DÉCISION D'EXÉCUTION (UE) 2021/1073 DE LA COMMISSION

du 28 juin 2021

établissant les spécifications techniques et les règles relatives à la mise en œuvre du cadre de confiance pour le certificat COVID numérique de l'UE établi par le règlement (UE) 2021/953 du Parlement européen et du Conseil

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2021/953 du Parlement européen et du Conseil relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19 ([1]), et notamment son article 9, paragraphes 1 et 3,

considérant ce qui suit:

(1) Le règlement (UE) 2021/953 définit le certificat COVID numérique de l'UE, qui sert à prouver qu'une personne a été vaccinée contre la COVID-19, a effectué un test dont le résultat est négatif ou s'est rétablie d'une infection.

(2) Pour que le certificat COVID numérique de l'UE soit opérationnel dans toute l'Union, il est nécessaire d'établir les spécifications techniques et les règles permettant de compléter et de délivrer et vérifier de manière sécurisée les certificats COVID numériques, de garantir la protection des données à caractère personnel, de définir la structure commune de l'identifiant unique du certificat et de délivrer un code-barres valide, sécurisé et interopérable. Ce cadre de confiance constitue également un premier pas pour s'efforcer d'assurer l'interopérabilité avec les normes internationales et les systèmes technologiques et pourrait, à ce titre, servir de modèle en vue d'une coopération au niveau mondial.

(3) La capacité de lire et d'interpréter le certificat COVID numérique de l'UE requiert une structure de données commune et un consensus sur la destination de chaque champ de données de la charge utile et sur les valeurs pouvant lui être assignées. Pour favoriser cette interopérabilité, il est nécessaire de définir une structure de données coordonnée commune pour le cadre du certificat COVID numérique de l'UE. Les orientations relatives à ce cadre ont été élaborées par le réseau «santé en ligne» établi sur la base de la directive 2011/24/UE du Parlement européen et du Conseil ([2]). Ces orientations devraient être prises en considération lors de l'établissement des spécifications techniques applicables au format et à la gestion de la confiance pour le certificat COVID numérique de l'UE. Il convient de définir une spécification pour la structure des données et de déterminer des mécanismes d'encodage, ainsi qu'un mécanisme d'encodage de transport dans un format optique lisible par machine (QR) pouvant être visualisé sur l'écran d'un appareil mobile ou imprimé sur papier.

(4) Outre les spécifications techniques relatives au format et à la gestion de la confiance du certificat COVID numérique de l'UE, il convient d'établir les règles générales à suivre pour compléter les certificats en ce qui concerne les valeurs codées à mentionner dans ledit certificat. La Commission devrait actualiser et publier régulièrement les ensembles de valeurs mettant en œuvre ces règles, en se fondant sur les travaux y afférents du réseau «santé en ligne».

(5) En application du règlement (UE) 2021/953, les certificats authentiques constituant le certificat COVID numérique de l'UE doivent être identifiables individuellement au moyen d'un identifiant unique du certificat, compte tenu du fait que plusieurs certificats peuvent être délivrés aux citoyens pendant la durée de validité du règlement (UE) 2021/953. L'identifiant unique du certificat doit consister en une chaîne alphanumérique et les États membres devraient veiller à ce qu'il ne contienne aucune donnée le reliant à d'autres documents ou identifiants, tels que des numéros de passeport ou de carte d'identité, afin d'empêcher l'identification du titulaire. Aux fins de garantir l'unicité de l'identifiant du certificat, il convient d'établir les spécifications techniques et les règles applicables à sa structure commune.

([1]) JO L 211 du 15.6.2021, p. 1.

([2]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

(6) La sécurité, l'authenticité, la validité et l'intégrité des certificats constituant le certificat COVID numérique de l'UE et leur conformité au droit de l'Union en matière de protection des données sont essentielles pour qu'ils soient acceptés par tous les États membres. Ces objectifs sont réalisés par le cadre de confiance établissant les règles de délivrance et de vérification fiables et sûres des certificats COVID numériques de l'UE, ainsi que les infrastructures à cet effet. Le cadre de confiance devrait notamment reposer sur une infrastructure à clés publiques avec une chaîne de confiance allant des autorités sanitaires des États membres ou d'autres autorités de confiance aux différentes entités délivrant les certificats COVID numériques de l'UE. Par conséquent, afin de garantir un système d'interopérabilité à l'échelle de l'UE, la Commission a mis en place un système central de passerelle pour le certificat COVID numérique de l'UE (le «service passerelle»), qui stocke les clés publiques utilisées à des fins de vérification. Lorsque le certificat à code QR est scanné, la signature numérique est vérifiée à l'aide de la clé publique correspondante, préalablement stockée dans ce service passerelle central. Des signatures numériques peuvent être utilisées pour garantir l'intégrité et l'authenticité des données. Les infrastructures à clés publiques établissent la confiance en reliant les clés publiques aux émetteurs de certificats. Dans le service passerelle, plusieurs certificats de clé publique sont utilisés à des fins d'authenticité. Afin d'assurer l'échange sécurisé des données se rapportant aux clés publiques entre les États membres et de permettre une large interopérabilité, il est nécessaire de déterminer les certificats de clé publique qui peuvent être utilisés et de prévoir de quelle manière ils devraient être générés.

(7) La présente décision permet de mettre en œuvre les exigences du règlement (UE) 2021/953 en réduisant au minimum le traitement des données à caractère personnel pour le limiter à ce qui est nécessaire pour rendre opérationnel le certificat COVID numérique de l'UE et en contribuant à ce que leur mise en œuvre, par les responsables du traitement finals, respecte la protection des données dès la conception.

(8) Conformément au règlement (UE) 2021/953, les autorités ou autres instances désignées chargées de délivrer les certificats sont les responsables du traitement définis à l'article 4, point 7), du règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]) dans le rôle qui leur est dévolu quant au traitement des données à caractère personnel au cours du processus de délivrance. En fonction de la manière dont les États membres organisent le processus de délivrance, il peut y avoir une ou plusieurs autorités ou instances désignées, telles que des services de santé régionaux. Conformément au principe de subsidiarité, ce choix appartient aux États membres. Par conséquent, les États membres sont les mieux placés pour veiller à ce que, lorsqu'il existe plusieurs autorités ou autres entités désignées, leurs responsabilités respectives soient clairement attribuées, qu'il s'agisse de responsables du traitement distincts ou conjoints (notamment des services de santé régionaux créant un portail des patients commun pour la délivrance des certificats). De même, en ce qui concerne la vérification des certificats par les autorités compétentes de l'État membre de destination ou de transit, ou par les opérateurs de services transfrontières de transport de voyageurs qui sont tenus en vertu du droit national de mettre en œuvre certaines mesures de santé publique pendant la pandémie de COVID-19, ces vérificateurs doivent se conformer aux obligations qui leur incombent en vertu des règles régissant la protection des données.

(9) Aucun traitement de données à caractère personnel ne s'effectue par l'intermédiaire du service passerelle pour le certificat COVID numérique de l'UE, ledit service se bornant à héberger les clés publiques des autorités signataires. Ces clés sont liées aux autorités signataires et ne permettent pas la réidentification directe ou indirecte d'une personne physique à laquelle un certificat a été délivré. En tant que gestionnaire du service passerelle, la Commission ne devrait donc être ni responsable du traitement ni sous-traitant de données à caractère personnel.

(10) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([4]) et a rendu un avis le 22 juin 2021.

(11) Étant donné que les spécifications techniques et les règles sont nécessaires à l'application du règlement (UE) 2021/953 à partir du 1er juillet 2021, l'application immédiate de la présente décision est justifiée.

(12) Dès lors, eu égard à la nécessité d'une mise en œuvre rapide du certificat COVID numérique de l'UE, la présente décision devrait entrer en vigueur le jour de sa publication,

([3]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([4]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les spécifications techniques relatives au certificat COVID numérique de l'UE établissant la structure des données générique, les mécanismes d'encodage et le mécanisme d'encodage de transport dans un format optique lisible par machine figurent à l'annexe I.

Article 2

Les règles à suivre pour compléter les certificats visés à l'article 3, paragraphe 1, du règlement (UE) 2021/953 figurent à l'annexe II de la présente décision.

Article 3

Les exigences définissant la structure commune de l'identifiant unique du certificat figurent à l'annexe III.

Article 4

Les règles de gouvernance applicables aux certificats de clé publique en ce qui concerne le service passerelle pour le certificat COVID numérique de l'UE prenant en charge les aspects d'interopérabilité du cadre de confiance figurent à l'annexe IV.

La présente décision entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 28 juin 2021.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

FORMAT ET GESTION DE LA CONFIANCE

Structure de données générique, mécanismes d'encodage et mécanisme d'encodage de transport dans un format optique lisible par machine (ci-après dénommé «QR»)

1. Introduction

Les spécifications techniques décrites dans la présente annexe contiennent une structure de données générique et des mécanismes d'encodage pour le certificat COVID numérique de l'UE (*EU Digital COVID Certificate* — DCC). Elles définissent également un mécanisme d'encodage de transport dans un format optique lisible par machine (*Quick Response* — QR), qui peut être affiché sur l'écran d'un appareil mobile ou être imprimé. Les formats du conteneur du certificat sanitaire électronique figurant dans les présentes spécifications sont génériques, mais, dans ce contexte, ils servent à porter le DCC.

