,660. This value is then double checked to see if it roughly corresponds to what has been estimated in both steps. If this is not the case, either the relative effort estimation or the monetary value estimation step has to be repeated.

Now that the score of '1' has been assigned a monetary value (~EUR 50,000), the costs of all other items can be inferred and the total architecture cost estimated. The table below represents the results of this final step of the cost estimation example.

Table 55:Results of the cost examination example

Item	Relative Score	Cost (EUR)
Delivery of client component	3	150 000
Infrastructure of client component	1	50 000
Delivery of server component	1	50 000
Infrastructure of server component	4	200 000
Delivery of communication link	0	0
Infrastructure of communication link	2	100 000
Total	11	EUR 550 000

Annex C. Piloting an online application portal

The online application portal pilot project is a small-scale implementation of a full-scale project to evaluate the feasibility, time and cost, and to identify any unforeseen risks and/or issues that were not detected, prior to the final release of the portal. The purpose is to have a gradual approach towards a successful outcome with an efficient allocation of effort and money.

Given the large number of stakeholders and the scope of the portal, the pilot has been subdivided into two major phases:

1. the definition phase
2. the delivery phase (optional).

Please note that phase 2 provides a real-world implementation of the online application process and thus handles real data and integrates with the VIS. Because of this, it could be that this phase of the pilot project must be supported by a legal basis. During the first phase, the decision could be made that the execution of the second phase is not necessary. Therefore, this study positions the delivery phase as being optional.

1.1. Objectives of the pilot project

1.1.1. Definition phase

The pilot programme concept should start with a definition phase, in which the necessary preparations for the launch of the pilot project are made. These preparations aim to:

1. identify and research the pain points for consulates and applicants;
2. identify opportunities for technological improvement for the identified pain points;
3. validate the proof of concept;
4. build a prototype realisation of the online application portal;
5. prepare the governance and coordination landscape required to deliver an actual pilot programme.

The outcome of this phase would be a common understanding, with clearly defined responsibilities, expectations and requirements for all Schengen countries participating in the pilot project. Furthermore, the requirements of the pilot portal will have been clearly explored and identified.

1.1.2. Delivery phase

The second phase covers technical aspects relating to the online application portal. In particular, the delivery phase aims to achieve the following objectives.

- Test the digital user journey and its associated features – assess whether the digital user journey is easy to understand for the users and whether the technical features behind it offer the expected results.
- Refine the coordination and governance landscape previously described in the definition phase – the governance and coordination phase lays down the initial landscape on which the coordination and governance efforts are based. However, during the operation of a pilot portal, new challenges could arise which could require modifications to this landscape.
- Detect integration problems for countries of varying levels of technological maturity – to assess any technical integration difficulties for the Schengen countries. In particular, Schengen countries of all levels of technological maturity should be considered in the pilot project in order to identify specific challenges they may encounter. This will greatly reduce the risk of issues arising during the full-scale rollout.

- Detect loopholes and security vulnerabilities – to assess any areas where further security considerations need to be taken into account.
- Better understand storage and network requirements – by observing the storage and network requirements during a pilot project, the estimates presented by the feasibility study can be further refined in order to better predict and inform Schengen countries of the storage and network requirements they would need to foresee in the full-scale online application portal.
- Fine-tune cost estimations and budgets – by observing the costs during a pilot project, the cost estimates presented by a preliminary cost-benefit analysis can be further refined in order to better predict and inform Schengen countries of the costs they will incur in the full-scale online application portal.

1.2. Features and technical requirements

Typically, a pilot project does not contain all the features of the full-scale release. In order to identify the essential features of the pilot project, the objectives listed above are mapped to the features of the online application portal and the requisite technical considerations. Any features that are not critical for testing the objectives are left out of the pilot project.

1.2.1. Definition phase

The definition phase follows design thinking principles by following a user-centric approach to designing the requirements of an application.

First, before going into detail as to what is delivered during this phase, the stakeholders that are needed in these collaborative discussions need to be identified. In particular, the following parties should be involved:

- Schengen country representatives;
- European Commission representatives;
- eu-LISA representatives;
- an independent coordination partner to facilitate the design thinking and service design process discussions.

The first phase involves creating and validating a prototype. First, this prototype is described at a high level, after which subsequent iterations will further refine and eventually create a working prototype. The table below presents the suggested steps in order to build the prototype. While the table lists the steps sequentially, an iterative approach is advised, e.g. the outcomes of a certain step could identify issues or shortcomings of an earlier step; in this case, the earlier step should be revisited and further refined.

Table 56: Design thinking steps in the definition phase

Description	Features/Requirements
Step 1: Develop the user journey This step defines the user of the pilot portal. By using the principles of design thinking and collaboration among the stakeholders, the user requirements will be laid down.	This step involves: 1. defining user personas (consulate officers, border guards, applicants, etc.) reflecting the average users of the portal; 2. identifying pain points (as identified earlier) and areas of improvement for these personas; 3. coming up with user stories that illustrate the usual transactions users will need to perform.
Step 2: Draw up mock-ups Once the user requirements of the pilot portal have become clear, this step aims to visualise this user journey through the application portal. By visually running through the application process, shortcomings of the previous step can be identified.	This step requires the participants to visualise the user journey through so-called mock-ups. These mock-ups illustrate what a user would see on their screen during the application process. The mock-ups should include the actual fields, buttons and pop-ups a user could encounter during the online application process. Once the mock-ups have been created, the user stories identified in the first step must be simulated to validate whether all requirements are actually met.

Description	Features/Requirements
Step 3: Clickable mock-ups This step enhances the previous paper-based mock-ups by implementing them in an application. This allows a user to navigate through the online process as if they were actually applying online. This extra refinement will allow an extra layer of validation and will identify areas where the user friendliness of the application can be improved.	Instead of paper-based mock-ups, these mock-ups are visualised on computer screens. The screens should be clickable to simulate the actual navigation through the online application portal. As the mock-ups do not contain any logic, even the most complex features can be represented by a simple mock-up screen.
Step 4: Prototype implementation This covers the prototype implementation of the pilot portal. It develops an interactive prototype consisting of some minimal, yet critical, features. The idea is to test, on a standalone version (isolated from the internet), whether the portal delivers the expected outcomes from a concept point of view. When this outcome is positive, the prototype can be transformed into an actual pilot project. The objective of the prototype is to demonstrate that the design and concept of the online application portal are feasible.	The prototype should contain: • the online application form; • a dynamic questionnaire to identify the decision-taking Schengen country. The prototype is a standalone version, and thus not connected to the public internet. However, the logic for distributing application files to Schengen countries can be tested regardless by simulating the national systems' features/behaviours in the proof of concept (access to their development or acceptance environment could also be considered). This will allow testing of the distribution of application files to Schengen countries and the required interfaces on both sides, without requiring Schengen countries to make modifications in their national systems. This prototype is **not** accessible for external users and is simply used for internal validation.

Once the prototype has been developed and tested, an analysis should be conducted on the feasibility of continuing the pilot project. If this analysis yields positive results, the stakeholders should continue the process by laying down the governance and coordination landscape to be used for the pilot project. This does not involve the creation of any technical piece of software. It is purely aimed at laying down governance and coordination principles and smoothing the operation of these going forward.

The representatives should continue to meet regularly until they have:

- set up common specification agreements;
- identified Single Points of Contact, roles and responsibilities of the parties involved;
- set up a coordination and escalation model;
- set up a change request model, e.g. when a Schengen country wants to reflect a new national requirement in the online portal;
- decided the scope and participating countries of the portal testing phase;
- agreed on the budgetary implications;
- discussed the regulatory impacts of the pilot.

1.2.2. Delivery phase

The portal testing phase involves rolling out an operational portal. However, multiple considerations need to be take into account in the scope of delivering such an online application portal.

Upon successful validation of the Proof of Concept in the previous phase, it is recommended that the pilot portal be rolled out in multiple releases, henceforth called Minimum Viable Products (MVPs). Subsequent iterations of MVPs would gradually offer more features to the online application portal, consequentially allowing the testing of different objectives over time. The pilot would consist of at least six MVPs.

The table below describes the features of each MVP and their associated objectives.

Table 57: List of critical features or requirements per MVP

Description	Features/Requirements
MVP 1: Minimum release to selected applicants This MVP offers the most basic of services to the applicants. This first iteration offers the ability to applicants to fill out their application form through the portal. It does not yet offer the ability to attach any documents to the application file (these still need to be submitted in person). Please note that this MVP (and the subsequent MVPs) is/are not visible from the public internet, and the applicants mentioned in this paragraph are only able to access the portal upon receiving an invitation to partake in the pilot project. The objective of this MVP is simply to test whether the first version of the online application portal is accessible to its intended users and to see if the applications are correctly distributed to the participating Schengen countries (now in a real-world scenario).	The pilot portal should support: • the online application form; • configuration capabilities; • a check-box to confirm data are complete and accurate; • a dynamic questionnaire to identify the decision-taking Schengen country. The pilot portal should already experiment and test the ease with which the portal can be configured by the Schengen countries. This has to be included from the very first stage because making this change at the end could take considerable effort. From an integration point of view, it is recommended that the complete integration layer not be adopted immediately. Due to the limited scope of the pilot project, one-to-one connections[169] can be implemented between the pilot portal and the national systems. For security reasons, at this stage, the pilot portal should not be accessible through the public internet. Only a selected number of participants should receive secure access to the online application portal by means of an invitation. This first MVP only integrates with a single, low complexity third country. Integration with other, more complex, third countries is considered in a subsequent MVP.
MVP 2: Upload document expansion This MVP aims to expand the pilot portal by allowing the applicants to attach electronic files to their application (such as supporting documents and travel document information). Upon the successful release of this MVP, the selected applicants will be able to fully submit a complete application file through the pilot portal. The objective of this MVP is to expand the portal so it can support the full application process for applicants.	The pilot portal should be expanded so as to support the following features: • dynamic questionnaires in order to: — identify the type of information, e.g. supporting documents, the user needs to provide; • interactive guidance; • ability to submit a travel document: — filling in the travel document information in form fields; — uploading a scan of the travel document; • ability to submit supporting documents: — uploading the supporting documents in native format; — uploading a scan of the supporting documents; • malware/virus detection of uploaded documents; • the online payment gateway.
MVP 3: Additional third country integration This MVP involves including a third country of a higher complexity than the initial third country considered up to now. The objective of this MVP is to assess the risks and challenges associated with another third country profile.	This MVP does not make any functional changes to the pilot portal, but requires integration with another third country.
MVP 4: Data quality expansion This MVP expands the online portal to cover the automated data quality checks. The objective of this MVP is to be able, at the end, to assess the digital user journey and its impact on the quality of the applications submitted.	The pilot portal should be expanded so as to support: • input format checks of application form fields; • format checks of the uploaded documents; • data quality checks of the documents submitted (size, brightness, etc.)

[169] In one-to-one connections, communicating systems have a direct link between them. In small scale information systems, such as the pilot project, this is a feasible approach as only a very limited number of systems need to be connected (the portal + the systems of a handful of Schengen countries). The alternative solution, an integration layer, acts as a communication intermediary. The major benefit of such an integration is that a change to one system does not necessarily require a change to all systems connected to it. Therefore, once many systems need to be connected, it is advisable not to use one-to-one connections. This integration layer is proposed in the hybrid system architecture and is implemented later on in MVP 3.

Description	Features/Requirements
MVP 5: Transition to the integration layer This MVP leaves the online portal as it is, but focuses on the integration between the central and national systems. Instead of the direct connections operated up to now, an initial version of the integration layer is procured and implemented. The objective of this MVP is to identify any areas for improvement of the governance and coordination landscape, and to assess any technical difficulties Schengen countries could encounter.	This requires the modification of the direct communication channels between the pilot portal and the national systems. Instead of these direct communication channels, the integration layer, as set out in by the body of this document, need to be implemented.
MVP 6: Accessibility through the public internet This MVP exposes the pilot portal to the internet. It will no longer only be accessible to a number of selected applicants. The objective of this MVP is to identify whether the pilot portal has any security vulnerabilities.	The pilot portal should be accessible through the public internet, worldwide. Strict monitoring policies need to be in place in order to react immediately to any attacks.
(optional) MVP 7: Further expansion This Annex only describes the most critical MVPs, as they cover the most essential objectives and requirements. Of course, the MVPs could be expanded until all of the online application portal's features have been reached.	Features that were not deemed as critical in terms of testing the objectives of the online application portal are: • scanning the travel document's MRZ code; • identifying visa exempt travellers; • interaction with the applicant; • chatbot assistance; These features could be implemented in subsequent MVPs. Furthermore, the above MVPs are limited to a specific scope of participating countries. Subsequent MVPs could not only change the features of the portal, but also expand the scope of the pilot project by considering more countries.

The last two objectives (better understand network and storage requirements and fine-tune budgetary implications) are not explicitly mentioned in the table above. These two objectives are implicit in all MVP stages. Because the MVPs add features to the pilot projects incrementally, the network and storage requirements and the budgetary implications can be observed in even more detail, as the costs associated with each added feature will be clearer than with a 'big-bang' pilot portal.

1.3. Timeline

The body of this document listed a timeline in which the pilot project would be rolled out and where it sits within the overall online application portal's release cycle. The figure below zooms in on the pilot project timeline itself, and maps the previously described phases (and associated MVPs) to the timeline.

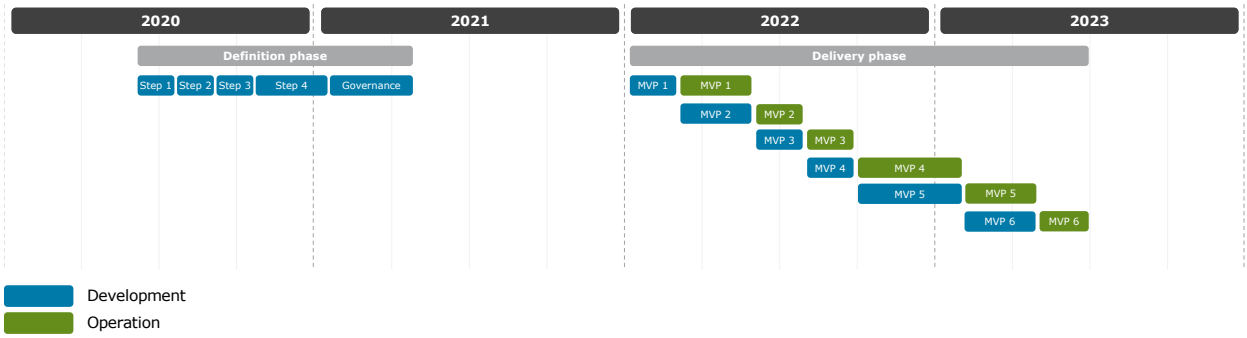

Figure 19: Proposed timeline for the phases and MVPs

There are a couple of observations to be made in connection with this timeline:

1. The time to implement MVP 1 seems short in comparison to the prototype development (Step 4). However, as the prototype, already developed in the first phase, implements an isolated portal with nearly the same features, many aspects could be reused. The bulk of the development effort of MVP 1 lies in the integration requirements with the participating Schengen countries' national systems.
2. MVP 5 takes considerably longer to develop than the other MVPs. This is because of the complexities associated with integrating the pilot portal with the national systems through an integration layer.
3. Even though MVP 6 does not change the logic of the online portal or national systems, the security considerations that come with making the pilot portal visible on the public internet would require a significant effort.

1.4. Selecting the participating countries

A major consideration in the pilot project is the decision on which countries to involve in the pilot project. To scope the pilot project, two kinds of countries must be selected:

- countries whose residents will be able to use the online application portal to apply for a Schengen visa;
- one or more Schengen countries to participate in the pilot project.

1.4.1. Selecting the third countries

To select these third countries, multiple criteria must be considered, such as:

- size of the country,
- number of visa applications,
- capability and capacity to adapt,
- number of visas issued or refusal rate,
- the average profile of the visa applicants.

The proposed pilot project (with the various MVPs described above) starts by considering only one country from which applicants can apply through the portal. Initially, it is important to note that the security of the Schengen Area remains of the utmost importance. Therefore, a country that poses little migratory or security risk should be considered (for the worst-case scenarios). Furthermore, it is advisable to avoid extreme examples (large third countries with a very large number of applications, e.g. China, or countries with barely any applications, e.g. South Sudan).

Once the integration with a low complexity country has been realised, MVP 3 introduces the integration with another country of higher complexity. This higher complexity could be defined based on many criteria, e.g. higher migratory risk, higher technological maturity, strict specific national regulations. Considering such a higher complexity third country will provide insightful information about specific challenges that could arise in situations that are more complex in order to prepare the rollout for the full-scale online application portal. It is advised that the pilot portal be tested in situations that are more difficult.

As mentioned in the table above, not all applicants should be allowed to participate in the pilot project from the start. Only MVP 6 considers making the pilot portal visible to the internet. Therefore, aside from selecting a country, a selection should be made as to which applicants are able to apply through the pilot portal. These selected applicants should be invited to partake in the pilot project.

1.4.2. Selecting the participating Schengen countries

Scoping the country from which applicants can apply for a Schengen visa is not enough. Additionally, the number of Schengen countries to which those applicants can submit an application should be limited. If this were not the case, the pilot project would involve long and complex coordination and governance meetings, considerable investment on the part of all countries and a longer preparation phase overall. Therefore, this section lists criteria based on which a number of Schengen countries can be selected to be invited to participate to the pilot project.

1. The Schengen country must receive Schengen visa applications from the residents of the selected countries.
2. The Schengen country must be willing to participate in the pilot project. Countries must be made aware of their expectations prior to their enrolment in the pilot project.
3. Countries should be selected based on their technological maturity. It is recommended that at least one country, and at most two, be considered from each category of technological maturity (no current portal, operating a moderately advanced portal, and operating an advanced portal). This will ensure risks and difficulties in all areas can be identified during the pilot project. Furthermore, this will shed more light on the benefits accruing to countries in each category.

Aside from these criteria, there are no strict rules with which the selected Schengen countries should comply. This leads to a pilot project where applicants from the selected third countries could apply to a set of three to six Schengen countries.

1.5. Cost estimation

This section presents an estimation of the costs associated with both phases based on the cost-benefit analysis conducted in the body of this document. The estimation considers the costs incurred on a central level (by the Commission) and the estimated costs that would be incurred by each participating Schengen country. The costs presented are average costs and could vary based on the technological maturity of the participating Schengen country.

The costs of the first phase are estimated based on the observation that they mostly involve meetings between the different stakeholders. For this purpose, the costs were calculated based on the following parameters:

- the time for the first phase (as presented in the timeline above);
- the frequency of meetings during this time period, e.g. once per week;
- the stakeholders involved:
    - central representatives to facilitate the meetings and represent the interests of the Schengen Area;
    - national representatives to represent the interests of the Schengen countries;
    - external facilitators to guide the pilot project phase;
    - developers to create the clickable mock-ups and prototype;
- the number of stakeholders that participate in each meeting per category:
    - for the first three steps it has been assumed that only half the national representatives will attend as their presence is not strictly necessary;
    - for the final, governance, step, all national representatives would be present;
- their time committed per stakeholder category, e.g. national representatives will only be involved during the meetings and will not incur a significant amount of work outside the meetings, while the external facilitators will be committed half or full-time in preparing the meetings and processing the outcomes;
- the price per day per stakeholder category, including salary, travelling costs or any other expenses:
    - on the assumption that the costs for the central representatives, external facilitators and developers are incurred by the central body;
- the development of the mock-ups and the prototype do not require any special hardware, so the infrastructure costs are negligible and thus not considered;
- software and hardware costs are included in the pricing of the developer, as the software and hardware needed to build the clickable mock-ups and the prototype should be part of an average developer's kit.

Based on the above assumptions, the costs presented in the table below have been estimated for the first phase of the pilot project. The national costs are presented per country. As the fourth assumption assumes not all national representatives are present at all times, the costs below represent average costs per country.

Table 58: Costs associated with the first phase of the pilot project

	Central costs	National costs
Costs for the first phase	EUR 1.0-1.9 million	EUR 28 000-52 000

The costs for the second phase are derived from the costs estimated for the full-scale rollout of the online application portal as described in the CBA (please see Annex A). The following assumptions have been used to derive these costs.

