DECYZJA nr 2/2020 WSPÓLNEGO KOMITETU USTANOWIONEGO NA MOCY UMOWY MIĘDZY UNIĄ EUROPEJSKĄ A KONFEDERACJĄ SZWAJCARSKĄ W SPRAWIE POWIĄZANIA ICH SYSTEMÓW HANDLU UPRAWNIENIAMI DO EMISJI GAZÓW CIEPLARNIANYCH

z dnia 5 listopada 2020 r.

w sprawie zmiany załącznika I i II do umowy oraz przyjęcia norm technicznych powiązania [2021/1034]

WSPÓLNY KOMITET,

uwzględniając Umowę między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych ([1]) („umowa"), w szczególności jej art. 3 ust. 7 i art. 13 ust. 2,

a także mając na uwadze, co następuje:

(1) W decyzji nr 2/2019 Wspólnego Komitetu z dnia 5 grudnia 2019 r. ([2]) zmieniono załączniki I i II do umowy, tym samym spełniając warunki wymagane do ustanowienia powiązania, które określono w umowie.

(2) W następstwie przyjęcia decyzji nr 2/2019 Wspólnego Komitetu i na podstawie art. 21 ust. 3 umowy strony wymieniły się swoimi instrumentami ratyfikacji lub zatwierdzenia, ponieważ uznały, że spełnione zostały wszystkie warunki wymagane do ustanowienia powiązania, które określono w umowie.

(3) Zgodnie z art. 21 ust. 4 umowy weszła ona w życie dnia 1 stycznia 2020 r.

(4) Załącznik I do umowy należy zmienić zgodnie z art. 13 ust. 2 umowy w celu zapewnienia sprawnej zmiany administrowania operatorami statków powietrznych przypisanymi Szwajcarii po raz pierwszy, biorąc pod uwagę postępy poczynione w ustanawianiu powiązania rejestrów.

(5) Aby uwzględnić najnowsze zmiany i zapewnić wyższy poziom elastyczności na potrzeby ustanowienia powiązania rejestrów wymaganego na mocy umowy, należy zmienić załącznik II do umowy zgodnie z art. 13 ust. 2 umowy celem zapewnienia większego, ale równoważnego zestawu technologii służących utworzeniu powiązania rejestrów.

(6) Na podstawie art. 3 ust. 7 umowy administrator rejestru Szwajcarii i centralny administrator Unii powinni opracować normy techniczne powiązania oparte na zasadach określonych w załączniku II do umowy. W normach technicznych powiązania należy opisać szczegółowe wymogi ustanowienia solidnego i bezpiecznego połączenia między dodatkowym dziennikiem transakcji Szwajcarii (SSTL) a dziennikiem transakcji Unii Europejskiej (EUTL). Normy techniczne powiązania powinny stać się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

(7) Zgodnie z art. 13 ust. 1 umowy Wspólny Komitet powinien uzgodnić wytyczne techniczne celem zapewnienia prawidłowego wykonania umowy, w tym wytyczne techniczne dotyczące ustanowienia solidnego i bezpiecznego połączenia między SSTL a EUTL. Wytyczne techniczne można opracować w ramach grupy roboczej utworzonej na podstawie art. 12 ust. 5 umowy. Grupa robocza powinna składać się co najmniej z administratora rejestru Szwajcarii i centralnego administratora Unii i powinna wspierać Wspólny Komitet w wykonywaniu jego funkcji na mocy art. 13 umowy.

(8) Z uwagi na techniczny charakter wytycznych i konieczność dostosowania ich do bieżących zmian wytyczne techniczne przygotowane przez administratora rejestru Szwajcarii i centralnego administratora Unii powinny zostać przedłożone Wspólnemu Komitetowi w celach informacyjnych lub, w stosownych przypadkach, w celu zatwierdzenia,

([1]) Dz.U. L 322 z 7.12.2017, s. 3.

