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) [2021/1034]

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 das „Abkommen"), insbesondere auf Artikel 3 Absatz 7 und Artikel 13 Absatz 2,

in Erwägung nachstehender Gründe:

(1) Mit dem Beschluss Nr. 2/2019 des Gemeinsamen Ausschusses vom 5. Dezember 2019 ([2]) wurden die Anhänge I und II des Abkommens geändert, sodass die im Abkommen festgelegten Bedingungen für die Verknüpfung erfüllt sind.

(2) Nach Annahme des Beschlusses Nr. 2/2019 des Gemeinsamen Ausschusses tauschten die Vertragsparteien im Einklang mit Artikel 21 Absatz 3 des Abkommens ihre Ratifizierungs- oder Genehmigungsurkunden aus, da sie alle Bedingungen für eine Verknüpfung im Sinne des Abkommens erfüllt sehen.

(3) Im Einklang mit Artikel 21 Absatz 4 des Abkommens ist das Abkommen am 1. Januar 2020 in Kraft getreten.

(4) Anhang I des Abkommens sollte in Übereinstimmung mit Artikel 13 Absatz 2 des Abkommens geändert werden, indem den bisherigen Fortschritten bei der Registerverknüpfung Rechnung getragen wird, um bei der Verwaltung der Luftfahrzeugbetreiber, die erstmals der Schweiz zugeordnet werden, einen reibungslosen Übergang sicherzustellen.

(5) Damit die jüngsten Entwicklungen Berücksichtigung finden und eine größeres Maß an Flexibilität bei der Registerverknüpfung gemäß dem Abkommen gewährleistet wird, sollte Anhang II des Abkommens in Übereinstimmung mit dessen Artikel 13 Absatz 2 geändert werden, sodass eine größere Auswahl an gleichwertigen Technologien für die Einrichtung der Registerverknüpfung besteht.

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

(7) Im Einklang mit Artikel 13 Absatz 1 des Abkommens sollte sich der Gemeinsame Ausschuss auf technische Leitlinien zur Gewährleistung der ordnungsgemäßen Umsetzung des Abkommen einigen, die unter anderem die Einrichtung einer soliden und gesicherten Verbindung zwischen dem SSTL und dem EUTL betreffen. Die technischen Leitlinien können von einer gemäß Artikel 12 Absatz 5 des Abkommens eingesetzten Arbeitsgruppe erarbeitet werden. Die Arbeitsgruppe sollte mindestens den Schweizer Registerverwalter und den Zentralverwalter des Unionsregisters umfassen und den Gemeinsamen Ausschuss bei seinen Aufgaben gemäß Artikel 13 des Abkommens unterstützen.

(8) Wegen des technischen Inhalts der Leitlinien und der Notwendigkeit, sie an laufende Entwicklungen anzupassen, sollten die vom Schweizer Registerverwalter und vom Zentralverwalter des Unionsregisters erarbeiteten Leitlinien dem Gemeinsamen Ausschuss zur Information und gegebenenfalls zur Genehmigung vorgelegt werden —

([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).

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Anhang I Teil B Nummer 17 Absatz 2 des Abkommens erhält folgende Fassung:

„Die Schweiz übernimmt die Verwaltung der ihr nach dem Inkrafttreten dieses Abkommens erstmals zugeordneten Luftfahrzeugbetreiber nach dem 30. April des Jahres der Zuordnung und sobald die vorläufige Registerverbindung betriebsbereit ist."

Artikel 2

Anhang II Absatz 4 des Abkommens erhält folgende Fassung:

„In den LTS ist festzulegen, dass die Kommunikation zwischen dem SSTL und dem EUTL in Form eines gesicherten Austauschs von Webdienstmeldungen auf der Grundlage der folgenden oder gleichwertiger Technologien (*) erfolgt:

— Webdienste mit Simple Object Access Protocol (SOAP),

— hardwarebasiertes virtuelles privates Netzwerk (VPN),

— erweiterbare Auszeichnungssprache (XML),

— digitale Signatur und

— Netzzeitprotokolle (Network Time Protocols).

_____

(*) Diese Technologien werden derzeit für den Verbindungsaufbau zwischen dem Unionsregister und dem internationalen Transaktionsprotokoll bzw. zwischen dem Schweizer Register und dem internationalen Transaktionsprotokoll genutzt."

Artikel 3

Die technischen Verknüpfungstandards (LTS) im Anhang dieses Beschlusses werden angenommen.

Artikel 4

Im Einklang mit Artikel 12 Absatz 5 des Abkommens wird eine Arbeitsgruppe eingesetzt. Sie unterstützt den Gemeinsamen Ausschuss bei der Gewährleistung der ordnungsgemäßen Umsetzung des Abkommens, einschließlich der Erarbeitung von technischen Leitlinien für die Umsetzung der LTS.