2. Terminologie

Aux fins de la présente annexe, on entend par «émetteurs» les organismes qui utilisent les présentes spécifications pour délivrer des certificats sanitaires et par «vérificateurs» les organismes acceptant les certificats sanitaires comme preuve du statut sanitaire. On entend par «participants» les émetteurs et les vérificateurs. Certains aspects définis dans la présente annexe, tels que la gestion d'un espace de noms et la distribution des clés cryptographiques, doivent faire l'objet d'une coordination entre les participants. Il est supposé qu'une partie, ci-après dénommée le «secrétariat», accomplit ces tâches.

3. Format du conteneur du certificat sanitaire électronique

Le format du conteneur du certificat sanitaire électronique (*Electronic Health Certificate* — «HCERT») est conçu pour fournir un véhicule uniforme et normalisé pour les certificats sanitaires délivrés par les différents émetteurs (ci-après les «émetteurs»). Les présentes spécifications ont pour objet d'harmoniser la manière dont ces certificats sanitaires sont représentés, encodés et signés dans le but d'en faciliter l'interopérabilité.

La capacité de lire et d'interpréter un DCC délivré par un émetteur requiert une structure de données commune et un accord sur la signification de chaque champ de données de la charge utile. Pour faciliter cette interopérabilité, on définit une structure de données commune coordonnée en utilisant un schéma «JSON» qui constitue le cadre du DCC.

3.1. *Structure de la charge utile*

La charge utile est structurée et encodée au format CBOR (*Concise Binary Object Representation* — représentation concise d'objet binaire) avec une signature numérique au format COSE (*CBOR Object Signing and Encryption* — signature et chiffrement d'objet en représentation concise d'objet binaire). Cette structure est communément appelée «jeton CBOR pour la toile» (*CBOR Web Token* — CWT) et est définie dans la RFC 8392 ([1]). La charge utile, telle que définie dans les sections suivantes, est transportée dans une revendication hcert.

L'intégrité et l'authenticité de l'origine des données de la charge utile doivent être vérifiables par le vérificateur. Pour permettre ce mécanisme, l'émetteur doit signer le CWT au moyen d'un système de signature électronique asymétrique tel que défini dans la spécification COSE (RFC 8152 ([2])).

3.2. *Revendications CWT*

3.2.1. Vue d'ensemble de la structure CWT

En-tête protégé

— Algorithme de signature (alg, étiquette 1)

— Identifiant de clé (*Key Identifier* — ci-après «kid», étiquette 4)

Charge utile

— Émetteur (*Issuer* — ci-après «iss», clé de revendication 1, facultatif, ISO 3166-1 alpha-2 de l'émetteur)

— Délivré le (*Issued At* — ci-après «iat», clé de revendication 6)

— Délai d'expiration (exp, clé de revendication 4)

— Certificat sanitaire (hcert, clé de revendication -260)

— Certificat COVID numérique de l'UE v1 (eu_DCC_v1, clé de revendication 1)

Signature

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

3.2.2. Algorithme de signature

Le paramètre de l'algorithme de signature (alg) indique quel algorithme est utilisé pour créer la signature. Il doit respecter voire être plus strict que les lignes directrices actuelles du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS) résumées dans les paragraphes suivants.

Un algorithme primaire et un algorithme secondaire sont définis. L'algorithme secondaire ne devrait être utilisé que si l'algorithme primaire n'est pas acceptable dans le cadre des règles et réglementations imposées à l'émetteur.

Afin de garantir la sécurité du système, toutes les mises en œuvre doivent intégrer l'algorithme secondaire. C'est pourquoi tant l'algorithme primaire que l'algorithme secondaire doivent être mis en œuvre.

Les niveaux définis par le SOG-IS pour les algorithmes primaire et secondaire sont les suivants:

— Algorithme primaire: l'algorithme primaire est l'algorithme de signature numérique à courbe elliptique (*Elliptic Curve Digital Signature Algorithm* — ECDSA) tel que défini à la section 2.3 de la norme (ISO/IEC 14888–3:2006), utilisant les paramètres P–256 définis à l'appendice D (D.1.2.3) de la norme (FIPS PUB 186–4) en combinaison avec l'algorithme de hachage SHA–256 tel que défini dans la fonction 4 de la norme (ISO/IEC 10118–3:2004).

Cela correspond au paramètre ES256 de l'algorithme COSE.

— Algorithme secondaire: l'algorithme secondaire est le RSASSA-PSS tel que défini dans la (RFC 8230 ([3])) avec un modulus de 2048 bits en combinaison avec l'algorithme de hachage SHA–256 tel que défini dans la fonction 4 de la norme (ISO/IEC 10118–3:2004).

Cela correspond au paramètre de l'algorithme COSE: PS256.

3.2.3. Identifiant de clé

La revendication d'identifiant de clé (kid) indique le certificat de signataire de documents (DSC) contenant la clé publique qui doit être utilisé par le vérificateur pour vérifier l'exactitude de la signature numérique. La gouvernance des certificats de clé publique, y compris les exigences applicables aux DSC, est décrite à l'annexe IV.

La revendication d'identifiant de clé (kid) est utilisée par les vérificateurs pour sélectionner la bonne clé publique à partir d'une liste de clés appartenant à l'émetteur indiqué dans la revendication d'émetteur (iss). Plusieurs clés peuvent être utilisées parallèlement par un émetteur pour des raisons administratives et lors de la reconduction des clés. L'identifiant de clé n'est pas un champ critique pour la sécurité. Pour cette raison, il peut également être placé dans un en-tête non protégé si nécessaire. Les vérificateurs doivent accepter les deux options. Si les deux options sont présentes, c'est l'identifiant de clé dans l'en-tête protégé qu'il y a lieu d'utiliser.

En raison du raccourcissement de l'identifiant (pour des raisons de limitation de la taille), la probabilité est faible, mais pas nulle, que la liste globale des certificats de signataire de documents (*Document Signer Certificates* — DSC) acceptés par un vérificateur puisse contenir des DSC avec un double kid. C'est la raison pour laquelle le vérificateur doit vérifier tous les DSC présentant ce kid.

3.2.4. Émetteur

La revendication d'émetteur (iss) est une valeur de chaîne qui peut, à titre facultatif, contenir le code pays ISO 3166-1 alpha-2 de l'entité délivrant le certificat sanitaire. Cette revendication peut être utilisée par un vérificateur pour identifier la série de DSC à utiliser pour la vérification. La clé de revendication 1 est utilisée pour identifier cette revendication.

3.2.5. Délai d'expiration

La revendication de délai d'expiration (exp) doit contenir un horodatage au format date numérique (comme précisé dans la RFC 8392 ([4]), section 2) indiquant la période pendant laquelle cette signature particulière sur la charge utile doit être considérée comme valide, après quoi un vérificateur doit rejeter la charge utile considérée comme ayant expiré. L'objectif du paramètre d'expiration est d'imposer une limite à la durée de validité du certificat sanitaire. La clé de revendication 4 est utilisée pour identifier cette revendication.

Le délai d'expiration ne doit pas dépasser la période de validité du DSC.

([3]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org).

3.2.6. Délivré le

La revendication «délivré le» (iat) doit contenir un horodatage au format date numérique (comme précisé dans la RFC 8392 ([5]), section 2) indiquant la date à laquelle le certificat sanitaire a été créé.

Le champ «délivré le» ne doit pas contenir une date antérieure à la période de validité du DSC.

Les vérificateurs peuvent appliquer des mesures supplémentaires dans le but de limiter la validité du certificat sanitaire en fonction de la date de délivrance. La clé de revendication 6 est utilisée pour identifier cette revendication.

3.2.7. Revendication de certificat sanitaire

La revendication de certificat sanitaire (hcert) est un objet JSON (RFC 7159 ([6])) contenant les informations relatives au statut sanitaire. Plusieurs types de certificat sanitaire peuvent exister sous la même revendication, le DCC en étant un.

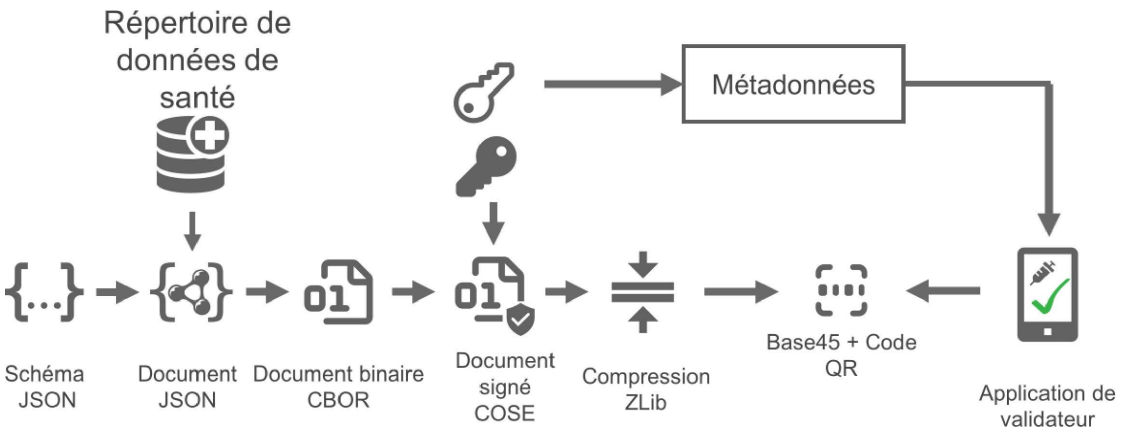
Le format JSON sert uniquement pour les schémas. Le format de représentation est le CBOR, tel que défini dans la (RFC 7049 ([7])). Il se peut que les développeurs des applications ne décodent ou n'encodent jamais vers et depuis le format JSON et qu'ils utilisent la structure en mémoire.