([2]) Decyzja nr 2/2019 Wspólnego Komitetu ustanowionego na mocy Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych z dnia 5 grudnia 2019 r. zmieniająca załączniki I i II do Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych (Dz.U. L 314 z 29.9.2020, s. 68).

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Akapit drugi pkt 17 część B załącznika I do umowy otrzymuje brzmienie:

„Operatorzy statków powietrznych przypisani Szwajcarii po raz pierwszy po wejściu w życie niniejszej Umowy są administrowani przez Szwajcarię po dniu 30 kwietnia roku przypisania i po uruchomieniu tymczasowego powiązania rejestrów.”.

Artykuł 2

Akapit czwarty załącznika II do umowy otrzymuje brzmienie:

„Normy techniczne powiązania wskazują, że komunikacja między SSTL a EUTL polega na bezpiecznej wymianie wiadomości usług sieciowych przy zastosowaniu następujących technologii (*) lub równoważnych:

— usług sieciowych wykorzystujących SOAP (ang. Simple Object Access Protocol),

— sprzętowej wirtualnej sieci prywatnej (VPN),

— XML (Extensible Markup Language),

— podpisu cyfrowego, oraz

— protokołów synchronizacji czasu.

(*) Technologie te obecnie stosuje się do tworzenia połączenia między rejestrem Unii a międzynarodowym dziennikiem transakcji, a także między rejestrem Szwajcarii a międzynarodowym dziennikiem transakcji.”.

Artykuł 3

Niniejszym przyjmuje się normy techniczne powiązania załączone do niniejszej decyzji.

Artykuł 4

Niniejszym tworzy się grupę roboczą na mocy art. 12 ust. 5 umowy. Grupa robocza wspiera Wspólny Komitet w zapewnieniu prawidłowego wykonania umowy, w tym w przygotowaniu wytycznych technicznych dotyczących wdrożenia norm technicznych powiazania.

Grupa robocza składa się co najmniej z administratora rejestru Szwajcarii i centralnego administratora Unii.

Artykuł 5

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w Brukseli dnia 5 listopada 2020 r.

W imieniu Wspólnego Komitetu	Sekretarz ze strony Unii Europejskiej	Przewodniczący
Sekretarz ze strony Szwajcarii	*Beatriz*YORDI	*Caroline*BAUMANN
Maja-Alexandra DITTEL		

ZAŁĄCZNIK

Normy techniczne powiązania na podstawie art. 3 ust. 7 Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych

NORMY DOTYCZĄCE TYMCZASOWEGO ROZWIĄZANIA

1. **Glosariusz**

Tabela 1-1

Akronimy i definicje branżowe

Akronim/termin	Definicja
Uprawnienie	Uprawnienie do emisji jednej tony ekwiwalentu dwutlenku węgla w określonym okresie, które jest ważne jedynie na potrzeby spełnienia wymogów w ramach EU ETS lub ETS Szwajcarii
CH	Konfederacja Szwajcarska
CHU	Szwajcarskie uprawnienia do emisji ogólnych (termin „CHU2" jest stosowany jako skrót od 2 okresu rozliczeniowego dotyczącego uprawnień CHU)
CHUA	Szwajcarskie uprawnienie do emisji lotniczych
COP	Wspólne procedury operacyjne opracowane wspólnie przez strony umowy w celu uruchomienia powiązania między EU ETS a ETS Szwajcarii
ETR	Rejestr handlu emisjami
ETS	System handlu emisjami
UE	Unia Europejska
EUA	Unijne uprawnienie do emisji ogólnych
EUAA	Unijne uprawnienie do emisji lotniczych
EUCR	Skonsolidowany rejestr Unii Europejskiej
EUTL	Dziennik transakcji Unii Europejskiej
Rejestr	System rejestracji uprawnień przyznanych na podstawie ETS służący do śledzenia własności uprawnień utrzymywanych na rachunkach elektronicznych
SSTL	Dodatkowy dziennik transakcji Szwajcarii
Transakcja	Proces w rejestrze dotyczący przekazywania uprawnienia z jednego rachunku na inny
System dziennika transakcji	Dziennik transakcji zawiera zapis każdej propozycji transakcji wysyłanej z jednego rejestru do drugiego