- The online application portal has more features than the pilot project portal. However, development costs are not linear to the scale of a system (developing a system for 10 users is not 10 times as expensive as developing the same system for one user).
- The pilot application portal will not process the same amount of data as the full online application portal. However, the central systems must to support the portal and new connections need to be created (the one-to-one connections, which are then transformed into the integration layer).
- The participating countries will need to make the same modifications to their national systems in terms of software. However, in terms of infrastructure, as the number of third countries is limited, a lower investment is needed.
- There are fewer stakeholders involved in the pilot project, which reduces the effort (and thus cost) relating to agreements and coordination between all parties involved.

The table below shows the costs incurred during the second phase of the pilot project by applying the above assumptions to the previously estimated values.

Table 59: Costs associated with the second phase of the pilot project

	Central system	Per participating Schengen country
Costs for the second phase	EUR 4.2-7.8 million	EUR 0.95-1.8 million

Annex D. The online application portal and data protection

This Annex presents additional data protection considerations to take into account for the development of the online application portal. In particular, this Annex lists six data protection measures that need to be taken for the online application portal.

As discussed in main body of this study, the proposed portal requires the development of a public website and an application for mobile devices. This website will be used by third country nationals applying for a Schengen visa.

1.1. Privacy notice

The online application portal will need a privacy notice published on the public website and on the mobile application.

The privacy notice should contain, at least, the following information:

- identity and contact details of the controller;
- contact details of the data protection officer;
- The purposes of processing for which the personal data are intended, i.e. assessing whether the entry of the applicant into the Schengen Area could pose a security, illegal immigration or high epidemic risk in the Schengen Area;
- the legal basis for the processing;
- recipients or categories of recipients of the personal data;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation, and the existence or absence of an adequacy decision by the Commission or reference to the appropriate or suitable safeguards, and the means by which to obtain a copy of them or where they have been made available;
- the data retention period or, if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject, or, where applicable, the right to object to processing or the right to data portability;
- the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the European Data Protection Supervisor (EDPS);
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling.

The information is to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

1.2. Cookie notice

The online application portal will need to have a cookie notice to be published on the public website and on the mobile app, which includes at least the following information:

- what cookies are;
- how cookies work;
- types of cookie used on the public website and mobile app;
- the purpose of the cookies;
- how visitors to the public website or app for mobile devices can consent to the use of cookies.

1.3. Secure account service

The online application portal will require a secure service to be established to enable applicants to provide the additional information or documentation required for each use case.

Because of confidentiality considerations, strong authentication measures are necessary for applicants to log in to the online secure account service. Furthermore, it is a requirement to ensure that only those types of personal data that are necessary for strong authentication of the applicant are requested when logging into the secure account service. The types of personal data to be requested from the applicant are:

- application number,
- unique code,
- travel document number,
- country of issue of the travel document,
- date of issue and of expiry of the travel document.

1.4. Online application form

It is a requirement to ensure that the digital application form on the public website and on the mobile application only collect personal data that relate strictly to the processing of the visa application.

The public portal of the online application portal will require provision of a data collection statement on the online application form or easy accessibility of such a statement via a hyperlink.

1.5. Online verification tool

The online application portal will require an online verification tool on the public website and the mobile application to allow applicants to verify the status of their visa application and check the validity period of their visa. Similar to the secure account service, strong authentication measures will need to be put in place for applicants to log in to the online verification tool.

1.6. Declaring that data are accurate and complete (“Consent tool”)

The online application portal will require an online consent tool for the public website and the mobile application. This is to allow applicants to consent to processing of their personal data by the online application portal for an additional period of no more than three years after the end of the validity period of the travel authorisation and to withdraw their consent at any time.

In particular, the system is required to ensure that the applicant provides consent unambiguously, for example by ticking a check box. The applicant needs to be informed in advance of the purposes for which their personal data are being retained in central or national systems.

Annex E. Option analysis for visa application

This Annex presents the detailed description of the different digital elements that Schengen countries could adopt to enhance the visa application process. Table 61 lists all the options presented during the first and second workshop with the experts from the Schengen countries. Elements with a checkmark (✓) were investigated after the workshop. The others were discarded after workshop one or two, because the opinion of the experts was that they were not feasible or generally not preferred. For an analysis of the implications and the possible synergies of some options presented in this Annex, please refer to Annex G.

Table 60: Overview of all the different options for the visa application

Business architecture		
Functional block	**Options**	**Analysed in this study**
Submit visa application form	Premium electronic application form	✓
	Interactive electronic application form	✓
	Basic electronic application form	✓
	Paper application	✓
Travel document	Read electronic travel document (MRZ reader code)	✓
	Fill in travel document information	✓
	Scan and upload travel document	✓
	Physically provide travel document	✓
Supporting documents	Third party gateways	✓
	Submit electronic document in electronic format (upload documents)	✓
	Submit paper-based document in an electronic format (scan documents)	✓
	Provide documents at the consulate or at visa application centre (in paper)	✓
Collect fingerprints	Collect fingerprints from anywhere	✓
	Collect fingerprints from self-service kiosks	
	Collect facial images with a mobile kit	✓
	Collect facial images at the consulate or visa application centre	✓
Collect other biometric identifiers	Collect facial images from anywhere	✓
	Collect facial images from self-service kiosks	
	Collect facial images at the premises of certified service providers	
	Collect facial images with a mobile kit	✓
	Collect facial images at the consulate or visa application centre	✓
Declaring that data are accurate and complete	Smart implicit declaration	✓
	Advanced digital declaration	
	Basic digital declaration	✓
	Facial recognition declaration	
	Paper-based signature	

Business architecture		
Functional block	Options	Analysed in this study
Pay the visa fee	Payment gateway	✓
	Integrated visa fee payment	
	Redirect to national payment websites	✓
	Pay the visa fee at the consulate or visa application centre	
Interaction with applicant: appointment management tool	Fully centralised appointment management	✓
	Redirection to national / ESP appointment tools	
Interaction with applicant: check visa status	Fully centralised visa status checking tool	✓
Interaction with applicant: appointment management tool	Fully centralised electronic notification tool	✓
System architecture		
System architecture scenario	Centralised process	✓
	Hybrid	✓

1.1. Submit visa application form

This section presents the options for applicants in submitting the visa application form.

1.1.1. Option 1.1: Premium electronic application form

This option has two major characteristics that would contribute to a full digital experience for the applicant, and ensure time efficiency gains when applying for a visa.

First, applicants would answer some general questions, i.e. 'where are you from?', 'where are you going?', 'what is the duration and purpose of your trip?' Based on the information provided, the applicant would be redirected to the relevant visa form for their application. The form would already include some information (retrieved from the initial questions the applicant replied to). Subsequently, the applicant would reply to additional personalised questions with interactive guidance throughout the questionnaire. This guidance would provide the appropriate instructions and alerts to support the applicant in answering correctly all the questions compiled in the visa application form. Additional clarification on how to fill in the application form could be explained using an interactive communication channel, e.g. a chatbot, between the applicant and the EU entity responsible.

Second, applicants would have the option of using the automated method for filling in the application. Through this method, certain fields in the application form would be pre-filled, hence enhancing the application form filling in process and submission. Basic information registered on the user account associated and retained from a prior visa application can be used for the pre-filling.[170] According to information obtained during the national interview with the Consulate of Norway in Manila (Philippines), this process is already being used and brings significant benefits for some applicants who are not required to re-insert their personal data. Storing the personal data in the online IT tool during a fixed period mainly simplifies the application process for frequent repeat applicants.

In addition to using data from the user account (retained from previous applications), part of the application form can also be automatically filled in by scanning the travel document's Machine Readable Zone (MRZ) and uploading a picture to the web service. The image would then be processed and subsequently read the information embedded in the code. This information would then be used to automatically fill out the relevant fields in the application form.

[170] For this, and according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), applicants shall consent their data to be retained for future applications. A tool similar to the ETIAS consent tool could thus be expected.

1.1.2. Option 1.2: Interactive electronic application form

Similar to the previous option, the main purpose behind this option is to enable applicants to answer personalised questions fully tailored to their profile, with interactive guidance throughout the questionnaire. However, this option does not allow applicants to use the automated method to fill in some sections of the application form, implying that applicants would need to do so manually.

Although the pre-fill would not be available, the interactive digital application form would help the applicant answer all the questions by providing the appropriate instructions and alerts. Additional clarification on how to fill in the application form could be explained through an interactive communication channel, e.g. a chatbot, between the applicant and the EU entity responsible.

1.1.3. Option 1.3: Basic electronic application form

This option provides all applicants with a standardised application form, which can be filled in and submitted in a single-step journey. The data requested in the application form consist of generic and non-personalised fields to be filled in by the applicants. This generic form implies a reduced involvement of the applicant during the application process and does not promote user interaction. It creates difficulties for less experienced users in completing the visa application efficiently and effectively.

1.1.4. Option 1.4: Paper application

According to Article 10 of the current Visa Code,[171] *"[...] applicants shall appear in person when lodging an application"* whether in a consulate representing a Schengen country in a third country or at a visa application centre premises. It is worth noting that, in the status quo, the completed application form must be submitted by each applicant directly on paper.

1.2. Travel document

Currently, applicants provide their travel documents (as well as printed versions of the supporting documents) at the consulates or the visa application centres. Once a decision has been made, the applicant can retrieve their travel document (which can be collected at the consulate or visa application centre).

1.2.1. Option 2.1: Read electronic travel document

This first option would enable applicants with an electronic travel document, e.g. passports, to upload the details included in the chip directly into their visa application. This option entails the applicants uploading their travel document's details without being required to provide their travel document physically either to the consulate or the visa application centre.

This option would only be available to applicants who had been granted a visa in the past 59 months.[172] Therefore, this implies that these applicants would already have provided their biometric data and that their travel document had been checked at the premises of the consulate or visa application centre. This would ensure the necessary security level required in the visa application process, as the travel document of the applicant would already have been examined.

This option thus does not apply to first-time applicants, nor to applicants whose travel document has been renewed. In the latter circumstances, the applicant might have been granted a visa in the last 59 months, but the travel document is no longer necessarily the same one and hence needs to be examined again. Applicants whose visa application has been rejected will be considered as first-time applicants and this option does not therefore apply to them.

---

171 Article 10, Visa Code.

172 Recital 10 and Article 13(3) of the Visa Code.

In terms of geographical scope, this option would only be available for those countries with electronic travel documents. Of the 105 countries currently held to visa requirements to enter the Schengen Area, 43% provide their nationals with electronic passports[173]. This option could therefore apply to 45 countries. This number is expected to increase with the current trend to digitalisation.

The technical solution for implementing this option would be software reading the information on the passport. For this purpose, the MRZ code as well as the front page of the travel document need to be scanned by the camera of a smartphone or a picture thereof uploaded to the web service. The software would then subsequently read the chip in the travel document. The information, i.e. personal information, document information, chip info, validity, document signing certificate, embedded in the travel document would then be displayed. The information can be subsequently shared and uploaded in the application form.

There are apps currently available on the market, which offer these services. Some examples of these are ReadID – NFC Passport Reader[174] or PassportImageDecoder.[175]

Applicants would in any case still have to upload a scanned version of the biographic data page of their travel document as required by the VIS Revision proposal (Article 7 (a) (d)). The scan of the biographic data page will be uploaded to VIS.

1.2.2. Option 2.2: Fill in travel document information

As for the previous option, this option would only apply to those applicants who had been granted a visa in the past 59 months (and thus, whose biometrics are still valid), and whose passport had not been renewed during that time.

This option would entail applicants providing the information, i.e. name, family name, date of birth, travel document number, expiry date and issuing country of their travel document themselves. The application form would therefore include some fields where the applicant can input the information from the travel document. In this option, applicants would not be required to upload any scanned version of their travel document.

1.2.3. Option 2.3: Scan and upload travel document

As in the other options, the scope of this option is also limited. For security reasons, it will only apply to those applicants who were granted a visa in the previous 59 months (and thus, whose biometrics are still valid), and whose passport has not been renewed in the same time frame.

In this option, applicants will be required to upload an electronic copy of their travel document. This implies applicants scanning their travel document and uploading the copy to their application form. As indicated by some of the interviewees, consulates examine all the pages of a travel document in order to verify the stamps and stays of the third country national. For this reason, if the third country national is exempt from providing their travel document, it might be advisable to require the applicant to scan a copy of all the pages of their travel document. However, the EES will indicate in future when and how long the third country national remained in the Schengen Area. In this case, a scan of all the pages of the travel document would not be necessary.

1.2.4. Option 2.4: Physically provide travel document

This option refers to the current situation. This entails applicants, regardless of their profile, i.e. first time applicant or not, needing to submit their travel document together with their application form and the supporting documents. Submitting the travel document means that its authenticity can be verified, which ensures that the necessary security standards are met in the visa processing. In this way, it is possible to derive the third country national's application for a Schengen short-stay visa, the biometrics and the travel document.

[173] See: https://www.schengenvisainfo.com/who-needs-schengen-visa/
[174] See: https://play.google.com/store/apps/details?id=nl.innovalor.nfciddocshowcase&hl=en_US
[175] See: https://play.google.com/store/apps/details?id=at.mroland.android.apps.imagedecoder&hl=fr

1.3. Supporting documents

The list of documents required varies across Schengen countries and depends on the purpose of travel, type of applicant, and the third country. They are provided in a paper format and kept at the consulate for a minimum of two years.[176]

The supporting documents to be submitted by applicants differ across the third countries held to visa requirements. The supporting documents required also depend on the type of applicant and the purpose of travel. The table below provides an overview of the main categories of supporting documents required together with a non-exhaustive list of examples of documents.

Table 61: Non-exhaustive list of supporting documents[177]

General requirements for all visa applicants		Specific requirements according to the purpose of travel	
Category	**Examples of documents required**	**Purpose**	**Examples of documents required**
Proof of intended transport	Round trip booking	**Business**	• Signed invitation from Schengen country company • Letter from employer
Proof of accommodation	• Voucher or booking from the hotel • Confirmation of stay on a campus • Confirmation of stay in medical institutions	**Tourism/private visit**	• Signed invitation • Copy of relevant documents proving the family relationship • Work confirmation letter from employer with indication of annual leave
Proof of solvency	• Bank statement (3 last months) • Salary slips (3 last months) • Certificate of real estate property	**Official mission**	• Note from the institution responsible • A *note verbale* from the Ministry of Foreign Affairs
Document to be provided by employee	Letter from the employer	**Medical treatment**	Official document of the receiving medical institution
Document to be provided by company owners	Original state certificate of state registration	**Education/training**	Certificate of enrolment at an education establishment
Document to be provided by students	Proof of enrolment in school or university	**Political, scientific, cultural, sport or religious event**	Signed invitation from the organising authority
Documents to be provided by minors	• Original birth certificate • Consent of the parental authority and/or legal guardian	**Airport transit**	• A valid entry permit for the country of destination • Proof of reservation of onward journey

As displayed above, the nature of the supporting documents varies. Some of the documents are provided by private third parties, such as banks and hotels, while others are issued by public entities, e.g. birth certificate, original state certificate of state registration. The nature, or origin, of the supporting documents needs to be taken into account when designing the options for dematerialising these.

The options for the submission of supporting documents are explained below. The options for this process are not mutually exclusive, and thus several of them could be combined.

During the second workshop, no consensus was found on which documents could be presented electronically and which on paper. It was pointed out that this depends significantly on three criteria namely, migration risk, profile, and nature of the document.

176 Article 37(3) of Visa Code.

177 This table is based on desk research, including the Annexes to the European Commission Implementing Decision establishing the list of supporting documents to be presented by visa applicants in Angola, Armenia, Azerbaijan, Cuba and Palestine, C(2015) 1585 final.

1.3.1. Option 3.1: Third party gateways

Two sub-options exist and are described below as hypothesis 1 and 2. During a workshop with experts, it was generally agreed that this option should not be discarded. It was seen as offering significant benefit for travel sponsors to simplify the process and increase trustworthiness. However, it was noted this would be hard to implement worldwide, as some countries would be more willing than others to provide this option.

Hypothesis 1

A possible digital option that could be embraced is the creation of third party gateways in the online application portal. This option would consist of gateways, i.e. channels directly connecting the portal (via a web service or an Application Programming Interface (API)) to third parties who are the source of the supporting documents.

In practical terms, the online application portal would display the supporting document that the applicant needs to provide, based on the applicant's to the initial questions, i.e. where are you from? Where are you travelling? What is the purpose of the travel? and their profile (minor, first-time applicant, not first-time applicant). The applicant would subsequently indicate the source to be contacted for each of the required supporting documents. The portal would afterwards launch a request directly to the third parties indicated, which would be required to provide the supporting document. This option would ensure that the document was directly issued by the source, ensuring the authenticity of the document uploaded and decreasing the risks of fraud.

The source to be reached out to would vary depending on the supporting document to be provided. Private entities would be contacted for some of the supporting documents, such as round trip booking, bank statements or hotel booking, while public entities would provide other types of document, such as birth certificates, proof of legal residence, marriage certificate, and certificate of state registration.

A certain number of Schengen countries suggested this option during national interviews, including Austria, Belgium, and France, as well as by two of the three visa application centres interviewed.

Hypothesis 2

Another subset of this option could be to prompt third parties to validate the supporting documents uploaded by the applicants. In this case, third parties would not be required to disclose any information but to validate the supporting document (OK/NOT OK answer). This option would be a hybrid between the option presented above and the one below.

1.3.2. Option 3.2: Submit electronic documents in an electronic format

Similar to the previous option presented above, the application portal will display the list of supporting documents to be provided based on the profile of the applicant. However, this option puts the burden on the applicants instead of on the third parties (as in the first option above). In this option, applicants would indeed be required to upload the electronic versions of the required supporting documents. This option would therefore not include scanned paper-based documents, as all the required documents would already be in an electronic format.

The uploading tool would include a quality assurance feature before submission. This feature would ensure the minimum quality level of documents based on a pre-determined list of configurable parameters, e.g. resolution, format size, readability index, too dark/too light.

Although this option aims to dematerialise the supporting documents as much as possible, some supporting documents would still need to be submitted in paper format. As indicated in the workshop and during national interviews, some supporting documents could be only checked in paper format. This is due to some of the features of the document, e.g. stamp, quality of the paper. This would apply in particular to public documents, such as birth certificates and marriages certificates. According to one of the interviewees at national level, this type of document would represent less than 5% of the supporting documents to be submitted as part of the visa application process.[178]

[178] National interview with Italian authorities.

In this option, consulates would in any case reserve their right to request the original supporting documents for thorough assessment.

1.3.3. Option 3.3: Submit paper-based document in an electronic format

This option would allow applicants to upload the required supporting documents electronically by scanning them. As in the previous options, the applicant would receive guidance on the supporting documents to be provided based on the person's profile and the purpose of the trip.

Once the documents were uploaded, the online application portal would perform a quality check to ensure the supporting documents were meeting some quality standards. For this purpose, some parameters would be configured in the online application portal, such as resolution, format size or readability index, too dark/too light.

As in the previous option, some supporting documents would still need to be submitted in paper format. As previously explained, this is due to the features of some documents, e.g. stamp, quality of the paper.

Likewise, consulates would in this option as well reserve their right to request the original supporting documents for thorough assessment.

1.3.4. Option 3.4: Provide documents at the consulate or visa application centre

This last option refers to the current situation. In this case, applicants provide the supporting documents in a paper-based format at the premises of the consulate or visa application centre. The consulate keeps a scanned copy of the supporting documents for a period of 2-3 years, while the originals are returned to the applicant at the end of the examination procedure.

1.4. Collect fingerprints

This section and the following one present the options for collecting fingerprints from visa-required third country nationals. Under the Visa Code, Schengen countries authorities are required to shall collect two types of biometric identifiers, i.e. 10 fingerprints and a digital facial image of the applicant taken live pursuant to the Visa Code as amended by the new VIS Regulation.

Both the collection of fingerprints and the collection of the facial image follow similar operational procedures and present similar challenges. Applicants normally submit both identifiers at the same time, i.e. when presenting themselves at the consulate or visa application centre. Moreover, the collection of both identifiers is subject to identical security standards, as Schengen countries authorities need both the fingerprints and the facial image for the same identification and verification purpose. However, there are also two key differences:

- First, current legislation requires all applicants, including non-first-time ones, to have their photograph scanned or taken at the time of the application. However, non-first-time applicants do not need to submit their fingerprints if they have done so in the previous 59 months and there is no doubt as to their identity. As a result, options for collection of fingerprints and of a facial image may differ for non-first-time applicants.
- Second, fingerprints and facial images are collected by using different types of equipment. This means that options may differ from a technological standpoint.

These are the reasons for presenting separate options for collecting biometric identifiers that are mutually exclusive. For collecting fingerprints, four options have been identified.

