2025/908

23.5.2025

BESCHLUSS Nr. 1/2024 DES DURCH DAS ABKOMMEN ZWISCHEN DER EUROPÄISCHEN UNION UND DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT ZUR VERKNÜPFUNG IHRER JEWEILIGEN SYSTEME FÜR DEN HANDEL MIT TREIBHAUSGASEMISSIONEN EINGESETZTEN GEMEINSAMEN AUSSCHUSSES

vom 4. Dezember 2024

im Hinblick auf die Änderung des Anhangs II des Abkommens sowie der gemeinsamen Verfahrensvorschriften und der technischen Verknüpfungsstandards [2025/908]

DER GEMEINSAME AUSSCHUSS —

gestützt auf das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen ([1]) (im Folgenden „Abkommen"), insbesondere auf Artikel 9 und Artikel 13 Absatz 2,

in Erwägung nachstehender Gründe:

(1) Der Beschluss Nr. 2/2019 des Gemeinsamen Ausschusses ([2]) sah eine vorläufige Lösung für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz vor.

(2) Auf seiner dritten Sitzung ist der Gemeinsame Ausschuss dahingehend übereingekommen, dass die Kosteneffizienz einer dauerhaften Verknüpfung zwischen dem Unionsregister und dem Register der Schweiz geprüft werden muss.

(3) In seiner fünften Sitzung hat sich der Gemeinsame Ausschuss auf den Bericht, der von der mit den Beschlüssen Nr. 1/2020 ([3]) und Nr. 2/2020 ([4]) des Gemeinsamen Ausschusses eingesetzten Arbeitsgruppe vorgelegt wurde, geeinigt. In diesem Bericht hat die Arbeitsgruppe ein Konzept für die Umsetzung der dauerhaften Verknüpfung zwischen dem Unionsregister und dem Register der Schweiz geprüft und empfohlen.

(4) Um den technischen Anforderungen der dauerhaften Verknüpfung zwischen dem Unionsregister und dem Register der Schweiz Rechnung zu tragen und die Bestimmungen des Anhangs II des Abkommens vor dem Hintergrund der technologischen Entwicklungen zu straffen, sollte Anhang II des Abkommens geändert werden.

(5) Um die Kohärenz der gemeinsamen Verfahrensvorschriften und der technischen Verknüpfungsstandards mit Anhang II des Abkommens zu gewährleisten, sollten diese Dokumente ebenfalls geändert werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Anhang II des Abkommens wird durch den in Anhang I dieses Beschlusses festgelegten Wortlaut ersetzt.

(2) Die in Artikel 3 Absatz 6 des Abkommens genannten gemeinsamen Verfahrensvorschriften sind in Anhang II dieses Beschlusses festgelegt. Sie ersetzen die im Anhang des Beschlusses Nr. 1/2020 festgelegten gemeinsamen Verfahrensvorschriften.

([1]) ABl. L 322 vom 7.12.2017, S. 3.

([2]) Beschluss Nr. 2/2019 des mit dem Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen eingesetzten Gemeinsamen Ausschusses vom 5. Dezember 2019 zur Änderung der Anhänge I und II des Abkommens zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen (ABl. L 314 vom 29.9.2020, S. 68).

([3]) Beschluss Nr. 1/2020 des durch das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen eingesetzten gemeinsamen Ausschusses vom 5. November 2020 über die Annahme gemeinsamer Verfahrensvorschriften (ABl. L 226 vom 25.6.2021, S. 2).

([4]) Beschluss Nr. 2/2020 des mit dem Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen eingesetzten Gemeinsamen Ausschusses vom 5. November 2020 zur Änderung der Anhänge I und II des Abkommens und zur Annahme technischer Verknüpfungsstandards (LTS) (ABl. L 226 vom 25.6.2021, S. 16).

(3) Die in Artikel 3 Absatz 7 des Abkommens genannten technischen Verknüpfungsstandards sind in Anhang III dieses Beschlusses festgelegt. Sie ersetzen die im Anhang des Beschlusses Nr. 2/2020 festgelegten technischen Verknüpfungsstandards.

Artikel 2

Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

Geschehen zu Brüssel am 4. Dezember 2024.

Für den Gemeinsamen Ausschuss

Sekretariat für die Europäische Union	*Der Vorsitz*	*Sekretariat für die Schweiz*
Ruben VERMEEREN	Beatriz YORDI	Thomas MEIER

ANNEX I

„ANHANG II

TECHNISCHE VERKNÜPFUNGSSTANDARDS

Für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz wurde 2020 eine vorläufige Lösung umgesetzt. Ab 2023 wird sich die Registerverknüpfung zwischen den beiden Emissionshandelssystemen schrittweise zu einer dauerhaften Verknüpfung entwickeln, die voraussichtlich spätestens 2024 umgesetzt wird und die das Funktionieren der verknüpften Märkte in Bezug auf die Vorteile der Marktliquidität und die Ausführung von Transaktionen zwischen den beiden verknüpften Systemen in einer Weise ermöglichen wird, die einem einzigen, aus zwei Systemen bestehenden Markt entspricht, sodass die Marktteilnehmer so handeln können, als befänden sie sich auf einem einzigen Markt, der nur den individuellen Regulierungsvorschriften der Vertragsparteien unterliegt.

In den technischen Verknüpfungsstandards (Linking Technical Standards, im Folgenden „LTS“) ist Folgendes festgelegt:

— Architektur der Kommunikationsverbindung

— Kommunikationsverbindung zwischen dem SSTL und dem EUTL

— Sicherheit der Datenübermittlung

— Liste der Funktionen (Transaktionen, Kontenabstimmung usw.)

— Festlegung der Transportschicht

— Anforderungen an die Datenprotokollierung

— Betriebsregelungen (Helpdesk, Unterstützung)

— Strategie für die Kommunikationsaktivierung und Prüfverfahren

— Sicherheitsprüfverfahren

In den LTS ist festzulegen, dass die Verwalter alle angemessenen Maßnahmen ergreifen sollen, um zu gewährleisten, dass das SSTL und das EUTL sowie die Verknüpfung täglich rund um die Uhr funktionsbereit sind, und dass Unterbrechungen der Funktionsfähigkeit des SSTL, des EUTL und der Verknüpfung auf ein Minimum zu reduzieren sind.

In den LTS sind zusätzliche Sicherheitsvorschriften für das Schweizer Register, das SSTL, das Unionsregister und das EUTL enthalten, die in einem «Sicherheitsmanagementplan» dokumentiert werden. Insbesondere ist in den LTS Folgendes festzulegen:

— Falls der Verdacht besteht, dass die Sicherheit des Schweizer Registers, des SSTL, des Unionsregisters oder des EUTL beeinträchtigt wurde, informieren die beiden Vertragsparteien einander unverzüglich darüber und unterbrechen die Verknüpfung zwischen dem SSTL und dem EUTL.

— Die Vertragsparteien verpflichten sich, im Falle einer Sicherheitsverletzung Informationen unverzüglich auszutauschen. Soweit die technischen Einzelheiten verfügbar sind, tauschen der Registerverwalter der Schweiz und der Zentralverwalter der Union innerhalb von 24 Stunden, nachdem festgestellt wurde, dass es sich bei einem Sicherheitsvorfall um eine Sicherheitsverletzung handelt, einen Bericht aus, in dem der Vorfall beschrieben ist (Datum, Ursache, Auswirkungen, Abhilfemaßnahmen).

Das in den LTS festgelegte Sicherheitsprüfverfahren muss abgeschlossen sein, bevor die Kommunikationsverbindung zwischen dem SSTL und dem EUTL aufgebaut wird, und immer, wenn eine neue Version des SSTL oder des EUTL erforderlich ist.

In den LTS sind neben der Produktionsumgebung zwei Testumgebungen vorgesehen: eine Testumgebung für Entwickler und eine Abnahmeumgebung.

Die Vertragsparteien legen durch den Schweizer Registerverwalter und den Zentralverwalter der Union den Nachweis vor, dass ihre Systeme im Einklang mit den in den LTS festgelegten Sicherheitsanforderungen in den vorhergehenden 12 Monaten einer unabhängigen Sicherheitsbewertung unterzogen wurden. Alle wichtigen neuen Versionen der Software werden im Einklang mit den in den LTS festgelegten Sicherheitsanforderungen einer Sicherheitsprüfung und insbesondere Penetrationstests unterzogen. Der Penetrationstest darf nicht vom Entwickler der Software oder einem Subunternehmer des Softwareentwicklers durchgeführt werden."

ANHANG II

GEMEINSAME VERFAHRENSVORSCHRIFTEN GEMÄß ARTIKEL 3 ABSATZ 6 DES ABKOMMENS ZWISCHEN DER EUROPÄISCHEN UNION UND DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT ZUR VERKNÜPFUNG IHRER JEWEILIGEN SYSTEME FÜR DEN HANDEL MIT TREIBHAUSGASEMISSIONEN

Verfahren für die dauerhafte Registerverknüpfung

Inhaltsverzeichnis

1. GLOSSAR 7
2. EINLEITUNG 7
2.1. Geltungsbereich 8
2.2. Adressaten 8
3. VORGEHEN UND STANDARDS 8
4. VORFALLMANAGEMENT 9
4.1. Ermittlung und Aufzeichnung von Vorfällen 9
4.2. Einstufung und Erstsupport 9
4.3. Untersuchung und Diagnose 10
4.4. Lösung und Wiederherstellung 10
4.5. Abschluss des Vorfalls 10
5. PROBLEMMANAGEMENT 11
5.1. Ermittlung und Aufzeichnung eines Problems 11
5.2. Problempriorisierung 11
5.3. Untersuchung und Diagnose eines Problems 11
5.4. Problemlösung 11
5.5. Abschluss eines Problems 11
6. ANFRAGEERLEDIGUNG 11
6.1. Einleitung einer Anfrage 11
6.2. Erfassung und Analyse von Anfragen 12
6.3. Genehmigung der Anfrage 12
6.4. Anfrageerledigung 12
6.5. Anfrageeskalation 12
6.6. Überprüfung der Anfrageerledigung 12
6.7. Abschluss der Anfrage 12
7. ÄNDERUNGSMANAGEMENT 12
7.1. Änderungsanfrage 13
7.2. Bewertung und Planung einer Änderung 13
7.3. Genehmigung einer Änderung 13
7.4. Durchführung der Änderung 13
8. RELEASEMANAGEMENT 13
8.1. Planung des Releases 14
8.2. Aufbau und Testen des Releasebündels 14
8.3. Vorbereitung der Einführung 14
8.4. Zurücksetzen des Releases 15

8.5. Überprüfung und Abschluss des Releases 15
9. SICHERHEITSVORFALL-MANAGEMENT 15
9.1. Kategorisierung von Informationssicherheitsvorfällen 15
9.2. Handhabung von Informationssicherheitsvorfällen 15
9.3. Identifizierung eines Sicherheitsvorfalls 16
9.4. Analyse eines Sicherheitsvorfalls 16
9.5. Bewertung der Schwere eines Sicherheitsvorfalls, Eskalation und Berichterstattung 16
9.6. Berichterstattung über die Reaktion auf einen Sicherheitsvorfall 16
9.7. Überwachung, Kapazitätsaufbau und kontinuierliche Verbesserung 16
10. INFORMATIONSSICHERHEITS-MANAGEMENT 17
10.1. Identifizierung sensibler Informationen 17
10.2. Sensibilitätsstufen von Informationswerten 17
10.3. Bezeichnung des Eigentümers von Informationswerten 17
10.4. Registrierung sensibler Informationen 17
10.5. Behandlung sensibler Informationen 18
10.6. Zugangsmanagement 18
10.7. Zertifikat-/Schlüsselmanagement 18

1. GLOSSAR

Tabelle 1-1

Abkürzungen und Begriffsbestimmungen

Abkürzung/Begriff	Begriffsbestimmung
Zertifizierungsstelle	Stelle, die digitale Zertifikate ausstellt
CH	Schweizerische Eidgenossenschaft
EHS	Emissionshandelssystem
EU	Europäische Union
IMT	Incident Management Team (Vorfallmanagement-Team)
Informationswert	Eine Information, die für ein Unternehmen oder eine Organisation von Wert sind
IT	Information Technology (Informationstechnologie)
ITIL	Information Technology Infrastructure Library (Bibliothek für Informationstechnologie-Infrastruktur)
ITSM	IT-Servicemanagement
LTS	Linking Technical Standards (technische Verknüpfungsstandards)
Register	Ein Verbuchungssystem für im Rahmen des EHS ausgestellte Zertifikate, das das Eigentum an in elektronischen Konten verbuchten Zertifikaten verfolgt
RFC	Request for Change (Änderungsanfrage)
SIL	Sensitive Information List (Verzeichnis sensibler Informationen)
SR	Service Request (Dienstanfrage)
Wiki	Website, auf der Nutzer Informationen und Wissen austauschen können, indem sie über einen Webbrowser direkt Inhalte hinzufügen oder anpassen

2. EINLEITUNG

Das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen vom 23. November 2017 (im Folgenden „Abkommen“) sieht die gegenseitige Anerkennung von Emissionszertifikaten vor, die für die Einhaltung der Vorschriften im Rahmen des Emissionshandelssystems der Europäischen Union (im Folgenden „EU-EHS“) oder des Emissionshandelssystems der Schweiz (im Folgenden „EHS der Schweiz“) genutzt werden können. Um die Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz zu operationalisieren, wird eine direkte Verknüpfung zwischen dem Transaktionsprotokoll der Europäischen Union (European Union Transaction Log, im Folgenden „EUTL“) des Unionsregisters und dem Schweizer Zusatztransaktionsprotokoll (Swiss Supplementary Transaction Log, im Folgenden „SSTL“) des Schweizer Registers eingerichtet, sodass im Rahmen eines der beiden EHS vergebene Emissionszertifikate von einem Register in das andere übertragen werden können (Artikel 3 Absatz 2 des Abkommens). Für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz wurde 2020 eine vorläufige Lösung umgesetzt. Ab 2023 wird sich die Registerverknüpfung zwischen den beiden Emissionshandelssystemen schrittweise zu einer dauerhaften Verknüpfung entwickeln, die voraussichtlich spätestens 2024 umgesetzt wird und die das Funktionieren der verknüpften Märkte in Bezug auf die Vorteile der Marktliquidität und die Ausführung von Transaktionen zwischen den beiden verknüpften Systemen in einer Weise ermöglichen wird, die einem einzigen, aus zwei Systemen bestehenden Markt entspricht, sodass die Marktteilnehmer so handeln können, als befänden sie sich auf einem einzigen Markt, der nur den individuellen Regulierungsvorschriften der Vertragsparteien unterliegt. (Anhang II des Abkommens).