Die Arbeitsgruppe umfasst mindestens den Schweizer Registerverwalter und den Zentralverwalter der Union.

Artikel 5

Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

Geschehen zu Brüssel am 5. November 2020.

Im Namen des Gemischten Ausschusses	Der Vorsitz	Sekretariat für die Schweiz
Sekretariat für die Europäische Union	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

ANHANG

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 VORLÄUFIGE LÖSUNG

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 EU-EHS oder des EHS der Schweiz gültig ist.
CH	Schweizerische Eidgenossenschaft
CHU	Allgemeine CH-Zertifikate (die Abkürzung „CHU2“ bezeichnet CH-Zertifikate des zweiten Verpflichtungszeitraums)
CHUA	CH-Luftverkehrszertifikat
Gemeinsame Verfahrensvorschriften	Von den Vertragsparteien des Abkommens gemeinsam erstellte gemeinsame Verfahrensvorschriften zur 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/Begriff	Begriffsbestimmung
Asymmetrische Kryptografie	Verwendung öffentlicher und privater Schlüssel zur Ver- und Entschlüsselung von Daten
Zertifizierungsstelle	Stelle, die digitale Zertifikate ausstellt

Abkürzung/Begriff	Begriffsbestimmung
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
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 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 das „Abkommen“) sieht die gegenseitige Anerkennung von Emissionszertifikaten vor, die für die Einhaltung der Vorschriften im Rahmen des Emissionshandelssystems der Europäischen Union (im Folgenden das „EU-EHS“) oder des Emissionshandelssystems der Schweiz (im Folgenden das „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 muss bis Mai 2020 oder so bald wie möglich danach eine vorläufige Lösung eingeführt werden. Die Vertragsparteien arbeiten zusammen, um so bald wie möglich die vorläufige Lösung durch eine dauerhafte Registerverknüpfung zu ersetzen (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 treten in Kraft, sobald sie durch Beschluss des Gemeinsamen Ausschusses angenommen wurden.

Der Gemeinsame Ausschuss soll die in diesem Dokument festgehaltenen LTS mit seinem Beschluss Nr. 2/2020 annehmen. Im Einklang mit diesem Beschluss ersucht der Gemeinsame Ausschuss den Schweizer Registerverwalter und den Zentralverwalter der Union, weitere technische Leitlinien zur Operationalisierung der Verknüpfung zu erarbeiten und sicherzustellen, dass diese laufend an den technischen Fortschritt und die neuen Anforderungen in Bezug auf die Sicherheit der Verknüpfung und ihr wirksames und effizientes Funktionieren angepasst werden.

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 Prozesses und Verfahren erforderlich, um sie 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. Obwohl die vorgesehene dauerhafte Registerverknüpfung auf Webdiensten beruhen wird, wird bei der vorläufigen Lösung stattdessen ein Dateiaustauschmechanismus verwendet.

Die technische Lösung verwendet Folgendes:

— ein Transferprotokoll für den sicheren Austausch von Meldungen,

— Meldungen im XML-Format,

— XML-basierte digitale Signatur und Entschlüsselung,

— VPN-Anwendung oder gleichwertiges Netz für die sichere Datenübermittlung.

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 wird sich auf ihr eigenes Archiv der eingegangenen Meldungen stützen.

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.