Tabela 1-2

Techniczne akronimy i definicje

Akronim	Definicja
Kryptografia asymetryczna	Wykorzystuje klucze publiczne i prywatne do zaszyfrowania i odszyfrowania danych
Centrum certyfikacji	Podmiot, który wydaje certyfikaty elektroniczne

Akronim	Definicja
Klucz kryptograficzny	Informacja, która określa wynik funkcjonalny algorytmu kryptograficznego
Odszyfrowywanie	Proces odwrotny do szyfrowania
Podpis cyfrowy	Technika matematyczna stosowana do sprawdzania autentyczności i integralności wiadomości, oprogramowania lub dokumentu elektronicznego
Szyfrowanie	Proces przekształcenia informacji lub danych w kod, w szczególności aby uniemożliwić dostęp osobom nieupoważnionym
Przyjmowanie pliku	Proces odczytywania pliku
Zapora sieciowa	Urządzenie lub oprogramowanie bezpieczeństwa monitorujące i kontrolujące przychodzący i wychodzący ruch sieciowy na podstawie wcześniej określonych reguł
Monitorowanie pulsu	Okresowy sygnał generowany i monitorowany przez sprzęt lub oprogramowanie celem wskazania normalnego funkcjonowania lub zsynchronizowania innych części systemu komputerowego
IPSec	Protokół IP Security Zestaw protokołów sieciowych, które uwierzytelniają i szyfrują pakiety danych w celu zapewnienia bezpiecznej szyfrowanej komunikacji między dwoma komputerami za pośrednictwem sieci protokołu internetowego
Testy penetracyjne	Praktyka testowania systemu komputerowego, sieci lub aplikacji internetowej służąca znalezieniu luk w zabezpieczeniach, które mógłby wykorzystać atakujący
Proces uzgadniania	Proces zapewniania, aby dwa zbiory wpisów były zgodne
VPN	Wirtualna sieć prywatna
XML	Rozszerzalny język znaczników Pozwala programistom na stworzenie własnych niestandardowych znaczników umożliwiających określanie, przesyłanie, sprawdzanie i interpretowanie danych między aplikacjami i między organizacjami

2. **Wprowadzenie**

Umowa między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych z dnia 23 listopada 2017 r. („umowa") przewiduje wzajemne uznawanie uprawnień do emisji, które można wykorzystać na potrzeby dostosowania się do wymogów systemu handlu uprawnieniami do emisji Unii Europejskiej („EU ETS") lub systemu handlu uprawnieniami do emisji Szwajcarii („ETS Szwajcarii"). W celu uruchomienia powiązania między EU ETS a ETS Szwajcarii ustanowione zostanie bezpośrednie powiązanie między dziennikiem transakcji Unii Europejskiej (EUTL) rejestru Unii a dodatkowym dziennikiem transakcji Szwajcarii (SSTL) rejestru Szwajcarii, co umożliwi bezpośrednie przekazywanie między rejestrami uprawnień do emisji wydanych w ramach któregokolwiek z ETS (art. 3 ust. 2 umowy). W celu uruchomienia powiązania między EU ETS i ETS Szwajcarii w maju 2020 r. lub możliwie szybko po tej dacie zostanie wdrożone tymczasowe rozwiązanie. Strony współpracują w celu jak najszybszego zastąpienia tymczasowego rozwiązania stałym powiązaniem rejestrów (załącznik II do umowy).