1.4.1. Option 4.1: Collect fingerprints from anywhere

The main purpose behind this option is to allow all applicants (including first-timers) to submit their fingerprints from any location with internet access, thereby exempting them from the obligation to present themselves at the consulate or at a visa application centre. It is the option that comes closest to a fully digitised visa application

process, as applicants would just need to connect to the internet – which in most cases they can do from home or by go to a nearby 'internet café'.

This option can be implemented using different technological solutions described below.

- The use of a mobile application for the scanning and submission of fingerprints: Applicants would use the touch sensitivity of a smartphone screen to scan each of their 10 fingerprints, save the scans, and then submit them as attachments in the online application portal.
- A tool embedded in the mobile version of the online application portal: When providing all the necessary information in the online application portal, the applicant would land on the page for submitting the fingerprints, then would scan and submit each of their fingerprints directly in the portal. This solution would rely on the same technology as the previous solution.
- Devices allowing fingerprint recognition are equipped with fingerprint readers, which are most commonly developed according to the interfaces of the Windows Biometric Framework (WBF)[179] to allow the identification of their users. This option would mean that applicants would be able to submit their applications from computers equipped with this technology. When landing on the page for submitting the fingerprints, they would be allowed to use their computer's fingerprint reader to scan and submit each fingerprint.

1.4.2. Option 4.2: Collect fingerprints in self-service kiosks

With this option, applicants would be required to provide their fingerprints in a secure and controlled environment: special kiosks. Such kiosks would consist of booths located in selected environments and equipped with technology for scanning fingerprints (as well as the facial image – this option will be covered again in the following paragraph on the collection of the facial image). Within this option, multiple Schengen countries could be allowed to reach agreements to share the same kiosks.

Such kiosks could be located in public administration offices of the third countries, such as the premises of municipal authorities, governmental agencies and immigration authorities. This would represent a compromise between accessibility – each third country could host more kiosks than consulates or visa application centres – and security – as kiosks would be used under the oversight of public officials. During the workshop, the suggestion was made that the use of kiosks supervised by duly authorised officials would be even more secure than the submission of fingerprints on the premises of visa application centres. This is because the presence of a duly authorised official would be seen as a higher guarantee of trustworthiness than is the case in the visa application centres – although the latter are constantly monitored by Schengen countries.[180]

Alternatively, kiosks could be located only on the premises of Schengen countries. In this case, however, it is very likely that the number of kiosk locations would not be greater than the number of current locations of consulates and visa application centres, because consulates are usually the only official representation of the Schengen countries in third countries.

Applicants could first log in to their application account; their fingerprints would be subsequently uploaded to their application dossier. In both cases, i.e. on Schengen country or third country premises, duly authorised officers of the Schengen country would supervise the submission of the fingerprints.

1.4.3. Option 4.3: Collect fingerprints with mobile kit

The scenario envisaged by this option would, on the one hand, enable applicants to submit their fingerprints as they are currently required to, i.e. on consulate/visa application centre premises. On the other hand, it would build on the status quo by offering an additional opportunity to third country nationals, especially those living a considerable distance away from the closest consular post or visa application centre.

[179] For an introduction to the WBF, see the following article: https://www.bayometric.com/windows-biometric-framework/.

[180] According to the input from an interview with the Belgian Ministry of Foreign Affairs, Schengen countries authorities cannot easily verify whether the visa application centre complies with its obligation to erase all data collected from the applicant when submitting the application.

Two different models of mobile collection of biometrics – fingerprints and facial image – are currently in place: a government-managed model (public) and a private model (managed by visa application centres).

Of the Schengen countries interviewed, Belgium is the only one to have adopted a government-based model for mobile collection of biometrics. The Belgian Ministry of Foreign Affairs offers Chinese citizens the possibility of enrolling their biometric identifiers by addressing themselves to special missions deployed once every two weeks in certain regions of the country. Such missions work as follows: a representative from a Belgian consulate in China and a representative from the visa application centre contracting with Belgium reach a remote area of China and enable third country nationals to submit their biometrics via a mobile enrolment kit. In this way, third country nationals do not need to travel to the closest consulate/visa application centre for submitting their biometric identifiers.

In the private model, the major visa application centres around the world provide a mobile biometrics enrolment service as part of their so called "added-value services", i.e. optional services provided on top of the basic visa application services against a service fee surcharge. From interviews with TLSContact and VFSGlobal, it was understood that individual applicants or groups of applicants can ask to use this service at any location of their choice (even at their homes), as long as the visa application centres cover that particular region. Visa application centres do not offer mobile biometrics enrolment services in all third countries in which they operate. In certain regions subject to high seasonality peaks, visa application centres also open temporary visa application centres (so called 'pop-up' centres).[181]

Both models –public and private– could be considered; they are not mutually exclusive.

1.4.4. Option 4.4: Collect fingerprints at the consulate or visa application centre

This option would not change the current situation in any way. First-time applicants, and applicants whose fingerprints have expired, would still need to present themselves at the premises of the responsible consulate or visa application centre to submit their fingerprints in person.

1.5. Collect other biometric identifiers

This section identifies the following five options for collecting facial images.

1.5.1. Option 5.1: Collect facial images from anywhere

This option shares the purpose of option 1 for the collection of fingerprints (see above), i.e. it is designed to exempt applicants from travelling to the consulate or visa application centre. The different nature of the biometric identifier, however, calls for different technological solutions. The following solutions have been identified.

- The use of a digital camera complying with minimum quality standards, e.g. megapixel and image processing capabilities.
- The use of mobile applications specifically designed for the remote collection of pictures. Amongst the solutions available on the market, image capture and verification software developed by WorldReach appears to merit particular attention.[182] Amongst the possibilities offered by WorldReach is an application that links the travel document to a facial image taken live. The applicant would scan the photo in their travel document, then take an extremely short (ca. 4 microseconds) video of his/her face to avert any risk of fraud (the software would check the changing light effects to verify authenticity). The result of the video is a digital image of the applicant's face. The software would then compare the two images to verify the two identities. There are already some findings available with regard to this option.

    — The Home Office of the United Kingdom is the world's first public authority to deploy a technology allowing for remote capture of the facial image from certain categories of applicants. Since 2018, the

[181] Input from the interview with VFSGlobal.

[182] Worldreach is a private company based in Ontario, Canada, which offers remote identity and document verification solutions. The official website of Worldreach displays the solutions available on the market: https://worldreach.com/.

Home Office has allowed applicants eligible for the EU Settlement Scheme[183] to verify their identity remotely using the solution provided by Worldreach. However, at the time of writing, the Home Office is not currently planning to extend this option to other categories of foreign citizens and/or travel authorisations. Therefore, the remote enrolment of the facial image is only allowed for a category of persons presenting an extremely low risk of security and illegal immigration, i.e. EU citizens.

— Interviews with border officials revealed that certain third countries allow the remote submission of the facial image by third country nationals applying for a national visa. This is the case for Iran and Cambodia. These countries exempt applicants from appearing physically in consulates or visa application centres, and allow them to scan a digital photo fulfilling certain requirements, e.g. in terms of size, dimensions, colours, positioning, etc.[184] However, research would be needed, if ever possible, to ascertain whether the security and immigration standards applied by the Iranian and Cambodian authorities are comparable to those applied by the Schengen countries.

1.5.2. Option 5.2: Collect facial images from self-service kiosks

This option is not to be understood in isolation from the same option outlined above for the collection of fingerprints. Indeed, to maximise efficiency, self-service kiosks should enable applicants to submit both biometric identifiers during the same visit, while being supervised by a duly authorised official. For that purpose, it is essential that they be equipped with the appropriate technology for scanning fingerprints and taking a digital image of the required quality.

1.5.3. Option 5.3: Collect facial images at the premises of certified service providers

In this option, applicants could avoid travelling to the location of consulates/visa application centres and turn to duly certified third parties operating in the business of professional photography. During an interview with national authorities, it was pointed out that Iran has introduced this option in their official visa application procedure. Iranian authorities do not require visa applicants to consult a certified photographer, but strongly recommend that they do so in order to avoid receipt of poor quality facial images.[185]

With this option, the process of identification is conceptually similar to the typical identification process occurring at the premises of visa application centres, inasmuch as the staff of a private third party would collect the facial image in both cases. The public authority link would therefore be weaker than in the self-service kiosk option, because no duly authorised official would supervise the collection of the facial image. It remains to be seen, therefore, whether the Schengen countries would be willing to entrust a new category of third parties with the collection of these biometric identifiers. Visa application centres that are responsible for the collection of biometrics employ duly trained staff and are constantly liable to the outsourcing Schengen country. The question of whether professional photographers can offer the same degree of trustworthiness and reliability would probably affect the feasibility of this option.

The operational process for submitting the facial image also affects security. If applicants were allowed to collect the file with the digital image and subsequently submit it on their own, Schengen countries authorities would not be sure whether the submitted file contains the actual digital image taken at the photo service provider and whether it has been uploaded by the true applicant. To avert this risk, the photo service provider could be required to submit the file immediately after the collection of the image by letting the applicant access their online application account.

[183] The EU Settlement Scheme is a programme targeting EU citizens currently enjoying free movement rights in the UK. With the UK set to withdraw from the EU in 2019, these citizens will have to apply to the EU Settlement Scheme in order to keep living and working in the UK after 30 June 2021. Official information on who should apply and how can be found at: https://www.gov.uk/settled-status-eu-citizens-families.

[184] Official information with regard to Iran can be found at: https://evisatraveller.mfa.ir/en/request/image_tools/. Official information with regard to Cambodia can be found at: https://www.cambodiaimmigration.org/faq/what-are-the-required-documents-for-cambodia-e-visa.

[185] Official information about the recommendation to use professional photo service providers can be found at: https://evisatraveller.mfa.ir/en/request/digital_image_requirement/?title_name=photo.

1.5.4. Option 5.4: Collect facial images with a mobile kit

This option should be understood together with the equivalent option outlined above with regard to the collection of fingerprints. Third country nationals could enrol their facial image, together with their fingerprints, at the locations of the missions deployed by the Schengen countries and/or by visa application centres.

1.5.5. Option 5.5: Collect facial images at the consulate or visa application centre

This option refers to the current situation. All required applicants would still need to present themselves to the premises of a consulate or visa application centre to enrol their facial image.

1.6. Declaring that data are accurate and complete

This section identifies the following five options to enable applicants to declare that data provided in the application form along with the supporting documents are correct, complete and reliable.

1.6.1. Option 6.1: Smart implicit declaration

With this option, there is no longer any need to collect the applicant's signature as the applicant's submission and the payment of the fee implicitly confirm the applicant's declaration. This option was retrieved from the group discussion held by the Visa Working Party[186] on the electronic signature of the online visa application. Moreover, it was found that this option is already in place in some Schengen countries. As emerged during the national interview with the Consulate of Norway in Manila (Philippines), the following procedure has been in use: after submitting the visa application and paying the visa fee through the online IT tool, applicants receive a receipt, which states that the application has been successfully lodged and that the applicant declares that the data provided during the process are accurate and complete. In order to collect the biometrics directly in a visa application centre, applicants need to print and deliver the receipt but without requiring any signature. However, in order to align with the Visa Code,[187] this procedure is no longer carried out.

1.6.2. Option 6.2: Advanced digital declaration

This option provides applicants with the ability to declare the correctness and completeness of the data submitted through a certified electronic signature. Currently, there are several solutions on the market offering these services. Examples include DocuSign[188] and Adobe Fill & Sign.[189] However, these require applicants to be able to provide their signature through a touch screen computer or a smartphone.

1.6.3. Option 6.3: Basic digital declaration

Under the latest developments in the preparation of ETIAS[190] and in accordance with Article 17(1) of Regulation (EU) 2018/1240[191], before submitting the application form, it is mandatory for the applicant to tick the appropriate box(es) to declare that the data they have submitted are authentic, complete, correct and reliable to the best of their knowledge. The tick box additionally serves the purpose of confirming that the applicant has understood the conditions for entry referred to in Article 6 of Regulation (EU) 2016/399 and that they may be requested to provide the relevant supporting document at each entry and that the statements made by them are accurate and reliable.

---

186 Visa Working Party – e-visa: Improving the current visa process with online visa application 12546/17 (Brussels, 3 October 2017).
187 Article 11(1), Visa Code.
188 See: https://play.google.com/store/apps/details?id=com.docusign.ink&hl=en_AU
189 See: https://play.google.com/store/apps/details?id=com.adobe.fas&hl=en_AU
190 Draft Implementing Act laying down the requirements on the format of personal data to be inserted in the application form as well as on the parameters and the verifications to be implemented in order to ensure the completeness of the application and coherence of the data, pursuant to Article 17(9) of ETIAS Regulation.
191 Article 17(1), ETIAS Regulation.

1.6.4. Option 6.4: Facial recognition declaration

This option was raised during the workshop held on 28 March 2019. The scenario envisaged by this option would rely on a facial recognition feature embedded in certain personal computers or smartphones. Thus, like option 2, implementation would require applicants to acquire specific equipment.

1.6.5. Option 6.5: Paper-based signature

In the current paper-based visa application process, the applicant is requested to provide a physical signature by writing in the appropriate signature field provided at the end of the application form submission.

1.7. Pay the visa fee

Paying the visa fee is a crucial mandatory step in the visa application process. This section presents the options identified for this process step. The experts during workshop two highlighted the need for different payment methods to be available, including euro and in local currency. Furthermore, the discussions revealed that there are many differences between Schengen countries. For example, Norway obliges applicants to pay digitally in all third countries (with an adoption rate of 98%).

1.7.1. Option 7.1: Central gateway, single account

Once the visa application form has been uploaded together with the required supporting documents, and the biometrics enrolled (if applicable), the visa applicants will be invited to pay the visa application fee. At this point, the system will display some technical measures (such as Captchas or Honeypots) to prevent any non-human action against the system. Subsequently, applicants will be redirected to a payment gateway operated by a bank or financial intermediary for payment of the travel authorisation fee. The applicant will subsequently be invited to enter data relevant for the processing of the payment. If the applicant is visa fee-exempt, they will not be redirected to such a gateway.

In this option, the payments are collected in a single bank account held at EU level. All visa fees are collected in this central account, and refunds are taken from it. After a predetermined amount of time, the visa fees would be distributed to the appropriate Schengen countries. The experts during workshop two stressed that fees received through the central payment gateway should be split fairly, and that each Schengen country should receive a similar amount of fees to what they do currently.

1.7.2. Option 7.2: Central gateway, multiple accounts

This option is equivalent to the previous option in the sense that an applicant will be redirected to a single payment gateway, regardless of what country the person is applying to. The difference is that instead of channelling all visa fees to a central account, the gateway automatically redirects the fees to the appropriate Schengen country's account.

1.7.3. Option 7.3: Multiple payment gateways

After discussions with a number of experts (through workshops), a possible option could consist of slightly changing the first option presented above. Instead of redirecting the applicant to the gateway payment, the portal would redirect the applicant to the national payment websites (of the Schengen country responsible for the examination form). This would leave the Schengen countries in control of the payment of the visa application fees.

During a workshop conducted with representatives of Schengen countries, this option was considered burdensome, as it would require every Schengen country to set up its own payment gateway.

1.7.4. Option 7.4: Pay the visa fee at the consulate or visa application centre

This option refers to the current situation. Currently, different payment options are available for the applicant depending on the IT solution offered by each of the Schengen countries. Four countries (Bulgaria, France, Norway and Sweden) have included an electronic payment method as a feature in their solution, while Italy is currently working on an online payment tool. However, the most common method of payment is still cash, as borne out by the interviews with national bodies, the interviews with visa application centres and the workshops.

1.8. Interact with applicant: Appointment tool

This feature allows applicants to book an online appointment to provide the biometrics, supporting documents or other specific information required at the premises of the consulate or to book an interview when responsible authorities wish to check the third country national in person. Each Schengen country has to develop their own appointment management tool.

1.8.1. Option 8.1: Fully centralised appointment management

This option was discarded after workshop two, because of the major effort needed to tweak the portal to all the needs of the Schengen countries. Furthermore, it would require identity and access management tools to ensure a secure account service for each consulate.

1.8.2. Option 8.2: Redirection to national/ESP appointment tools

Generally, the experts from the Schengen countries preferred this option, as it seemed to have less impact on the current way of working. Furthermore, the need for appointments differs very much between Schengen countries. In some consulates, no appointment is needed at all because of the very low number of visa requests. The Schengen countries felt that integration of the national appointment tools and the online application portal could nevertheless potentially be a cumbersome exercise. This because of the very high number of appointment tools within each Schengen country.

1.9. Interact with applicant: visa checking tool

This feature allows applicants to check the status of the application and consult information about the issued visa.

1.9.1. Option 9.1: Fully centralised visa status checking tool

This option was generally well received by the Schengen country experts. Some experts pointed out, however, that not much information can be given during the examination process except from “registered or processed”. Nevertheless, the benefit of a traveller being able to view the validity period of their travel document was valued, the more so because of the potential abolition of the paper visa.

1.10. Interact with applicant: notification tool

This feature makes it possible to inform applicants of the main milestones of the full visa process by means of an electronic notification. Applicants may receive different types of notifications such as a reminder of the scheduled appointment, notification of the visa issuance decision (without containing the outcome) and notification of the expiry date of the biometrics provided.

1.10.1. Option 10.1: Fully centralised notification tool

This option was generally well received by the Schengen country experts. It was pointed out that the use of text messages or email would be preferable to the tool. The experts also highlighted the fact that the notification of the decision on the examination should not contain the outcome of the decision. This is because it might have implications for the deadline for appealing (which occurs through the visa status checking tool).

Annex F. Options analysis for digital visa

This Annex presents options for digitalising the paper-based format of the Schengen visa sticker. First, the Annex outlines the rationale for abolishing the visa sticker by explaining the downsides of issuing visa holders with a sticker. Then, it proposes an option, i.e. a digital visa, which no longer entails a paper-based visa sticker. Subsequently, the Annex develops the implications of this option and the synergies that can be attained with other EU and non-EU experiences. For an analysis on the implications and the possible synergies of the options presented in this Annex, please refer to Annex H.

1.1. Challenges of the visa sticker and the digital visa

The visa sticker is an official paper document issued by the consulate after the decision to grant a visa to the applicant. It displays important information and data about the visa and the traveller.[192] The sticker is currently a mandatory item linking the visa application process and the visa verification process. As such, the sticker's life cycle involves all the stakeholders with a role to play in Schengen visa processing. This section presents the challenges a paper-based visa sticker entails, both during the pre-travel and during the travel phases.

1.1.1. Challenges caused by the visa sticker

The table below provides an overview of the challenges arising from the visa sticker during both the pre-travel and the travel phases.

Table 62: Challenges of the visa sticker per stakeholder

Stakeholder	Challenge
Applicant/visa holder	• Needs to come back to consulate/visa application centre to collect travel document with sticker affixed; • Has reduced mobility while application is being examined; • Spends time at the border to allow authorities to check the sticker and the biometrics (in an ideal situation.).
Consulates	• Need to deploy personnel to fill in and affix stickers (low added-value activities); • Incur costs for storing stickers securely.
Schengen countries	• Incur costs for procuring the sticker production service and paying the sticker manufacturing company; • Incur costs for transporting stickers to the consulates securely; • Incur costs paying consulate staff and maintaining sticker filling in (personalisation) equipment.
Schengen border authorities	Risk being inclined to check only the sticker (against counterfeiting and forgery) at the border without carrying out biometric verification vs VIS (and, if applicable, national systems)

1.2. The option: the digital visa

The digital visa setting outlined in Section 3 would help tackling the above-mentioned challenges and would also make borders more secure for the following reasons.

- First, border control authorities would be forced to rely on the traveller's biometrics, as the sticker would be abolished. As a result, the verification rate of biometric identifiers against VIS will arguably rise dramatically.
- Second, the interoperability package bringing together the current and future information systems for border management will enable authorities to have access to all the necessary data for carrying out the verification and – if needed – identification of the third country nationals.

[192] Pursuant to Annex VII of the Visa Code, the sticker displays information about; the type of visa issued, i.e. airport transit visa, long-stay visa, or Schengen visa; the period of validity and duration of the visa, i.e. the number of days during which the holder may stay in the territory, including the first and last day of validity; the territorial validity of the visa, i.e. whether it is valid in the whole Schengen Area or just in certain countries; the place and date of issuance; the number of the travel document to which the sticker has been affixed; name, surname and personal data about the visa holder.

- Third, the Schengen countries would exploit the potential of digital visas for ensuring the application of the conditions that justified the visa issuance thanks to the synergy with the EES for detecting overstayers.