Gemäß Artikel 3 Absatz 6 des Abkommens legen der Schweizer Registerverwalter und der Zentralverwalter der Union gemeinsame Verfahrensvorschriften für technische oder andere Fragen fest, die für das Funktionieren der Verknüpfung erforderlich sind; dabei tragen sie den Prioritäten der innerstaatlichen Rechtsvorschriften Rechnung. Die von den Verwaltern entwickelten gemeinsamen Verfahrensvorschriften werden wirksam, sobald sie durch Beschluss des Gemeinsamen Ausschusses angenommen wurden.

Der Gemeinsame Ausschuss hat die gemeinsamen Verfahrensvorschriften mit seinem Beschluss Nr. 1/2020 angenommen. Der Gemeinsame Ausschuss wird die in diesem Dokument festgehaltenen aktualisierten gemeinsamen Verfahrensvorschriften mit seinem Beschluss Nr. 1/2024 annehmen. Im Einklang mit diesem Beschluss und den Ersuchen des Gemeinsamen Ausschusses haben der Schweizer Registerverwalter und der Zentralverwalter der Union weitere technische Leitlinien zur Operationalisierung der Verknüpfung erarbeitet und werden diese Leitlinien aktualisieren, um sie laufend an den technischen Fortschritt und die neuen Anforderungen in Bezug auf die Sicherheit der Verknüpfung und deren wirksames und effizientes Funktionieren anzupassen.

2.1. **Geltungsbereich**

Dieses Dokument stellt den Konsens der Vertragsparteien über die Schaffung der verfahrenstechnischen Grundlagen der Verknüpfung zwischen den Registern des EU-EHS und des EHS der Schweiz dar. Es gibt zwar einen Überblick über die allgemeinen Verfahrensanforderungen für Funktionen, doch sind weitere technische Leitlinien erforderlich, um die Verknüpfung zu operationalisieren.

Für das ordnungsgemäße Funktionieren der Verknüpfung sind weitere technische Spezifikationen erforderlich, um sie weiter zu operationalisieren. Gemäß Artikel 3 Absatz 7 des Abkommens werden diese Aspekte eingehend in dem Dokument mit technischen Verknüpfungsstandards (Linking Technical Standards, LTS) geregelt, das gesondert durch einen Beschluss des Gemeinsamen Ausschusses angenommen werden soll.

Die gemeinsamen Verfahrensvorschriften sollen sicherstellen, dass die IT-Dienste im Zusammenhang mit dem Funktionieren der Verknüpfung zwischen den Registern des EU-EHS und des EHS der Schweiz wirksam und effizient ausgeführt werden, namentlich im Hinblick auf die Erledigung von Dienstanfragen, die Behebung von Dienstausfällen und von Problemen sowie auf die Durchführung von betrieblichen Routineaufgaben im Einklang mit internationalen Normen für das IT-Servicemanagement.

Für die dauerhafte Registerverknüpfung sind lediglich die folgenden gemeinsamen Verfahrensvorschriften erforderlich, die Teil des vorliegenden Dokuments sind:

— Vorfallmanagement

— Problemmanagement

— Anfrageerledigung

— Änderungsmanagement

— Releasemanagement

— Sicherheitsvorfall-Management

— Informationssicherheits-Management

2.2. **Adressaten**

Zielgruppe dieser gemeinsamen Verfahrensvorschriften sind die Supportteams des Registers der EU bzw. der Schweiz.

3. **VORGEHEN UND STANDARDS**

Der folgende Grundsatz gilt für alle gemeinsamen Verfahrensvorschriften:

— Die EU und die Schweiz vereinbaren, die gemeinsamen Verfahrensvorschriften auf der Grundlage der Version 4 der Bibliothek für Informationstechnologie-Infrastruktur (ITIL) festzulegen. Praktiken aus diesem Standard werden herangezogen und an den besonderen Bedarf im Zusammenhang mit der dauerhaften Registerverknüpfung angepasst.

— Die für die Regelung der gemeinsamen Verfahrensvorschriften erforderliche Kommunikation und Abstimmung zwischen den beiden Vertragsparteien erfolgt über die Register-Servicedesks der Schweiz und der EU. Aufgaben werden stets innerhalb einer Vertragspartei zugewiesen.

— Besteht Uneinigkeit über die Handhabung einer gemeinsamen Verfahrensvorschrift, so wird diese von beiden Servicedesks gemeinsam untersucht und gelöst. Kann keine Einigung erzielt werden, wird die Suche nach einer gemeinsamen Lösung an die nächsthöhere Ebene eskaliert.

Eskalationsebenen	EU	CH
Erste Ebene	Servicedesk der EU	Servicedesk der Schweiz
Zweite Ebene	EU-Operationsmanager	Anwendungsmanager des Schweizer Registers
Dritte Ebene	Gemeinsamer Ausschuss (der diese Zuständigkeit angesichts des Artikels 12 Absatz 5 des Abkommens delegieren könnte)	
Vierte Ebene	Gemeinsamer Ausschuss, falls auf der dritten Ebene delegiert wird	

— Jede Vertragspartei kann die Verfahren für den Betrieb ihres eigenen Registersystems unter Berücksichtigung der Anforderungen an diese gemeinsamen Verfahrensvorschriften und der damit verbundenen Schnittstellen festlegen.

— Die gemeinsamen Verfahrensvorschriften werden durch ein IT-Servicemanagement-Tool (ITSM-Tool) unterstützt, insbesondere in Bezug auf Vorfallmanagement, Problemmanagement und Anfrageerledigung sowie die Kommunikation zwischen den beiden Vertragsparteien.

— Darüber hinaus ist der Informationsaustausch per E-Mail zulässig.

— Beide Vertragsparteien stellen sicher, dass die Anforderungen an die Informationssicherheit im Einklang mit den Handhabungsanweisungen erfüllt werden.

4. **VORFALLMANAGEMENT**

Ziel des Vorfallmanagement-Prozesses ist es, das normale Leistungsniveau von IT-Diensten so schnell wie möglich nach einem Vorfall mit möglichst geringer Störung der Geschäftsabläufe wiederherzustellen.

Darüber hinaus sollte das Vorfallmanagement für Berichtszwecke Aufzeichnungen über Vorfälle führen und sich in andere Prozesse eingliedern, um ständige Verbesserungen zu erzielen.

Allgemein betrachtet umfasst das Vorfallmanagement die folgenden Tätigkeiten:

— Ermittlung und Aufzeichnung von Vorfällen

— Einstufung und Erstsupport

— Untersuchung und Diagnose

— Lösung und Wiederherstellung

— Abschluss des Vorfalls

Während der gesamten Dauer eines Vorfalls muss die kontinuierliche Handhabung von Eigentumsrechten, Überwachung, Verfolgung und Kommunikation durch den Vorfallmanagement-Prozess gewährleistet sein.

4.1. **Ermittlung und Aufzeichnung von Vorfällen**

Ein Vorfall kann von einem Supportteam, durch automatisierte Überwachungstools oder durch technisches Personal im Zuge der Routineüberwachung ermittelt werden.

Ein ermittelter Vorfall muss aufgezeichnet werden; dabei ist ihm eine eindeutige Kennung zuzuweisen, die eine ordnungsgemäße Verfolgung und eine ordnungsgemäße Überwachung ermöglicht. Die eindeutige Kennung eines Vorfalls ist die Kennung, die ihm im gemeinsamen Ticketsystem des Servicedesks der Vertragspartei (EU oder Schweiz), die den Vorfall festgestellt hat, zugewiesen wird; sie muss in jeder Mitteilung im Zusammenhang mit dem Vorfall angegeben werden.

Anlaufstelle für alle Vorfälle sollte der Servicedesk der Vertragspartei sein, der das Ticket erfasst hat.

4.2. **Einstufung und Erstsupport**

Durch die Einstufung eines Vorfalls soll verstanden und ermittelt werden, welches System und/oder welcher Dienst von einem Vorfall in welchem Umfang betroffen ist. Um wirksam zu sein, sollte der Vorfall bei der Einstufung im ersten Anlauf zur korrekten Ressource geroutet werden, sodass der Vorfall schneller gelöst werden kann.

In der Einstufungsphase sollte der Vorfall nach seiner Wirkung und Dringlichkeit kategorisiert und priorisiert werden, damit er innerhalb eines Zeitrahmen behandelt wird, der der Priorität gerecht wird.

Besteht die Möglichkeit, dass der Vorfall sich auf die Vertraulichkeit oder die Integrität sensibler Daten und/oder auf die Systemverfügbarkeit auswirkt, muss der Vorfall außerdem als Sicherheitsvorfall deklariert und nach dem Verfahren behandelt werden, das im Kapitel „Sicherheitsvorfallmanagement“ dieses Dokuments festgelegt ist.

Soweit möglich nimmt der Servicedesk, der das Ticket erfasst hat, eine erste Diagnose vor. Zu diesem Zweck stellt der Servicedesk fest, ob es sich bei dem Vorfall um einen bekannten Fehler handelt. Ist dies der Fall, so ist der Lösungsweg oder die Ausweichlösung bereits bekannt und dokumentiert.

Konnte der Servicedesk den Vorfall lösen, so wird er den Vorfall zu diesem Zeitpunkt abschließen, da der Primärzweck des Vorfallmanagements erfüllt wurde (nämlich die schnelle Wiederherstellung des Dienstes für den Endnutzer). Anderenfalls eskaliert der Servicedesk den Vorfall zur weiteren Untersuchung und Diagnose an die geeignete Resolvergruppe.

4.3. **Untersuchung und Diagnose**

Die Untersuchung und Diagnose von Vorfällen erfolgt, wenn der Servicedesk einen Vorfall nicht im Rahmen der Erstdiagnose lösen kann und dieser daher in geeigneter Weise eskaliert wird. Die Eskalation von Vorfällen ist Teil des Untersuchungs- und Diagnoseprozesses.

Eine gemeinsame Praxis in der Untersuchungs- und Diagnosephase ist der Versuch, den Vorfall unter kontrollierten Bedingungen nachzuvollziehen. Bei der Untersuchung und Diagnose eines Vorfalls ist wichtig, dass die richtige Abfolge der Ereignisse, die zu dem Vorfall geführt haben, deutlich wird.

Mit der Eskalation wird anerkannt, dass ein Vorfall auf der derzeitigen Supportebene nicht gelöst werden kann und an eine Supportgruppe auf höherer Ebene oder an die andere Vertragspartei weitergeleitet werden muss. Die Eskalation kann auf zwei Wegen erfolgen: horizontal (funktionsabhängig) oder vertikal (hierarchisch).

Der Servicedesk, der den Vorfall aufgezeichnet und ausgelöst hat, ist dafür verantwortlich, den Vorfall an die geeignete Ressource zu eskalieren und den Gesamtstatus und die Zuweisung des Vorfalls zu verfolgen.

Die Vertragspartei, der der Vorfall zugewiesen wurde, ist dafür verantwortlich, sicherzustellen, dass die angeforderten Maßnahmen zügig durchgeführt werden, und ihren eigenen Servicedesk auf dem Laufenden zu halten.

4.4. **Lösung und Wiederherstellung**

Die Vorfalllösung und die Wiederherstellung finden statt, sobald der Vorfall vollständig verstanden wurde. Eine Lösung für einen Vorfall zu finden bedeutet, dass ein Weg gefunden wurde, um Abhilfe zu schaffen. Der Akt der Anwendung der Lösung ist die Wiederherstellungsphase.

Wurde der Dienstausfall von den geeigneten Ressourcen behoben, so wird der Vorfall an den zuständigen Servicedesk zurückgeleitet, der den Vorfall erfasst hat; der Servicedesk bestätigt dem Initiator des Vorfalls, dass der Fehler berichtigt wurde und der Vorfall abgeschlossen werden kann. Die Erkenntnisse aus der Bearbeitung des Vorfalls sind für die künftige Verwendung aufzuzeichnen.

Die Wiederherstellung kann von IT-Supportpersonal durchgeführt werden oder durch Übermittlung von zu beachtenden Anweisungen an den Endnutzer.

4.5. **Abschluss des Vorfalls**

Der Abschluss ist der letzte Schritt des Vorfallmanagement-Prozesses und erfolgt kurz nach der Lösung des Vorfalls.

Aus der Checkliste der Tätigkeiten, die in der Abschlussphase durchzuführen sind, werden die folgenden hervorgehoben:

— Überprüfung der Kategorie, in die der Vorfall ursprünglich eingeordnet wurde;

— ordnungsgemäße Erfassung aller Informationen zu dem Vorfall;

— ordnungsgemäße Dokumentation des Vorfalls und Aktualisierung der Wissensbasis;

— angemessene Kommunikation mit allen direkt oder indirekt von dem Vorfall betroffenen Beteiligten.

Ein Vorfall ist förmlich abgeschlossen, sobald der Servicedesk die Vorfallabschlussphase ausgeführt und die andere Vertragspartei darüber unterrichtet hat.

Ein einmal geschlossener Vorfall wird nicht wieder geöffnet. Tritt ein Vorfall innerhalb kurzer Zeit erneut auf, wird nicht der ursprüngliche Vorfall wieder geöffnet, sondern stattdessen muss ein neuer Vorfall erfasst werden.

Wird der Vorfall sowohl vom Servicedesk der EU als auch von dem der Schweiz verfolgt, so ist der Servicedesk, der das Ticket erfasst hat, für den endgültigen Abschluss zuständig.

5. **PROBLEMMANAGEMENT**

Dieses Verfahren sollte immer dann angewandt werden, wenn ein Problem ermittelt und dadurch der Problemmanagement-Prozess ausgelöst wird. Das Problemmanagement konzentriert sich auf Qualitätssteigerung und die Verringerung der Zahl der gemeldeten Vorfälle. Ein Problem kann einen oder mehrere Vorfälle verursachen. Wird ein Vorfall gemeldet, so besteht das Ziel des Vorfallmanagements darin, den Dienst so schnell wie möglich wiederherzustellen, was auch Ausweichlösungen umfassen kann. Wird ein Problem gestellt, so besteht das Ziel darin, den Ursprung des Problems zu untersuchen, um herauszufinden, welche Änderung gewährleistet, dass das Problem und die entsprechenden Vorfälle nicht mehr auftreten.