La clé de revendication à utiliser pour identifier cette revendication est -260.

Les chaînes de l'objet JSON doivent être normalisées conformément à la composition canonique des formes de normalisation (*Normalisation Form Canonical Composition* — NFC) définie dans la norme Unicode. Les applications de décodage devraient toutefois être permissives et robustes à ces égards, et l'acceptation de tout type de conversion raisonnable est fortement encouragée. Si des données non normalisées sont trouvées au cours du décodage ou dans le cadre de fonctions de comparaisons ultérieures, les mises en œuvre devraient se comporter comme si les données entrées étaient normalisées conformément à la NFC.

4. Sérialisation et création de la charge utile du DCC

En ce qui concerne la structure de sérialisation, la séquence suivante est utilisée:



Le processus commence par l'extraction de données, par exemple à partir d'un répertoire de données de santé (ou d'une source externe de données), structurant les données extraites conformément aux schémas de DCC définis. Lors de ce processus, la conversion au format de données défini et la transformation pour la lisibilité humaine peuvent avoir lieu avant le début de la sérialisation vers le format CBOR. Les abréviations (acronymes) des revendications doivent correspondre, dans tous les cas, aux noms d'affichage avant la sérialisation et après la désérialisation.

Le contenu des données nationales facultatives n'est pas autorisé dans les certificats délivrés conformément au règlement (UE) 2021/953 ([8]). Le contenu des données est limité aux éléments de données définis dans l'ensemble minimal de données spécifié dans le règlement (UE) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19, JO L 211 du 15.6.20211, p. 1.

5. **Encodages de transport**

5.1. *Brut*

Pour les interfaces de données arbitraires, le conteneur du HCERT et ses charges utiles peuvent être transférés tels quels, en utilisant n'importe quel transport de données sous-jacent, sûr et fiable à 8 bits. Ces interfaces peuvent comprendre une communication en champ proche (*Near-Field Communication* — NFC), un Bluetooth ou un transfert via un protocole de couche application, par exemple le transfert d'un HCERT de l'émetteur vers l'appareil mobile du titulaire.

Si le transfert du HCERT de l'émetteur vers le titulaire est basé sur une interface de présentation uniquement (par exemple, SMS, courrier électronique), l'encodage de transport brut n'est évidemment pas applicable.

5.2. *Code-barres*

5.2.1. Compression de la charge utile (CWT)

Afin de réduire la taille et d'améliorer la vitesse et la fiabilité du processus de lecture du HCERT, le CWT doit être comprimé, en utilisant le ZLIB (RFC 1950 ([9])) et le mécanisme de compression Deflate, au format défini dans la RFC 1951 ([10]).

5.2.2. Code-barres QR 2D

Afin de mieux gérer les équipements anciens conçus pour fonctionner sur des charges utiles ASCII, le CWT comprimé est encodé au format ASCII à l'aide de Base45 avant d'être encodé en un code-barres 2D.

Le format QR tel que défini dans la norme (ISO/IEC 18004:2015) doit être utilisé pour la génération du code-barres 2D. Un taux de correction d'erreur de «Q» (environ 25 %) est recommandé. Étant donné que Base45 est utilisé, le code QR doit utiliser l'encodage alphanumérique (mode 2, indiqué par les symboles 0010).

Afin que les vérificateurs puissent détecter le type de données encodées et sélectionner le système de décodage et de traitement approprié, les données encodées avec Base45 (conformément à la présente spécification) doivent avoir pour préfixe la chaîne d'identifiant de contexte «HC1:». Les versions futures de la présente spécification ayant une incidence sur la compatibilité rétrospective devront définir un nouvel identifiant de contexte, tandis que le caractère suivant la mention «HC» devra être tiré du jeu de caractères [1-9A-Z]. L'ordre des augmentations est défini selon cette séquence, c'est-à-dire d'abord [1-9], puis [A-Z].

Il est recommandé de faire apparaître le code optique sur le média de présentation avec une diagonale comprise entre 35 mm et 60 mm, afin de prendre en compte les lecteurs à optique fixe pour lesquels le média de présentation doit être placé à la surface du lecteur.

Si le code optique est imprimé sur papier à l'aide d'une imprimante à basse résolution (< 300 dpi), il faut veiller à ce que la forme carrée de chaque symbole (point) du code QR soit parfaitement respectée. Si l'échelle n'est pas proportionnelle, certaines lignes ou colonnes du QR comporteront des symboles rectangulaires, ce qui nuira à la lisibilité dans de nombreux cas.

6. **Format des listes de confiance (*trust lists*) (listes de CSCA et de DSC)**

Chaque État membre est tenu de fournir une liste mentionnant une ou plusieurs autorités nationales de signature de certificats (*Country Signing Certificate Authorities* — CSCA) et une liste de tous les certificats de signataire de documents (*Document Signer Certificates* — DSC) valides, et de tenir ces listes à jour.

6.1. *Simplification relative aux CSCA/DSC*

À partir de la présente version des spécifications, les États membres ne peuvent présumer que les informations relatives aux listes de révocation de certificat (*Certificate Revocation List* — CRL) puissent être utilisées, ou que la période d'utilisation des clés privées puisse être vérifiée par les responsables de la mise en œuvre.

Le principal mécanisme de validation consistera plutôt dans le fait que le certificat figure dans la version la plus récente de cette liste de certificats.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

6.2. *Infrastructure à clé publique (ICP) des DVLMe (OACI) et centres de confiance*

Les États membres peuvent avoir recours à une CSCA distincte, mais peuvent également communiquer leurs certificats CSCA de DVLMe et/ou DSC existants; ils peuvent même choisir de se procurer ceux-ci auprès de centres de confiance (commerciaux) et les communiquer. Toutefois, un DSC doit toujours être signé par la CSCA communiquée par cet État membre.

7. **Considérations de sécurité**

Lors de la conception d'un système fondé sur la présente spécification, les États membres identifient, analysent et contrôlent certains éléments liés à la sécurité.

Les éléments qui devraient être pris en considération sont au minimum les suivants:

7.1. *Durée de validité de la signature du HCERT*

L'émetteur du HCERT est tenu de limiter la durée de validité de la signature en précisant le délai d'expiration de la signature. Le titulaire d'un certificat sanitaire est ainsi tenu de le renouveler périodiquement.

La durée de validité acceptable peut être déterminée par des contraintes pratiques. Par exemple, un voyageur peut ne pas avoir la possibilité de renouveler le certificat sanitaire au cours d'un voyage à l'étranger. Toutefois, il se peut également qu'un émetteur envisage la possibilité d'une quelconque compromission de la sécurité l'obligeant à retirer un DSC (ce qui invalide tous les certificats sanitaires délivrés au moyen de la clé dont la validité se situe encore dans leur période de validité). Les conséquences d'un tel événement peuvent être limitées en procédant régulièrement à la reconduction des clés de l'émetteur et en exigeant le renouvellement de tous les certificats sanitaires, à intervalles raisonnables.

7.2. *Gestion des clés*

La présente spécification repose largement sur des mécanismes cryptographiques solides pour garantir l'intégrité des données et l'authentification de l'origine des données. Il est donc nécessaire de préserver la confidentialité des clés privées.

La confidentialité des clés cryptographiques peut être compromise de différentes manières, par exemple:

— le processus de génération des clés peut être déficient, donnant lieu à des clés fragiles,

— les clés peuvent être vulnérables du fait d'une erreur humaine,

— les clés peuvent être volées par des délinquants externes ou internes,

— les clés peuvent être calculées à l'aide d'une analyse cryptographique.

Afin d'atténuer les risques liés à une éventuelle faiblesse de l'algorithme de signature, exposant les clés privées à une compromission par analyse cryptographique, la présente spécification recommande à tous les participants de mettre en œuvre un algorithme de signature secondaire de secours, fondé sur des paramètres différents ou un problème mathématique différent de celui du primaire.

En ce qui concerne les risques mentionnés liés aux modalités de fonctionnement des émetteurs, des mesures d'atténuation visant à garantir un contrôle efficace doivent être mises en œuvre, de manière à générer, stocker et utiliser les clés privées dans des modules matériels de sécurité (*Hardware Security Modules* — HSM). Il est vivement recommandé d'utiliser des HSM pour la signature des certificats sanitaires.

Indépendamment de la question de savoir si un émetteur décide d'utiliser ou non des HSM, il convient d'établir un calendrier de reconduction de clés dans lequel la fréquence des reconductions est proportionnelle à la vulnérabilité des clés aux réseaux externes, aux autres systèmes et au personnel. Un calendrier de reconduction bien choisi limite également les risques associés aux certificats sanitaires délivrés par erreur, car il permet à un émetteur de révoquer ces certificats par lots, en procédant au retrait d'une clé, si nécessaire.

7.3. *Validation des données d'entrée*

Les présentes spécifications peuvent être utilisées d'une manière qui implique de recevoir des données provenant de sources non fiables versées dans des systèmes qui peuvent être essentiels à la mission concernée. Afin de minimiser les risques associés à ce vecteur d'attaque, tous les champs d'entrée doivent être correctement validés par type, longueur et contenu des données. La signature de l'émetteur doit également être vérifiée avant tout traitement du contenu du HCERT. Toutefois, la validation de la signature de l'émetteur implique de parcourir d'abord l'en-tête protégé de l'émetteur, dans lequel un assaillant potentiel peut tenter d'injecter des informations soigneusement conçues pour compromettre la sécurité du système.