This paragraph presents the option for a digital visa and explains the rationale behind the three points above.

After the submission of the application, the consulate and/or the competent authority of the Schengen country would carry out the risk assessment and examination of the application. If the applicant poses no risks, then the authorities would take the decision to issue a visa and notify that decision to the applicant.[193]

Consulates would not issue a visa sticker. They would simply send a visa issuance notification, including a secure verification code, to the email (either via a mobile application that can use the email address as a means to confirm the user's identity or an email account accessible from different devices (laptop, tablet, smartphone, etc.)) or to the online application account of the third country national.

A traveller web service would need to be built in the event that no online application option is selected and the digital visa is implemented on its own. The traveller web service would enable provision of automatic notifications (and possibly barcodes) to third country nationals by using a read-only link to VIS. The visa holder would then travel with their travel document.

The authorities responsible for checks at the Schengen external borders and within the territory of the Schengen Area would, as is today already the case, use, the travel document and biometric identifiers to query VIS for verification purposes. In other words, border guards would adopt the same procedures that are mandatory at present to verify that the biometric data stored in VIS belong to the person who is about to cross the border.

Prior to the third country national's boarding, carriers would use the travel document to query the read-only database through the carrier gateway, as provided for in Article 45b of the future VIS Regulation. Carriers would read an "OK" answer in case the information on the third country national's travel document match all the data stored in the read-only database, i.e. the data extracted from VIS. On the contrary, they would receive a "NOT OK" answer if the third country national does not hold a valid visa or a mismatch is detected. Finally, certain third parties, e.g. accommodation service providers, financial institutions or employers, may be authorised, or required by domestic law, to check whether a third country national holds a valid visa. Those third parties would use one of the offline fallback solutions envisaged below to do that.

If the third country national happens to lose their travel document, the competent authorities could verify their identity via their biometrics in VIS, as well as whether the person is in possession of a valid visa.

In association with the digital visa, the Commission and the Schengen countries may deem an offline fallback solution necessary for the reasons and in the light of the factors described in the next section.

1.2.1. The need for an offline fallback solution?

The proposed option for verifying the visa relies on the 24/7 availability of the central systems/databases, i.e. VIS and the carrier gateway, including the architecture behind them. However, there are reason why one of the systems involved might not be accessible that are explained in what follows.

Central VIS downtime

As highlighted in Section 3 above, the central VIS database may run into a Schengen-wide downtime period for technical reasons, although it is an extremely unlikely event thanks to the usual VIS availability rates (see Table 9 above).

Moreover, the VIS architecture is built in such a way as to keep unavailability risks to a minimum. Should the VIS database not be accessible due to a technical issue involving the primary data centre, a backup data centre would become operational, ensuring full access to the VIS database. Currently, the switching process from the primary to the secondary server takes approximately 20 minutes. eu-LISA is already working towards an active-active configuration of the data centre, which would guarantee 24/7 availability. Therefore, in the future scenario, access

[193] The authorities would also notify the applicant in the event the visa applied for has been rejected.

to VIS would be ensured continuously with no switching period. It would only be technically impossible to access VIS because of a VIS-specific failure only if both data centres experienced technical problems at the same time. This is an extremely unlikely event.

Lack of Internet connection.

VIS might, of course, be operating normally, but the source of the technical impossibility of accessing VIS might come from the local area network (which is not an area of responsibility of eu-LISA). Consequently, central authorities need to guarantee that there is no network downtime (redundancy of lines, increased bandwidth, etc.)

Nevertheless, a wide variety of technical problems may leave a particular area disconnected from the internet. This may affect both the Schengen Area and outside. In the Schengen Area, the network may be off in a major airport or seaport as well as in a (remote) land region, either along the external border or inside the territory. Interviews conducted with Schengen country authorities confirmed the need to take into account the risk of border crossing points and immigration authorities being unable to connect to VIS. Nevertheless, this risk will arguably become less and less likely over time.

If the failure is outside the Schengen Area, the network may fail in an airport or seaport in a third country. This may be a slightly more likely risk, as many of the visa-required third countries still have a long way to go before full internet coverage. Some of them may not be using the most reliable technology to ensure continued connectivity.

Arguably, the impact of network failure in the third country on border security would be lower than the impact of a network failure at the Schengen border. Despite a network failure in the country of departure, i.e. if carriers do not manage to verify the traveller's visa via the carrier gateway prior to departure, the traveller would still be checked upon arrival at a Schengen border crossing point. It is extremely unlikely that both the third country and the Schengen border crossing point would be experiencing lack of connectivity.

These two reasons nevertheless justify the need for an offline fallback solution to the digital visa.

In addition, the abolition of the sticker would have an impact on third country authorities. Certain Schengen countries have signed bilateral agreements with a number of third countries providing for the latter's authorities to perform checks, possibly helped out by Schengen liaison officers. To this end, third country authorities could in theory be provided with a third country gateway accessible in the same way and providing the same information, i.e. an "OK/NOT OK" answer, as the carrier gateway. However, although the technology would allow this, a less disruptive solution for third country authorities should be provided for in the short term.

The same goes for Schengen police authorities within the Schengen Area. Although they could be equipped with mobile devices for connecting to VIS directly, the context in which they operate requires a handier and less complex solution. The use cases for third country and Schengen police authorities lead to reconsideration of the scope and purpose the offline fallback solution: whilst being a strictly exceptional measure for carriers and border control authorities, it would become the customary mode of verification for third country and Schengen police authorities.

1.2.2. Criteria to design the offline fallback solution to verify the visa

The impossibility of reaching VIS, and the policy and operational context of third country authorities and Schengen police authorities, are the reason why this study suggests endorsing a digital visa solution with a fallback procedure enabling offline verification. This would be to the benefit of the authorities and the Schengen Area as a whole, but also of third country nationals, who would be able to prove they hold a valid visa in any circumstances.

The question that arises at this point is what would be nature of such offline fallback solution. Its technical configuration is crucial in the light of the security as well as budgetary implications for the Schengen countries. A number of criteria have been identified that the design of such solution should take into account. The criteria are:

1. user-friendliness,
2. likelihood of VIS unreachability,
3. legal validity in exceptional circumstances,
4. undesirability of a "new sticker".

User-friendliness

The offline fallback solution should be easy to use for all the stakeholders involved. First, third country nationals, including internet-illiterate ones, should be able to easily acquire and use the offline proof. They should not be required to spend any significant amount of money and/or time to that effect. Second, the offline solution should keep to a minimum the need for training required for border control authorities.

Likelihood of VIS being unreachable

The technical infrastructure and the investment behind the offline fallback solution need to be commensurate to its actual benefits. Put differently, a careful assessment should be made of how often carriers and/or authorities would need to resort to an offline tool for verifying visas due to the impossibility of reaching VIS.

It is known that VIS-specific failures are extremely rare and should become less and less frequent thanks to technical improvements.

As to a lack of an internet connection in a region inside the Schengen Area, police authorities can overcome this issue by checking the third country national in an area connected to the internet,[194] or by providing his/her data to the authority's headquarters (whose staff would normally be able to connect to VIS). However, this would only enable verification based on the travel document number, and not on the third country national's biometric data. Only by verifying the person's identity on the spot through VIS would this be possible. In that regard, Article 19 of the VIS Regulation provides that duly authorised authorities shall have access to VIS through the visa sticker number[195] *in combination* with the person's fingerprints. Similar considerations would apply to border checks. Moreover, Schengen border authorities would also need access to VIS for verification purposes, as provided for by Article 20 of the VIS Regulation.

Legal validity in exceptional circumstances

With the abolition of the sticker, biometric verification in VIS would become the primary and legally binding procedure for checking the traveller's eligibility to cross the Schengen border. This would need to be reflected in law. By the same token, the law should clearly state that the offline fallback solution for verifying visas could be used as a valid proof only in exceptional circumstances, i.e. when it is technically impossible to access the data stored in VIS.

Undesirability of a "new sticker"

An appropriate technical configuration of the offline fallback solution should nonetheless complement any such legal obligations on the Schengen authorities.

The offline fallback solution clearly should not replicate the same security and immigration challenges that arise from the use of the visa sticker and the way it is checked in practice. This is a likely risk of an offline tool for verifying visas. The sticker-related challenges explained at the beginning of this section are largely attributable to the fact that the sticker is a tool that does not enable biometric verification, but offers a satisfactory degree of reliability and security. Therefore, border officers may be inclined to rely solely on it.

It follows that any offline fallback solution designed to back up the digital visa in case of technical failure should not defeat the purpose of abolishing the sticker by replicating its weaknesses. In order to achieve this, it may be advisable for any offline fallback solution to be designed to carry very limited security features with a view to discouraging border control authorities from clearing third country nationals merely after checking their offline proof. The legal constraint may not be enough in the light of the above-mentioned statistic on the percentage of visas checked in VIS at the border (around 50%). The design of the offline fallback solution should therefore reinforce – and not weaken – the compliance-inducing effect of the digital visa on border control authorities with respect to their obligation to check the traveller's biometric identifiers.

[194] For example, by transferring the third country national to an area with internet access and then checking him/her on the spot, or by reaching the police headquarters along with the third country national. The legal authority to take such actions may depend on the domestic law of each Member State.

[195] Not to be considered in a digital visa scenario.

The above considerations may therefore lead to an offline fallback solution purposely designed *not to be* as reliable as the sticker currently is (and, of course, way less reliable than biometric verification). In turn, this requirement would justify just a limited amount of investment by the Schengen countries in the development of the offline solution. There would be no state-of-the-art security feature requiring costly commitments.

On the other hand, the above reasoning may be at odds with the need to fulfil the objectives of the VIS Regulation. Article 2[196] states that the purpose of VIS is, *inter alia*, to facilitate and strengthen checks at the border and within the Schengen Area; to assist in the identification of illegally staying third country nationals; and to contribute to preventing threats to the security of the Schengen Area, including by detecting and investigating terrorism or other serious criminal offences.

An offline fallback solution designed according to the above principles would certainly not offer the same guarantees as the digital visa. The VIS and the whole Schengen border management system might not be able to achieve these objectives to the same standards if they were to allow a downgrade of the verification mechanism, albeit in exceptional circumstances and for an arguably extremely limited number of third country nationals.

The sections below outline the three offline fallback solutions profiled in this study.

1.2.3. Offline fallback solution – option C1: visa issuance notification

Option C1 would consist of the notification sent by the consulate to the third country national to confirm the issuance of the visa. The notification would display the following information:

1. the number of the notification / visa reference number (replacing the visa sticker number);
2. the name and surname of the visa holder;
3. a "valid for" heading, indicating the territory in which the visa holder is entitled to travel;
4. a "from - to" heading, indicating the period of validity of the visa;
5. a "number of entries" heading, indicating how many times the visa holder is entitled to cross the Schengen border with the visa;
6. a "duration of visit" heading, indicating the maximum number of days allowed per visit;
7. the date and place of issuance of the visa;
8. the number of the passport with which the visa is linked;
9. the type of visa using letters A and C;
10. the Schengen country and the authority issuing the visa;
11. the mandatory or national entries of the issuing Schengen country or other information about the visa holder, e.g. whether the person is a member of the family of a EU citizen, a minor, etc.;
12. the facial image of the visa holder;

Visa holders would be entitled to show the notification to carriers, third country authorities and Schengen authorities. Visa holders would be free to decide whether to print out the notification or show it on the screen of their mobile device/tablet, as long as the information is readable.

1.2.4. Offline fallback solution – option C2: non-signed barcode

Option C2 would consist of the visa issuance notification plus a barcode generated by the consulate. Even if a barcode would be harder to falsify compared to the mere visa issuance notification, the EBCGA and eu-LISA confirmed that, in the current state of technology, it is rather easy to counterfeit a non-protected barcode.[197] Therefore, even if the notification were sent over a secure email address, the message would contain no safeguards to prevent fraud or counterfeiting.

The carriers, third country authorities and Schengen authorities would read the notification, verify the information contained therein, and verify the official markings. If the information were embedded in a barcode, all these stakeholders would need to use barcode readers and/or a specific application on appropriate smartphones to

[196] Article 2 of the Proposal for a Regulation amending the VIS Regulation, as amended by the European Parliament
[197] Interviews held with the EBCGA and eu-LISA.

verify the information on visas. In the latter case, they would use the same technology currently used by certain consulates to read the data provided by visa applicants in their applications.[198]

Nothing would prevent carriers or authorities from carrying out additional checks in case of doubt, for instance by calling their headquarters or (in the case of carriers and third country authorities) seeking support from Schengen officers.

1.2.5. Offline fallback solution – option C3: digitally signed barcode

Option C3 would still rely on the notification sent by the consulate, but would consist of a secure 2D barcode automatically generated by a software solution embedded in the issuing country's national system and signed digitally by the designated central authority of the issuing Schengen country. In addition to the information that would be included in the simple barcode, the digitally signed 2D barcode could also host the traveller's facial image. The inclusion of the facial image is likely to increase the size of the barcode.[199] However, the barcode is supposed to be shown on a screen or on a common piece of paper. Therefore, the barcode size should not be regarded as a meaningful limitation.

Therefore, the digitally signed barcode would be more secure than the simple notification/barcode for two reasons.

- First, it would be way less prone to forgery and counterfeiting. It is indeed easier to counterfeit a simple barcode than an official cryptographic key;
- Second, it would enable the stakeholders involved in the visa verification to have access to the traveller's biometric information.

It is true it would not be possible to verify any such biometric information against any database. Nevertheless, it would be an additional verification feature at the disposal of carriers and authorities. (For instance, they could manually check the digital facial image against the traveller standing in front of them).

It is worth mentioning that option C3 may rely on the results of ongoing discussions between European Commission and representatives from the Schengen countries within the Article 6 Committee with regard to a barcode to be printed on the visa sticker.[200] The barcode will include the same data and information currently provided by the sticker, and is supposed to mark a transition from the current sticker-based verification towards the use of the barcode without a sticker.

The digital visa option proposed here goes a step further because it does not rely on any physical support to verify the traveller's identity in ordinary circumstances, i.e. when VIS is reachable. Conversely, the option C3 offline fallback solution would closely resemble the barcode conceived by DG HOME. It is worth stressing that Schengen countries could use the infrastructure currently in place for authenticating and digitally signing passports to digitally sign such a barcode, with no need for new and costly technical arrangements.[201]

The Schengen countries would rely on the results of the automated checks of application data against the EU systems during the examination phase. If no grounds for refusal were found, the visa information currently printed only on the sticker by consulate staff would be encoded in a barcode by the national system, digitally signed by the central authorities, and sent over to the consulate to print it on the sticker.

From an operational point of view, the implementation of such option would require Schengen border and police authorities to be equipped with smartphones and mobile applications to read the barcodes. Most Schengen countries already do or will soon issue such smartphones for ordinary checks to their respective authorities. The requisite mobile applications are publicly available on the mobile application market: German authorities are currently using SealVer to read refugee arrival documents.

198 For instance, Italian, German and Estonian consulates use this system. Germany uses a solution offered by Videx: official guidance and information can be found at https://videx.diplo.de/videx/desktop/index.html

199 Interviews with DG HOME B.2 officials.

200 To that end, the Commission has recently approved a new regulation on the standard format of the visa sticker. The new sticker, which is currently being purchased by certain Member States, includes a place for hosting a barcode.

201 Interviews with DG HOME B.2 officials.

Annex G. Implications and synergies of the proposed options for the digital application

1.1. Online visa application

1.1.1. Implications

The first and most important outcome of the online application portal would be an important increase in the number of 'first-time-right' applications, i.e. travellers getting their application right the first time they submit it, including the country they are applying to, the type of visa they are requesting and the supporting documentation they are submitting.

Consulates

Consulates (and visa application centres) will save a significant amount of resources by eliminating paper applications. Estimates of time gained from lower error rates in applications and reduced examination times are as high as 80-95% for Norway[202] and the UK. Consular officers will spend the time on more value-added tasks screening risk-weighted applications and interviewing high-risk applicants. In addition, and although more significant in the supporting documents, consulates will no longer need to transport and store the visa application forms hence reducing relevant expenditure.

Next, a unique digital visa portal will standardise the visa practices across Schengen countries' consulates based on data-driven algorithms that translate the common visa policy into checks and alerts.

Schengen countries

Schengen countries' administrations will be able to ensure standardised visa practices and reduce variances in local practices across consulates in the same Schengen country due to the implementation of a common online portal, hence increasing their control over visa policy.

The interactive data-driven algorithms of the online application will make it possible to adapt traveller queries based on the answers provided in the portal and also enable the behaviour of travellers to be checked, hence activating a behind-the-scenes risk analysis. It will make it possible to detect fraudulent applications more easily and faster. It is worth noting, that this advanced feature of checking the behaviour of the traveller would be more technically complex than only personalising the questions in the online application according to applicants' answers.

By lowering the complexity and raising the quality of service of the visa application process, Schengen countries are likely to attract even more travellers.

Applicants

Travellers will save time and money as they would no longer need to travel to a consulate or a visa application centre to submit a paper application. They will also save time from an intuitive, straightforward visa application guided by personalised queries, and appropriate instructions and alerts, to get the application the 'first-time-right'.

[202] Retrieved from the national interview with the consulate of Norway in Manila.

All applicants must be in a position submit an online application. Similar to what is stated in recital 18[203] on the ETIAS Regulation, "it should be possible for travellers to authorise commercial intermediaries to create and submit an application on their behalf", in order to tackle technology illiteracy or lack of access to technology in some emerging countries or remote locations.

1.1.2. Synergies

Public Website and Mobile App (ETIAS)

- Objective: Enable an individual to submit the travel authorisation application form, to pay the travel authorisation fee and to make use of the secure account service to upload additional information.
- Features: The public website and mobile app provide general information, an online application form, a verification tool and consent tool, the rights of data subjects and period of data storage, a list of FAQs, a request for support option for third country nationals and a form allowing reports of abuses by commercial intermediaries.
- Specifications

    — The public website and mobile app shall enable the applicants to provide:

        - The data required in the application form;
        - To pay the travel authorisation fee;

    — The website and mobile app shall make the application form widely available and easily accessible free of charge;
    — Accessible to persons with disabilities;
    — Available in all the official languages of the Schengen countries;
    — A step-by-step guide to the application shall be made available;
    — Inform applicants of the languages which may be used when filling in the application form;
    — Provide the applicant with a secure account to load and store data or documentation;
    — Inform applicants of their right to an appeal if their travel authorisation has been refused, revoked or annulled;
    — Enable applicants to indicate if the purpose of their intended stay relates to humanitarian grounds or international obligations.

1.2. Travel document

1.2.1. Implications

The implications of this option would be as follows.

Consulates (and visa application centres)

In this option, consulates would not be required to manually examine the travel document of the applicants, thus leading to a cost saving in terms of time. In this case, consulates will receive the scanned copy of the biographic page, which will be uploaded to VIS.

For the other types of applicants, consulates will also receive a scanned copy of the biographic page to be uploaded to VIS. Subsequently, consulates will be required to make a manual examination of the travel document. This would entail the same workload as in the current situation.

[203] Recital 2 of ETIAS Regulation.

Applicants

This option will mean considerable cost savings for the applicant. The application process is expensive and cumbersome for the applicant, particularly taking into account the time and resources spent in making personal appearances at the consulate. This option ensures certain third country nationals, i.e. those having received a visa in the past 59 months, and thus whose biometrics are still valid, and whose travel document has not been renewed, do not need to travel to a consulate or VAC.

In addition, this option would also enable applicants to keep their travel document while a decision is made on their application. The mobility of applicants will not therefore be restricted during the examination process, as they would have their travel document with them.

For the other types of applicants, this option brings in some minor changes in comparison with the current situation. In this case, applicants will be required to provide the information about their travel document and verify the MRZ code produced by the system, as well as providing a scanned copy of the biographic page of their travel document. The physical submission of the travel document would still be required for security reasons.

1.2.2. Synergies

This combined solution is to be implemented in ETIAS where applicants have two choices.

1) Provide their travel document number, together with additional information (nationality, date of birth, sex, expiry date of passport). Based on the information provided, the system will automatically produce a MRZ code that the applicants will need to verify and amend if necessary. This verification and amendment step is key, as not all the countries follow ICAO standards and recommendations (particularly in relation to the transliterations recommended for use by states) to create the code;
2) Take a photograph to the travel document' MRZ code in order to automatically fill in the personal fields of the application form. Based on the data presented on the screen, the applicant needs to verify and amend the information if necessary.