5.1. **Ermittlung und Aufzeichnung eines Problems**

Je nachdem, welche Vertragspartei das Ticket initiiert hat, ist entweder der Servicedesk der EU oder derjenige der Schweiz die Anlaufstelle für Fragen im Zusammenhang mit einem Problem.

Die einmalige Kennung eines Problems ist die vom IT-Servicemanagement zugewiesene Kennung. Sie muss in jeder Mitteilung im Zusammenhang mit dem Problem angegeben werden.

Ein Problem kann durch einen Vorfall ausgelöst oder auf Eigeninitiative mit dem Ziel geöffnet werden, im System ermittelte Mängel zu einem beliebigen Zeitpunkt zu beheben.

5.2. **Problempriorisierung**

Zwecks einfacherer Verfolgung können Probleme unter Berücksichtigung der Wirkung und Häufigkeit der damit zusammenhängenden Vorfälle genau wie Vorfälle nach ihrem Schweregrad und ihrer Priorität kategorisiert werden.

5.3. **Untersuchung und Diagnose eines Problems**

Jede Vertragspartei kann auf ein Problem hinweisen; der Servicedesk der Vertragspartei, von der die Initiative ausgeht, ist dafür verantwortlich, das Problem zu erfassen, es der geeigneten Ressource zuzuweisen und den Gesamtstatus des Problems zu verfolgen.

Die Resolvergruppe, an die das Problem eskaliert wurde, ist für die zügige Behandlung des Problems und die Kommunikation mit dem Servicedesk verantwortlich.

Auf Anfrage sind beide Vertragsparteien dafür verantwortlich, sicherzustellen, dass die zugewiesenen Maßnahmen durchgeführt werden, und ihren eigenen Servicedesk auf dem Laufenden zu halten.

5.4. **Problemlösung**

Die Resolvergruppe, der das Problem zugewiesen wurde, ist verantwortlich dafür, das Problem zu lösen und dem Servicedesk ihrer eigenen Vertragspartei sachdienliche Informationen zu übermitteln.

Die Erkenntnisse aus der Bearbeitung des Problems sind für die künftige Verwendung aufzuzeichnen.

5.5. **Abschluss eines Problems**

Ein Problem ist förmlich geschlossen, sobald das Problem durch die Umsetzung der Änderung behoben wurde. Die Phase des Problemabschlusses wird von dem Servicedesk wahrgenommen, der das Problem erfasst und den Servicedesk der anderen Vertragspartei darüber informiert hat.

6. **ANFRAGEERLEDIGUNG**

Bei dem Prozess der Anfrageerledigung handelt es sich um das durchgehende Management einer Anfrage nach einem neuen oder bestehenden Dienst vom Zeitpunkt ihrer Registrierung und Genehmigung bis zum Abschluss. Bei Dienstanfragen handelt es sich in der Regel um kleine, vordefinierte, wiederholbare, häufige, vorab genehmigte und verfahrenstechnische Anfragen.

Die wichtigsten Schritte werden nachstehend kurz beschrieben:

6.1. **Einleitung einer Anfrage**

Die Angaben zu einer Dienstanfrage werden dem Servicedesk der EU oder dem der Schweiz per E-Mail, Telefon oder über das IT-Servicemanagement-Tool oder jeden anderen vereinbarten Kommunikationskanal übermittelt.

6.2. **Erfassung und Analyse von Anfragen**

Anlaufstelle für alle Dienstanfragen sollte der Servicedesk der EU oder derjenige der Schweiz sein, je nachdem, welche Vertragspartei die Dienstanfrage eingeleitet hat. Der Servicedesk ist dafür verantwortlich, die Dienstanfrage mit der gebotenen Sorgfalt zu erfassen und zu analysieren.

6.3. **Genehmigung der Anfrage**

Der Sachbearbeiter des Servicedesks der Vertragspartei, die die Dienstanfrage eingeleitet hat, prüft, ob für die Anfrage etwaige Genehmigungen der anderen Vertragspartei erforderlich sind, und holt diese gegebenenfalls ein. Wird die Dienstanfrage nicht genehmigt, aktualisiert der Servicedesk das Ticket und schließt es.

6.4. **Anfrageerledigung**

Dieser Schritt dient der wirksamen und effizienten Bearbeitung von Dienstanfragen. Hierbei ist unter folgenden Fällen zu unterscheiden:

— Die Erledigung der Dienstanfrage betrifft nur eine Vertragspartei. In diesem Fall erteilt diese Vertragspartei die Arbeitsaufträge und koordiniert die Ausführung.

— Die Erledigung der Dienstanfrage betrifft sowohl die EU als auch die Schweiz. In diesem Fall erteilen die Servicedesks die Arbeitsaufträge in ihrem Zuständigkeitsbereich. Der Ablauf der Erledigung der Dienstanfrage wird von den beiden Servicedesks gemeinsam koordiniert. Die Gesamtverantwortung trägt der Servicedesk, der die Dienstanfrage erhalten und initiiert hat.

Sobald die Dienstanfrage erledigt wurde, muss sie den Status „Erledigt“ (Resolved) erhalten.

6.5. **Anfrageeskalation**

Der Servicedesk kann die offene Dienstanfrage erforderlichenfalls an die geeignete Ressource (Drittpartei) eskalieren.

Eskaliert wird an die jeweilige Drittpartei, d. h. der Servicedesk der EU muss den Servicedesk der Schweiz einschalten, um an eine Schweizer Drittpartei zu eskalieren und umgekehrt.

Die Drittpartei, an die die Dienstanfrage eskaliert wurde, ist für die zügige Behandlung der Dienstanfrage und die Kommunikation mit dem Servicedesk, der diese Anfrage eskaliert hat, verantwortlich.

Der Servicedesk, der die Dienstanfrage erfasst hat, ist für die Verfolgung des Gesamtstatus und der Zuweisung einer Dienstanfrage verantwortlich.

6.6. **Überprüfung der Anfrageerledigung**

Der zuständige Servicedesk unterzieht die Aufzeichnungen zu der Dienstanfrage vor dem Abschluss einer abschließenden Qualitätskontrolle. So soll sichergestellt werden, dass die Dienstanfrage tatsächlich bearbeitet wurde und dass alle zur Beschreibung des Lebenszyklus der Dienstanfrage erforderlichen Angaben mit hinreichenden Einzelheiten vorliegen. Darüber hinaus sind die Erkenntnisse aus der Bearbeitung der Anfrage für die künftige Verwendung aufzuzeichnen.

6.7. **Abschluss der Anfrage**

Sind sich die Vertragsparteien, denen die Anfrage zugewiesen wurde, einig, dass die Dienstanfrage erledigt wurde, und betrachtet der Urheber der Anfrage den Fall als gelöst, so wird als Nächstes der Status „Abgeschlossen“ (Closed) erteilt.

Eine Dienstanfrage wird förmlich abgeschlossen, sobald der Servicedesk, der die Anfrage erfasst hat, die Anfrageabschlussphase abgewickelt und den Servicedesk der anderen Vertragspartei unterrichtet hat.

7. **ÄNDERUNGSMANAGEMENT**

Das Änderungsmanagement soll sicherstellen, dass alle Änderungen zur Kontrolle von IT-Infrastruktur effizient und zeitnah nach standardisierten Methoden und Verfahren durchgeführt werden, damit die Zahl und die Auswirkungen etwaiger Vorfälle in diesem Zusammenhang auf den Dienst möglichst gering gehalten werden. Änderungen der IT-Infrastruktur können sich reaktiv infolge von Problemen oder von außen auferlegten Anforderungen, z. B Änderungen der Rechtsvorschriften, oder proaktiv ergeben, indem eine Verbesserung von Effizienz und Wirksamkeit angestrebt wird oder um unternehmerische Initiativen zu ermöglichen oder zu reflektieren.

Der Änderungsmanagement-Prozess umfasst verschiedene Schritte, bei denen jede Einzelheit einer Änderungsanfrage für die künftige Nachverfolgung erfasst wird. Diese Prozesse gewährleisten, dass die Änderung vor ihrer Einführung validiert und getestet wird. Der Releasemanagement-Prozess sorgt für eine erfolgreiche Einführung.

7.1. **Änderungsanfrage**

Eine Änderungsanfrage (RFC) wird dem Änderungsmanagement-Team zur Validierung und Genehmigung vorgelegt. Anlaufstelle für alle Änderungsanfragen sollte der Servicedesk der EU oder derjenige der Schweiz sein, je nachdem, welche Vertragspartei die Anfrage eingeleitet hat. Der Servicedesk ist dafür verantwortlich, die Anfrage mit der gebotenen Sorgfalt zu erfassen und zu analysieren.

Änderungsanfragen können ausgelöst werden durch

— einen Vorfall, der eine Änderung verursacht;

— ein bestehendes Problem, das zu einer Änderung führt;

— einen Endnutzer, der eine neue Änderung anfragt;

— eine Änderung infolge laufender Wartungsarbeiten;

— Änderungen von Rechtsvorschriften.

7.2. **Bewertung und Planung einer Änderung**

Diese Phase umfasst die Bewertung von Änderungen und Planungstätigkeiten. Dazu gehören Priorisierung und Planungstätigkeiten zur Minimierung der Risiken und Auswirkungen.

Wenn die Durchführung der Änderungsanfrage sowohl die EU als auch die Schweiz betrifft, überprüft die Vertragspartei, die die Anfrage erfasst hat, die Änderungsbewertung und -planung mit der anderen Vertragspartei.

7.3. **Genehmigung einer Änderung**

Eine eingeloggte Änderungsanfrage muss von der zuständigen Eskalationsebene genehmigt werden.

7.4. **Durchführung der Änderung**

Die Durchführung der Änderung erfolgt im Rahmen des Releasemanagement-Prozesses. Die Releasemanagement-Teams beider Vertragsparteien folgen bei der Planung und dem Testen ihren eigenen Prozessen. Die Änderung wird überprüft, sobald die Durchführung abgeschlossen ist. Um sicherzustellen, dass alles planmäßig abgewickelt wurde, wird der bestehende Änderungsmanagement-Prozess laufend überprüft und bei Bedarf aktualisiert.

8. **RELEASEMANAGEMENT**

Ein Release entspricht einer oder mehreren Änderungen eines IT-Dienstes, die in einem Releaseplan zusammengefasst sind und zusammen genehmigt, vorbereitet, aufgebaut, getestet und eingeführt werden. Bei einem Release kann es sich um eine Fehlerbehebung, eine Änderung der Hardware oder anderer Komponenten, Softwareänderungen, Aktualisierungen von Anwendungsversionen und/oder Änderungen der Dokumentation bzw. von Prozessen handeln. Jedes Release wird inhaltlich als Einheit verwaltet, getestet und eingeführt.

Releasemanagement zielt auf die Planung, den Aufbau, das Testen und die Validierung sowie die Schaffung der Fähigkeit ab, die konzipierten Dienste bereitzustellen, mit denen die Anforderungen der Beteiligten erfüllt und die angestrebten Ziele erreicht werden. Bei der Designkoordinierung werden für alle Änderungen des Dienstes Akzeptanzkriterien festgelegt und dokumentiert, die den Releasemanagement-Teams zur Verfügung gestellt werden.

Das Release besteht in der Regel aus mehreren Problembehebungen und Verbesserungen für einen Dienst. Es umfasst die erforderliche neue oder geänderte Software oder jegliche neue oder geänderte Hardware, die zur Umsetzung der genehmigten Änderungen erforderlich ist.

8.1. **Planung des Releases**

Als erster Schritt in diesem Prozess werden genehmigte Änderungen Releasebündeln zugewiesen und der Umfang und Inhalt des Releases festgelegt. Auf der Grundlage dieser Informationen wird als Teilprozess der Releaseplanung ein Zeitplan für den Aufbau, das Testen und die Einführung des Releases aufgestellt.

Bei der Planung sollte Folgendes festgelegt werden:

— Umfang und Inhalt des Releases;

— Risikobewertung und Risikoprofil des Releases;

— von dem Release betroffene Kunden/Nutzer;

— für das Release zuständiges Team;

— Bereitstellungs- und Einführungsstrategie;

— Ressourcen für das Release und dessen Einführung.

Die beiden Vertragsparteien unterrichten einander über ihre Releaseplanung und ihre Wartungsfenster. Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die Planung und legen ein gemeinsames Wartungsfenster fest.

8.2. **Aufbau und Testen des Releasebündels**

In der Aufbau- und Testphase im Rahmen des Releasemanagement-Prozesses wird zum einen das Konzept für die Ausführung des Releases oder des Releasebündels und die Wartung der kontrollierten Umgebungen vor der Vornahme der Änderung und zum anderen das Konzept für das Testen aller Änderungen in allen betroffenen Umgebungen nach dem Release festgelegt.

Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die Bereitstellungpläne und die Tests. Dies umfasst die folgenden Fragen:

— Wie und wann werden Releaseeinheiten und Dienstleistungskomponenten bereitgestellt?

— Was sind die typischen Vorlaufzeiten und was geschieht bei Verzögerungen?

— Wie kann der Fortschritt der Bereitstellung verfolgt und eine Bestätigung eingeholt werden?

— Was sind die Messgrößen für die Überwachung und Feststellung des Gelingens der Releasemaßnahme?

— Welches sind die gemeinsamen Testfälle für wichtige Funktionen und Änderungen?

Am Ende dieses Teilprozesses sind alle erforderlichen Releasekomponenten für den Schritt der realen Einführung bereit.

8.3. **Vorbereitung der Einführung**

Beim Teilprozess der Vorbereitung wird sichergestellt, dass Kommunikationspläne korrekt festgelegt werden und Mitteilungen bereitliegen, um an alle betroffenen Beteiligten und Endnutzer versandt zu werden, und dass das Release in den Änderungsmanagement-Prozess eingebunden wird, um zu gewährleisten, dass alle Änderungen kontrolliert durchgeführt und von den erforderlichen Gremien genehmigt werden.

Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die folgenden Tätigkeiten:

— Aufzeichnungen zur Änderungsanfrage für die Planung und Vorbereitung der Einführung in die Produktionsumgebung;

— Aufstellung des Durchführungsplans;

— Zurücksetzungskonzept, damit bei einer misslungenen Einführung der vorherige Stand wiederhergestellt werden kann;

— Mitteilungen an alle notwendigen Parteien;

— Einholung der Genehmigung für die Durchführung des Releases von der zuständigen Eskalationsebene.