8. **Gestion de la confiance**

La signature du HCERT nécessite une clé publique à vérifier. Les États membres doivent mettre ces clés publiques à disposition. En fin de compte, chaque vérificateur doit disposer d'une liste de toutes les clés publiques auxquelles il est disposé à accorder sa confiance (étant donné que la clé publique ne fait pas partie du HCERT).

Le système se compose de (seulement) deux couches; pour chaque État membre, un ou plusieurs certificats au niveau du pays, qui signent chacun un ou plusieurs certificats de signataire de documents qui sont utilisés dans les opérations quotidiennes.

Les certificats des États membres sont appelés certificats des autorités nationales de signature de certificats (CSCA) et sont (généralement) des certificats autosignés. Les États membres peuvent en avoir plusieurs (par exemple, en cas de décentralisation régionale). Ces certificats CSCA signent régulièrement les certificats de signataire de documents (DSC) utilisés pour signer les HCERT.

Le «secrétariat» joue un rôle fonctionnel. Il doit agréger et publier régulièrement les DSC des États membres, après les avoir vérifiés par rapport à la liste des certificats CSCA (qui ont été transmis et vérifiés par d'autres moyens).

La liste des certificats DSC qui en résulte doit ensuite fournir l'ensemble agrégé de clés publiques acceptables (et les *kids* correspondants) que les vérificateurs peuvent utiliser pour valider les signatures sur les HCERT. Les vérificateurs sont tenus d'aller chercher et de mettre à jour régulièrement cette liste.

Ces listes par État membre peuvent être adaptées au format convenant à la situation nationale. Ainsi, le format de fichier de cette liste de confiance (*trust list*) peut varier; par exemple, il peut s'agir d'un JWKS signé (format JWK conformément à la RFC 7517 ([11]), section 5) ou de tout autre format spécifique à la technologie utilisée dans cet État membre.

Pour garantir la simplicité du processus, les États membres peuvent à la fois communiquer leurs certificats CSCA existants à partir de leurs systèmes de DVLMe conformes aux normes de l'OACI ou, comme l'OMS le recommande, créer un système spécifiquement pour ce domaine de la santé.

8.1. *Identifiant de clé (kids)*

L'identifiant de clé (*kid*) est calculé lors de l'établissement de la liste des clés publiques de confiance à partir des DSC et consiste en une empreinte SHA-256 tronquée (8 premiers octets) du DSC encodée au format DER (brut).

Les vérificateurs n'ont pas besoin de calculer le *kid* sur la base du DSC et peuvent directement mettre l'identifiant de clé figurant dans le certificat sanitaire délivré en correspondance avec le *kid* figurant sur la *trust list*.

8.2. *Différences par rapport au modèle de confiance de l'ICP des DVLMe (OACI)*

Bien que fondé sur les meilleures pratiques du modèle de confiance de l'ICP des DVLMe de l'OACI, il convient de simplifier quelque peu le modèle dans un souci de rapidité:

— l'État membre peut soumettre plusieurs certificats CSCA,

— la période de validité du DSC (utilisation de la clé) peut être fixée à n'importe quelle durée ne dépassant pas celle du certificat CSCA et peut être absente,

— le DSC peut contenir des identifiants de politique (utilisation étendue de la clé) qui sont propres aux certificats sanitaires,

— les États membres peuvent choisir de ne jamais procéder à une vérification des révocations publiées et de se baser simplement sur les listes de DSC qu'ils obtiennent quotidiennement du secrétariat ou compilent eux-mêmes.

([11]) rfc7517 (ietf.org).

ANNEXE II

RÈGLES POUR COMPLÉTER LE CERTIFICAT COVID NUMÉRIQUE DE L'UE

Les règles générales concernant les ensembles de valeurs établies dans la présente annexe visent à assurer l'interopérabilité au niveau sémantique et permettent des mises en œuvre techniques uniformes pour le DCC. Les éléments figurant dans la présente annexe peuvent être utilisés pour les trois contextes différents (vaccination/test/rétablissement), tels que prévus par le règlement (UE) 2021/953. Seuls les éléments nécessitant une normalisation sémantique au moyen d'ensembles de valeurs codées sont énumérés dans la présente annexe.

La traduction des éléments codés dans la langue nationale relève de la responsabilité des États membres.

Pour tous les champs de données non mentionnés dans les descriptions des ensembles de valeurs ci-dessous, un encodage au format UTF-8 est recommandé (nom, centre de test, émetteur du certificat). Il est recommandé d'encoder les champs de données contenant les dates (date de naissance, date de vaccination, date du prélèvement de l'échantillon, date du premier résultat de test positif, dates de validité du certificat) conformément à la norme ISO 8601.

Si, pour une raison quelconque, les systèmes de codes privilégiés énumérés ci-dessous ne peuvent pas être utilisés, il est possible d'avoir recours à d'autres systèmes de codes internationaux et il y a lieu d'établir des orientations sur la manière de faire correspondre les codes de l'autre système à ceux du système privilégié. Le texte (les noms d'affichage) peut être utilisé, dans des cas exceptionnels, comme mécanisme de sauvegarde lorsque aucun code approprié n'est disponible dans les ensembles de valeurs définis.

Les États membres qui utilisent d'autres codages dans leurs systèmes devraient mettre ces codes en correspondance avec les ensembles de valeurs décrits. Les États membres sont responsables de ces éventuelles mises en correspondance.

Les ensembles de valeurs sont régulièrement mis à jour par la Commission avec le soutien du réseau «Santé en ligne» et du comité de sécurité sanitaire. Les ensembles de valeurs mis à jour sont publiés sur le site web concerné de la Commission, ainsi que sur la page web du réseau «Santé en ligne». Un historique des changements devrait être fourni.

1. **Maladie ou agent ciblé/Maladie ou agent dont le titulaire s'est rétabli: COVID-19 (SARS-CoV-2 ou un de ses variants)**

   Système de codes privilégié: SNOMED CT (nomenclature systématisée des termes cliniques en médecine).

   À utiliser dans les certificats 1, 2 et 3.

   Les codes sélectionnés doivent mentionner la COVID-19 ou, si des informations plus détaillées sur le variant génétique du SARS-CoV-2 sont nécessaires, mentionner ce variant dans le cas où ces informations détaillées sont indispensables pour des raisons épidémiologiques.

   Un exemple de code à utiliser est le code SNOMED CT 840539006 (COVID-19).

2. **Vaccin ou prophylaxie contre la COVID-19**

   Système de codes privilégié: SNOMED CT ou classification ATC (système de classification anatomique, thérapeutique et chimique).

   À utiliser dans le certificat 1.

   Des exemples de codes à utiliser issus des systèmes de codes privilégiés sont les codes SNOMED CT 1119305005 (vaccin antigénique SARS-CoV-2), 1119349007 (vaccin à ARNm SARS-CoV-2) ou J07BX03 (vaccins covid-19). L'ensemble de valeurs devrait être étendu lorsque de nouveaux types de vaccins sont mis au point et utilisés.

3. **Médicament vaccinal contre la COVID-19**

   Systèmes de codes privilégiés (par ordre de préférence):

   — registre des médicaments de l'Union européenne pour les vaccins bénéficiant d'une autorisation à l'échelle de l'Union (numéros d'autorisation),

   — un registre mondial des vaccins, tel que celui qui pourrait être établi par l'Organisation mondiale de la santé,

   — nom du médicament vaccinal dans les autres cas. Si le nom inclut des espaces blancs, il convient de remplacer ceux-ci par un trait d'union (–).

Nom de l'ensemble de valeurs: vaccin.

À utiliser dans le certificat 1.

Un exemple de code à utiliser, issu des systèmes de codes privilégiés, est EU/1/20/1528 (Comirnaty). Exemple de nom de vaccin à utiliser comme code: Sputnik–V (correspondant à Sputnik V).

4. **Titulaire de l'autorisation de mise sur le marché ou fabricant du vaccin contre la COVID-19**

Système de codes privilégié:

— code d'organisation provenant de l'Agence européenne des médicaments (EMA) [système concernant les substances, produits, organisations et référentiels (SPOR) pour les normes ISO IDMP],

— un registre mondial des titulaires d'autorisations de mise sur le marché ou des fabricants de vaccins, tel que celui qui pourrait être établi par l'Organisation mondiale de la santé,

— nom de l'organisation dans les autres cas. Si le nom inclut des espaces blancs, il convient de remplacer ceux-ci par un trait d'union (–).

À utiliser dans le certificat 1.

Un exemple de code à utiliser, issu des systèmes de codes privilégiés, est ORG-100001699 (AstraZeneca AB). Exemple de nom d'organisation à utiliser comme code: Sinovac–Biotech (correspondant à Sinovac Biotech).

5. **Nombre dans une série de doses ainsi que nombre total de doses dans la série**

À utiliser dans le certificat 1.