The solution of filling in the information in the travel document is currently implemented in some third countries, i.e. non-Schengen countries, such as Australia, Canada and the United Kingdom, where applicants are not required to physically provide their travel document.

1.3. Supporting documents

1.3.1. Implications

This option has the following implications:

Consulates

This option would bring efficiency gains in the examination process. Consulate staff would assess the supporting documents in an electronic format, reducing the time required for their assessment. For example, Norway has managed to decrease the verification process from 10 minutes on average to 2 minutes thanks to the dematerialisation of the documents. Besides, data analytics techniques can be applied to verify the authenticity of the documents provided. However, consulate staff might suffer of screen fatigue when assessing the documents in an electronic format.

This combination of options would also contribute to a considerable reduction in the real estate necessary for the storage of the applications and supporting documents. In addition to the storage capacity, it would considerably decrease the tasks relating to the management of the application form and supporting documents, i.e. receipt of the paper-based application dossier, scanning if necessary, classification, archiving, and destruction. The consulate could therefore allocate their resources to other, more critical, tasks.

Applicants

In this option, applicants would still need to provide either the required supporting documents (electronically or paper-based depending on the nature of the document) or the third party to contact. Applicants might still be required to provide the original supporting document if so requested by the consulate. However, it is likely that the application process would be shorter, as the examination process is expected to be faster, as indicated above.

Third parties

Third parties would take part in the visa application process by providing the requested supporting documents or by validating (OK/NOT OK) the validity and authenticity of the supporting documents. However, this would entail costs for them without a real incentive on their part to provide the documents requested.

Others

This option would have a positive impact on the environment, as it would help to reduce the environmental footprint.

1.3.2. Synergies

If required, it is mandatory for ETIAS applicants to submit additional information or documentation pursuant to Article 27 of the ETIAS Regulation. The submission of this additional information or documentation has to be via the secure account service.

Based on the latest draft of the Delegated Act[204], ETIAS applicants can submit the information or documentation via the secure account service in three formats:

- Portable Document Format (PDF);
- Joint Photographic Experts Group (JPEG);
- Portable Network Graphics (PNG).

The possibility of submitting documents electronically for a visa application is already in place in some third countries such as China, India, Russia, and Turkey[205].

1.4. Collecting biometrics

1.4.1. Implications

The current policy and regulatory landscape does not allow of implementation of such an option for visa-required third country nationals whose biometrics are not recorded in VIS.

These concepts are elaborated on below together with an outline of the implications for the most digital biometric enrolment options.

Consulates

Consular authorities and/or ESPs would lose the chance to meet the applicant in person and oversee the collection of biometrics. The presence of the applicant on the spot is necessary for consulates/ESPs to conduct the identity triangulation.[206] For the time being, the UK experience confirms such a conclusion, because the biometric enrolment

[204] Commission Delegated Decision (EU) .../... of 26.2.2019 on the definition of the requirements of the secure account service pursuant to Article 6(4) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, enabling applicants to provide any additional information or documentation required; https://ec.europa.eu/transparency/regdoc/rep/3/2019/EN/C-2019-1695-F1-EN-MAIN-PART-1.PDF.

[205] As indicated by the participants at the workshop of 28 March 2019.

[206] Input from strategic interviews, national interviews and workshop.

described above is only available to EU citizens, i.e. low-risk individuals whose travel documents – and the biometrics embedded therein – are considered trustworthy. The same does not go for visa-required individuals, who carry a much higher migration risk. The biometric matching enabled by the software mentioned above would not provide the same guarantees as the obligation for first-time applicants to appear in person in front of visa officers/ESP employees.

Consulates would also be required to collect biometrics when those provided by the applicant do not meet the quality standards.

Schengen countries

As this option would make the application process for visa-required third country nationals smoother, an increase in Schengen visa applications is expected. This is without prejudice to Article 24(2)(c) of the Visa Code as amended by the European Parliament. This Article makes it mandatory for the Schengen countries to issue multiple-entry visas to applicants who can prove their reliability and the need to travel frequently to the Schengen Area. This will, of course, relieve many of these applicants from applying for new single-entry visas. Nonetheless, digital biometric enrolment will arguably make it easier for many third country nationals to apply for a visa for the first time. Therefore, it is likely that more travellers would be granted a visa, and thus travel to the Schengen Area, contributing positively to the national economies of the countries visited. Schengen countries would also need to rely less on local headcount and real estate, i.e. consulates and visa application centres, for the collection of biometrics. Schengen countries' authorities would, however, incur the costs of outsourcing the facial image capture service to a private company, such as Worldreach.

Visa application centres

The role of visa application centres in the collection of biometrics would be drastically reduced.

Border control authorities

The compliance of the facial image with the required technical specifications will have a great impact on the border control and immigration authorities of the Schengen countries in the light of the EES Regulation and as of the entry into force of the new VIS Regulation. This is because, first, the new VIS Regulation provides that the digital facial image of the visa holder shall be used to launch a search in VIS to verify the identity of third country nationals whose fingerprints cannot be used.[207] Second, the facial image is amongst the data that border control authorities will use to verify the identity of third country nationals arriving at the Schengen external border. With the transition from the photograph to a digital, biometric facial image, it is of utmost importance that the facial image taken at the moment of application comply with the required technical specifications in order for it to be used for the purpose of biometric verification in VIS and the EES.

Applicants

Applicants would save time and money as they would no longer need to visit a consulate or visa application centre to submit their biometrics. The technological implications are that applicants would need to use a mobile device and/or a personal computer, or to turn to a third party that can provide them with such a device, in order to provide their fingerprints and facial image complying with the quality standards and requirements. Applicants may be in possession of appropriate devices, but unable to use them properly for submitting fingerprints in accordance to the required security and quality standards. This challenge would place a burden on Schengen countries – that would need to require new fingerprints – and for the applicant, who would need to carry out the process of fingerprint enrolment again.

[207] Article 18(6) of the Proposal for a Regulation amending the VIS Regulation.

In the light of the implications explained above, the digital option for biometric enrolment produces certain benefits (therefore the option should be explored), but is at odds with the current requirements of Schengen visa policy. Therefore, it is suggested that Schengen countries maintain the status quo for the time being.

After submitting their applications online, required applicants need to present themselves at the premises of the consulate or at a visa application centre to carry out the biometric enrolment, that is, submit their fingerprints and a facial image. In this option, the biometric enrolment is a supervised process in which duly authorised staff make sure that the applicant's biometric identifiers are linked to their travel document. By requiring applicants to submit their biometrics in person, consulate authorities ensure, by supervising the whole process in real time, that the person who in fact applies corresponds to the one owning the travel document and the biometric identifiers (identification).

The option described above is complemented by an additional solution: biometric enrolment via mobile kits. The Schengen countries authorise personnel from the consulates and/or visa application centres to organise missions throughout the territory of third countries.[208] Applicants can therefore book an appointment and enrol their biometrics in a temporary location much closer to their home than the consulate or visa application centre are. The mobile biometric enrolment would still be a supervised process ensuring the identification safeguards explained above.

1.4.2. Synergies

No synergies with ETIAS can be envisaged, since ETIAS does not require applicants to enrol their biometrics. Nor can any synergies with the EES be envisaged, as the EES will affect the verification phase.[209]

However, existing technologies and existing practices in countries such as the UK can be reused to implement the proposed option.

1.5. Declaring that data are accurate and complete

1.5.1. Implications

The implications of this option would be the following:

Consulates (and visa application centres)

Consulates will no longer require a printed and signed paper application, hence saving significant time and costs.

Schengen countries

Schengen countries' administrations will adopt a standardised and consistent method for applicants' declarations.

Applicants

Travellers will save time and money as they will no longer need to travel to a consulate or visa application centre to fill out and submit the signed paper-based application form. It is worth noting that currently the filling-in and submission of the signed application form could be done in one single journey. However, for those who now apply directly through an existing national online tool, the Visa Code still requires them to print out and travel to the consulate or visa application centre to provide the paper-based signature.

[208] Belgium is piloting mobile biometric enrolment in China and will soon do so in India. During interviews it was observed that, TLSContact and VFSGlobal currently offer a similar service (so-called 'added-value' service) to applicants willing to pay a higher service fee.

[209] It should be recalled that No synergies can be envisaged for options to collect biometrics. This is without prejudice to the fact that consulates will be required to automatically query EES from VIS when running checks on the biometrics are collected.

1.5.2. Synergies

The tick-box solution is being implemented in some Schengen countries online application national systems such as Visa-France.

Tick-Box (ETIAS)

In accordance with the latest developments in the preparation of ETIAS[210] and Article 17(1) of Regulation (EU) 2018/1240,[211] before submitting the application form, applicants are required to tick the appropriate box(es) to declare that the data they have submitted are authentic, complete, correct and reliable to the best of their knowledge. In addition to this main purpose, the tick box is also a declaration that:

- the applicant has understood the conditions for entry referred to in Article 6 of Regulation (EU) 2016/399 including the possibility of being requested to provide the relevant supporting document at each entry;
- the statements made by the applicant are accurate and reliable.

1.6. Paying the visa fee

1.6.1. Implications

The implications of this option are as follows:

Consulates (or visa application centres)

This option entails a bank or financial intermediary being in charge of the online payment. This would imply that the consulate staff (or the visa application centres) would no longer deal with the payment of the visa fees. The accounting process would therefore be centralised at national level, enabling a reduction in staff at the consulate level, while reducing the risks associated with to cash payments (which are still being made in some locations).

When a visa application centre lodges the applications on behalf of an applicant or a group of applicants, the visa application centre will pay the visa fee on behalf of the applicants as happens at present.

Schengen countries

The authority responsible for the state's financial receipts would receive the corresponding visa fees via the EU visa application portal (the frequency would still have to be defined), and not the consulates as in the current situation.

Applicants

Applicants would be required to proceed to pay the visa fee via a payment interface. However, there is a limited potential risk that applicants might not have the means (technological or other[212]) to make an electronic payment.

1.6.2. Synergies

In the ETIAS framework, a payment service provider domain, i.e. external to the ETIAS Central System, will be designed to allow the payment of the fee. This entails a bank or financial intermediary providing the payment service, i.e. the payment processing of the travel authorisation fees.

---

[210] Draft Implementing Act laying down the requirements on the format of personal data to be inserted in the application form as well as on the parameters and the verifications to be implemented in order to ensure the completeness of the application and coherence of the data, pursuant to Article 17(9) of ETIAS Regulation.

[211] Article 17(1), ETIAS Regulation.

[212] For example, not all applicants might have the financial means to have a credit card or meet the bank's conditions for obtaining a credit card. According to the interviews conducted, this is a quite frequent situation in India.

For security reasons, some payment methods have been discarded under ETIAS (such as bank transfer, direct debit, gift cards or vouchers, money order or bank draft, cash and cheque), and the only payment methods provided will be major credit card networks (such as Visa, MasterCard, American Express).

In order to submit their application, ETIAS applicants will be required to pay the travel authorisation fee. For this purpose, they will be redirected from the ETIAS website to the payment service provider domain.

The same approach could be reused for the payment of the visa fees. The same technical requirements and solution established for ETIAS could be adopted for visas.

Annex H. Implications and synergies of the proposed options for the digital visa

1.1. Digital visa

1.1.1. Implications

Consulates

Consulates would be free to reallocate staff and resources to tasks other than filling in and affixing the sticker unless national visas were still based on a paper sticker. After issuance of the visa, consulates would also have to send the applicant a notification, including the offline proof (whether it includes a list of information/barcode, or a digitally signed 2D barcode) to be carried throughout the travel and the stay in the Schengen Area and to be verified in the above-mentioned exceptional circumstances.

Border control authorities

With VIS being regularly reachable, border control authorities would not run the risk of letting in visa holders whose sticker has been falsified, as the digital visa structurally prevents the risk of falsification. In fact, the implementation of the EES will already allow border control authorities to query VIS for identity verification purposes without using the visa sticker.

With a simple notification with a non-signed barcode (option C2), border control authorities would also have a stronger incentive to query VIS than is the case today. This is because currently border officers, disregarding their obligations under the VIS Regulation, may trust the security inherent in the sticker and trust their ability to recognise counterfeited stickers. Conversely, a printout or a simple barcode would be items that border officers are not used to checking and that offer almost no safeguards compared to the sticker. It is therefore likely that border control authorities will increase their compliance rate with regard to their obligation to verify biometrics in VIS.

On the other hand, such a solution would force Schengen authorities to rely on easily falsifiable evidence in the event of it being technically impossible to access VIS. The viability of this solution should therefore take this risk into account, especially considering that it is the responsibility of the Schengen countries (and not of the visa verification proof) to ensure that border control authorities comply with their obligation to check VIS.

With a secure offline solution (such as option C2), border control authorities would still have to deal with a novel verification tool, of which they would not have much knowledge or experience. However, there is a risk that border control authorities would start trusting a very secure offline solution as an alternative to querying VIS every time. Therefore, a very secure offline solution might replicate the same challenges raised by the paper-based sticker.

From the technical equipment standpoint, all authorities at the external borders and within the territory would need to be equipped with mobile and/or fixed devices capable of connecting to VIS for verification purposes. However, as far as border checks are concerned, this requirement would not be the novelty of any possible digital visa Regulation, as border crossing points are already being equipped with such devices with a view to implementing the EES Regulation and the VIS Regulation.

Finally, there is an important implication relating to the security and immigration risk for the Schengen Area if it is technically impossible to access VIS. Consulates send third country nationals the notification at the time of issuance and the information included in it cannot be changed afterwards. Therefore, the question arises as to how to verify whether the status of the issued visa has changed, due to revocation or annulment, between the issuance and the arrival at the border/stay in the territory.

National authorities do update VIS data to reflect the revocation or annulment of the visa. They also notify third country nationals accordingly, usually by registered post. However, in a situation where it was technically impossible to access VIS, carriers and authorities would not be in a position to know about revocation or annulment based on the initial notification sent to the third country national upon issuance. Moreover, arguably, the security of the Schengen Area cannot rely on the good faith of third country nationals showing the revocation/annulment notification.[213]

Therefore, a security gap might arise insofar as the authorities could not guarantee that travellers checked offline still have a valid visa when leaving the third country and crossing the Schengen external border/staying on the Schengen territory. Nonetheless, the risk of such event is extremely low. Indeed, it would only occur if a third country national whose visa has been revoked or annulled crosses the Schengen border when VIS is not reachable, i.e. two extremely unlikely events would need to occur simultaneously.[214] Moreover, as border officers always have access to the most updated VIS database, the risk would even be confined to the event of the revocation or annulment being registered in VIS only *after* the border crossing point becomes unable to access the VIS database.

Schengen countries

Depending on the chosen offline solution, the central authorities of Schengen countries would need to allocate resources and make investments to equip border control and immigration authorities with the technology and tools for verifying visas offline. Depending on the technical solution for allowing offline verification of the visa, this option might have substantial budgetary implications for Schengen countries.

If the Schengen countries select option C2 as the offline fallback solution, they would need to invest between EUR 1.1-1.9 million (Schengen Area-wide) – see chapter 4 and Annex A for more information. Schengen countries should allocate public money to equip the authorities with barcode readers and/or appropriate smartphones. However, the use of appropriate smartphones across Schengen country authorities is already widespread and the Schengen countries may be incentivised to issue more devices following any introduction of the barcode as a result of discussion in the Article 6 Committee.

If the Schengen countries select option C3 as the offline fallback solution (digitally signed barcode), then higher investments will be necessary to extend and upgrade the Schengen countries' current PKI, i.e. between EUR 3 million and EUR 6 million Schengen Area-wide – see chapter 4 and Annex A. Border guards, police authorities and, if relevant, third parties would simply use an appropriate smartphone and application that is able to recognise the digital seal and read the content of the barcode.

Carriers

In ordinary circumstances, carriers would have access to minimum information on visa holders by connecting to the read-only database through the carrier gateway. This would require investments on the carriers' side in order to adapt their IT systems and train their personnel, although they are probably carrying out such changes at the present time in order to adapt to ETIAS and EES requirements. From the security standpoint, the verification of the entry conditions by carriers would be more secure thanks to the carrier gateway, because the "OK/NOT OK" answer would come directly from data extracted from VIS.

However, in the event of it being technically impossible to access VIS, carriers would have to rely on the offline solution, thereby facing a similar risk as the authorities with regard to revoked or annulled visas. However, this risk may have a different time dimension in the case of carriers. Indeed, carriers are able to carry out the verification only through the "OK/NOT OK" answer that relies on minimum data extracted from VIS. This has two implications.

a) First, given that the systems for carriers, i.e. the read-only database and the gateway, are separate from VIS, carriers will not necessarily be affected by any VIS downtime event. If VIS is unavailable due to technical reasons, carriers will still be able to obtain information from the most recent and updated version of the read-only database.

[213] Third country nationals may not have access to their email address and may therefore not even be aware of the revocation.

[214] The probability is described with more precision after collecting data on the number of visas revoked and annulled over the last few years.

b) Second, nonetheless, Article 45b of the new VIS Regulation provides that the read-only database should contain data extracted *daily* from VIS. If that means that there will be one data extraction from VIS per day, then the carriers will be able to rely on less updated data than the authorities will. Therefore, the answers provided to the carriers would miss any revocation or annulment occurring after the last update of the read-only database.

At a closer look, this second point applies to the ordinary scenario with no technical problems whatsoever. Indeed, it is not necessary that the carrier gateway or VIS be unreachable for the carrier gateway to be unable to spot the revoked/annulled visa (through a "NOT OK" answer). If the whole infrastructure works perfectly, but the revocation/annulment occur after the last update of the read-only database, carriers will still receive an incorrect answer when checking the traveller.

As already mentioned above, it has to be kept in mind that the likelihood of such an event is extremely low, and in any event, the Schengen border authorities will be responsible for carrying out identity checks, thereby detecting the revocation/annulment. Nevertheless, in such a case the traveller may be wrongfully allowed to board and reach the Schengen Area. This may have legal repercussions for carriers, which may incur penalties for failing to fulfil their obligations to check whether the traveller was authorised to cross the Schengen external border.

Visa holders

In ordinary circumstances, visa holders would save time during identity checks at the border. Border control authorities would no longer physically inspect the sticker, and would just need to query VIS, i.e. there would be one step fewer compared to the current verification process. Processing time at the border could decrease even more if the necessary checks against VIS were handled through e-gates. For example, the EasyPASS Automated Border Control (ABC) system operated at the Frankfurt airport in Germany needs on average 18 seconds to verify an incoming traveller (and just one second is necessary for the e-gate to run checks in the databases).[215] More time may be needed for the border guards to ask travel-related questions to the third country national – a practice that strengthens the verification of the entry conditions of visa-required travellers.

Visa holders would also save time and travel costs because they would no longer need to go back to the consulate/visa application centre to collect their travel document after the issuance of the visa. This also means that applicants would enjoy greater mobility during the examination phase, as they would be able to keep and use their travel document to travel elsewhere while waiting for a decision.

In the event of it being technically impossible to verify identity through VIS or the gateway, thanks to the offline solution (whether the basic or digitally signed one), visa holders would be able to show carriers and authorities proof that they hold a valid visa.

1.1.2. Synergies

This section presents the existing and envisaged technical components enabling synergies with the digital visa option. First, the digital visa would rely on the web service for carriers and on the EES verification process, which will allow border authorities to retrieve VIS data from the EES based on the traveller's travel document. Second, the digital visa would reuse the carrier gateway initially conceived for visas and provided for in the ETIAS Regulation.

Web Service for Carriers (EES)

- Objective: The web service should enable carriers to verify whether third country nationals holding a Schengen short-stay visa issued for one or two entries have already used the number of entries authorised by their visa; and, as provided for in the new VIS Regulation, to have access to information concerning multiple-entry visas as well.
- Features:

[215] See the Federal Office for Information Security of Germany – Automated Border Control based on (ICAO compliant) eMRTDs, 2012, p. 6., available at: https://www.nist.gov/sites/default/files/documents/2016/11/30/107_emrtd.pdf. Interviews with border control authorities of the Schengen countries confirmed that the current processing time at the border ranges from 15 to 20 seconds, in addition to the time needed to carry out the interview.

  - The web service is to provide carriers with an 'OK/NOT OK' answer.
  - The web service is to make use of a separate read only database updated on a daily basis via a one-way extraction of the minimum necessary subset of EES and VIS data.

- Specifications:

  - The carriers are to provide the following data:

    - surname (family name);
    - first name or names (given names);
    - date of birth;
    - nationality or nationalities;
    - gender;
    - the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents;
    - the date of expiry of the validity of the travel document or documents.