8.4. **Zurücksetzen des Releases**

Ist eine Einführung misslungen oder haben Tests ergeben, dass die Einführung ein Fehlschlag war oder die vereinbarten Akzeptanz-/Qualitätskriterien nicht erreicht hat, müssen die Releasemanagement-Teams beider Vertragsparteien zum vorigen Stand zurückkehren. Alle notwendigen Beteiligten müssen darüber unterrichtet werden, einschließlich der betroffenen/anvisierten Endnutzer. Bei erteilter Genehmigung kann der Prozess in jeder der vorangegangenen Phasen wieder aufgenommen werden.

8.5. **Überprüfung und Abschluss des Releases**

Bei der Überprüfung einer Einführung sollten folgende Tätigkeiten durchgeführt werden:

— Einholen von Feedback zur Kunden-/Nutzerzufriedenheit mit der Einführung bzw. zur Zufriedenheit mit der Dienstbereitstellung im Rahmen der Einführung (Sammeln des Feedbacks und dessen Auswertung für die kontinuierliche Verbesserung des Dienstes);

— Überprüfung aller nicht erfüllten Qualitätskriterien;

— Kontrolle, dass alle Maßnahmen, notwendigen Korrekturen und Änderungen vollständig sind;

— Sicherstellen, dass am Ende der Einführung keine Probleme in Bezug auf Fähigkeiten, Ressourcen, Kapazität oder Leistung auftreten;

— Kontrolle, dass alle Probleme, bekannten Fehler und Ausweichlösungen dokumentiert und von Kunden, Endnutzern, dem betrieblichen Support und anderen betroffenen Parteien akzeptiert werden;

— Überwachung von Vorfällen und Problemen, die durch die Einführung ausgelöst wurden (Early Life Support für operative Teams, wenn das Release Mehrarbeit verursacht hat);

— Aktualisierung der Supportdokumentation (d. h. Unterlagen mit technischen Informationen);

— förmliche Übergabe des eingeführten Releases an den Servicebetrieb;

— Dokumentation der gewonnenen Erkenntnisse;

— Einholen der Release-Kurzbeschreibung bei den Durchführungsteams;

— förmlicher Abschluss des Releases nach Überprüfung der Aufzeichnungen zur Änderungsanfrage.

9. **SICHERHEITSVORFALL-MANAGEMENT**

Das Sicherheitsvorfall-Management ist ein Prozess für den Umgang mit Sicherheitsvorfällen, der es ermöglichen soll, potenziell betroffene Beteiligte über den Vorfall zu unterrichten sowie Vorfälle zu bewerten und zu priorisieren; es umfasst auch die Reaktion auf den Vorfall, um eine tatsächliche, mutmaßliche oder potenzielle Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität von sensiblen Informationswerten zu beheben.

9.1. **Kategorisierung von Informationssicherheitsvorfällen**

Alle Vorfälle, die die Verknüpfung zwischen dem Unionsregister und dem Register der Schweiz beeinflussen, werden analysiert, um zu ermitteln, ob möglicherweise die Vertraulichkeit, Integrität oder Verfügbarkeit von im Verzeichnis sensibler Informationen (SIL) aufgeführten sensiblen Informationen verletzt wurde.

Ist dies der Fall, so wird der Vorfall als Informationssicherheitsvorfall kategorisiert, unverzüglich im IT-Servicemanagement-Tool registriert und als solcher bearbeitet.

9.2. **Handhabung von Informationssicherheitsvorfällen**

Sicherheitsvorfälle werden der Verantwortung der 3. Eskalationsebene zugeordnet; die Lösung der Vorfälle übernimmt ein spezielles Vorfallmanagement-Team (IMT).

Das Vorfallmanagement-Team ist verantwortlich für

— die Durchführung einer ersten Analyse, die Kategorisierung und die Schwereeinstufung des Vorfalls;

— die Koordinierung von Maßnahmen aller Beteiligten einschließlich der vollständigen Dokumentation der Vorfallanalyse, der zur Behebung des Vorfalls getroffenen Entscheidungen und aller ermittelten möglichen Schwachstellen;

— je nach Schwere des Sicherheitsvorfalls dessen zügige Eskalation an die geeignete Ebene zur Information und/oder Entscheidung.

Bei dem Prozess des Informationssicherheits-Managements werden alle Informationen zu Vorfällen in die höchste Sensibilitätsstufe für Informationen, auf jeden Fall aber nicht niedriger als „SENSITIVE: *ETS*“ eingestuft.

Im Falle einer laufenden Untersuchung und/oder einer Schwachstelle, die ausgenutzt werden könnte, wird die Information so lange als „SPECIAL HANDLING. *ETS Critical*“ eingestuft, bis Abhilfe geschaffen wurde.

9.3. **Identifizierung eines Sicherheitsvorfalls**

Je nach Art des Sicherheitsvorfalls bestimmt der Informationssicherheitsbeauftragte, welche geeigneten Organisationen einzubinden und am Vorfallmanagement-Team zu beteiligen sind.

9.4. **Analyse eines Sicherheitsvorfalls**

Das Vorfallmanagement-Team steht mit allen beteiligten Organisationen und gegebenenfalls den relevanten Mitgliedern von deren Teams in Kontakt, um den Vorfall genauer zu betrachten. Bei der Analyse wird ermittelt, in welchem Umfang die Vertraulichkeit, Integrität oder Verfügbarkeit eines Werts verloren gegangen ist, und bewertet, wie sich dies auf alle betroffenen Organisationen auswirkt. Anschließend werden Erst- und Folgemaßnahmen zur Behebung des Vorfalls und zur Verwaltung seiner Auswirkungen bestimmt, einschließlich der Auswirkungen dieser Maßnahmen auf die Ressourcen.

9.5. **Bewertung der Schwere eines Sicherheitsvorfalls, Eskalation und Berichterstattung**

Das Vorfallmanagement-Team bewertet die Schwere jedes neuen Sicherheitsvorfalls nach dessen Kategorisierung als Sicherheitsvorfall und leitet je nach seiner Schwere die erforderlichen Sofortmaßnahmen ein.

9.6. **Berichterstattung über die Reaktion auf einen Sicherheitsvorfall**

Das Vorfallmanagement-Team nimmt die Ergebnisse der Begrenzung des Vorfalls (Incident Containment) und der Wiederherstellung in den Bericht über die Reaktion auf den Informationssicherheitsvorfall auf. Der Bericht wird der 3. Eskalationsebene mit gesicherter E-Mail oder anderen gegenseitig akzeptierten gesicherten Kommunikationsmitteln übermittelt.

Die zuständige Vertragspartei überprüft die Ergebnisse der Begrenzung und Wiederherstellung und

— stellt die Verbindung des Registers wieder her, wenn dieses zuvor abgetrennt worden war;

— übernimmt die Vorfallkommunikation gegenüber den Registerteams;

— schließt den Vorfall ab.

Das Vorfallmanagement-Team sollte sachdienliche Einzelheiten in gesicherter Form in den Bericht über den Informationssicherheitsvorfall aufnehmen, um die kohärente Aufzeichnung und Kommunikation zu gewährleisten und zügige, angemessene Maßnahmen zur Begrenzung des Vorfalls zu ermöglichen. Nach der Fertigstellung übermittelt das Vorfallmanagement-Team zügig den endgültigen Bericht über den Informationssicherheitsvorfall.

9.7. **Überwachung, Kapazitätsaufbau und kontinuierliche Verbesserung**

Das Vorfallmanagement-Team erstattet über alle Sicherheitsvorfälle an die 3. Eskalationsebene Bericht. Die Berichte werden von dieser Eskalationsebene verwendet, um Folgendes zu ermitteln:

— Schwachstellen bei Sicherheitskontrollen und/oder beim Betrieb, die verbesserungsbedürftig sind;

— mögliche Notwendigkeit, dieses Verfahren zu verbessern, sodass wirksamer auf Vorfälle reagiert werden kann;

— Möglichkeiten für Schulung und Kapazitätsaufbau zur weiteren Stärkung der Resilienz von Registersystemen in Bezug auf die Informationssicherheit, um das Risiko künftiger Vorfälle zu verringern und deren Auswirkungen zu minimieren.

10. **INFORMATIONSSICHERHEITS-MANAGEMENT**

Das Informationssicherheits-Management zielt darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit von vertraulichen Informationen, Daten und IT-Dienstleistungen einer Organisation sicherzustellen. Neben den technischen Komponenten, darunter deren Design und Erprobung (siehe technische Verknüpfungsstandards, LTS), sind die folgenden gemeinsamen Verfahrensvorschriften erforderlich, um die Sicherheitsanforderungen für die dauerhafte Registerverknüpfung zu erfüllen.

10.1. **Identifizierung sensibler Informationen**

Zur Bewertung der Sensibilität einer Information wird ermittelt, in welchem Umfang sich eine Sicherheitsverletzung im Zusammenhang mit dieser Information auf die Geschäftstätigkeit auswirken könnte (z. B. finanzielle Verluste, Imageschaden, Rechtsverletzung usw.).

Die sensiblen Informationswerte werden auf der Grundlage ihrer Auswirkungen auf die Verknüpfung ermittelt.

Die Sensibilitätsstufe dieser Information wird anhand der für diese Verknüpfung anwendbaren Sensibilitätsskala bewertet, die im Abschnitt „Behandlung von Informationssicherheitsvorfällen“ dieses Dokuments eingehender behandelt wird.

10.2. **Sensibilitätsstufen von Informationswerten**

Sobald der Informationswert ermittelt wurde, wird er nach folgenden Regeln eingestuft:

— Wird die Vertraulichkeits-, die Integritäts- oder die Verfügbarkeitsstufe auch nur in einem Fall als HOCH erachtet, wird der Wert als „SPECIAL HANDLING: *ETS Critical*“ eingestuft;

— wird die Vertraulichkeits-, die Integritäts- oder die Verfügbarkeitsstufe auch nur in einem Fall als MITTEL erachtet, wird der Wert als „SENSITIVE: *ETS*“ eingestuft;

— werden die Vertraulichkeits-, die Integritäts- und die Verfügbarkeitsstufen durchweg als NIEDRIG erachtet, wird der Wert als „SENSITIVE: *ETS Joint Procurement*“ (Kennzeichnung EU)/“LIMITED: ETS“ (Kennzeichnung CH) eingestuft.

10.3. **Bezeichnung des Eigentümers von Informationswerten**

Für alle Informationswerte sollte es einen bezeichneten Eigentümer geben. Informationswerte des EHS, die zu der Verknüpfung zwischen dem EUTL und dem SSTL gehören oder damit in Verbindung stehen, sollten in ein gemeinsames Inventarverzeichnis der Informationswerte aufgenommen werden, das von den beiden Vertragsparteien geführt wird. Informationswerte des EHS außerhalb der Verknüpfung zwischen dem EUTL und dem SSTL sollten in ein Inventarverzeichnis der Informationswerte aufgenommen werden, das von der jeweiligen Vertragspartei geführt wird.

Die Eigentumsrechte an jedem Informationswert, der zu der Verknüpfung zwischen dem EUTL und dem SSTL gehört oder damit in Verbindung steht, müssen von den beiden Vertragsparteien vereinbart werden. Die Bewertung der Sensibilität eines Informationswerts ist Aufgabe des Eigentümers.

Die Position des Eigentümers sollte dem Wert des ihm zugeordneten Informationswerts angemessen sein. Die Verantwortung des Eigentümers für den Wert und die Verpflichtung zur Wahrung der erforderlichen Vertraulichkeits-, Integritäts- und Verfügbarkeitsstufe sollten vereinbart und förmlich festgelegt werden.

10.4. **Registrierung sensibler Informationen**

Alle sensiblen Informationen werden im Verzeichnis sensibler Informationen registriert.

Wenn sich die Aggregation von sensiblen Informationen stärker auswirken könnte als eine einzelne Information, wird dies gegebenenfalls berücksichtigt und im Verzeichnis sensibler Informationen registriert (z. B. ein in der Systemdatenbank gespeicherter Datensatz).

Das Verzeichnis sensibler Informationen ist nicht statisch. Bedrohungen, Schwachstellen, die Wahrscheinlichkeit oder die Folgen von Sicherheitsvorfällen im Zusammenhang mit den Werten können sich ohne Vorankündigung ändern, und es ist möglich, dass neue Werte in den Betrieb der Registersysteme eingeführt werden.

Deswegen wird das Verzeichnis sensibler Informationen regelmäßig überprüft, und alle neuen als sensibel eingestuften Informationen werden unverzüglich im Verzeichnis sensibler Informationen registriert.

Das Verzeichnis sensibler Informationen muss für jeden Eintrag mindestens folgende Angaben enthalten:

— Beschreibung der Information

— Eigentümer der Information

— Sensibilitätsstufe

— Angabe, ob die Informationen personenbezogene Daten enthalten

— weitere Angaben soweit erforderlich

10.5. **Behandlung sensibler Informationen**

Sensible Informationen, die außerhalb der Verknüpfung zwischen dem Unionsregister und dem Schweizer Register verarbeitet werden, werden im Einklang mit den Handhabungsanweisungen behandelt.

Sensible Informationen, die über die Verknüpfung zwischen dem Unionsregister und dem Schweizer Register verarbeitet werden, werden im Einklang mit den Sicherheitsanforderungen der Vertragsparteien behandelt.

10.6. **Zugangsmanagement**

Ziel des Zugangsmanagements ist es, autorisierten Nutzern die Berechtigung zur Nutzung eines Dienstes zu erteilen und gleichzeitig den Zugang von nicht autorisierten Nutzern zu verhindern. Das Zugangsmanagement wird manchmal auch als „Berechtigungsmanagement“ oder „Identitätsmanagement“ bezeichnet.

Für die dauerhafte Registerverknüpfung und ihren Betrieb benötigen die beiden Vertragsparteien Zugang zu den folgenden Komponenten:

— Wiki: ein kollaboratives Umfeld für den Austausch gemeinsamer Informationen wie Releaseplanung;

— IT-Servicemanagement-Tool für das Vorfall- und Problemmanagement (siehe Kapitel 3 „Vorgehen und Standards“);

— Informationsaustauschsystem: Jede Vertragspartei stellt ein System für den sicheren Austausch von Meldungen bereit, über das Meldungen, die Transaktionsdaten enthalten, übermittelt werden.

Der Schweizer Registerverwalter und der Zentralverwalter der Union sorgen dafür, dass Zugänge auf dem neuesten Stand sind, und fungieren für ihre jeweilige Vertragspartei als Anlaufstelle für Tätigkeiten des Zugangsmanagements. Anträge auf Zugang werden im Einklang mit den Verfahren für die Anfrageerledigung behandelt.