Deux champs:

1) nombre de doses administrées en un cycle

2) nombre de doses attendues pour un cycle complet (spécifique pour une personne au moment de l'administration)

Par exemple, 1/1 ou 2/2 indiquera que le cycle est achevé; y compris l'option 1/1 pour les vaccins comprenant deux doses, mais pour lesquels le protocole appliqué par l'État membre consiste à administrer une dose aux citoyens chez lesquels la COVID-19 a été diagnostiquée avant la vaccination. Le nombre total de doses dans la série devrait être indiqué tel qu'il ressort des informations disponibles au moment de l'administration de la dose. Par exemple, si, lors de la dernière injection en date, il s'avère qu'un vaccin spécifique nécessite une troisième injection (rappel), le second chiffre du champ doit l'indiquer (par exemple 2/3, 3/3, etc.).

6. **État membre ou pays tiers dans lequel le vaccin a été administré/le test a été effectué**

Système de codes privilégié: codes pays ISO 3166.

À utiliser dans les certificats 1, 2 et 3.

Contenu de l'ensemble de valeurs: la liste complète des codes à 2 lettres, disponible sous la forme d'un ensemble de valeurs défini dans la spécification FHIR (*Fast Healthcare Interoperability Resources* — ressources d'interopérabilité rapide des soins de santé) (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Type de test**

Système de codes privilégié: nomenclature LOINC (*Logical Observation Identifiers Names and Codes* — codes et noms d'identifiants d'observation logique).

À utiliser dans le certificat 2 et le certificat 3 si le soutien à la délivrance de certificats de rétablissement sur la base de types de test autres que le NAAT (*nucleic acid amplification test* — test d'amplification des acides nucléiques) est instauré par un acte délégué.

Les codes figurant dans cet ensemble de valeurs doivent faire référence à la méthode de test et être sélectionnés au minimum pour établir une distinction entre les tests NAAT et les tests RAT (*rapid antigen test* — test rapide de détection d'antigènes) comme indiqué dans le règlement (UE) 2021/953.

Un exemple de code à utiliser, issu des systèmes de codes privilégiés, est LP217198-3 (immunodosage rapide).

8. **Nom du fabricant et dénomination commerciale du test utilisé (facultatifs pour les tests NAAT)**

Système de codes privilégié: liste, établie par le comité de sécurité sanitaire (CSS), des tests rapides de détection d'antigènes, mise à jour par le JRC (base de données sur les dispositifs de diagnostic in vitro et les méthodes de dépistage de la COVID-19).

À utiliser dans le certificat 2.

Le contenu de l'ensemble de valeurs doit inclure la sélection d'un test rapide de détection d'antigènes figurant sur la liste commune et actualisée des tests rapides de détection d'antigènes pour le diagnostic de la COVID-19, établie sur la base de la recommandation du Conseil publiée au JO C 24 du 22.1.2021, p. 1, et approuvée par le comité de sécurité sanitaire. La liste est mise à jour par le JRC dans la base de données sur les dispositifs de diagnostic in vitro et les méthodes de dépistage de la COVID-19 à l'adresse suivante: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Pour ce système de codes, il convient d'utiliser des champs pertinents tels que l'identifiant du dispositif de test, le nom du test et du fabricant, en respectant le format structuré du JRC disponible à l'adresse suivante: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Résultat du test**

Système de codes privilégié: SNOMED CT.

À utiliser dans le certificat 2.

Les codes sélectionnés doivent permettre de faire la distinction entre les résultats de test positifs et négatifs (détectés ou non détectés). Des valeurs supplémentaires (telles que «indéterminé») peuvent être ajoutées si les cas d'utilisation le requièrent.

Des exemples de codes à utiliser, issus du système de codes privilégié, sont 260415000 (non détectés) et 260373001 (détectés).

ANNEXE III

STRUCTURE COMMUNE DE L'IDENTIFIANT UNIQUE DU CERTIFICAT

1. **Introduction**

Chaque certificat COVID numérique de l'UE comporte un identifiant unique du certificat (*unique certificate identifier* — UCI) qui favorise l'interopérabilité des DCC. L'UCI peut être utilisé pour vérifier le certificat. Les États membres sont chargés de la mise en œuvre de l'UCI. L'UCI est un moyen de vérifier l'authenticité du certificat et, le cas échéant, d'établir un lien vers un système d'enregistrement, par exemple, un système d'information sur la vaccination (*immunisation information system* — IIS). Cet identifiant doit également permettre aux États membres d'attester (sur papier et par voie numérique) que des personnes ont été vaccinées ou testées.

2. **Composition de l'identifiant unique du certificat**

L'UCI doit avoir une structure et un format communs facilitant l'interprétabilité des informations par l'homme et/ou par la machine et peut porter sur des éléments tels que l'État membre de vaccination, le vaccin lui-même et un identifiant propre à l'État membre. Cela assure aux États membres une certaine souplesse pour le formater, en respectant pleinement la législation en matière de protection des données. L'ordre des différents éléments suit une hiérarchie définie qui peut permettre de modifier les blocs à l'avenir sans nuire à l'intégrité structurelle.

Les solutions possibles pour la composition de l'UCI constituent un spectre dans lequel la modularité et l'interprétabilité par l'homme sont les deux principaux paramètres de diversification et une caractéristique fondamentale:

— modularité: la mesure dans laquelle le code est composé de blocs constitutifs distincts contenant des informations sémantiquement différentes,

— interprétabilité par l'homme: la mesure dans laquelle le code est porteur de sens ou peut être interprété par le lecteur humain,

— unique à l'échelle mondiale; l'identifiant du pays ou de l'autorité est bien géré; et chaque pays (autorité) est censé bien gérer son segment de l'espace de noms en ne recyclant jamais les identifiants et en ne les réassignant pas. La combinaison de ces éléments garantit que chaque identifiant est unique à l'échelle mondiale.

3. **Exigences générales**

En ce qui concerne l'UCI, les exigences à respecter sont les suivantes:

1) Jeu de caractères: seuls les caractères alphanumériques US-ASCII majuscules («A» à «Z», «0» à «9») sont autorisés, avec des caractères spéciaux supplémentaires séparateurs selon la RFC3986 ([1]) ([2]), à savoir {'/','#',':'}.

2) Longueur maximale: pour les concepteurs, l'objectif devrait être une longueur de 27 à 30 caractères ([3]).

3) Préfixe de version: fait référence à la version du schéma UCI. Le préfixe de version est «01» pour la présente version du document; le préfixe de version est composé de deux chiffres.

4) Préfixe du pays: le code pays est spécifié par la norme ISO 3166-1. Les codes plus longs [c'est-à-dire 3 caractères et plus (par exemple, «UNHCR»)] sont réservés à une utilisation future.

5) Suffixe de code/Somme de contrôle

5.1. Les États membres devraient utiliser une somme de contrôle lorsqu'une transmission, une transcription (humaine) ou une autre forme de corruption peuvent se produire (c'est-à-dire en cas d'utilisation en version imprimée).

5.2. La somme de contrôle ne doit pas être utilisée pour valider le certificat et ne fait pas techniquement partie de l'identifiant, mais sert à vérifier l'intégrité du code. Cette somme de contrôle devrait être le résumé ISO 7812-1 (LUHN-10) ([4]) de l'UCI entier au format de transport filaire/numérique. La somme de contrôle est séparée du reste de l'UCI par un caractère «#».

([1]) rfc3986 (ietf.org).

([2]) Les champs correspondant, par exemple, au sexe, au numéro de lot, au centre d'administration, à l'identification du professionnel de santé ou à la prochaine date de vaccination peuvent ne pas être nécessaires à des fins autres que médicales.

([3]) Pour la mise en œuvre avec des codes QR, les États membres pourraient envisager d'utiliser un jeu supplémentaire de caractères d'une longueur maximale totale de 72 caractères (y compris les 27 à 30 caractères de l'identifiant proprement dit) pour transmettre d'autres informations. Il appartient aux États membres de définir les spécifications de ces informations.

([4]) L'algorithme Luhn mod N est une extension de l'algorithm de Luhn (aussi appelé algorithme mod 10) utilisé pour les codes numériques, qui sert par exemple à calculer les sommes de contrôle des numéros de cartes de crédit. L'extension permet à l'algorithme de fonctionner avec des séquences de valeurs dans n'importe quelle base (en l'occurrence, des caractères alphabétiques).

Il convient de veiller à la compatibilité rétrospective: les États membres qui, au fil du temps, modifient la structure de leurs identifiants (dans la version principale, actuellement fixée à v1) doivent veiller à ce que deux identifiants identiques représentent le même certificat ou la même déclaration de vaccination. En d'autres termes, les États membres ne peuvent pas recycler les identifiants.

4. **Options en matière d'identifiants uniques pour les certificats de vaccination**

Les lignes directrices du réseau «Santé en ligne» concernant les certificats de vaccination vérifiables et les éléments d'interopérabilité de base ([5]) offrent aux États membres et à d'autres parties diverses options qui peuvent coexister entre différents États membres. Les États membres peuvent déployer ces diverses options dans différentes versions du schéma UCI.