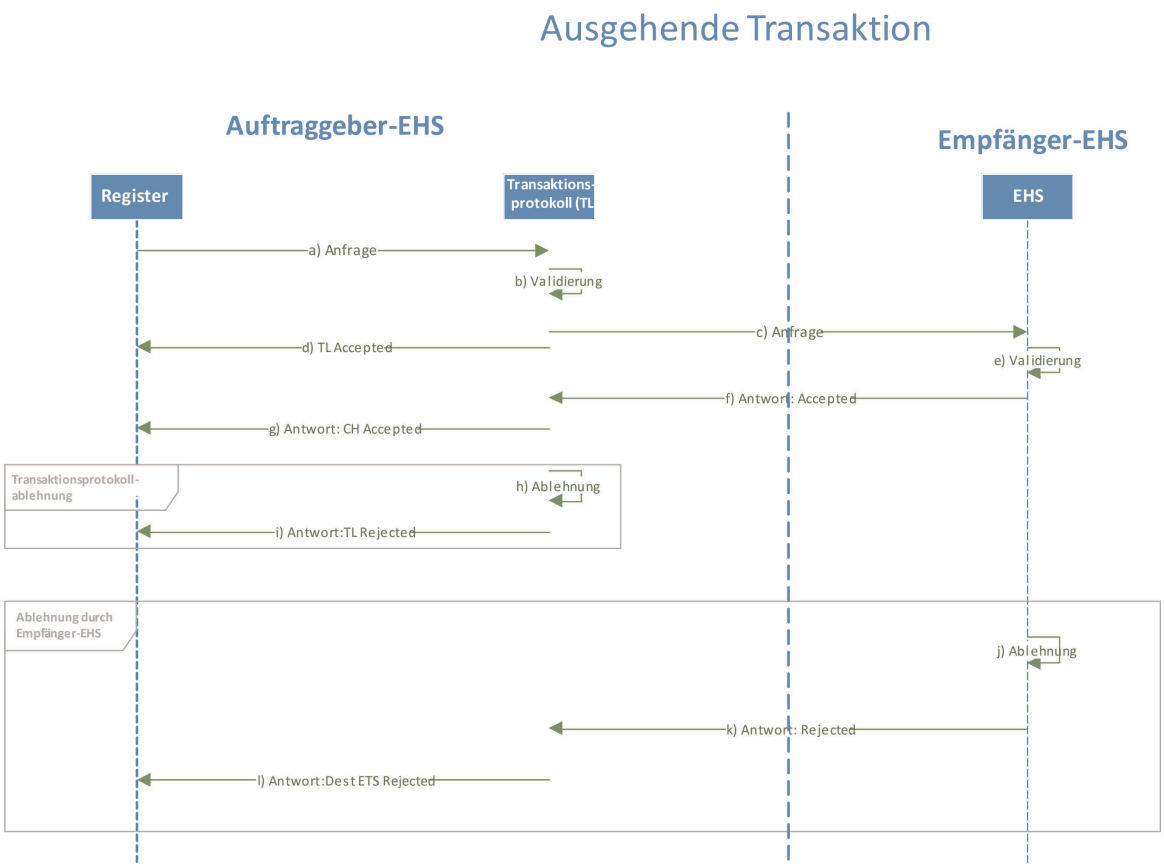
3.1.3. Eingabefenster

Die vorläufige Lösung 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 vorstehende Ablaufdiagramm zeigt alle spezifischen ausgehenden Transaktionsflüsse.

Hauptfluss „Normaltransaktion“ (entsprechend den Schritten in obiger 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 den Schritten in obiger Zeichnung, ebenfalls beginnend bei Buchstabe a):

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

Dann:

b) Das Transaktionsprotokoll validiert die Anfrage nicht.

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

Alternativfluss „Ablehnung im EHS“ (entsprechend den Schritten in obiger Zeichnung, beginnend bei Buchstabe a):

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.

Dann:

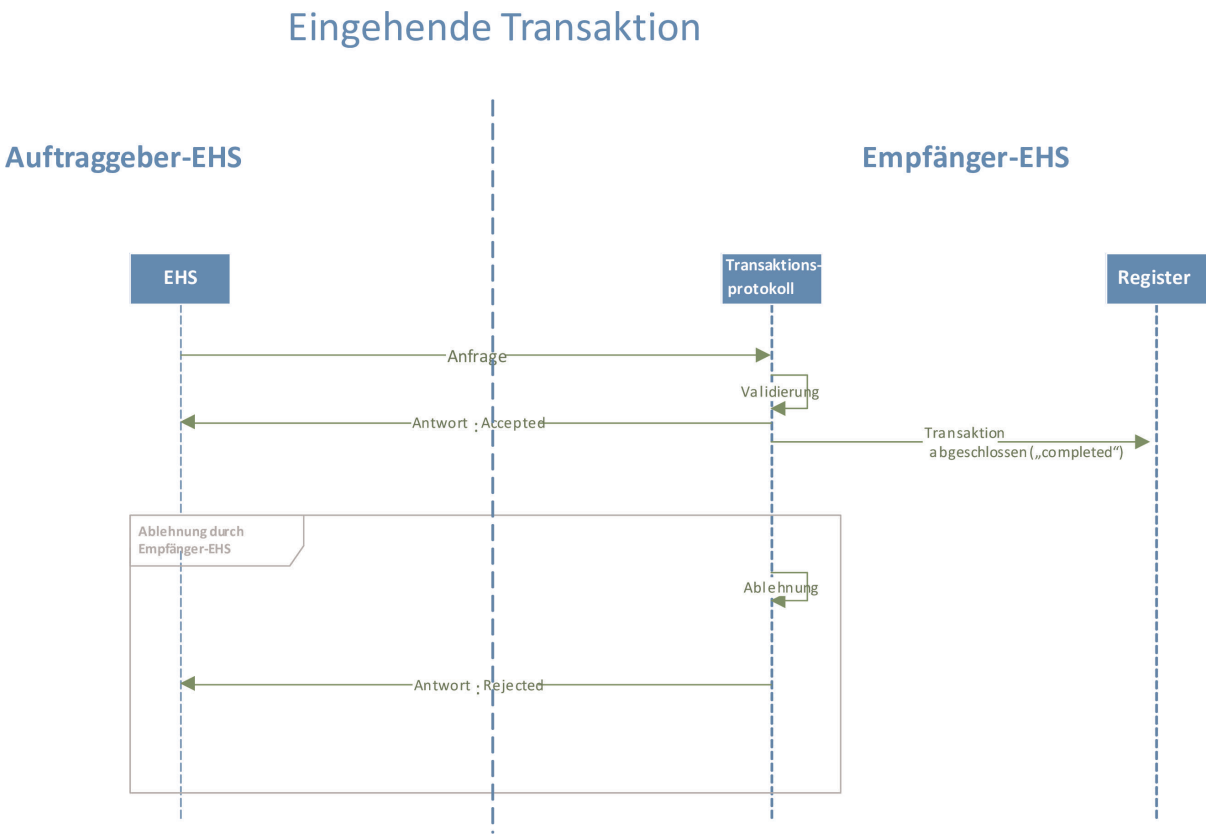
e) Das Transaktionsprotokoll des Empfänger-EHS validiert die Anfrage nicht.