10.7. **Zertifikat-/Schlüsselmanagement**

Jede Vertragspartei ist für ihr eigenes Zertifikat-/Schlüsselmanagement (Generierung, Registrierung, Speicherung, Installation, Verwendung, Erneuerung, Aufhebung, Backup und Wiedererlangung von Zertifikaten/Schlüsseln) verantwortlich. Wie in den technischen Verknüpfungsstandards beschrieben, werden nur digitale Zertifikate verwendet, die von einer Zertifizierungsstelle ausgestellt wurden, der beide Vertragsparteien vertrauen. Die Handhabung und Speicherung von Zertifikaten/Schlüsseln muss den Bestimmungen der Handhabungsanweisungen folgen.

Jede Aufhebung und/oder Erneuerung von Zertifikaten und Schlüsseln muss von beiden Vertragsparteien koordiniert werden. Dies geschieht im Einklang mit den Verfahren für die Anfrageerledigung.

Der Schweizer Registerverwalter und der Zentralverwalter der Union tauschen Zertifikate/Schlüssel über ein gesichertes Kommunikationsmittel im Einklang mit den Bestimmungen der Handhabungsanweisungen aus.

Jede Überprüfung von Zertifikaten/Schlüsseln in jedem Kommunikationsmittel zwischen den Parteien erfolgt auf einem zweiten Kanal („out of band“).

ANHANG III

TECHNISCHE VERKNÜPFUNGSSTANDARDS (LTS) GEMÄß ARTIKEL 3 ABSATZ 7 DES ABKOMMENS ZWISCHEN DER EUROPÄISCHEN UNION UND DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT ZUR VERKNÜPFUNG IHRER JEWEILIGEN SYSTEME FÜR DEN HANDEL MIT TREIBHAUSGASEMISSIONEN

Standards für die dauerhafte Registerverknüpfung

Inhaltsverzeichnis

1. GLOSSAR 21
2. EINLEITUNG 22
2.1. Geltungsbereich 22
2.2. Adressaten 23
3. ALLGEMEINE BESTIMMUNGEN 23
3.1. Architektur der Kommunikationsverbindung 23
3.1.1. Austausch von Meldungen 23
3.1.2. XML-Meldungen – übergeordnete Beschreibung 23
3.1.3. Eingabefenster 24
3.1.4. Fluss von Transaktionsmeldungen 24
3.2. Sicherheit der Datenübermittlung 26
3.2.1. Firewall und Netzwerkverbindung 26
3.2.2. Virtuelles privates Netzwerk (VPN) 26
3.2.3. IPSec-Umsetzung 27
3.2.4. Transferprotokoll für den sicheren Austausch von Meldungen 27
3.2.5. XML-Verschlüsselung und Signatur 27
3.2.6. Kryptografische Schlüssel 27
3.3. Liste der Funktionen im Rahmen der Verknüpfung 27
3.3.1. Geschäftstransaktionen 28
3.3.2. Abgleichprotokoll 28
3.3.3. Test-Meldung 28
3.4. Anforderungen an die Datenprotokollierung 29
3.5. Betriebsvoraussetzungen 29
4. VERFÜGBARKEITSVORGABEN 30
4.1. Gestaltung der Kommunikationsverfügbarkeit 30
4.2. Initialisierungs-, Kommunikations-, Reaktivierungs- und Testplan 30
4.2.1. Interne IKT-Infrastrukturtests 31
4.2.2. Kommunikationstests 31
4.2.3. Vollständige Systemtests (Ende-zu-Ende-Tests) 31
4.2.4. Sicherheitsprüfungen 31
4.3. Abnahme-/Testumgebungen 32
5. VERTRAULICHKEITS- UND INTEGRITÄTSVORSCHRIFTEN 32
5.1. Infrastruktur für die Sicherheitsprüfung 32
5.2. Unterbrechung der Verknüpfung und Vorschriften für ihre Reaktivierung 32
5.3. Vorschriften für Sicherheitsverletzungen 33

5.4. Leitlinien für Sicherheitsprüfungen 33
5.4.1. Software 33
5.4.2. Infrastruktur 34
5.5. Vorschriften für die Risikobewertung 34

1. **GLOSSAR**

Tabelle 1-1

Verwaltungstechnische Abkürzungen und Begriffsbestimmungen

Abkürzung/Begriff	Begriffsbestimmung
Zertifikat	Ein Zertifikat, das zur Emission von einer Tonne Kohlendioxidäquivalent in einem bestimmten Zeitraum berechtigt und das ausschließlich zur Erfüllung der Anforderungen im Rahmen des EHS einer der beiden Seiten gültig ist
CH	Schweizerische Eidgenossenschaft
CHU	Zertifikate für ortsfeste Anlagen, auch „CHU2“ (unter Bezugnahme auf den zweiten Verpflichtungszeitraum des Kyoto-Protokolls), ausgestellt von CH
CHUA	CH-Luftverkehrszertifikat
COP	Gemeinsame Verfahrensvorschriften. Gemeinsam entwickelte Verfahren für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz
EHR	Emissionshandelsregister
EHS	Emissionshandelssystem
EU	Europäische Union
EUA	Allgemeines EU-Zertifikat
EUAA	EU-Luftverkehrszertifikat
EUCR	Konsolidiertes Register der Europäischen Union
EUTL	Transaktionsprotokoll der Europäischen Union
Register	Ein Verbuchungssystem für im Rahmen des EHS ausgestellte Zertifikate, das das Eigentum an in elektronischen Konten verbuchten Zertifikaten verfolgt
SSTL	Schweizer Zusatztransaktionsprotokoll
Transaktion	Ein Vorgang in einem Register, der die Übertragung eines Zertifikats von einem Konto auf ein anderes umfasst
Transaktionsprotokollsystem	Im Transaktionsprotokoll sind die einzelnen vorgeschlagenen Transaktionen erfasst, die von einem Register an das andere übermittelt werden

Tabelle 1-2

Technische Abkürzungen und Begriffsbestimmungen

Abkürzung	Begriffsbestimmung
Asymmetrische Kryptografie	Verwendung öffentlicher und privater Schlüssel zur Ver- und Entschlüsselung von Daten
Zertifizierungsstelle	Stelle, die digitale Zertifikate ausstellt
Kryptografischer Schlüssel	Eine Information, die die funktionale Ausgabe eines kryptografischen Algorithmus bestimmt
Entschlüsselung	Rückgängigmachung der Verschlüsselung
Digitale Signatur	Ein mathematisches Verfahren zur Validierung der Authentizität und Integrität einer Meldung, einer Software oder eines digitalen Dokuments
Verschlüsselung	Die Umwandlung von Informationen oder Daten in einen Code, insbesondere um unbefugten Zugriff zu verhindern
Dateieingabe	Das Lesen einer Datei

Abkürzung	Begriffsbestimmung
Firewall	Netzsicherheitsanwendung oder -software zur Überwachung und Kontrolle des ein- und ausgehenden Netzverkehrs auf der Grundlage vorab festgelegter Regeln
Heartbeat-Überwachung	Periodisches Signal, das von Hardware oder Software erzeugt und überwacht wird, um Normalbetrieb zu bestätigen oder andere Teile eines Computersystems zu synchronisieren
IPSec	IP-Sicherheit (IP SECurity). Netzwerkprotokollsuite, die die Datenpakete authentifiziert und verschlüsselt, um eine sichere verschlüsselte Kommunikation zwischen zwei Computern über ein Internetprotokollnetz zu ermöglichen
Penetrationstest	Test eines Computersystems, eines Netzwerks oder einer Web-Anwendung, um Sicherheitslücken zu finden, die ein Angreifer ausnutzen könnte
Abgleichverfahren	Verfahren, mit dem sichergestellt wird, dass zwei Datensätze übereinstimmen
VPN	Virtuelles privates Netzwerk
XML	Erweiterbare Auszeichnungssprache. Mit ihrer Hilfe können Designer ihre eigenen maßgeschneiderten Tags erstellen und so die Definition, Übermittlung, Validierung und Interpretation von Daten zwischen Anwendungen und zwischen Organisationen ermöglichen.

2. **EINLEITUNG**

Das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen vom 23. November 2017 (im Folgenden „Abkommen“) sieht die gegenseitige Anerkennung von Emissionszertifikaten vor, die für die Einhaltung der Vorschriften im Rahmen des Emissionshandelssystems der Europäischen Union (im Folgenden „EU-EHS“) oder des Emissionshandelssystems der Schweiz (im Folgenden „EHS der Schweiz“) genutzt werden können. Um die Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz zu operationalisieren, wird eine direkte Verknüpfung zwischen dem Transaktionsprotokoll der Europäischen Union (European Union Transaction Log, im Folgenden „EUTL“) des Unionsregisters und dem Schweizer Zusatztransaktionsprotokoll (Swiss Supplementary Transaction Log, im Folgenden „SSTL“) des Schweizer Registers eingerichtet, sodass im Rahmen eines der beiden EHS vergebene Emissionszertifikate von einem Register in das andere übertragen werden können (Artikel 3 Absatz 2 des Abkommens). Für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz wurde 2020 eine vorläufige Lösung umgesetzt. Ab 2023 wird sich die Registerverknüpfung zwischen den beiden Emissionshandelssystemen schrittweise zu einer dauerhaften Verknüpfung entwickeln, die voraussichtlich spätestens 2024 umgesetzt wird und die das Funktionieren der verknüpften Märkte in Bezug auf die Vorteile der Marktliquidität und die Ausführung von Transaktionen zwischen den beiden verknüpften Systemen in einer Weise ermöglichen wird, die einem einzigen, aus zwei Systemen bestehenden Markt entspricht, sodass die Marktteilnehmer so handeln können, als befänden sie sich auf einem einzigen Markt, der nur den individuellen Regulierungsvorschriften der Vertragsparteien unterliegt (Anhang II des Abkommens).

Gemäß Artikel 3 Absatz 7 erstellen der Schweizer Registerverwalter und der Zentralverwalter der Union technische Verknüpfungsstandards (Linking Technical Standards, LTS) auf Basis der Grundsätze in Anhang II des Abkommens, in dem die Anforderungen für eine solide und gesicherte Verbindung zwischen dem SSTL und dem EUTL im Einzelnen beschrieben sind. Die von den Verwaltern entwickelten LTS werden wirksam, sobald sie durch Beschluss des Gemeinsamen Ausschusses angenommen wurden.

Der Gemeinsame Ausschuss hat die technischen Verknüpfungsstandards mit seinem Beschluss Nr. 2/2020 angenommen. Der Gemeinsame Ausschuss wird die in diesem Dokument festgehaltenen aktualisierten technischen Verknüpfungsstandards mit seinem Beschluss Nr. 1/2024 annehmen. Im Einklang mit diesem Beschluss und den Ersuchen des Gemeinsamen Ausschusses haben der Schweizer Registerverwalter und der Zentralverwalter der Union weitere technische Leitlinien zur Operationalisierung der Verknüpfung erarbeitet und werden diese Leitlinien aktualisieren, um sie laufend an den technischen Fortschritt und die neuen Anforderungen in Bezug auf die Sicherheit der Verknüpfung und deren wirksames und effizientes Funktionieren anzupassen.

2.1. **Geltungsbereich**

Dieses Dokument stellt den Konsens der Vertragsparteien über die Schaffung der technischen Grundlagen der Verknüpfung zwischen den Registern des EU-EHS und des EHS der Schweiz dar. Es gibt zwar einen Überblick über die grundlegenden technischen Spezifikationen im Hinblick auf Architektur-, Dienstleistungs- und Sicherheitsanforderungen, doch sind weitere genaue Anleitungen erforderlich, um die Verknüpfung zu operationalisieren.

Für das ordnungsgemäße Funktionieren der Verknüpfung sind weitere Prozesse und Verfahren erforderlich, um die Verknüpfung weiter zu operationalisieren. Gemäß Artikel 3 Absatz 6 des Abkommens werden diese Aspekte eingehend in den gemeinsamen Verfahrensvorschriften geregelt, die gesondert durch einen Beschluss des Gemeinsamen Ausschusses angenommen werden.

2.2. **Adressaten**

Dieses Dokument ist an den Schweizer Registerverwalter und den Zentralverwalter der Union gerichtet.

3. **ALLGEMEINE BESTIMMUNGEN**

3.1. **Architektur der Kommunikationsverbindung**

Dieser Abschnitt enthält eine Beschreibung der allgemeinen Architektur der Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz sowie der verschiedenen dazugehörigen Komponenten.

Da Sicherheit ein Schlüsselelement für die Definition der Architektur der Registerverknüpfung ist, wurden alle Maßnahmen ergriffen, um über eine solide Architektur zu verfügen. Die dauerhafte Registerverknüpfung nutzt einen Datenaustauschmechanismus zur Umsetzung einer sicheren Air-Gap-Verbindung.

Die technische Lösung verwendet Folgendes:

— ein Transferprotokoll für den sicheren Austausch von Meldungen,

— Meldungen im XML-Format,

— XML-basierte digitale Signatur und Entschlüsselung,

— VPN.

3.1.1. *Austausch von Meldungen*

Die Kommunikation zwischen dem Unionsregister und dem Schweizer Register erfolgt auf der Grundlage eines Mechanismus für den Austausch von Meldungen über gesicherte Kanäle. Jede Seite stützt sich auf ihr eigenes Archiv der eingegangenen Meldungen.

Beide Vertragsparteien führen ein Protokoll über die eingegangenen Meldungen, einschließlich Angaben zur Verarbeitung.

Fehler oder ein unerwarteter Status sind als Warnung zu melden und die Supportteams sollten Kontakt miteinander aufnehmen.

Fehler und unerwartete Ereignisse werden unter Einhaltung der im Vorfallmanagementprozess in den gemeinsamen Verfahrensvorschriften festgelegten operativen Verfahren behandelt.

3.1.2. *XML-Meldungen – übergeordnete Beschreibung*

Eine XML-Meldung enthält eines der folgenden Elemente:

— eine oder mehrere Transaktionsanfragen und/oder eine oder mehrere Transaktionsantworten;

— ein Vorgang/eine Antwort im Zusammenhang mit dem Abgleich;

— eine Test-Meldung.

Jede Meldung enthält eine Kopfzeile mit folgenden Informationen:

— Herkunfts-EHS;

— laufende Nummer.