([5]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

ANNEXE IV

GOUVERNANCE DES CERTIFICATS DE CLÉ PUBLIQUE

1. Introduction

L'échange sécurisé et fiable de clés de signature pour les certificats COVID numériques de l'UE (*Digital COVID certificates*, DCC) entre les États membres s'effectue par l'intermédiaire du service passerelle des certificats COVID numériques de l'UE (*Digital COVID Certificate Gateway*, DCCG), qui sert de répertoire central des clés publiques. Le DCCG donne aux États membres les moyens de publier les clés publiques correspondant aux clés privées qu'ils utilisent pour signer des certificats COVID numériques. Les États membres utilisateurs peuvent avoir recours au DCCG pour obtenir en temps voulu des clés publiques actualisées. Par la suite, le DCCG pourra être étendu pour permettre l'échange d'informations supplémentaires fiables fournies par les États membres, telles que des règles de validation concernant les DCC. Le modèle de confiance du cadre DCC est une infrastructure à clé publique (ICP). Chaque État membre a une ou plusieurs autorités nationales de signature de certificats (CSCA), dont les certificats ont une durée de vie relativement longue. Selon la décision de l'État membre, il peut s'agir d'une CSCA identique à celle utilisée pour les documents de voyage lisibles par machine ou d'une autorité différente. La CSCA délivre des certificats de clé publique pour les signataires de documents nationaux (c'est-à-dire les signataires des DCC), dont la durée de vie est brève, qui sont appelés certificats de signataire de documents (DSC). La CSCA joue un rôle d'ancre de confiance, de sorte que les États membres utilisateurs peuvent utiliser le certificat CSCA pour valider l'authenticité et l'intégrité des DSC qui changent régulièrement. Une fois la validation effectuée, les États membres peuvent fournir ces certificats (ou uniquement les clés publiques qu'ils contiennent) à leurs applications de validation des DCC. Outre les CSCA et les DSC, le DCCG utilise également les ICP pour authentifier les transactions, signer les données, comme base d'authentification et comme moyen de garantir l'intégrité des canaux de communication entre les États membres et le DCCG.

Les signatures numériques peuvent être utilisées pour garantir l'intégrité et l'authenticité des données. Les ICP établissent la confiance en associant des clés publiques à des identités vérifiées (ou des émetteurs). Cela est nécessaire pour permettre aux autres participants de vérifier l'origine des données et l'identité de l'interlocuteur et de décider s'ils peuvent leur accorder leur confiance. Le DCCG fait appel à des certificats de clé publique multiples à des fins d'authenticité. La présente annexe définit les certificats de clé publique utilisés et la manière dont ils doivent être conçus pour permettre une large interopérabilité entre les États membres. Elle fournit davantage de détails sur les certificats de clé publique nécessaires ainsi que des orientations sur les modèles de certificats et les périodes de validité pour les États membres qui souhaitent avoir leur propre CSCA. Étant donné que les DCC doivent être vérifiables pendant un laps de temps déterminé (à compter de la délivrance, expiration après un certain délai), il est nécessaire de définir un modèle de vérification pour toutes les signatures apposées sur les certificats de clé publique et les DCC.

2. Terminologie

Le tableau suivant contient les abréviations et la terminologie utilisées dans la présente annexe.

Terme	Définition
Certificat	Ou certificat de clé publique. Certificat X.509 v3 contenant la clé publique d'une entité
CSCA	Autorité nationale de signature de certificats
DCC	Certificat COVID numérique de l'UE. Document numérique signé contenant des informations sur la vaccination, les tests ou le rétablissement
DCCG	Service passerelle du certificat COVID numérique de l'UE. Système utilisé pour l'échange de DSC entre les États membres.
$DCCG_{TA}$	Certificat d'ancre de confiance du DCCG. La clé privée correspondante est utilisée pour signer la liste de tous les certificats CSCA hors ligne.
$DCCG_{TLS}$	Certificat de serveur TLS (*Transport Layer Security* — Sécurité de la couche de transport) du DCCG.
DSC	Certificat de signataire de documents. Certificat de clé publique de l'autorité de signature des documents d'un État membre (par exemple, un système autorisé à signer des DCC). Ce certificat est délivré par la CSCA de l'État membre.
ECDSA	Algorithme de signature numérique à courbe elliptique. Algorithme de signature cryptographique reposant sur les courbes elliptiques
État membre	État membre de l'Union européenne

Terme	Définition
mTLS	TLS mutuels. Protocole de sécurité de la couche de transport avec authentification mutuelle
NB	Système d'arrière-plan national d'un État membre
NB_{CSCA}	Certificat CSCA d'un État membre (il peut y en avoir plus d'un)
NB_{TLS}	Certificat d'authentification client TLS d'un système d'arrière-plan national
NB_{UP}	Certificat utilisé par un système d'arrière-plan national pour signer des paquets de données qui sont téléversés dans le DCCG
ICP	Infrastructure à clé publique. Modèle de confiance reposant sur les certificats de clé publique et les autorités de certification
RSA	Algorithme de cryptographie asymétrique reposant sur la factorisation des nombres entiers, utilisé pour les signatures numériques ou le chiffrement asymétrique

3. **Flux de communication et services de sécurité du DCCG**

La présente section donne un aperçu des flux de communication et des services de sécurité dans le système du DCCG. Elle définit également les clés et certificats utilisés pour protéger la communication, les informations téléversées, les DCC et une *trust list* signée qui contient tous les certificats CSCA enrôlés. Le DCCG fonctionne comme une plateforme de données qui permet l'échange de paquets de données signés pour les États membres.

Les paquets de données téléversés sont fournis par le DCCG «en l'état», ce qui signifie que le DCCG n'ajoute ni ne supprime aucun DSC des paquets qu'il reçoit. Le système d'arrière-plan national (*national backend* — NB) des États membres est en mesure de vérifier l'intégrité et l'authenticité de bout en bout des données téléversées. En outre, les systèmes d'arrière-plan nationaux et le DCCG utiliseront l'authentification mutuelle TLS pour établir une connexion sécurisée. Ces mesures s'ajoutent aux signatures figurant dans les données échangées.

3.1. *Authentification et établissement de la connexion*

Le DCCG utilise le protocole TLS avec authentification mutuelle pour établir un canal crypté authentifié entre le système d'arrière-plan national de l'État membre (NB) et l'environnement du service passerelle. Par conséquent, le DCCG détient un certificat de serveur TLS, dit «$DCCG_{TLS}$», et les systèmes d'arrière-plan nationaux détiennent un certificat client TLS — appelé NB_{TLS}. Les modèles de certificat sont fournis à la *section 5*. Tous les systèmes d'arrière-plan nationaux peuvent fournir leur propre certificat TLS. Ce certificat sera explicitement placé sur liste blanche et il peut par conséquent être délivré par une autorité de certification publique de confiance (par exemple, une autorité de certification qui respecte les exigences de base du CA/Browser Forum), par une autorité nationale de certification ou être autosigné. Chaque État membre est responsable de ses données nationales et de la protection de la clé privée utilisée pour établir la connexion avec le DCCG. L'approche «Apporter son propre certificat» requiert une procédure d'enregistrement et d'identification bien définie, ainsi que des procédures de révocation et de renouvellement, qui sont décrites aux sections 4.1, 4.2 et 4.3. Le DCCG utilise une liste blanche sur laquelle les certificats TLS des NB sont inscrits lorsque leur enregistrement a été effectué avec succès. Seuls les NB qui s'authentifient au moyen d'une clé privée correspondant à un certificat figurant sur la liste blanche peuvent établir une connexion sécurisée avec le DCCG. Le DCCG utilisera également un certificat TLS qui permet aux NB de vérifier qu'ils établissent effectivement une connexion avec le «véritable» DCCG et non avec une entité malveillante qui se fait passer pour le DCCG. Le certificat du DCCG sera fourni aux NB après un enregistrement effectué avec succès. Le certificat $DCCG_{TLS}$ sera délivré par une autorité de certification publique de confiance (incluse dans tous les principaux navigateurs). Il incombe aux États membres de vérifier que leur connexion au DCCG est sécurisée (par exemple, en vérifiant l'empreinte digitale du certificat $DCCG_{TLS}$ du serveur auquel ils sont connectés par rapport à celle qui a été fournie après l'enregistrement).

3.2. *Autorités nationales de signature de certificats et modèle de validation*

Les États membres participant au cadre DCCG doivent faire appel à une CSCA pour délivrer les DSC. Un État membre peut avoir plusieurs CSCA (par exemple, en cas de décentralisation régionale). Chaque État membre peut soit avoir recours aux autorités de certification existantes, soit mettre en place une autorité de certification spécifique (éventuellement autosignée) pour le système de DCC.

Les États membres doivent présenter leur(s) certificat(s) CSCA à l'exploitant du DCCG lors de la procédure officielle d'enrôlement. Après l'enregistrement réussi de l'État membre (voir la section 4.1 pour plus de détails), l'exploitant du DCCG mettra à jour une *trust list* signée contenant tous les certificats CSCA actifs dans le cadre du DCC. L'exploitant du DCCG utilisera une paire de clés asymétriques dédiée pour signer la *trust list* et les certificats dans un environnement hors ligne. La clé privée ne sera pas stockée dans le système du DCCG en ligne, afin qu'un attaquant ne puisse pas compromettre la *trust list* si le système en ligne est compromis. Le certificat d'ancre de confiance correspondant $DCCG_{TA}$ sera fourni aux systèmes d'arrière-plan nationaux lors du processus d'enrôlement.

Les États membres peuvent obtenir la *trust list* auprès du DCCG pour leurs procédures de vérification. La CSCA est définie comme l'autorité de certification (CA) qui délivre des DSC, c'est pourquoi les États membres qui utilisent une hiérarchie d'autorités de certification à plusieurs niveaux (par exemple, CA racine — > CSCA — > DSC) doivent fournir l'autorité de certification subordonnée qui délivre les DSC. Dans ce cas, si un État membre fait appel à une autorité de certification existante, le système de DCC fera abstraction de tout ce qui se trouve au-dessus de la CSCA et ne placera sur la liste blanche que la CSCA en tant qu'ancre de confiance (même s'il s'agit d'une CA subordonnée). C'est le modèle de l'OACI, qui n'autorise que 2 niveaux — une CSCA «racine» et un DSC «feuille» signé par cette seule CSCA.