Carrier Gateway (ETIAS)

- Objective: Enable carriers to check the validity of a travel authorisation.
- Features:

  - The carrier gateway uses a separate read-only database updated on a daily basis via a one-way extraction of the minimum necessary subset of data stored in ETIAS.
  - The carrier gateway must check who is accessing ETIAS on behalf of the carrier.

- Specifications:

  - Carriers provide the data contained in the machine-readable zone of the travel document and indicate the Schengen country of entry.
  - The carrier gateway is to provide an 'OK/NOT OK' answer indicating whether the person has a valid travel authorisation.

System interoperability for verification (EES)

With the EES up and running, the visa sticker for verification purposes will already become less relevant. This is because authorities at all border crossing points will be able to verify visas by accessing VIS information from the EES.

Annex I. Business process architecture

This Annex presents the current Schengen visa application process as well as the digital journey envisioned for the three relevant steps of the visa processing: apply for a visa, examine visa application and verify visa. Moreover, this section displays, for the digital journey, the detailed process and data workflow for each of the three main steps.

1.1. Current Schengen visa application process

1.1.1. Apply for a visa

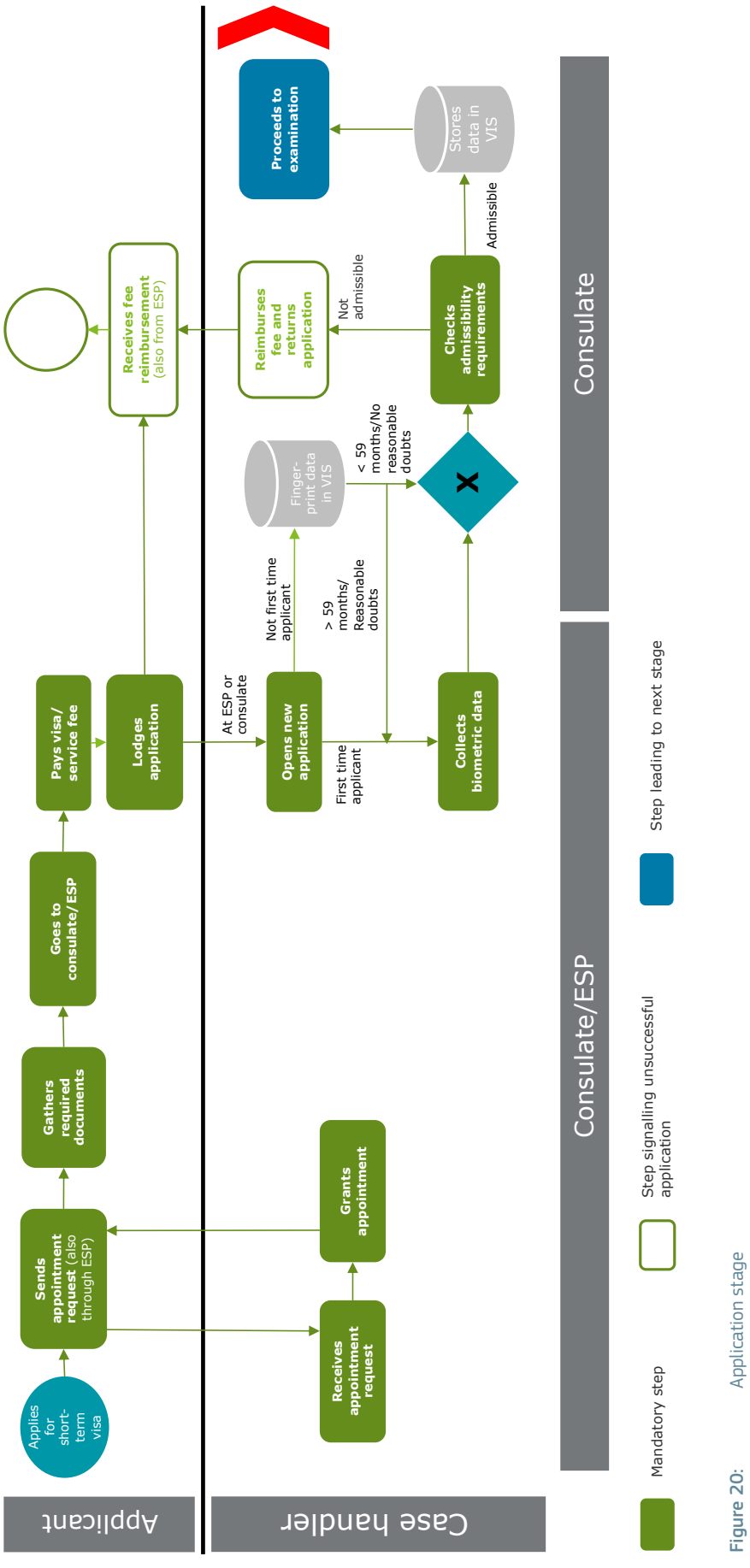

Figure 20: Application stage

1.1.2. Examine visa application

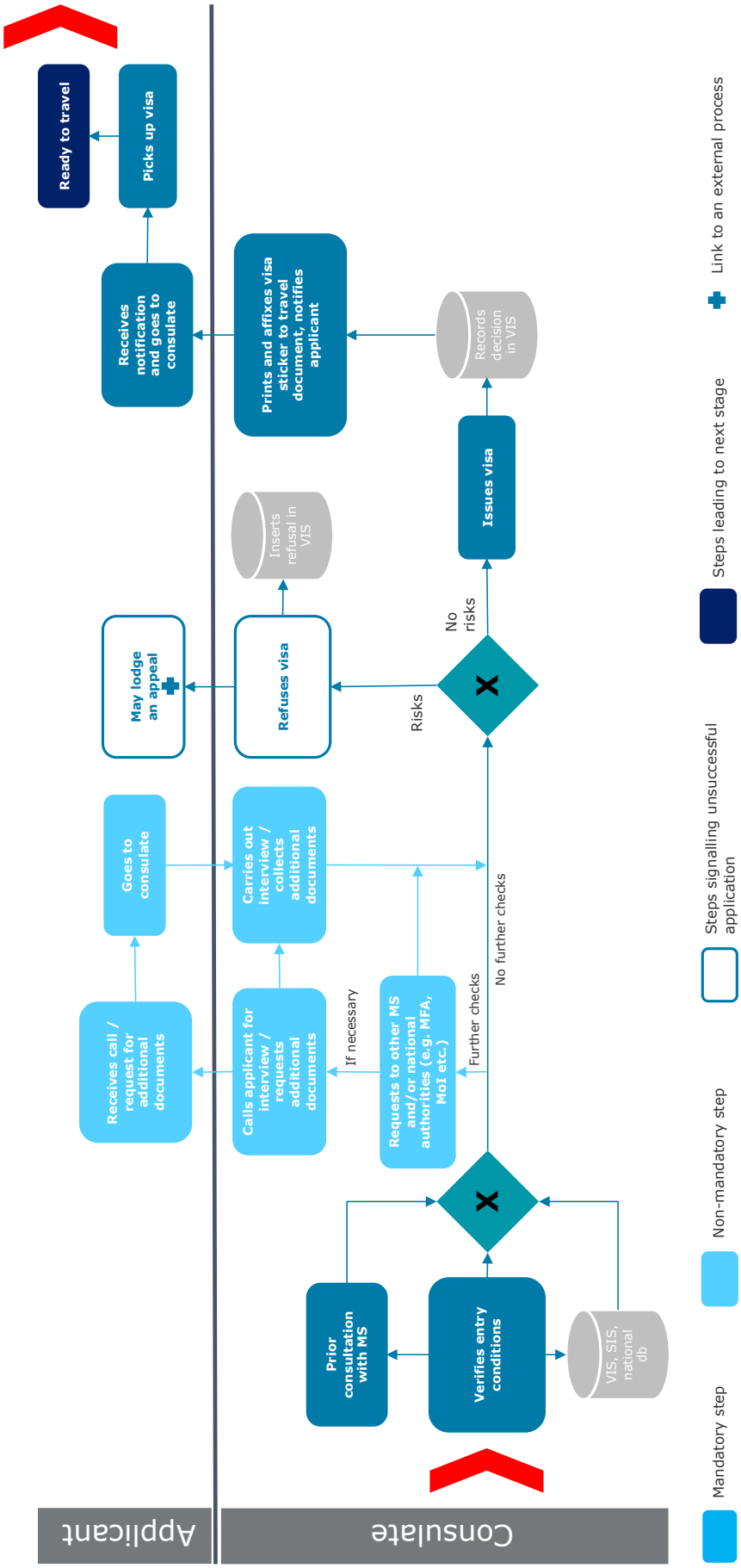

Figure 21: Examination stage

1.1.3. Verify visa

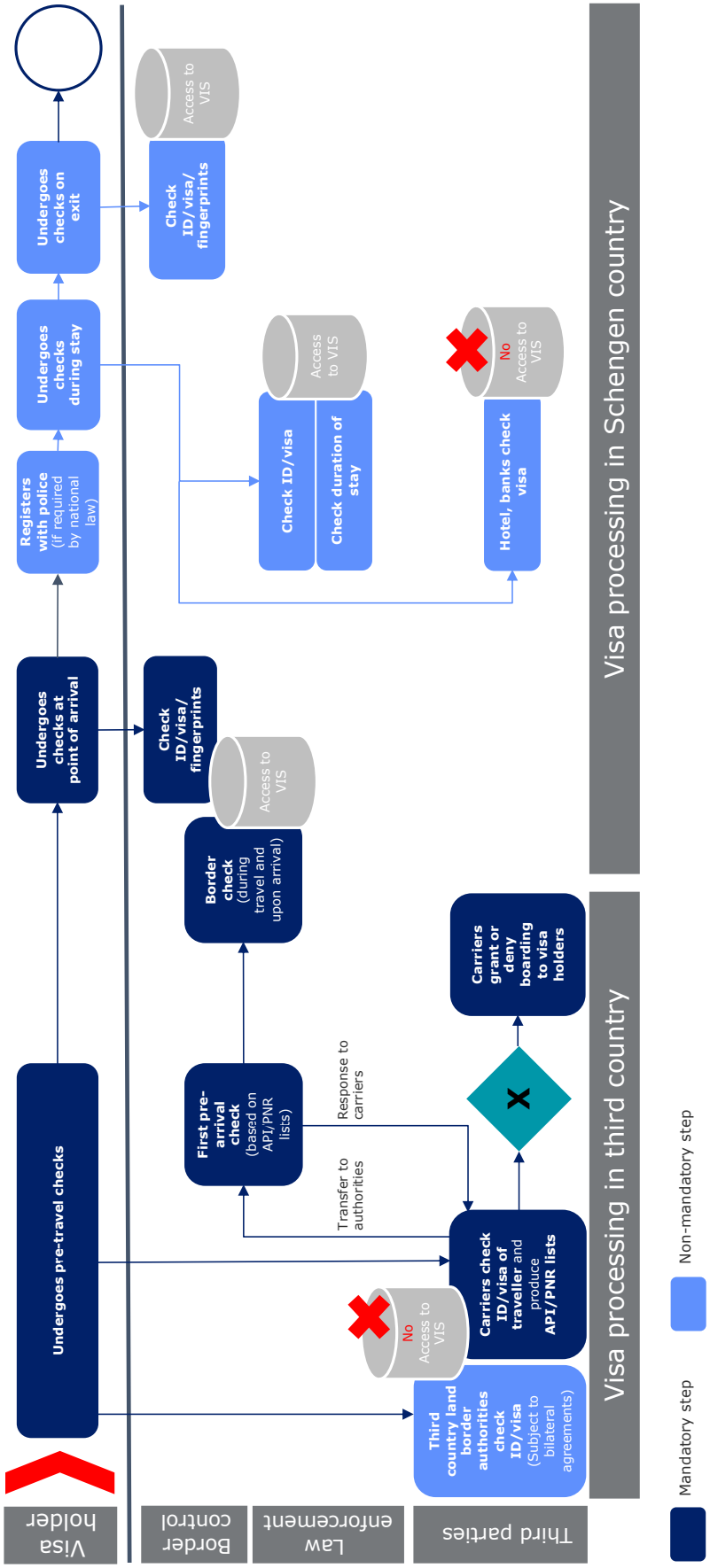

Figure 22: Visa verification before and after entering the Schengen Area

1.2. Digital visa journey and its associated processes

1.2.1. Apply for a visa

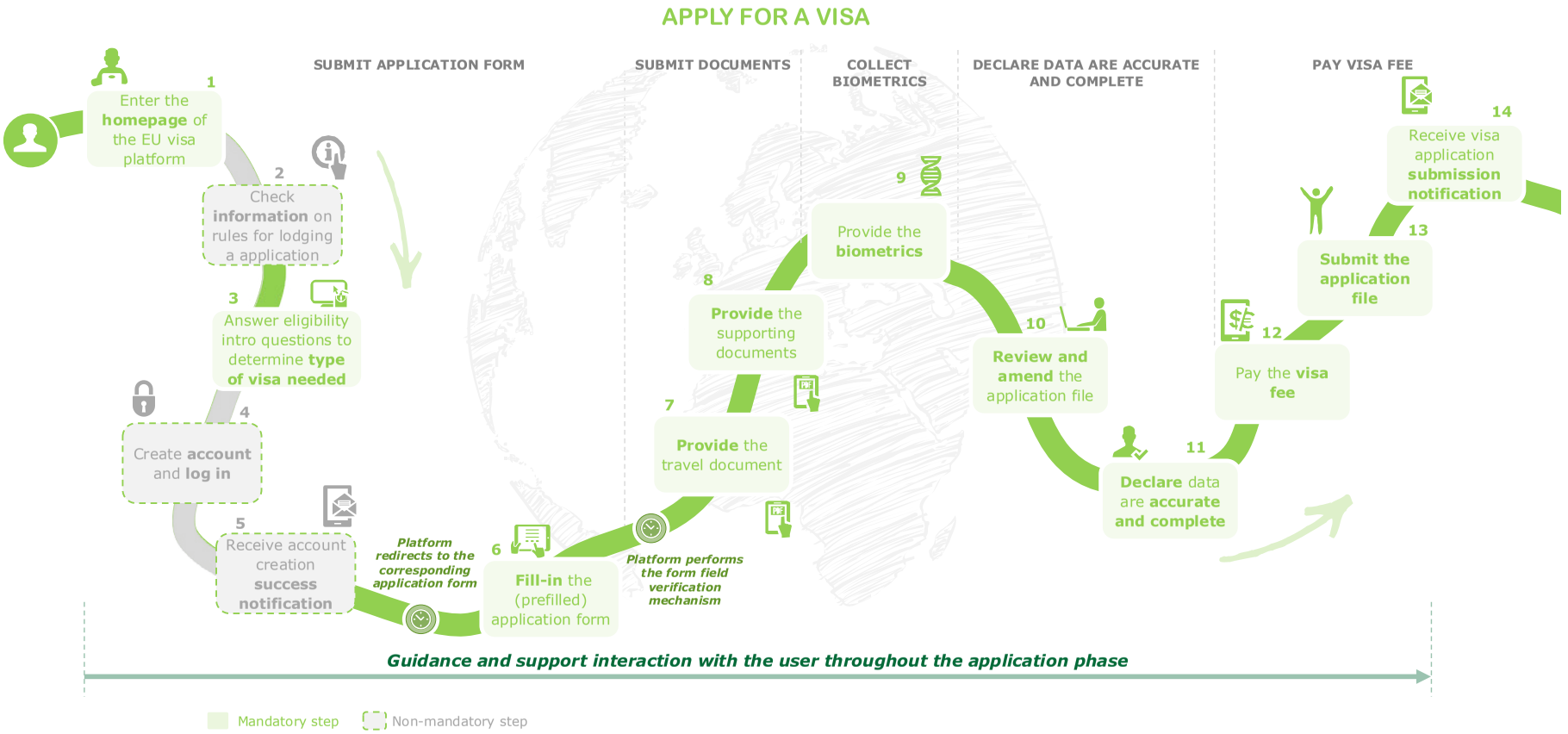

Figure 23: Visa application digital journey

During the online visa application, the system automatically performs the admissibility by analysing the requirements and uniqueness of an application. If the system detects an inconsistency or error in a certain application file, a message is sent to the visa officer listing the inconsistencies and sending a correction request to the applicant via the application system. If the applicant performs the correction, the system again performs the admissibility check, but if the application remains inadmissible, the reimbursement process is activated and the file is closed. In addition, the case worker also carries out a confirmation of the admissibility of the application file during the examination process.

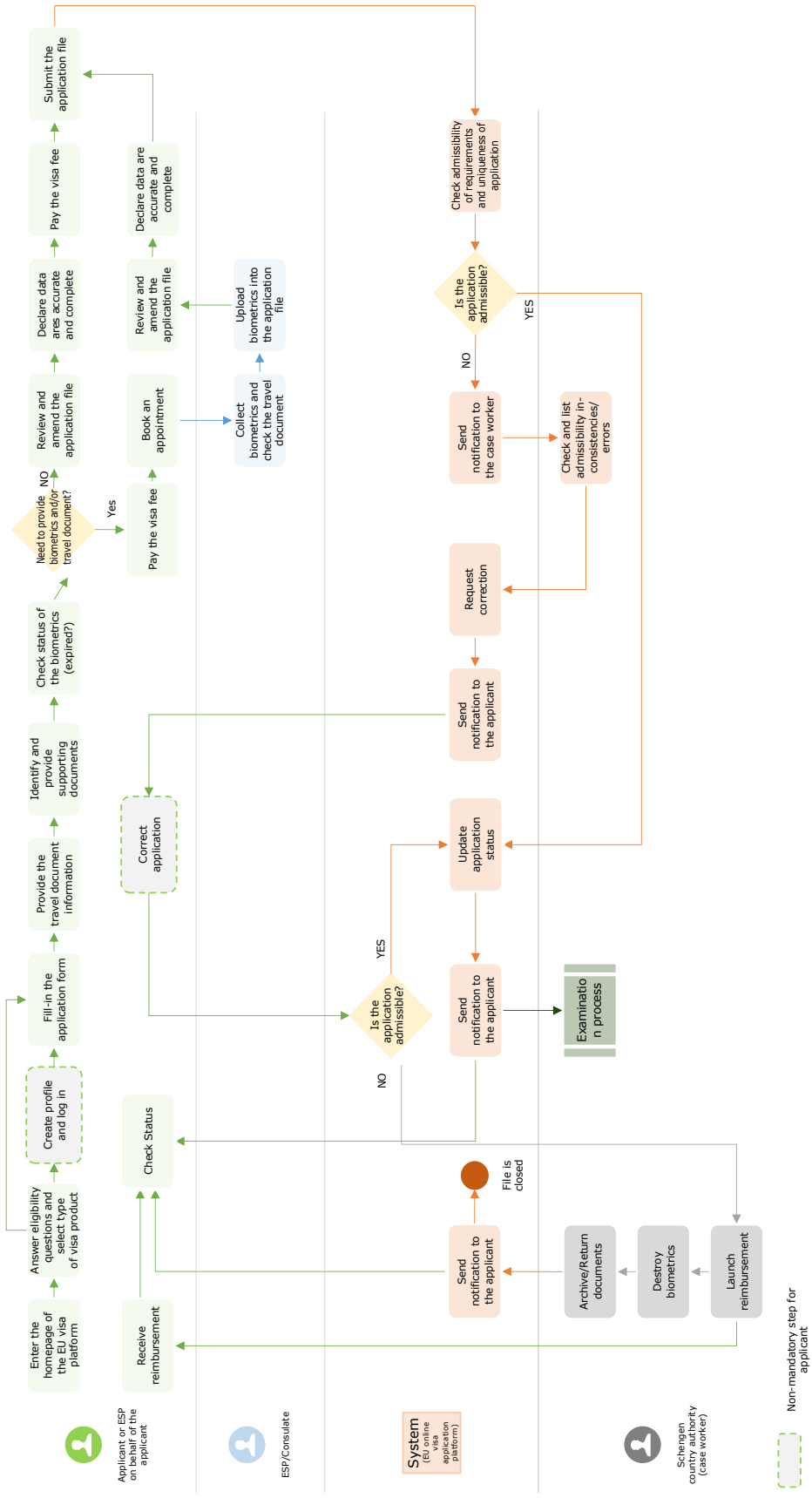

Figure 24: Future digital visa online application process workflow

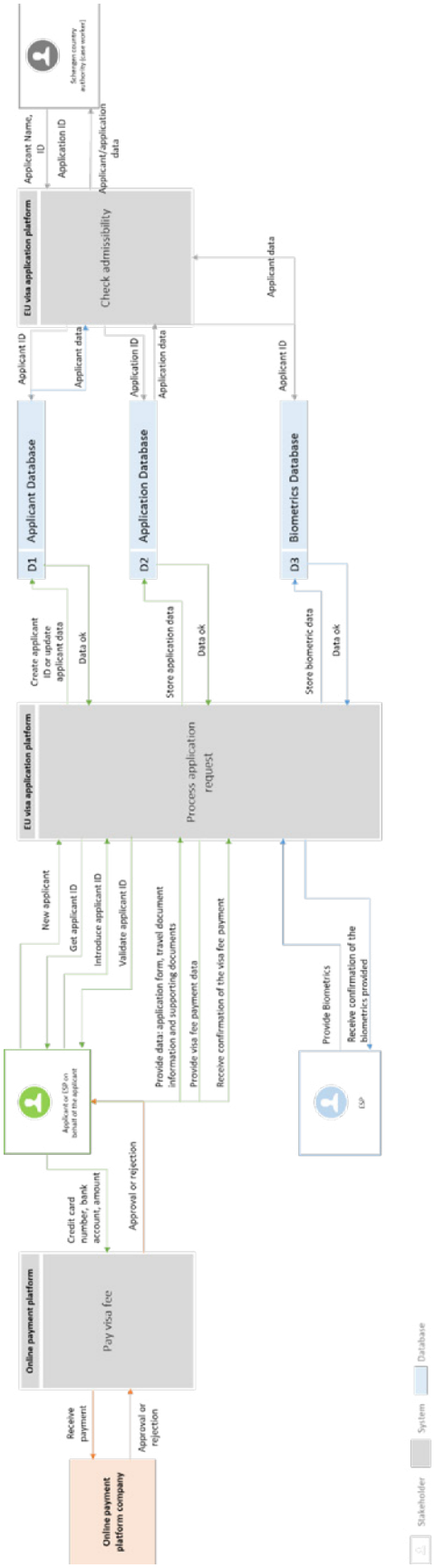

Figure 25: Visa online application process data workflow

1.2.2. Examine visa application

Although the examination process is out of scope, it is of interest to show the interrelationships between the EU online application portal and the national and central systems. Furthermore, since the approach is user-centric and the examination process has several stages in which the case worker needs to interact with the applicant, it is necessary to show this interaction as well.