3.1.3. *Eingabefenster*

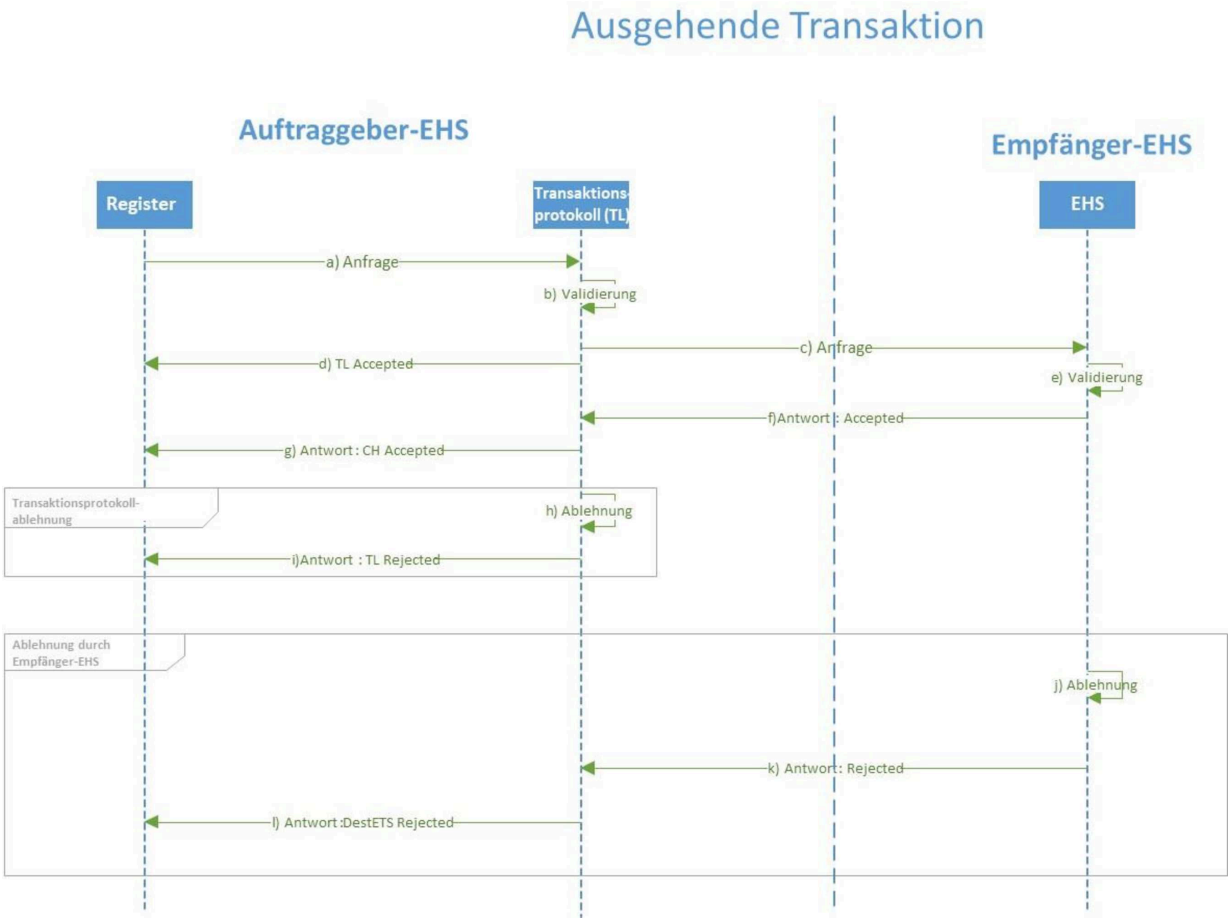
Die dauerhafte Registerverknüpfung basiert auf vordefinierten Eingabefenstern, an die sich eine Reihe benannter Ereignisse anschließen. Über die Verknüpfung eingegangene Transaktionsanfragen werden nur in vordefinierten Zeitabständen eingegeben. Eingabefenster umfassen eine technische Validierung für ausgehende und eingehende Transaktionen. Darüber hinaus können täglich Abgleiche erfolgen und manuell ausgelöst werden.

Änderungen der Häufigkeit und/oder der Zeitpunkte dieser Ereignisse werden unter Einhaltung der im Prozess der Anfrageerledigung in den gemeinsamen Verfahrensvorschriften festgelegten operativen Verfahren behandelt.

3.1.4. *Fluss von Transaktionsmeldungen*

Ausgehende Transaktionen

Hier geht es um Transaktionen aus Sicht des Auftraggeber-EHS. Das folgende Ablaufdiagramm zeigt den spezifischen Fluss:



Der Hauptfluss zeigt die folgenden Schritte (siehe obige Zeichnung):

a) Im Auftraggeber-EHS wird die Transaktionsanfrage vom Register an das Transaktionsprotokoll geschickt, sobald alle geschäftlichen Wartezeiten abgelaufen sind (gegebenenfalls Wartezeit von 24 Stunden).

b) Das Transaktionsprotokoll validiert die Transaktionsanfrage.

c) Die Transaktionsanfrage wird an das Bestimmungs-EHS gesendet.

d) Die Annahmebestätigung wird an das Register des Herkunfts-EHS gesendet.

e) Das Bestimmungs-EHS validiert die Transaktionsanfrage.

f) Das Bestimmungs-EHS sendet die Annahmebestätigung an das Transaktionsprotokoll des Herkunfts-EHS zurück.

g) Das Transaktionsprotokoll sendet die Annahmebestätigung an das Register.

Alternativfluss „Ablehnung im Transaktionsprotokoll“ (entsprechend der obigen Zeichnung, beginnend bei Buchstabe a im Hauptfluss):

a) Im Herkunfts-EHS wird die Transaktionsanfrage vom Register an das Transaktionsprotokoll geschickt, sobald alle geschäftlichen Wartezeiten abgelaufen sind (gegebenenfalls Wartezeit von 24 Stunden).

b) Das Transaktionsprotokoll validiert die Anfrage nicht.

c) Eine Ablehnungsmeldung wird an das Register des Herkunfts-EHS gesendet.

Alternativfluss „Ablehnung im EHS“ (entsprechend der obigen Zeichnung, beginnend bei Buchstabe d im Hauptfluss):

a) Im Herkunfts-EHS wird die Transaktionsanfrage vom Register an das Transaktionsprotokoll geschickt, sobald alle geschäftlichen Wartezeiten abgelaufen sind (gegebenenfalls Wartezeit von 24 Stunden).

b) Das Transaktionsprotokoll validiert die Transaktion.

c) Die Transaktionsanfrage wird an das Bestimmungs-EHS gesendet.

d) Die Annahmemeldung wird an das Register des Herkunfts-EHS gesendet.

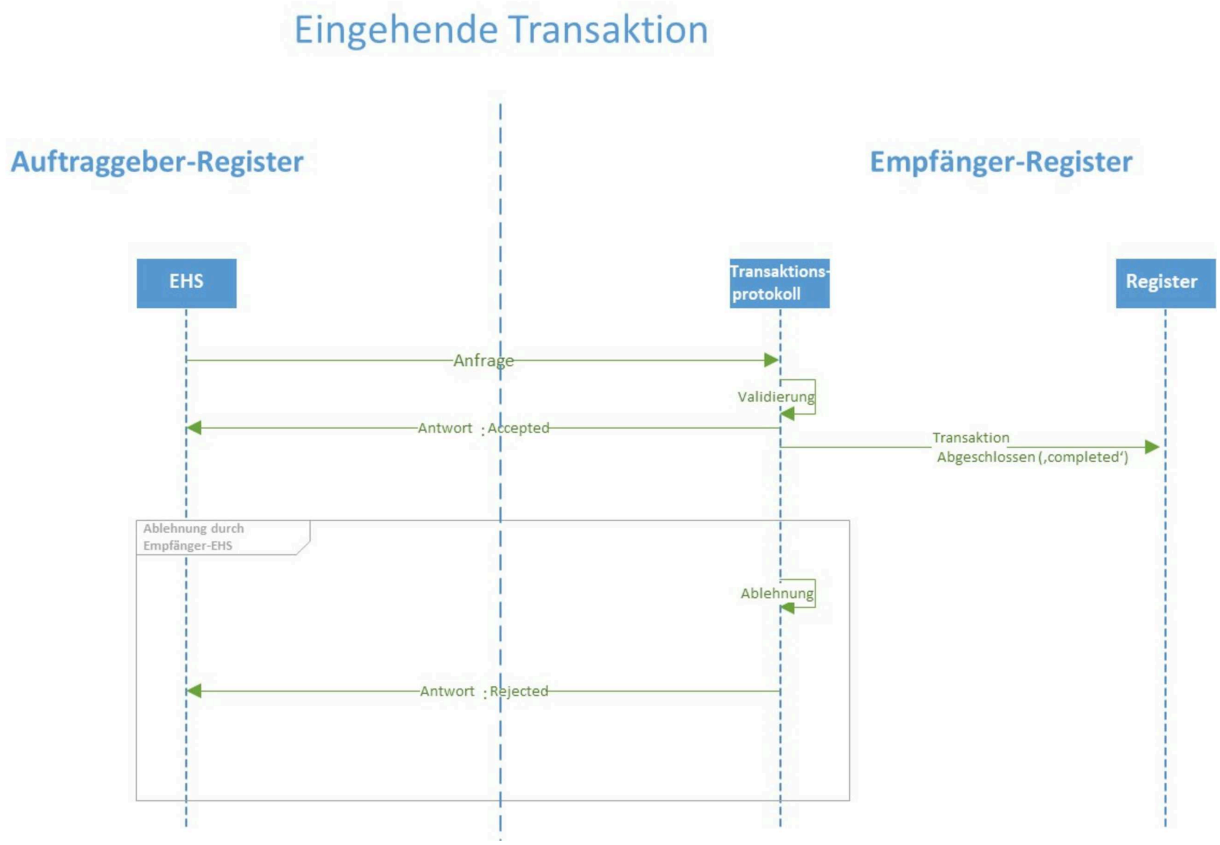
e) Das Transaktionsprotokoll des Empfänger-EHS validiert die Anfrage nicht.

f) Das Empfänger-EHS sendet die Ablehnungsbestätigung an das Transaktionsprotokoll des Auftraggeber-EHS.

g) Das Transaktionsprotokoll sendet die Ablehnungsbestätigung an das Register.

Eingehende Transaktionen

Hier geht es um Transaktionen aus Sicht des Empfänger-EHS. Das folgende Ablaufdiagramm zeigt den spezifischen Fluss:



Das Diagramm zeigt Folgendes:

1) Wenn das Transaktionsprotokoll des Empfänger-EHS die Anfrage validiert, sendet es die Annahmemeldung an das Auftraggeber-EHS und eine Meldung „transaction completed“ (Transaktion abgeschlossen) an das Register des Empfänger-EHS.

2) Wird eine eingehende Anfrage im Transaktionsprotokoll abgelehnt, wird die Transaktionsanfrage nicht an das Register des Empfänger-EHS gesendet.

Protokoll

Der Zyklus von Transaktionsmeldungen umfasst nur zwei Meldungen:

— Auftraggeber-EHS → Transaktionsvorschlag an das Empfänger-EHS

— Empfänger-EHS → Transaktionsantwort an das Auftraggeber-EHS: Entweder „accepted“ (angenommen) oder „rejected“ (abgelehnt) (unter Angabe des Ablehnungsgrundes)

  — Accepted: Transaktion ist „completed“ (abgeschlossen)

  — Rejected: Transaktion ist „terminated“ (eingestellt)

Transaktionsstatus

— Der Transaktionsstatus im Auftraggeber-EHS wird bei der Absendung der Anfrage auf „proposed“ (vorgeschlagen) gesetzt.

— Der Transaktionsstatus im Empfänger-EHS wird nach Eingang der Anfrage und während der Verarbeitung auf „proposed“ gesetzt.

— Der Transaktionsstatus im Empfänger-EHS wird nach Verarbeitung des Vorschlags auf „completed“/“terminated“ (abgeschlossen/eingestellt) gesetzt. Das Empfänger-EHS sendet dann die entsprechende Annahme-/Ablehnungsmeldung.

— Der Transaktionsstatus im Auftraggeber-EHS wird nach Eingang und Verarbeitung der Annahme/Ablehnung auf „completed“/“terminated“ gesetzt.

— Wenn keine Antwort eingeht, bleibt der Transaktionsstatus im Auftraggeber-EHS unverändert bei „proposed“.

— Das Empfänger-EHS setzt den Transaktionsstatus auf „terminated“, wenn eine etwaige vorgeschlagene Transaktion länger als 30 Minuten im Status „proposed“ verbleibt.

Vorfälle in Verbindung mit Transaktionen werden unter Einhaltung der im Vorfallmanagementprozess in den gemeinsamen Verfahrensvorschriften festgelegten operativen Verfahren behandelt.

3.2. **Sicherheit der Datenübermittlung**

Für die in der Übertragung befindlichen Daten gelten vier Sicherheitsstufen:

1) Netzzugangskontrolle: Firewall und Netzwerkverbindungsschicht

2) Verschlüsselung der Transportschicht: VPN

3) Verschlüsselung der Sitzungsschicht: Transferprotokoll für den sicheren Austausch von Meldungen

4) Verschlüsselung der Anwendungsschicht: XML-Inhaltsverschlüsselung und -Signatur

3.2.1. *Firewall und Netzwerkverbindung*

Die Verbindung wird über ein Netzwerk hergestellt, das durch eine Hardware-basierte Firewall geschützt ist. Die Firewall muss so konfiguriert sein, dass nur „registrierte“ Kunden Verbindungen zum VPN-Server herstellen können.

3.2.2. *Virtuelles privates Netzwerk (VPN)*

Die gesamte Kommunikation zwischen den Vertragsparteien wird durch Verwendung eines virtuellen privaten Netzwerks (VPN) geschützt. VPN-Technologien ermöglichen einen „VPN-Tunnel“ über ein Netz wie das Internet von einem Punkt zum anderen und schützen damit die gesamte Kommunikation. Vor der Einrichtung des VPN-Tunnels wird einem potenziellen Kundenendpunkt ein digitales Zertifikat ausgestellt, das es dem Kunden ermöglicht, während der Verbindungsverhandlungen seine Identität nachzuweisen. Jede Vertragspartei ist für die Installation des Zertifikats in ihrem VPN-Endpunkt verantwortlich. Über digitale Zertifikate greift jeder VPN-Endserver auf eine zentrale Stelle zu, um Authentifizierungsdaten auszuhandeln. Während des Aufbaus des Tunnels wird eine Verschlüsselung ausgehandelt, die gewährleistet, dass die gesamte Kommunikation durch den Tunnel geschützt ist.