Si un État membre exploite sa propre CSCA, il est responsable du fonctionnement sécurisé et de la gestion des clés de cette autorité. La CSCA joue le rôle d'ancre de confiance pour les DSC et, par conséquent, la protection de la clé privée de la CSCA est essentielle pour l'intégrité de l'environnement du DCC. Le modèle de vérification dans l'ICP des DCC est le modèle *shell*, qui prévoit que tous les certificats présents dans la validation du chemin du certificat doivent être valables à un moment précis (c'est-à-dire au moment de la validation de la signature). Par conséquent, les restrictions suivantes s'appliquent:

— la CSCA ne doit pas délivrer de certificats dont la durée de validité est supérieure à celle du certificat de la CA lui-même;

— le signataire de documents ne doit pas signer de documents dont la durée de validité est supérieure à celle du DSC proprement dit;

— les États membres qui exploitent leur propre CSCA doivent définir des périodes de validité pour leur CSCA et tous les certificats délivrés, et ils doivent prendre soin de renouveler les certificats.

La section 4.2 contient des recommandations concernant les périodes de validité.

3.3. *Intégrité et authenticité des données téléversées*

Les systèmes d'arrière-plan nationaux peuvent utiliser le DCCG pour téléverser et télécharger des paquets de données signés numériquement après une authentification mutuelle réussie. Au début, ces paquets de données contiennent les DSC des États membres. La paire de clés utilisée par le système d'arrière-plan national pour la signature numérique des paquets de données téléversés dans le système du DCCG est appelée «paire de clés du système d'arrière-plan national pour signature de téléversement» et on désigne le certificat de clé publique correspondant par l'abréviation NB_{UP}. Chaque État membre apporte son propre certificat NB_{UP}, qui peut être autosigné ou délivré par une autorité de certification existante, telle qu'une autorité de certification publique (c'est-à-dire une autorité de certification qui délivre des certificats conformément aux exigences de base du CA/Browser Forum). Le certificat NB_{UP} doit être différent de tous les autres certificats utilisés par l'État membre (certificats CSCA, client TLS ou DSC).

Les États membres doivent fournir le certificat de téléversement à l'exploitant du DCCG au cours de la procédure d'enregistrement initiale (voir la section 4.1 pour plus de détails). Chaque État membre est responsable de ses données nationales et doit assurer la protection de la clé privée utilisée pour signer les téléversements.

D'autres États membres peuvent vérifier les paquets de données signés à l'aide des certificats de téléversement fournis par le DCCG. Le DCCG vérifie l'authenticité et l'intégrité des données téléversées au moyen du certificat de téléversement du NB avant que les données ne soient fournies aux autres États membres.

3.4. *Exigences relatives à l'architecture technique du DCCG*

Les exigences relatives à l'architecture technique du DCCG sont les suivantes:

— le DCCG utilise l'authentification TLS mutuelle pour établir une connexion cryptée authentifiée avec les NB. Par conséquent, le DCCG tient à jour une liste blanche de certificats clients NB_{TLS} enregistrés,

— le DCCG utilise deux certificats numériques ($DCCG_{TLS}$ et $DCCG_{TA}$) avec deux paires de clés distinctes. La clé privée de la paire de clés $DCCG_{TA}$ est conservée hors ligne (et non sur les composants en ligne du DCCG),

— le DCCG tient à jour une *trust list* des certificats NB_{CSCA} signée avec la clé privée $DCCG_{TA}$,

— le chiffrement utilisé doit satisfaire aux exigences de la section 5.1.

4. **Gestion du cycle de vie des certificats**

4.1. *Enregistrement des systèmes d'arrière-plan nationaux*

Les États membres doivent s'enregistrer auprès de l'exploitant du DCCG pour participer au système du DCCG. La présente section décrit la procédure technique et opérationnelle qui doit être suivie pour enregistrer un système d'arrière-plan national.

L'exploitant du DCCG et l'État membre doivent échanger des informations sur les personnes à contacter pour des questions techniques sur le processus d'enrôlement. Il est présumé que ces personnes de contact bénéficient d'une habilitation de leur État membre et que leur identification/authentification est effectuée par d'autres canaux. Par exemple, l'authentification peut être réalisée lorsque la personne chargée des contacts techniques d'un État membre fournit par courriel les certificats sous forme de fichiers cryptés par mot de passe et communique par téléphone à l'exploitant du DCCG le mot de passe correspondant. D'autres canaux sécurisés définis par l'exploitant du DCCG peuvent également être utilisés.

L'État membre doit fournir trois certificats numériques au cours du processus d'enregistrement et d'identification:

— le certificat TLS de l'État membre NB_{TLS}

— le certificat de téléversement de l'État membre NB_{UP}

— le(s) certificat(s) CSCA de l'État membre NB_{CSCA}

Tous les certificats fournis doivent respecter les exigences définies à la section 5. L'exploitant du DCCG vérifiera que le certificat fourni satisfait aux exigences de la section 5. Après l'identification et l'enregistrement, l'exploitant du DCCG:

— ajoute le(s) certificat(s) NB_{CSCA} à la *trust list* signée au moyen de la clé privée correspondant à la clé publique $DCCG_{TA}$;

— ajoute le certificat NB_{TLS} à la liste blanche du point de terminaison TLS du DCCG;

— ajoute le certificat NB_{UP} au système du DCCG;

— fournit le certificat de clé publique $DCCG_{TA}$ et $DCCG_{TLS}$ à l'État membre.

4.2. *Autorités de certification, périodes de validité et renouvellement*

Si un État membre souhaite exploiter sa propre CSCA, les certificats CSCA peuvent être des certificats autosignés. Ils jouent le rôle d'ancre de confiance de l'État membre et, par conséquent, l'État membre doit prendre des mesures robustes pour protéger la clé privée correspondant à la clé publique du certificat CSCA. Il est recommandé aux États membres d'utiliser un système hors ligne pour leur CSCA, c'est-à-dire un système informatique qui n'est connecté à aucun réseau. L'accès au système doit être soumis à un contrôle multiple (par exemple, selon le principe des quatre yeux). Après la signature des DSC, des contrôles opérationnels doivent être appliqués et le système qui détient la clé CSCA privée doit être stocké en toute sécurité et faire l'objet de contrôles d'accès rigoureux. Des modules de sécurité matériels ou des cartes intelligentes peuvent être utilisés pour renforcer la protection de la clé privée CSCA. Les certificats numériques prévoient une période de validité qui impose de respecter le renouvellement des certificats. Le renouvellement est nécessaire pour utiliser de nouvelles clés cryptographiques et adapter les tailles de clés lorsque de nouveaux progrès dans le domaine du calcul ou de nouvelles attaques menacent la sécurité de l'algorithme de cryptographie utilisé. Le modèle *shell* s'applique (voir section 3.2).

Sur la base d'une durée de validité d'un an pour les certificats COVID numériques, les durées de validité recommandées sont les suivantes:

— CSCA: 4 ans

— DSC: 2 ans

— téléversement: 1-2 ans

— authentification du client TLS: 1-2 ans

Pour que le renouvellement puisse avoir lieu en temps voulu, les périodes d'utilisation recommandées pour les clés privées sont les suivantes:

— CSCA: 1 an

— DSC: 6 mois

Les États membres doivent créer de nouveaux certificats de téléversement et de nouveaux certificats TLS en temps voulu, par exemple un mois avant la date d'expiration, afin de garantir un fonctionnement harmonieux. Les certificats CSCA et les DSC devraient être renouvelés au moins un mois avant que l'utilisation de la clé privée ne prenne fin (en tenant compte des procédures opérationnelles nécessaires). Les États membres doivent fournir à l'exploitant du DCCG des certificats CSCA, des certificats de téléversement et des certificats TLS actualisés. Les certificats périmés doivent être retirés de la liste blanche et de la *trust list*.

Les États membres et l'exploitant du DCCG doivent assurer le suivi de la validité de leurs propres certificats. Il n'existe pas d'entité centrale qui assure le suivi de la validité des certificats et en informe les participants.

4.3. *Révocation de certificats*

En général, les certificats numériques peuvent être révoqués par leur autorité de certification émettrice au moyen des listes de révocation des certificats ou du protocole de vérification des certificats en ligne (*Online Certificate Status Protocol Responder* — service OCSP). Les CSCA pour le système de DCC devraient fournir des listes de révocation de certificats (CRL). Même si ces CRL ne sont pas utilisées actuellement par les autres États membres, elles devaient être intégrées en prévision d'applications futures. Si une CSCA décide de ne pas fournir de CRL, les DSC de cette CSCA devront être renouvelés lorsque les CRL deviendront obligatoires. Pour la validation des DSC, les vérificateurs devraient utiliser les CRL et non le service OCSP. Il est recommandé que le système d'arrière-plan national procède à la validation nécessaire des DSC téléchargés à partir du DCCG et ne transmette aux validateurs de DCC nationaux qu'une série de DSC dignes de confiance et validés. Les validateurs des DCC ne devraient pas effectuer de contrôle de révocation sur les DSC dans le cadre de leur processus de validation. Cela correspond, notamment, au souci de protéger la vie privée des titulaires de DCC en prévenant tout risque que l'utilisation d'un DSC donné puisse être surveillée par le service OCSP qui lui est associé.