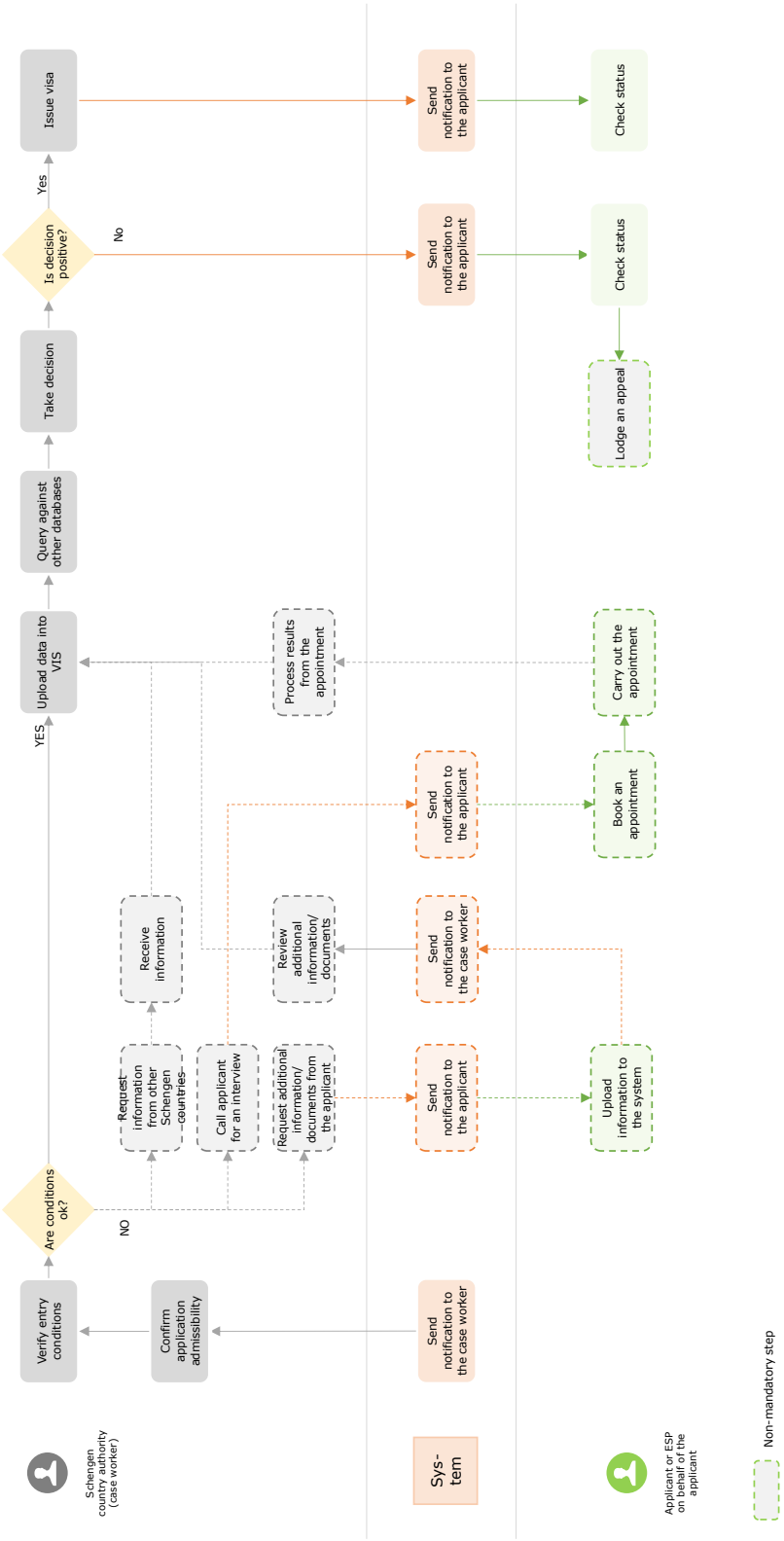

Figure 26: Visa examination process workflow[216]

[216] Data are uploaded into VIS only after the first automated admissibility check and after the visa officer confirms the application admissibility and verifies entry conditions.

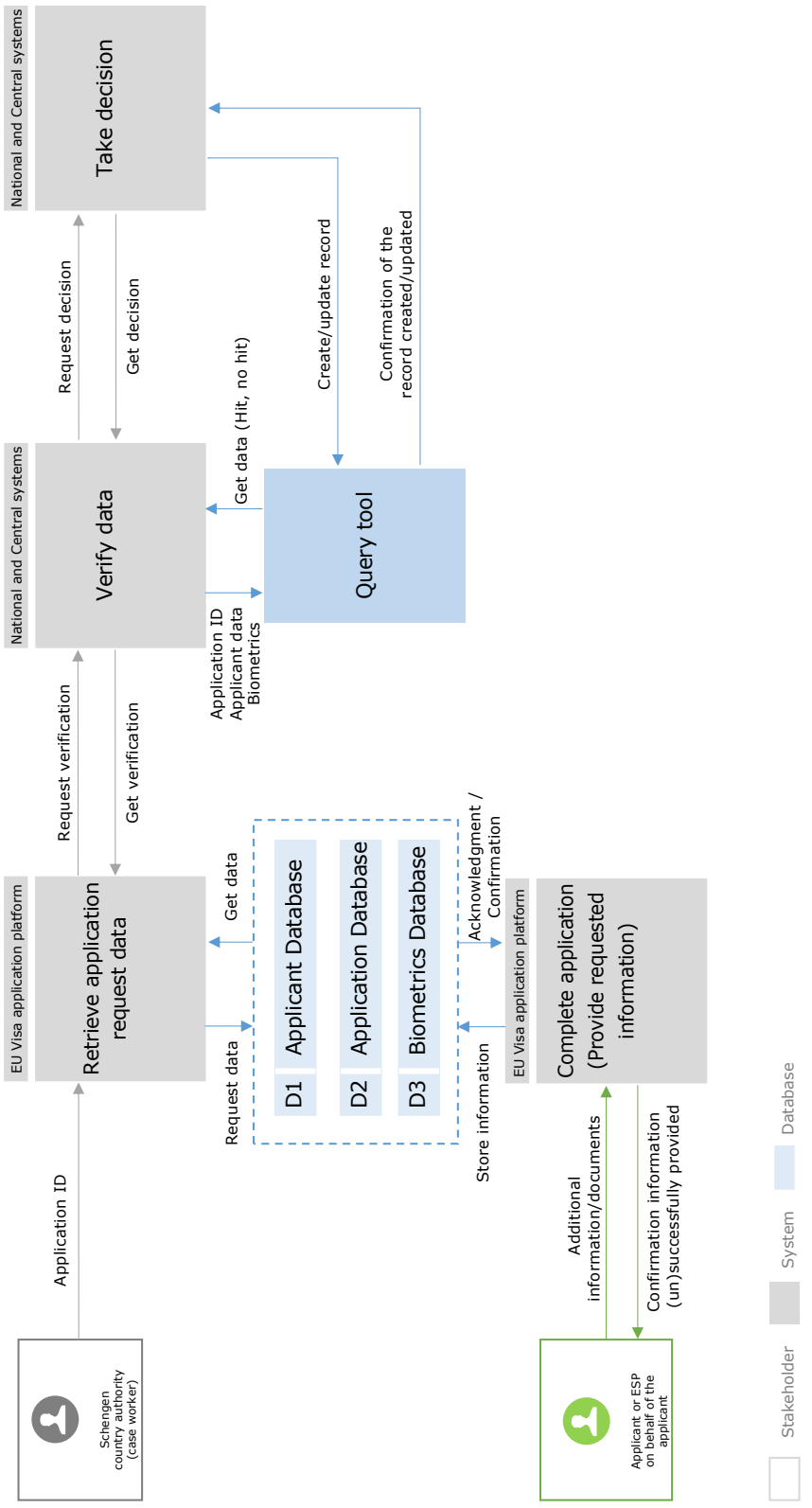

Figure 27: Visa examination process data workflow[217]

[217] Although the architecture and data flow will be developed, a query tool similar to ETIAS functional solution can establish the database connection between the VIS central system and the Europol domain and other eu-LISA systems (such as CIR, ECRIS-TCN, SIS II, Eurodac and EES).