Die VPN-Kundenendpunkte werden so konfiguriert, dass der VPN-Tunnel dauerhaft aufrechterhalten wird, damit jederzeit eine zuverlässige wechselseitige Echtzeit-Kommunikation zwischen den Vertragsparteien möglich ist.

Im Allgemeinen nutzt die Europäische Union die gesicherten transeuropäischen Telematikdienste für Behörden (sTESTA) als privates IP-gestütztes Netz. Daher eignet sich dieses Netz auch für die dauerhafte Registerverknüpfung.

3.2.3. *IPSec-Umsetzung*

Die Verwendung des IPSec-Protokolls zur Schaffung der Site-to-site-VPN-Infrastruktur ermöglicht die Site-to-site-Authentifizierung, die Datenintegrität und die Datenverschlüsselung. IPSec-VPN-Konfigurationen gewährleisten eine ordnungsgemäße Authentifizierung zwischen zwei Endpunkten einer VPN-Verbindung. Die Vertragsparteien identifizieren und authentifizieren den Remote-Client über die IPSec-Verbindung über ein digitales Zertifikat, das von einer von der anderen Seite anerkannten Zertifizierungsstelle bereitgestellt wird.

IPSec gewährleistet auch die Datenintegrität der gesamten über den VPN-Tunnel übertragenen Kommunikation. Die Datenpakete werden mithilfe der vom VPN erstellten Authentifizierungsinformationen gehasht und signiert. Die Vertraulichkeit der Daten wird auch dadurch gewährleistet, dass die IPSec-Verschlüsselung aktiviert wird.

3.2.4. *Transferprotokoll für den sicheren Austausch von Meldungen*

Die dauerhafte Registerverknüpfung stützt sich für den sicheren Datenaustausch zwischen den Vertragsparteien auf mehrere Verschlüsselungsschichten. Beide Systeme und ihre unterschiedlichen Umgebungen sind auf Netzwerkebene über VPN-Tunnel miteinander verbunden. In der Anwendungsschicht werden Dateien über ein Transferprotokoll für den sicheren Austausch von Meldungen in der Sitzungsschicht übertragen.

3.2.5. *XML-Verschlüsselung und -Signatur*

Innerhalb von XML-Dateien erfolgt die Signatur und Verschlüsselung auf zwei Ebenen. JedeTransaktionsanfrage, Transaktionsantwort und Abgleichmeldung wird einzeln digital signiert.

In einem zweiten Schritt wird jedes Unterelement des Elements „Meldung“ einzeln verschlüsselt.

Darüber hinaus wird als dritter Schritt und zur Gewährleistung der Integrität und Nichtabstreitbarkeit der gesamten Meldung das Wurzelelement digital signiert. Dies führt zu einem hohen Schutzniveau für die eingebetteten XML-Daten. Die technische Umsetzung entspricht den Standards des World Wide Web Consortiums.

Um die Meldung zu entschlüsseln und zu überprüfen, wird das Verfahren in umgekehrter Reihenfolge angewendet.

3.2.6. *Kryptografische Schlüssel*

Zur Verschlüsselung und Signatur wird ein Public-Key-Verschlüsselungsverfahren verwendet.

Für den Sonderfall IPSec wird ein digitales Zertifikat verwendet, das von einer Zertifizierungsstelle ausgestellt wurde, der beide Vertragsparteien vertrauen. Diese Zertifizierungsstelle prüft die Identität des Zertifikatinhabers und stellt Zertifikate aus, die zur positiven Identifizierung einer Organisation verwendet werden, und richtet sichere Datenkommunikationskanäle zwischen den Vertragsparteien ein.

Zur Signatur und Verschlüsselung von Kommunikationskanälen und Dateien werden kryptografische Schlüssel verwendet. Die öffentlichen Zertifikate werden von den Vertragsparteien digital über sichere Kanäle ausgetauscht und außerhalb des Bandes überprüft. Dieses Verfahren ist integraler Bestandteil des Informationssicherheitsmanagements in den gemeinsamen Verfahrensvorschriften.

3.3. **Liste der Funktionen im Rahmen der Verknüpfung**

Im Rahmen der Verknüpfung wird das Übertragungssystem für eine Reihe von Funktionen festgelegt, mit denen die aus dem Abkommen abgeleiteten Geschäftsabläufe umgesetzt werden. Die Verknüpfung umfasst auch die Spezifikation für das Abgleichverfahren und die Testmeldungen, die die Durchführung einer Heartbeat-Überwachung ermöglichen.

3.3.1. *Geschäftstransaktionen*

Aus geschäftlicher Sicht umfasst die Verknüpfung vier (4) Arten von Transaktionsanfragen:

— Externe Übertragung:

  — Nach dem Inkrafttreten der EHS-Verknüpfung sind EU- und CH-Zertifikate zwischen den Vertragsparteien austauschbar und somit vollständig übertragbar.

  — Eine Übertragung über die Verknüpfung erfolgt mithilfe eines Auftraggeberkontos in einem EHS und eines Empfängerkontos in dem anderen EHS.

  — Die Übertragung kann jede beliebige Menge von vier (4) Arten von Zertifikaten umfassen:

    — Allgemeine CH-Zertifikate (CHU)

    — CH-Luftverkehrszertifikate (CHUA)

    — Allgemeine EU-Zertifikate (EUA)

    — EU-Luftverkehrszertifikate (EUAA)

— Internationale Zuteilung:

Luftfahrzeugbetreiber, die von einem EHS verwaltet werden und Verpflichtungen aus dem anderen EHS sowie Anspruch auf kostenlose Zertifikate aus dem zweiten EHS haben, erhalten im Wege der internationalen Zuteilungstransaktion kostenlose Luftverkehrszertifikate aus dem zweiten EHS.

— Rückgängigmachung der internationalen Zuteilung:

Diese Transaktion findet statt, wenn kostenlose Zuteilungen von Zertifikaten an ein Luftfahrzeugbetreiberkonto durch das andere EHS vollständig rückgängig gemacht werden müssen.

— Rückübertragung einer Überschusszuteilung:

Ähnlich der Rückgängigmachung, jedoch muss die Zuteilung nicht vollständig rückgängig gemacht werden, vielmehr müssen lediglich die überschüssigen zugeteilten Zertifikate an das zuteilende EHS rückübertragen werden.

3.3.2. *Abgleichprotokoll*

Abgleiche finden erst statt, nachdem die Fenster für die Eingabe, Validierung und Verarbeitung von Meldungen geschlossen sind.

Abgleiche sind ein integraler Bestandteil der Sicherheits- und Kohärenzmaßnahmen der Verknüpfung. Beide Vertragsparteien einigen sich vor der Aufstellung eines Zeitplans auf den genauen Zeitpunkt des Abgleichs. Ein täglicher planmäßiger Abgleich kann stattfinden, wenn beide Vertragsparteien zustimmen. Nach jeder Eingabe wird zumindest ein planmäßiger Abgleich durchgeführt.

Auf jeden Fall kann jede Vertragspartei jederzeit manuelle Abgleiche einleiten.

Änderungen von Zeitpunkt und Häufigkeit der planmäßigen Abgleiche werden unter Einhaltung der im Prozess der Anfrageerledigung in den gemeinsamen Verfahrensvorschriften festgelegten operativen Verfahren behandelt.

3.3.3. *Test-Meldung*

Zur Prüfung der Ende-zu-Ende-Kommunikation ist eine Test-Meldung vorgesehen. Die Meldung enthält Daten, mit denen die Meldung als Test gekennzeichnet wird, und wird bei Eingang am anderen Ende beantwortet.

3.4. **Anforderungen an die Datenprotokollierung**

Um die beiden Vertragsparteien dabei zu unterstützen, genaue und kohärente Datensätze zu pflegen, und um Instrumente für das Abgleichverfahren zur Beseitigung von Unstimmigkeiten bereitzustellen, werden von beiden Vertragsparteien vier (4) Arten von Datenprotokollen geführt:

— Transaktionsprotokolle

— Abgleichprotokolle

— Meldungsarchiv

— Protokoll der internen Prüfung

Alle Daten in diesen Protokollen werden für die Zwecke der Fehlerbehebung mindestens drei (3) Monate lang aufbewahrt; ihre weitere Speicherung richtet sich nach dem jeweils für die Vertragsparteien in Bezug auf Audits geltenden Recht. Protokolldateien, die älter als drei (3) Monate sind, können in einem unabhängigen IT-System an einem sicheren Ort archiviert werden, sofern sie innerhalb einer angemessenen Frist abgerufen werden können oder darauf zugegriffen werden kann.

Transaktionsprotokolle

Sowohl das EUTL- als auch das SSTL-Teilsystem umfassen Transaktionsprotokollimplementierungen.

Konkret werden in den Transaktionsprotokollen Aufzeichnungen über jede vorgeschlagene Transaktion geführt, die an das andere EHS gesendet wird. Jede Aufzeichnung enthält alle Felder des Transaktionsinhalts und das anschließende Ergebnis der Transaktion (die Antwort des Empfänger-EHS). In den Transaktionsprotokollen werden auch Aufzeichnungen über die eingehenden Transaktionen sowie über die an das Herkunfts-EHS gesendete Antwort geführt.

Abgleichprotokolle

Das Abgleichprotokoll enthält eine Aufzeichnung jeder zwischen den beiden Vertragsparteien ausgetauschten Abgleichmeldung, einschließlich der Abgleich-Kennung, des Zeitstempels und des Ergebnisses des Abgleichs: Abgleichstatus „Pass“ (keine Abweichungen) oder „Discrepancies“ (Abweichungen). In der dauerhaften Registerverknüpfung sind Abgleichmeldungen integraler Bestandteil der ausgetauschten Meldungen und werden daher wie im Abschnitt „Meldungsarchiv“ beschrieben gespeichert.

Beide Vertragsparteien protokollieren jede Anfrage und ihre Antwort im Abgleichprotokoll. Obwohl die Informationen im Abgleichprotokoll nicht direkt im Rahmen des Abgleichs selbst ausgetauscht werden, kann der Zugang zu diesen Informationen erforderlich sein, um Unstimmigkeiten zu beseitigen.

Meldungsarchiv

Beide Parteien sind verpflichtet, eine Kopie der ausgetauschten Daten (die XML-Dateien), die gesendet und empfangen wurden, zu archivieren und anzugeben, ob das Format dieser Daten oder XML-Meldungen korrekt war.

Das Archiv dient vor allem für Audits, um einen Nachweis darüber zu erhalten, was an die andere Vertragspartei gesendet und von ihr empfangen wurde. Daher müssen zusammen mit den Dateien auch die entsprechenden Zertifikate archiviert werden.

Diese Dateien liefern außerdem zusätzliche Informationen für die Fehlerbehebung.

Protokoll der internen Prüfung

Diese Protokolle werden von jeder Vertragspartei selbst festgelegt und verwendet.

3.5. **Betriebsvoraussetzungen**

Der Datenaustausch zwischen beiden Systemen ist bei der dauerhaften Registerverknüpfung nicht völlig autonom; d. h., die Betreiber und Verfahren müssen die Verknüpfung operationalisieren. Zu diesem Zweck werden in diesem Prozess mehrere Rollen und Instrumente eingehend beschrieben.

4. VERFÜGBARKEITSVORGABEN

4.1. Gestaltung der Kommunikationsverfügbarkeit

Die Architektur der dauerhaften Registerverknüpfung ist im Grunde eine IKT-Infrastruktur und -Software, die die Kommunikation zwischen dem EHS der Schweiz und dem EU-EHS ermöglichen. Die Gewährleistung eines hohen Maßes an Verfügbarkeit, Integrität und Vertraulichkeit dieses Datenflusses wird somit zu einem wesentlichen Aspekt, der bei der Gestaltung der dauerhaften Registerverknüpfung zu berücksichtigen ist. Da es sich um ein Projekt handelt, bei dem die IKT-Infrastruktur, die maßgeschneiderte Software und die Prozesse eine entscheidende Rolle spielen, müssen alle drei Elemente berücksichtigt werden, um ein widerstandsfähiges System zu entwerfen.

Widerstandsfähigkeit der IKT-Infrastruktur

Das Kapitel „Allgemeine Bestimmungen“ dieses Dokuments enthält detaillierte Angaben zu den Bausteinen der Architektur. Im Hinblick auf die IKT-Infrastruktur wird mit der dauerhaften Registerverknüpfung ein widerstandsfähiges VPN-Netz eingerichtet, das sichere Kommunikationstunnel schafft, über die ein sicherer Austausch von Meldungen stattfinden kann. Andere Infrastrukturelemente werden für hohe Verfügbarkeit konfiguriert und/oder stützen sich auf Ausweichmechanismen.

Widerstandsfähigkeit der maßgeschneiderten Software

Die maßgeschneiderten Software-Module verbessern die Widerstandsfähigkeit, indem sie für einen bestimmten Zeitraum versuchen, die Kommunikation mit der anderen Seite erneut herzustellen, wenn diese aus irgendeinem Grund nicht verfügbar ist.

Widerstandsfähigkeit der Dienste

Bei der dauerhaften Registerverknüpfung findet der Datenaustausch zwischen den Vertragsparteien in vordefinierten Zeitabständen statt. Bei einigen der für den vorprogrammierten Datenaustausch erforderlichen Schritte ist ein manuelles Eingreifen der Systembetreiber und/oder Registerverwalter nötig. Unter Berücksichtigung dieses Aspekts und um die Verfügbarkeit und den Erfolg der Austausche zu erhöhen,

— sehen die Verfahrensvorschriften spezifische Zeitfenster für die Durchführung der einzelnen Schritte vor;

— nutzen die Software-Module für die dauerhafte Registerverknüpfung asynchrone Kommunikation;

— wird im Rahmen des automatischen Abgleichverfahrens festgestellt, ob es auf einer der Seiten Probleme bei der Eingabe von Dateien gab;

— werden Überwachungsprozesse (IKT-Infrastruktur und maßgeschneiderte Software-Module) in die Vorfallmanagementverfahren einbezogen und können diese auslösen (wie in den gemeinsamen Verfahrensvorschriften festgelegt). Diese Verfahren, die die Zeit bis zur Wiederherstellung des Normalbetriebs nach Vorfällen verkürzen sollen, sind unerlässlich, um hohe Verfügbarkeitsquoten zu gewährleisten.