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 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 oder gleichwertiges Netz für den sicheren Datentransport.

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 eine sichere Datentransporttechnologie geschützt. Im Falle eines virtuellen privaten Netzwerks (VPN) sollte die Infrastruktur auf Hardware oder virtuellen Anwendungen beruhen. 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.

Jede andere gleichwertige Lösung muss den oben genannten Grundsätzen entsprechen.

3.2.3. IPSec-Umsetzung

Wird eine VPN-Lösung verwendet, so ermöglicht die Verwendung des IPSec-Protokolls zur Schaffung der Site-to-site-VPN-Infrastruktur 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 vorläufige Lösung stützt sich für den sicheren Datenaustausch zwischen den Vertragsparteien auf mehrere Verschlüsselungsschichten. Beide Systeme und ihre unterschiedlichen Umgebungen sind auf Netzwerkebene über VPN-Tunnel oder gleichwertige sichere Datentransportnetze 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. Jede Transaktionsanfrage, 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. Kryptografischer 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. *Standards für Webdienste*

Webdienste werden für die vorläufige Lösung nicht genutzt. Es sei jedoch darauf hingewiesen, dass die Form und das Format der XML-Meldungen weitgehend unverändert bleiben werden. Mit der künftigen Einrichtung der dauerhaften Registerverknüpfung sollten Webdienste den Austausch von XML-Meldungen in Echtzeit ermöglichen.

3.5. *Webdienst-spezifische Definition*

Dieser Abschnitt gilt nicht für die vorläufige Lösung. Wie im vorangehenden Abschnitt erwähnt, werden Webdienste nur für die künftige dauerhafte Registerverknüpfung genutzt.

3.6. *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 umfasst 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 vorläufigen Lösung sind Abgleichmeldungen integraler Bestandteil der ausgetauschten Meldungen.

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.

3.7. *Betriebsvoraussetzungen*

Der Datenaustausch zwischen beiden Systemen ist bei der vorläufigen Lösung nicht völlig autonom; d. h., die Betreiber und Verfahren müssen die Verknüpfung operationalisieren.

4. **Verfügbarkeitsvorgaben**

4.1. *Gestaltung der Kommunikationsverfügbarkeit*

Die Architektur der vorläufigen Lösung 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 vorläufigen Lösung und 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 vorläufigen Verknüpfung ein widerstandsfähiges VPN-Netz (oder ein gleichwertiges 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 vorläufigen Lösung findet der Datenaustausch zwischen den Vertragsparteien während des gesamten Jahres in vordefinierten Zeitschlitzen 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 Betriebsverfahren spezifische Zeitfenster für die Durchführung der einzelnen Schritte vor;

— nutzen die Software-Module für die vorläufige Lösung 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 vorläufigen Lösung 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 vorläufige Lösung 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 Vertragsparteien 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 (oder ein gleichwertiges Netz für den sicheren Datentransport) 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 Vertragsparteien 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 vorläufige Verknüpfung 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 vorläufige Verknüpfung 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 Registers der Schweiz 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 (oder eines gleichwertigen Netzes) sind die drei Umgebungen völlig unabhängig voneinander, d. h. Hardware, Software, Datenbanken, virtuelle Umgebungen, IP-Adressen und Ports werden unabhängig voneinander eingerichtet und betrieben.

Das VPN-Layout umfasst zwei verschiedene Umgebungen, d. h. eine PROD-Umgebung und eine weitere unabhängige ACC- und TEST-Umgebung.

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 Produktionsinfrastruktur 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 Registers der Schweiz, 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 dargelegte 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 „ETS CRITICAL“ (EHS-höchst vertraulich) 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, und festgestellte Schwachstellen werden behoben. Tests werden entsprechend der in Abschnitt 5.4.1 dargestellten Methode unter Verwendung einer aktuellen Schwachstellendatenbank durchgeführt.

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 „ETS CRITICAL“ behandelt werden.