Les États membres peuvent retirer leurs DSC du DCCG de leur propre initiative en utilisant des certificats de téléversement et des certificats TLS valides. Lorsqu'un DSC est supprimé, tous les DCC délivrés avec ce DSC deviendront invalides lorsque les États membres consulteront les listes de DSC actualisées. La protection des clés privées correspondant aux DSC est cruciale. Les États membres doivent informer l'exploitant du DCCG lorsqu'ils doivent révoquer des certificats de téléversement ou TLS, par exemple en raison d'une compromission du système d'arrière-plan national. L'exploitant du DCCG peut alors retirer la confiance accordée au certificat concerné, par exemple en le supprimant de la liste blanche TLS. L'exploitant du DCCG peut supprimer les certificats de téléversement de la base de données DCCG. Les paquets signés avec la clé privée correspondant à ce certificat de téléversement deviendront invalides lorsque les systèmes d'arrière-plan nationaux retireront la confiance accordée au certificat de téléversement révoqué. Si un certificat CSCA doit être révoqué, les États membres doivent en informer l'exploitant du DCCG ainsi que les autres États membres avec lesquels ils entretiennent des relations de confiance. L'exploitant du DCCG publiera une nouvelle *trust list* sur laquelle le certificat concerné ne figurera plus. Tous les DSC émis par cette CSCA deviendront invalides lorsque les États membres mettront à jour leur magasin de confiance d'arrière-plan national. Si le certificat $DCCG_{TLS}$ ou le certificat $DCCG_{TA}$ doit être révoqué, l'exploitant du DCCG et les États membres doivent collaborer pour établir une nouvelle connexion TLS de confiance ainsi qu'une nouvelle *trust list*.

5. **Modèles de certificats**

La présente section énonce des exigences et fournit des orientations en ce qui concerne la cryptographie et établit également des exigences relatives aux modèles de certificat. Pour ce qui concerne les certificats DCCG, la présente section définit les modèles de certificats.

5.1. *Exigences cryptographiques*

Les algorithmes de cryptographie et les suites cryptographiques TLS seront choisis sur la base des recommandations en vigueur de l'Office fédéral allemand de la sécurité de l'information (BSI) ou du SOG-IS.Ces recommandations et celles d'autres institutions et organismes de normalisation sont similaires. Les recommandations figurent dans les orientations techniques TR 02102-1 et TR 02102-2 ([1]) ou dans les mécanismes cryptographiques approuvés du SOG-IS ([2]).

5.1.1. Exigences relatives au DSC

Les exigences prévues à l'annexe I, section 3.2.2 sont applicables. Par conséquent, il est vivement recommandé aux signataires de documents d'utiliser l'algorithme de signature numérique à courbe elliptique (ECDSA) avec la courbe NIST-p-256 (telle que définie à l'appendice D de la norme FIPS PUB 186-4). Les autres courbes elliptiques ne sont pas prises en charge. En raison des contraintes d'espace imposées par le DCC, les États membres ne devraient pas

([1]) BSI - Technical Guidelines TR-02102 (bund.de)
([2]) SOG-IS - Supporting documents (sogis.eu)

utiliser le RSA-PSS, même s'il est autorisé en tant qu'algorithme de secours. Si les États membres ont recours au RSA-PSS, ils doivent utiliser un modulus d'une taille de 2048 ou 3072 bits au maximum. SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits doit être utilisé comme fonction de hachage cryptographique (voir ISO/IEC 10118-3: 2004) pour la signature du DSC.

5.1.2. Exigences relatives aux certificats TLS, de téléversement et CSCA

Pour les certificats numériques et les signatures cryptographiques dans le contexte du DCCG, les principales exigences relatives aux algorithmes cryptographiques et à la longueur des clés sont résumées dans le tableau suivant (à partir de 2021):

Algorithme de signature	Taille de la clé	Fonction de hachage
ECDSA	Min. 250 bits	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits
RSA-PSS (bourrage recommandé) RSA-PKCS # 1 v1.5 (versions antérieures pour bourrage)	Min. 3000 bits modulus RSA *n* avec exposant public e > 2 ^ 16	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits
DSA	Min. 3000 bits nombre premier p, 250 bits clé q	SHA-2 avec une valeur de sortie d'une longueur ≥ 256 bits

La courbe elliptique recommandée pour l'ECDSA est la NIST-p-256 car elle est largement utilisée.

5.2. *Certificat CSCA (NB_{CSCA})*

Le tableau suivant fournit des indications sur le modèle de certificat NB_{CSCA} si un État membre décide d'exploiter sa propre CSCA pour le système de DCC.

Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,***c=<État membre exploitant la CSCA>**
Key usage	**certificate signing,***CRL signing* (au minimum)
Basic Constraints	**CA = true, path length constraints = 0**

Le nom du sujet doit être non vide et unique dans l'État membre considéré. Le code pays (c) doit correspondre à l'État membre qui utilisera ce certificat CSCA. Le certificat doit contenir un identifiant de clé du sujet (SKI) unique conforme à la RFC 5280 ([3]).

5.3. *Certificat de signataire de documents (DSC)*

Le tableau suivant fournit des orientations sur le DSC. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Serial Number	**numéro de série unique**
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,***c=<État membre utilisant ce DSC>**
Key Usage	**digital signature** (au minimum)

([3]) rfc5280 (ietf.org).

Le DSC doit être signé avec la clé privée correspondant à un certificat CSCA utilisé par l'État membre.

Les extensions suivantes doivent être utilisées:

— le certificat doit contenir un identifiant de clé de l'autorité (AKI) correspondant à l'identifiant de clé du sujet (SKI) du certificat de la CSCA émettrice,

— le certificat doit contenir un identifiant de clé du sujet (SKI) unique conforme à la RFC 5280 ([4]).

En outre, le certificat doit contenir l'extension du point de distribution de la CRL qui renvoie à la liste de révocation de certificats (CRL) fournie par la CSCA qui a émis le DSC.

Le DSC peut contenir une extension EKU (*extended key usage* — utilisation étendue de la clé) avec zéro ou plusieurs identifiants de la politique d'utilisation des clés qui limitent les types de HCERT que ce certificat est autorisé à vérifier. Si un ou plusieurs identifiants sont présents, les vérificateurs vérifient l'utilisation de la clé par rapport au HCERT stocké. Les valeurs d'utilisation étendue de la clé suivantes sont définies à cet effet:

Champ	Valeur
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pour les émetteurs «tests»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pour les émetteurs «vaccination»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pour les émetteurs «rétablissement»

En l'absence d'extension d'utilisation de la clé (c'est-à-dire pas d'extension ou zéro extension), ce certificat peut être utilisé pour valider tout type de HCERT. D'autres identifiants de politique d'utilisation étendue de la clé pertinents utilisés avec la validation des HCERT peuvent être définis par d'autres documents.

5.4. *Certificats de téléversement (NB_{UP})*

Le tableau suivant fournit des orientations pour le certificat de téléversement du système d'arrière-plan national. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,* **c=<État membre utilisant ce certificat de téléversement>**
Key Usage	**digital signature** (au minimum)

5.5. *Certificat d'authentification client TLS du système d'arrière-plan national (NB_{TLS})*

Le tableau suivant fournit des orientations pour le certificat d'authentification client TLS du système d'arrière-plan national. Les mentions en **gras** sont obligatoires (à inclure obligatoirement dans le certificat), les mentions en *italiques* sont recommandées (il est recommandé de les inclure). Pour les champs absents, aucune recommandation n'est formulée.

Champ	Valeur
Subject	**cn=<nom commun unique et non vide>,***o=<Prestataire>,* **c=<État membre sur le NB>**
Key Usage	**digital signature** (au minimum)
Extended key usage	client authentication (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org).

Le certificat peut également contenir le *server authentication (1.3.6.1.5.5.7.3.1)* de l'utilisation étendue de la clé, mais ce n'est pas obligatoire.

5.6. *Certificat de signature de la trust list ($DCCG_{TA}$)*

Le tableau suivant définit le certificat d'ancre de confiance du DCCG.

Champ	Valeur
Subject	**cn = Digital Green Certificate Gateway** ([5]), **o=<Prestataire>, c=<pays>**
Key Usage	**digital signature** (au minimum)

5.7. *Certificats de serveur TLS du DCCG ($DCCG_{TLS}$)*

Le tableau suivant définit le certificat TLS du DCCG.

Champ	Valeur
Subject	cn=<FQDN ou adresse IP du DCCG>, o=<Prestataire>, c=<pays>
SubjectAltName	dNSName: <Nom DCCG DNS> ou iPAddress: <adresse IP DCCG>
Key Usage	**digital signature** (au minimum)
Extended key usage	server authentication (1.3.6.1.5.5.7.3.1)

Le certificat peut également contenir le *client authentication (1.3.6.1.5.5.7.3.2)* de l'utilisation étendue de la clé, mais ce n'est pas obligatoire.

Le certificat TLS du DCCG doit être délivré par une autorité de certification de confiance publique (incluse dans tous les principaux navigateurs et systèmes d'exploitation, conformé

([5]) Le terme «Digital Green Certificate» au lieu de «EU Digital COVID Certificate» a été conservé dans ce contexte, car c'est cette terminologie qui a été codifiée et déployée dans le certificat avant que les colégislateurs ne s'accordent sur un nouveau terme.