1.3. Verify visa

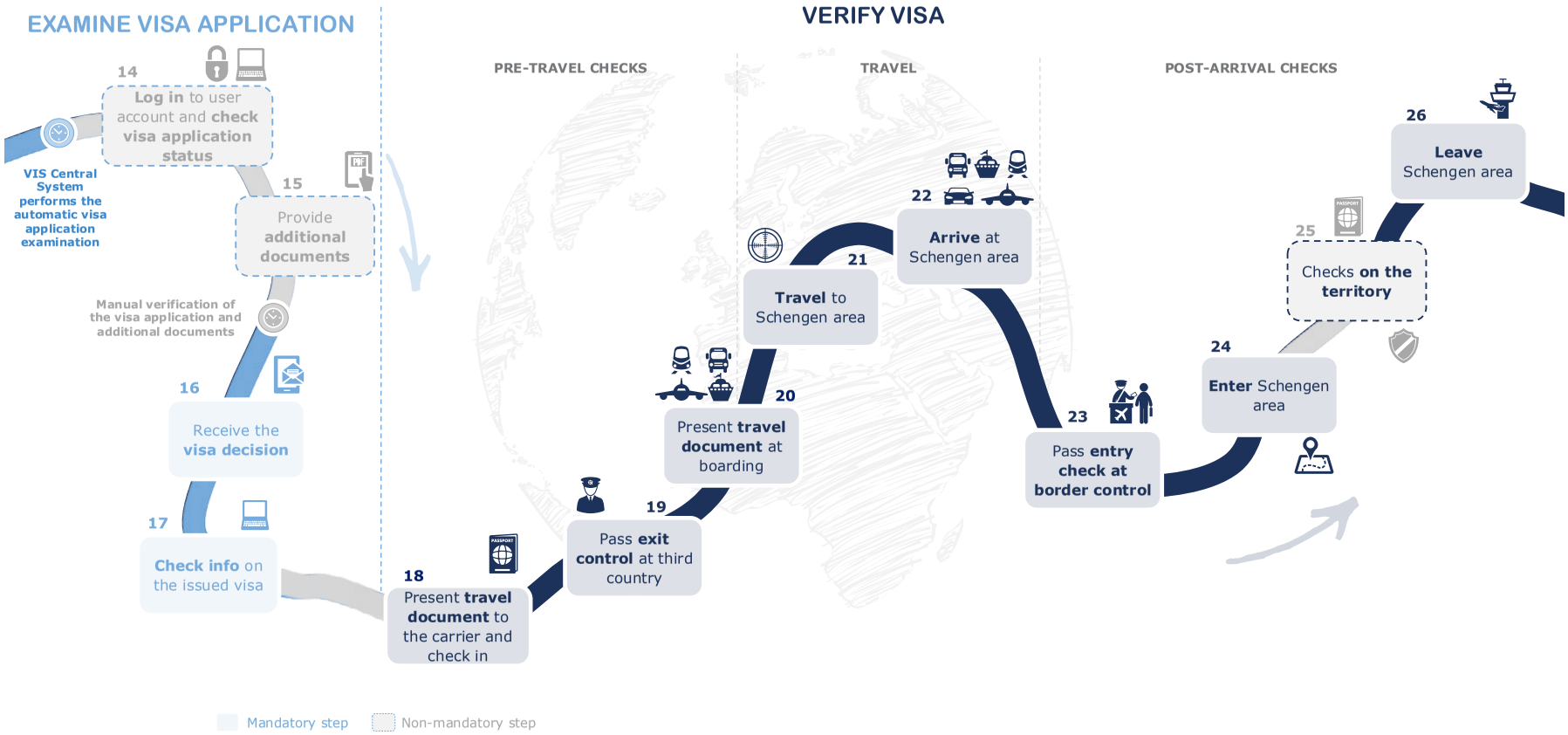

Figure 28: Digital user journey for the examination and verification of visa

1.3.1. Pre-travel checks

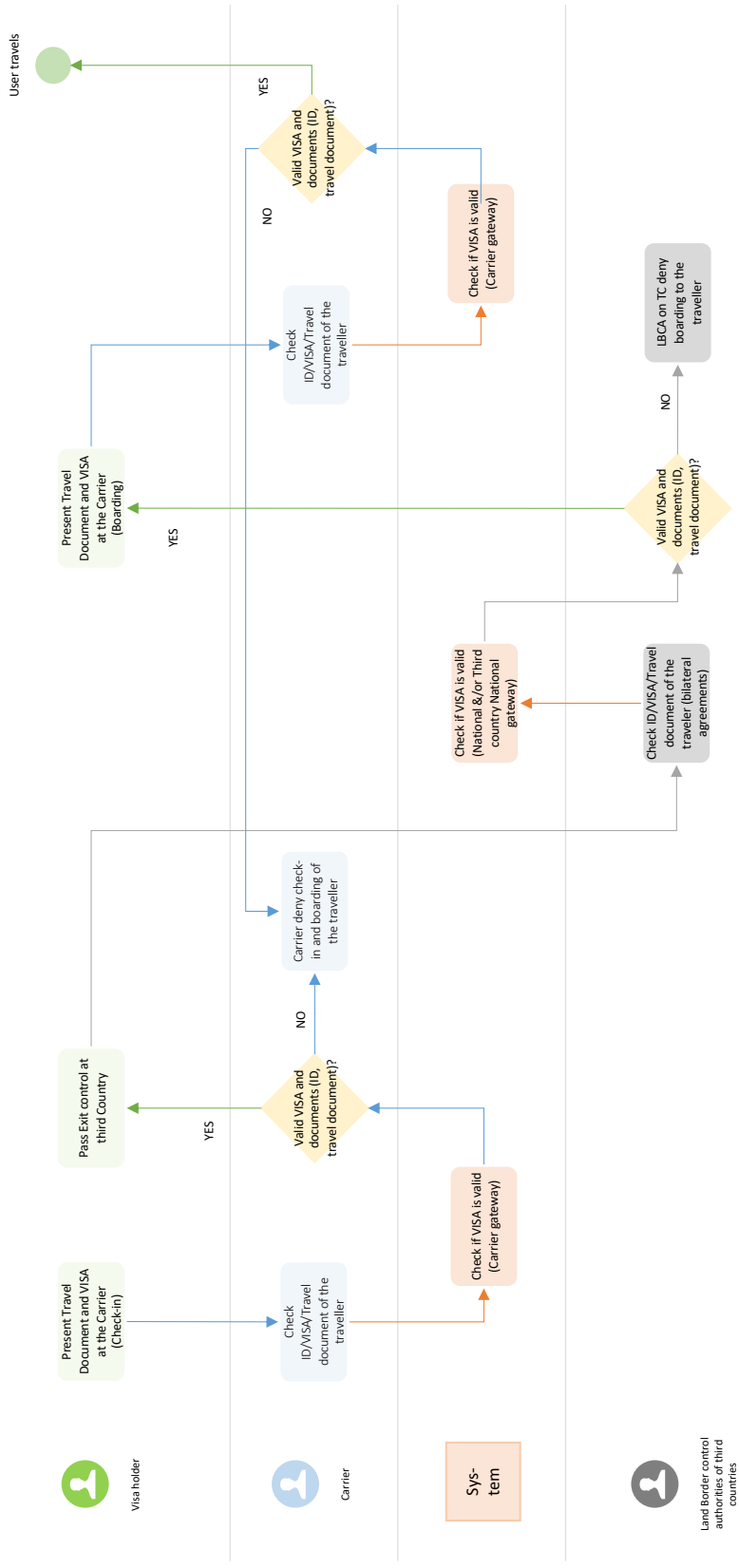

Figure 29: Future digital visa verification process workflow: Pre-travel

1.3.2. Arrival checks

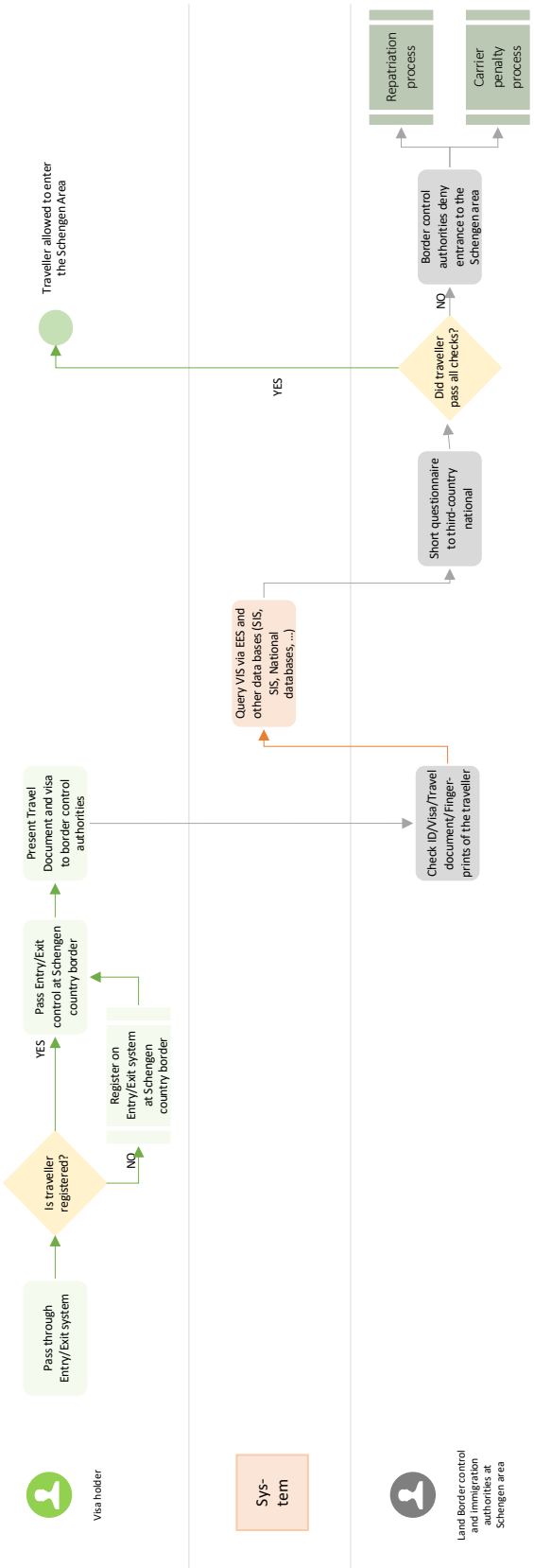

Figure 30: Future digital visa verification process workflow: Arrival checks

1.3.3. Post-arrival checks

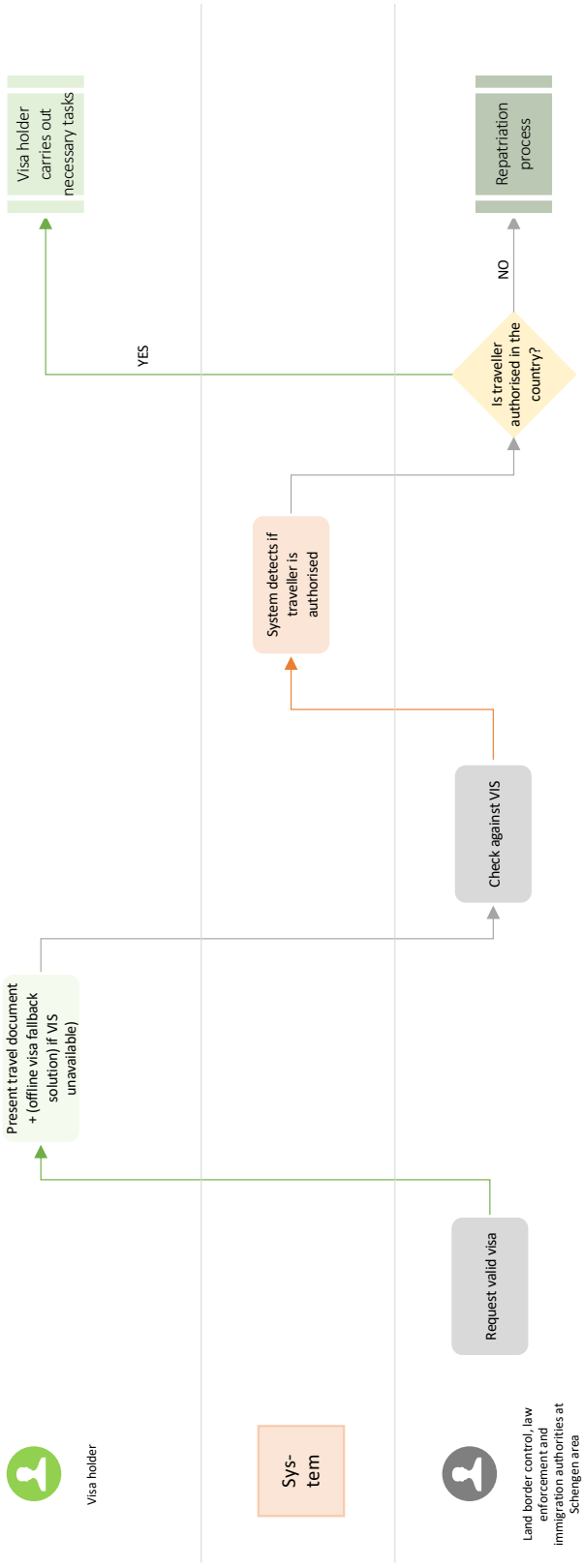

Figure 31: Future digital visa verification process workflow: Inland checks by land border control, law enforcements and immigration authorities

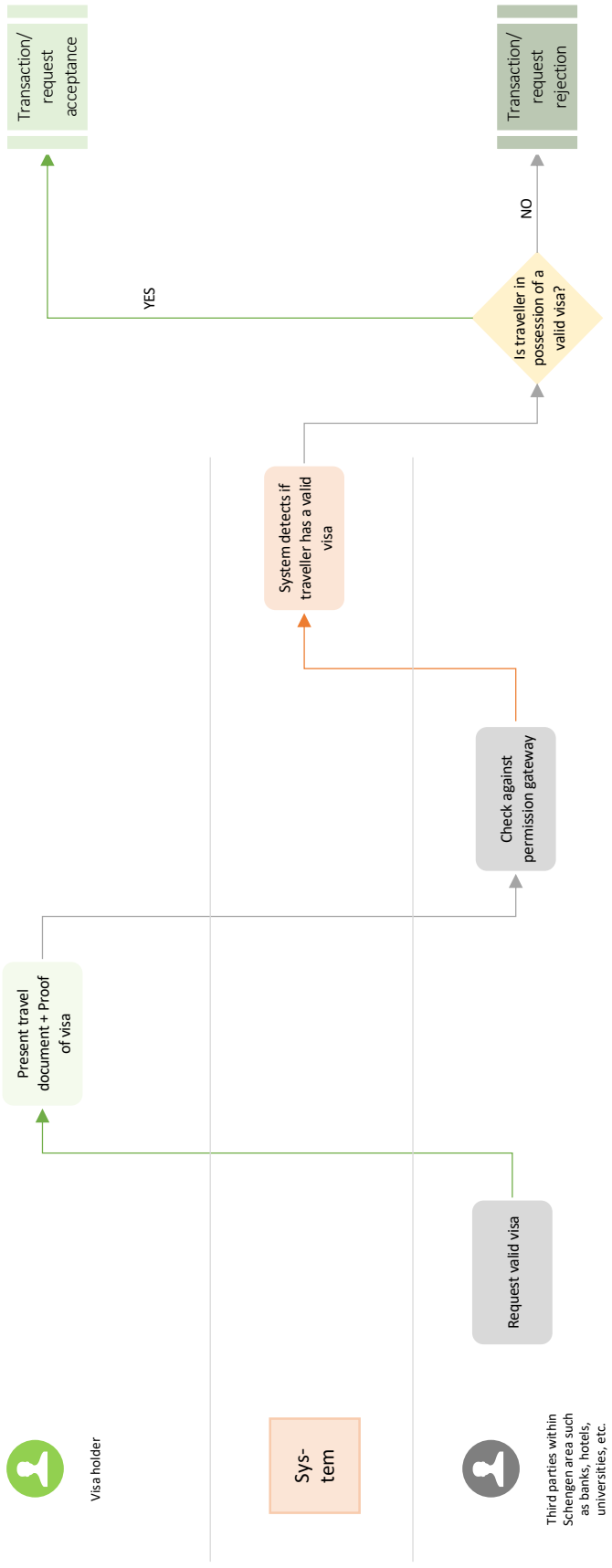

Figure 32: Future digital visa verification process workflow: Inland checks by third parties

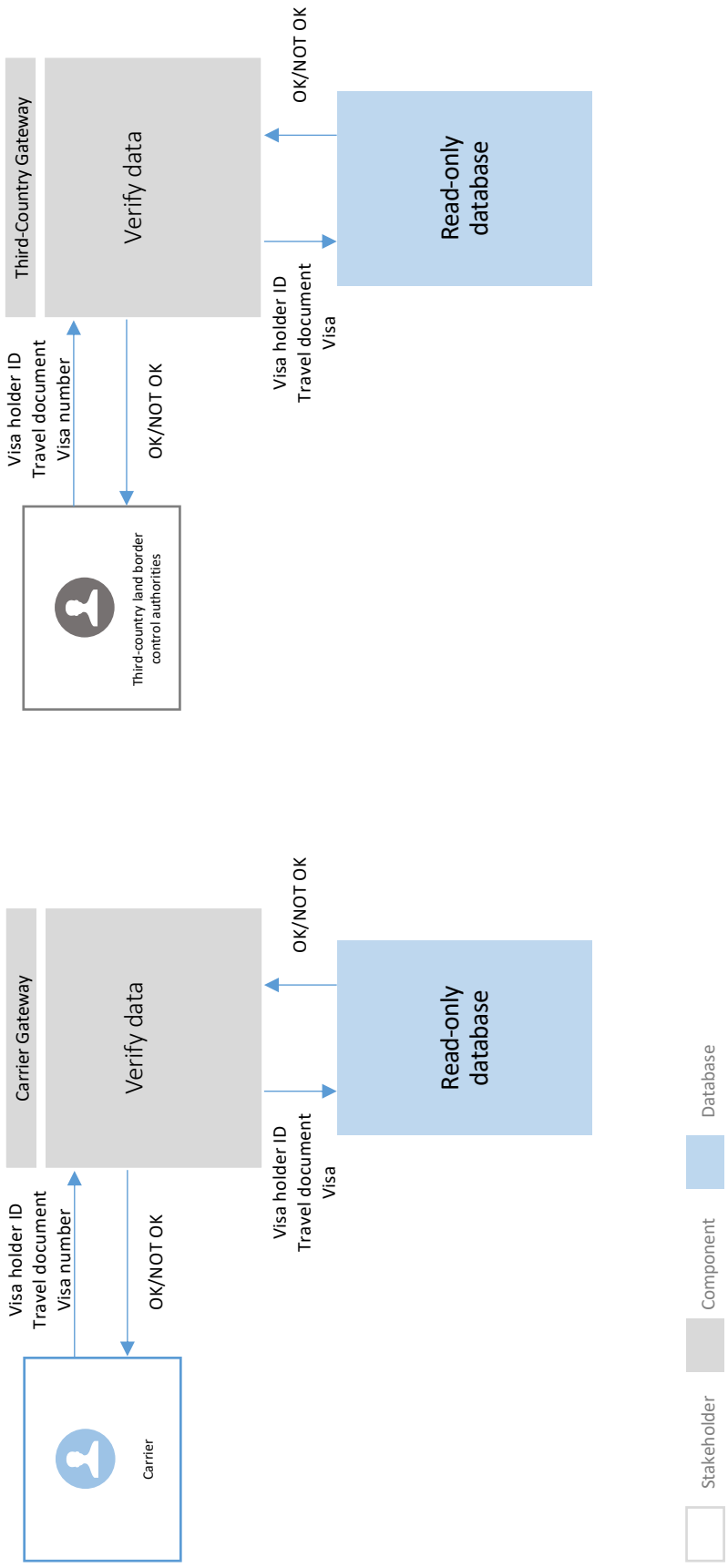

Figure 33: Verification of visa data workflow (1)

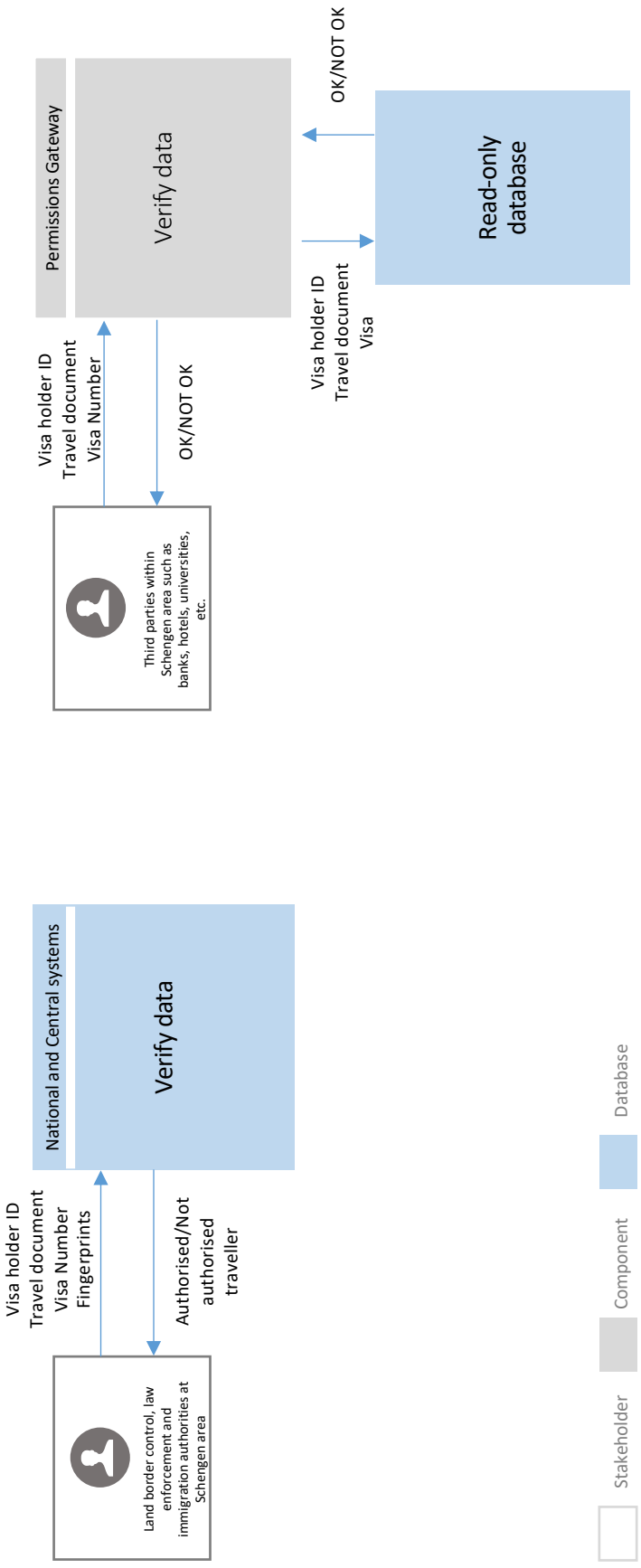

Figure 34: Verification of visa data workflow (2)

Annex J. Glossary

Table 63: Glossary

Abbreviation	Definition
ABC	Automated Border Control
AMS	Application Management System
API	Application Programming Interface
BMS	Biometric Matching Service
CBA	Cost-Benefit Analysis
CIR	Common Identity Repository
CRRS	Central Repository for Reporting and Statistics
CSCA	Country Signing Certification Authority
CSI	Common Shared Infrastructure
DG HOME	Directorate-General of the European Commission for Migration and Home Affairs
DMZ	Demilitarised Zone
EBCGA	European Border and Coast Guard Agency
EC	European Commission
ECRIS	European Criminal Records Information System
ECRIS-TCN	European Criminal Records Information System for Third Country Nationals
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EES Regulation	Regulation (EU) No 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen countries and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011
eMRTD	Electronic Machine-Readable Travel Document
ESP	External Service Provider
ETIAS	European Travel Information and Authorisation System
ETIAS Regulation	Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	European Asylum Dactyloscopy Database
EUROPOL	European Union Agency for Law Enforcement Cooperation
FAQ	Frequently Asked Questions
FTE	Full-Time Equivalent
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ICAO	International Civil Aviation Organisation
ICD	Interface Control Document
ID	Identity Document

Abbreviation	Definition
Interpol	The International Criminal Police Organization
ISO	International Organization for Standardization
IT	Information Technology
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
MB/s	Megabyte per second
MFA	Multi-Factor Authentication
MID	Multiple-Identity Detector
MRZ	Machine-Readable Zone
MVP	Minimum Viable Product
N/A	Not Available
NFC	Near-Field Communication
NUI	National Uniform Interface
PC	Personal Computer
PDF	Adobe Portable Document
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
SBC	Schengen Borders Code
Schengen Borders Code	Regulation (EC) No 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders
SD	Supporting document
SDLC	Software Development Life Cycle
SIS II	Schengen Information System (of the second generation)
SLA	Service Level Agreement
SMS	Short Message Service (Text message)
TCN	Third Country National
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
URL	Uniform Resource Locator
VAC	Visa Application Centre
VFA	Visa Facilitation Agreements
VIS	Visa Information System
VIS Regulation	Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Schengen countries on short-stay visas
VIS Revision	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA
Visa Code	Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas
WBF	Windows Biometric Framework

Annex K. Bibliography

This Annex presents the bibliography used for this report.

Strategic documents

C(2018) 251 final, Communication from the Commission to the European Parliament and the Council: Adapting the common visa policy to new challenges

C(2018) 7118 final, Communication from the Commission – European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission

Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU, 6 October 2017

COM(2016) 179 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government

Studies and reports

European Commission (DG HOME), SWD(2018) 195 final, Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, 16 May 2018

European Commission (DG HOME), SWD(2018) 77 final, Commission Staff Working Document, Impact Assessment accompanying the Proposal a Regulation of the European Parliament and of the Council for amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), 14 March 2018

European Commission (DG HOME), Feasibility of a Common Identity Repository (CIR), February 2018

JRC Technical Reports (Beslay, L. Galbally, J. Haraksim, R), Automatic fingerprint recognition: from children to elderly, 2018.

European Migration Network, Synthesis Report for the EMN Focussed Study 2017 Challenges and practices for establishing the identity of third country nationals in migration procedures, Final version, December 2017

European Commission (DG HOME), Public Consultation “Moving towards digital visa”, replies from Estonia, Finland, France, Latvia, Slovakia, Slovenia; replies from ACTE, ETOA, Fliggy, GBTA, HORTEC, PEARLE.

European Commission (DG HOME), Public Consultation “IT tools for visa applications”, individual Schengen countries factsheets.

Council of the European Union, Note of 3 October 2017 from the Presidency of the Council – Visa Working Party / Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein) – e-visa: improving the current visa processing with online visa application

Council of the European Union, Note of 4 September 2017 from the Presidency of the Council – Visa Working Party / Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein) – e-visa: improving the current visa processing with digital visa

European Commission (DG HOME), Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation, 14 October 2016

European Commission (DG HOME), SWD(2016) 328 final, Commission Staff Working Document, Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT, 14 October 2016

European Commission (DG HOME), Feasibility Study for a European Travel Information and Authorisation System (ETIAS), Final Report, 2016

European Commission (DG HOME), Impact assessment study supporting the review of the Union's visa policy to facilitate legitimate travelling, Final Report, July 2013European Parliament, Directorate-General for Internal Policies, The Commission's Legislative Proposal on Smart Borders: their Implications and Costs, Study, 2013.

European Commission, Policy study on an EU Electronic System for travel Authorization (EU ESTA), Final Report, February 2011

Presentations

European Commission (DG HOME Unit B.3), EU Interoperability Framework for Border Management Systems – Secure, Safe and Resilient Societies, 5 June 2018

European Commission, (DG HOME Unit B.3), Cross Border Digital Identity in the EU, 1 June 2017

Guidelines and best practice documents

European Commission (DG HOME Unit B.2), Enrolment Guidelines: Best Practice Recommendations for the Enrolment of Face and Fingerprint biometric samples for Travel and Identity Documents, 27 February 2019

European Border and Coast Guard Agency, Guidelines for Processing Third country Nationals through Automated Border Control, 11 March 2016

European Commission (DG HOME), Consolidated version of the Handbook for the processing of visa applications and the modification of issued visas, 9 July 2014

Websites

Visa application process

Bayometric.com, information on the Windows Biometric Framework (WBF): https://www.bayometric.com/windows-biometric-framework/

European Commission, Directorate-General for Migration and Home Affairs (DG HOME) – Schengen, Borders & Visas: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas_en

German Ministry of Foreign Affairs, VIDEX Online application solution: https://videx.diplo.de/videx/desktop/index.html

Google Play, information about DocuSign: https://play.google.com/store/apps/details?id=com.docusign.ink&hl=en_AU

Google Play, information about Fill & Sign:
https://play.google.com/store/apps/details?id=com.adobe.fas&hl=en_AU

Google Play, information about NCF Passport Reader:
https://play.google.com/store/apps/details?id=nl.innovalor.nfciddocshowcase&hl=en_US

Google Play, information about Passport Image Decoder:
https://play.google.com/store/apps/details?id=at.mroland.android.apps.imagedecoder&hl=fr

Visa sticker/digital visa

Australian Government – Department of Home Affairs: Tourist e-visa:
https://immi.homeaffairs.gov.au/visas/getting-a-visa/visa-listing/visitor-600/tourist-stream-overseas#About

Australian Government – Department of Home Affairs: First Work and Holiday e-visa:
https://immi.homeaffairs.gov.au/visas/getting-a-visa/visa-listing/work-holiday-462/first-work-holiday-462#About

Cambodian Immigration & e-visa Portal:
https://www.cambodiaimmigration.org/faq/what-are-the-required-documents-for-cambodia-e-visa

Government of the United Kingdom – Information on settled status for EU citizens:
https://www.gov.uk/settled-status-eu-citizens-families

International Civil Aviation Organisation – Doc 9303 Series on machine-readable travel documents:
https://www.icao.int/publications/pages/publication.aspx?docnum=9303.

Information and statistics about Schengen visas: https://www.schengenvisainfo.com/

Iranian Ministry of Foreign Affairs – Iranian e-visa: https://evisatraveller.mfa.ir/en/

WorldReach Software, Reaching travellers and citizens abroad, VisaReach:
https://worldreach.com/products/visareach/

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at:
https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696, or
– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union