4.2. Initialisierungs-, Kommunikations-, Reaktivierungs- und Testplan

Alle an der Architektur der dauerhaften Registerverknüpfung beteiligten Elemente müssen eine Reihe individueller und kollektiver Tests bestehen, um zu bestätigen, dass die Plattform auf der Ebene der IKT-Infrastruktur und der Informationssysteme betriebsbereit ist. Diese Betriebstests sind jedes Mal zwingend erforderlich, wenn die dauerhafte Registerverknüpfung auf der Plattform vom Status „suspended“ (unterbrochen) zu „operational“ (betriebsbereit) übergeht.

Die Aufnahme des Betriebs der Verknüpfung erfordert dann die erfolgreiche Durchführung eines vordefinierten Testplans. Dadurch wird bestätigt, dass jedes Register zunächst eine Reihe interner Tests durchgeführt hat, gefolgt von der Validierung der Ende-zu-Ende-Konnektivität, bevor mit der Übermittlung von Produktionstransaktionen zwischen beiden Vertragsparteien begonnen wird.

Der Testplan sollte die allgemeine Teststrategie und Einzelheiten zur Testinfrastruktur enthalten. Insbesondere sollte er für jedes Element in jedem Testblock Folgendes umfassen:

— die Testkriterien und -instrumente;

— die für die Durchführung des Tests zugewiesenen Rollen;

— die erwarteten Ergebnisse (positiv und negativ);

— den Zeitplan für die Prüfungen;

— die Protokollierung der Anforderungen an die Prüfergebnisse;

— die Dokumentation zur Fehlerbehebung;

— die Eskalationsvorschriften.

Als Prozess könnten die Tests zur Aufnahme des Betriebs in vier (4) Konzeptblöcke oder -phasen unterteilt werden:

4.2.1. *Interne IKT-Infrastrukturtests*

Diese Tests sind von beiden Registerverwaltern an jedem Ende einzeln durchzuführen und/oder zu prüfen.

Jedes Element der IKT-Infrastruktur ist an beiden Enden einzeln zu prüfen. Dies schließt jede einzelne Komponente der Infrastruktur ein. Diese Prüfungen können automatisch oder manuell durchgeführt werden, müssen jedoch sicherstellen, dass alle Elemente der Infrastruktur betriebsbereit sind.

4.2.2. *Kommunikationstests*

Diese Tests werden von jeder Vertragspartei einzeln eingeleitet; der Abschluss der Tests erfordert die Zusammenarbeit mit der anderen Vertragspartei.

Sobald die einzelnen Elemente betriebsbereit sind, müssen die Kommunikationskanäle zwischen beiden Registern getestet werden. Zu diesem Zweck überprüft jede Vertragspartei, ob der Internetzugang funktioniert, die VPN-Tunnel eingerichtet sind und eine Site-to-Site-IP-Konnektivität besteht. Die Erreichbarkeit der lokalen und Fern-Infrastrukturelemente und die IP-Konnektivität sollten dann dem anderen Ende bestätigt werden.

4.2.3. *Vollständige Systemtests (Ende-zu-Ende-Tests)*

Diese Tests sind an beiden Enden durchzuführen und die Ergebnisse der anderen Vertragspartei mitzuteilen.

Sobald die Kommunikationskanäle und die einzelnen Komponenten beider Register getestet sind, wird von jeder Seite eine Reihe simulierter Transaktionen und Abgleiche vorgenommen, die alle im Rahmen der Verknüpfung umzusetzenden Funktionen darstellen.

4.2.4. *Sicherheitsprüfungen*

Diese Tests sollen von beiden Registerverwaltern am jeweiligen Ende gemäß den Abschnitten 5.4 „Leitlinien für Sicherheitsprüfungen“ und 5.5 „Vorschriften für die Risikobewertung“ durchgeführt und/oder ausgelöst werden.

Erst wenn jede(r) der vier Phasen/Blöcke mit vorhersehbaren Ergebnissen abgeschlossen ist, kann die dauerhafte Registerverknüpfung als betriebsbereit betrachtet werden.

Testressourcen

Jede Vertragspartei stützt sich auf spezifische Testressourcen (spezifische Software und Hardware für die IKT-Infrastruktur) und entwickelt Testfunktionen in ihrem jeweiligen System, um die manuelle und kontinuierliche Validierung der Plattform zu unterstützen. Individuelle und kooperative manuelle Testverfahren können jederzeit von Registerverwaltern durchgeführt werden. Die Aufnahme des Betriebs an sich ist ein manueller Prozess.

Gleichzeitig ist vorgesehen, dass die Plattform in regelmäßigen Abständen automatische Kontrollen durchführt. Diese Kontrollen zielen darauf ab, die Verfügbarkeit der Plattform zu erhöhen, indem mögliche Infrastruktur- oder Softwareprobleme frühzeitig erkannt werden. Dieses Überwachungskonzept für die Plattform besteht aus zwei Elementen:

— Überwachung der IKT-Infrastruktur: Die Infrastruktur wird an beiden Enden von den IKT-Infrastrukturdienstleistern überwacht. Die automatischen Tests decken die verschiedenen Infrastrukturelemente und die Verfügbarkeit der Kommunikationskanäle ab.

— Überwachung der Anwendung: Mit den Software-Modulen für die dauerhafte Registerverknüpfung wird die Systemkommunikation auf der Anwendungsschicht (manuell und/oder in regelmäßigen Abständen) überwacht, um die Ende-zu-Ende-Verfügbarkeit der Verknüpfung zu testen, indem einige der Transaktionen über die Verknüpfung simuliert werden.

4.3. **Abnahme-/Testumgebungen**

Die Architektur des Unionsregisters und des Schweizer Registers umfasst die folgenden drei Umgebungen:

— Produktion (PROD): Diese Umgebung enthält die realen Daten und verarbeitet reale Transaktionen.

— Abnahme (ACC): Diese Umgebung enthält nicht-reale oder anonymisierte, repräsentative Daten. In dieser Umgebung validieren die Systembetreiber beider Vertragsparteien neue Releases.

— Test (TEST): Diese Umgebung enthält nicht-reale oder anonymisierte, repräsentative Daten. Diese Umgebung ist nur Registerverwaltern zugänglich und von beiden Vertragsparteien für Integrationstests zu nutzen.

Mit Ausnahme des VPN sind die drei Umgebungen völlig unabhängig voneinander, d. h. Hardware, Software, Datenbanken, virtuelle Umgebungen, IP-Adressen und Ports werden unabhängig voneinander eingerichtet und betrieben.

Im Hinblick auf das VPN-Layout muss die Kommunikation zwischen den drei Umgebungen völlig unabhängig sein, was durch die Verwendung von sTESTA gewährleistet wird.

5. **VERTRAULICHKEITS- UND INTEGRITÄTSVORSCHRIFTEN**

Die Sicherheitsmechanismen und -verfahren sehen für die Vorgänge im Zusammenhang mit der Verknüpfung zwischen dem Unionsregister und dem Schweizer Register eine Zwei-Personen-Methode (Vier-Augen-Prinzip) vor. Das Vier-Augen-Prinzip gilt, wann immer dies erforderlich ist, jedoch möglicherweise nicht für alle Schritte, die von Registerverwaltern unternommen werden.

Die Sicherheitsanforderungen werden im Sicherheitsmanagementplan berücksichtigt und behandelt, der auch Prozesse im Zusammenhang mit dem Umgang mit Sicherheitsvorfällen nach einer möglichen Sicherheitsverletzung umfasst. Der operative Teil dieser Prozesse wird in den gemeinsamen Verfahrensvorschriften beschrieben.

5.1. **Infrastruktur für die Sicherheitsprüfung**

Jede Vertragspartei verpflichtet sich zur Einrichtung einer Infrastruktur für die Sicherheitsprüfung (unter Verwendung der gemeinsamen Software und Hardware für die Erkennung von Schwachstellen in der Entwicklungs- und der Betriebsphase):

— die von der Produktionsumgebung getrennt ist;

— wo die Sicherheit von einem Team analysiert wird, das nicht an der Entwicklung und am Betrieb des Systems beteiligt ist.

Jede Vertragspartei verpflichtet sich, sowohl statische als auch dynamische Analysen durchzuführen.

Im Falle dynamischer Analysen (wie Penetrationstests) verpflichten sich beide Vertragsparteien, die Bewertungen im Allgemeinen auf die Test- und Abnahmeumgebungen (wie im Abschnitt 4.3 „Abnahme-/Testumgebungen“ definiert) zu beschränken. Ausnahmen von dieser Strategie bedürfen der Zustimmung beider Vertragsparteien.

Vor dem Einsatz in der Produktionsumgebung muss jedes Software-Modul der Verknüpfung (wie im Abschnitt 3.1 „Architektur der Kommunikationsverbindung“ definiert) einer Sicherheitsprüfung unterzogen werden.

Die Prüfinfrastruktur muss sowohl auf der Ebene des Netzes als auch auf der Ebene der Infrastruktur von der Produktion getrennt sein. Die Sicherheitsprüfungen, die erforderlich sind, um die Einhaltung der Sicherheitsanforderungen zu überprüfen, werden innerhalb der Prüfinfrastruktur durchgeführt.

5.2. **Unterbrechung der Verknüpfung und Vorschriften für ihre Reaktivierung**

Falls der Verdacht besteht, dass die Sicherheit des Schweizer Registers, des SSTL, des Unionsregisters oder des EUTL beeinträchtigt wurde, unterrichtet eine Vertragspartei die andere unverzüglich darüber und unterbricht die Verknüpfung zwischen dem SSTL und dem EUTL.

Die Verfahren für den Informationsaustausch, eine Entscheidung über die Unterbrechung und eine Entscheidung über die Reaktivierung sind Teil des Prozesses der Anfrageerledigung in den gemeinsamen Verfahrensvorschriften.

Unterbrechungen

Eine Unterbrechung der Registerverknüpfung gemäß Anhang II des Abkommens kann folgende Ursachen haben:

— verwaltungstechnische Gründe (z.B. Wartung), die geplant sind;

— Sicherheitsgründe (oder Ausfall der IT-Infrastruktur), die ungeplant sind.

Im Notfall unterrichtet eine Vertragspartei die andere Vertragspartei und unterbricht die Registerverknüpfung einseitig.

Wird beschlossen, die Registerverknüpfung zu unterbrechen, stellt jede Vertragspartei daher sicher, dass die Verknüpfung auf Netzwerkebene unterbrochen wird (durch Sperrung von Teilen oder der Gesamtheit der ein- und ausgehenden Verbindungen).

Die Entscheidung über die Unterbrechung der Registerverknüpfung – unabhängig davon, ob sie geplant oder ungeplant ist – wird nach dem Verfahren für das Änderungsmanagement oder das Sicherheitsvorfall-Management in den gemeinsamen Verfahrensvorschriften getroffen.

Reaktivierung der Kommunikation

Eine Entscheidung über die Reaktivierung der Registerverknüpfung wird auf die in den gemeinsamen Verfahrensvorschriften dargelegten Weise getroffen, und darf keinesfalls vor dem erfolgreichen Abschluss der Sicherheitsprüfverfahren gemäß den Abschnitten 5.4 „Leitlinien für Sicherheitsprüfungen“ und 4.2 „Initialisierungs-, Kommunikations-, Reaktivierungs- und Testplan“ erfolgen.

5.3. **Vorschriften für Sicherheitsverletzungen**

Bei einer Sicherheitsverletzung handelt es sich um einen Sicherheitsvorfall, der die Vertraulichkeit und Integrität vertraulicher Informationen und/oder die Verfügbarkeit des Systems, in dem sie verarbeitet werden, beeinträchtigt.

Vertrauliche Informationen sind im Verzeichnis vertraulicher Informationen aufgeführt und können im System oder in jedem damit zusammenhängenden Teil verarbeitet werden.

Informationen, die unmittelbar mit der Sicherheitsverletzung in Zusammenhang stehen, gelten als vertraulich, werden als „SPECIAL HANDLING: *ETS Critical*“ gekennzeichnet und im Einklang mit den Handhabungsanweisungen behandelt, sofern nichts anderes festgelegt ist.

Jede Sicherheitsverletzung wird gemäß dem Kapitel „Sicherheitsvorfallmanagement“ der gemeinsamen Verfahrensvorschriften behandelt.

5.4. **Leitlinien für Sicherheitsprüfungen**

5.4.1. *Software*

Zumindest alle größeren Releases der Software werden im Einklang mit den in den LTS festgelegten Sicherheitsanforderungen einer Sicherheitsprüfung, gegebenenfalls einschließlich eines Penetrationstests, unterzogen, um die Sicherheit der Verknüpfung und die entsprechenden Risiken zu bewerten.

Wenn in den letzten zwölf Monaten keine größeren Releases veröffentlicht wurden, wird das aktuelle System unter Berücksichtigung der Entwicklung der Cyberbedrohungslage in den letzten zwölf Monaten einem Sicherheitstest unterzogen.

Die Sicherheit der Registerverknüpfung wird in der Abnahmeumgebung und erforderlichenfalls in der Produktionsumgebung sowie unter Koordinierung und mit gegenseitigem Einverständnis beider Vertragsparteien getestet.

Beim Prüfen von Web-Anwendungen sind internationale offene Standards zu beachten, wie sie im Rahmen des Projekts „Open Web Application Security Project“ (OWASP) entwickelt wurden.

5.4.2. *Infrastruktur*

Die Infrastruktur, auf die sich das Produktionssystem stützt, wird regelmäßig (mindestens einmal monatlich) auf Schwachstellen geprüft; werden Schwachstellen festgestellt, werden diese nach dem gleichen Grundsatz wie im vorherigen Abschnitt unter Verwendung einer aktuellen Schwachstellendatenbank behoben.

5.5. **Vorschriften für die Risikobewertung**

Ist ein Penetrationstest anwendbar, so muss dieser in die Sicherheitsprüfung einbezogen werden.

Jede Vertragspartei kann ein spezialisiertes Unternehmen mit der Durchführung von Sicherheitsprüfungen beauftragen, sofern dieses Unternehmen

— über die Fähigkeiten für solche Sicherheitsprüfungen und entsprechende Erfahrungen verfügt;

— nicht direkt dem Entwickler der Software und/oder seinem Auftragnehmer unterstellt ist und weder an der Entwicklung der Software für die Verknüpfung beteiligt noch selbst Unterauftragnehmer des Entwicklers ist;

— eine Geheimhaltungsvereinbarung unterzeichnet hat, damit die Ergebnisse vertraulich bleiben und im Einklang mit den Handhabungsanweisungen als „SPECIAL HANDLING: ETS Critical“ behandelt werden.