Na podstawie art. 3 ust. 7 umowy administrator rejestru Szwajcarii i centralny administrator Unii opracowują normy techniczne powiązania oparte na zasadach określonych w załączniku II do umowy, opisując szczegółowe wymogi ustanowienia solidnego i bezpiecznego połączenia między SSTL i EUTL. Normy techniczne powiązania opracowane przez administratorów stają się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

Normy techniczne powiązania w formie przedstawionej w niniejszym dokumencie mają zostać przyjęte przez Wspólny Komitet jego decyzją nr 2/2020. Zgodnie ze wspomnianą decyzją Wspólny Komitet zwraca się do administratora rejestru Szwajcarii i centralnego administratora Unii o opracowanie dalszych wytycznych technicznych celem uruchomienia powiązania i zapewnienia, aby były stale dostosowywane do postępu technicznego i nowych wymogów związanych z bezpieczeństwem i ochroną tego powiązania oraz jego skutecznym i sprawnym funkcjonowaniem.

2.1. *Zakres*

Niniejszy dokument odzwierciedla wspólne rozumienie stron umowy w kwestii ustanowienia technicznych podstaw powiązania między rejestrami EU ETS i ETS Szwajcarii. Chociaż nakreślono w nim podstawę specyfikacji technicznych pod względem wymogów dotyczących architektury, obsługi i bezpieczeństwa, do uruchomienia powiązania potrzebne będą dalsze szczegółowe wytyczne.

Jeżeli chodzi o prawidłowe funkcjonowanie, powiązanie będzie wymagało procesów i procedur do dalszego uruchomienia. Zgodnie z art. 3 ust. 6 umowy kwestie te szczegółowo opisano w osobnym dokumencie na temat wspólnych procedur operacyjnych, który zostanie przyjęty odrębną decyzją Wspólnego Komitetu.

2.2. *Adresaci*

Niniejszy dokument skierowany jest do administratora rejestru Szwajcarii i centralnego administratora Unii.

3. **Przepisy ogólne**

3.1. *Architektura łącza komunikacyjnego*

Celem tej sekcji jest przedstawienie opisu ogólnej architektury uruchomienia powiązania między EU ETS i ETS Szwajcarii oraz związanych z tym poszczególnych komponentów.

Ponieważ bezpieczeństwo jest podstawową częścią określenia architektury powiązania rejestrów, wprowadzono wszelkie środki mające na celu zapewnienie solidnej architektury. Mimo że stałe powiązanie rejestrów będzie opierać się na usługach sieciowych, w ramach tymczasowego rozwiązania stosowany będzie zamiast tego mechanizm wymiany plików.

Rozwiązanie techniczne wykorzystuje:

— protokół bezpiecznego przekazywania wymiany wiadomości,

— wiadomości XML,

— podpis cyfrowy i szyfrowanie oparte na standardzie XML,

— urządzenie VPN lub równoważną sieć bezpiecznego przesyłania danych,

3.1.1. Wymiana wiadomości

Podstawą komunikacji między rejestrem Unii a rejestrem Szwajcarii będzie mechanizm wymiany wiadomości za pośrednictwem bezpiecznych kanałów. Każdy koniec będzie opierał się na własnym repozytorium otrzymanych wiadomości.

Obie strony będą prowadzić dziennik otrzymywanych wiadomości wraz ze szczegółowymi informacjami na temat przetwarzania.

Błędy lub nieoczekiwany status wymagają zgłoszenia jako w postaci ostrzeżenia oraz kontaktu między osobami należącymi do zespołów wsparcia.

Błędy i nieoczekiwane zdarzenia będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi zarządzania incydentami.

3.1.2. Wiadomość XML – opis wysokiego poziomu

Wiadomość XML obejmuje jeden z następujących elementów:

— co najmniej jeden wniosek o transakcję lub przynajmniej jedną odpowiedź na wniosek o transakcję,

— jedną operację/odpowiedź związaną z uzgodnieniem,

— jedną wiadomość testową.

Każda wiadomość zawiera nagłówek z:

— nazwą systemu ETS pochodzenia,

— numerem porządkowym.

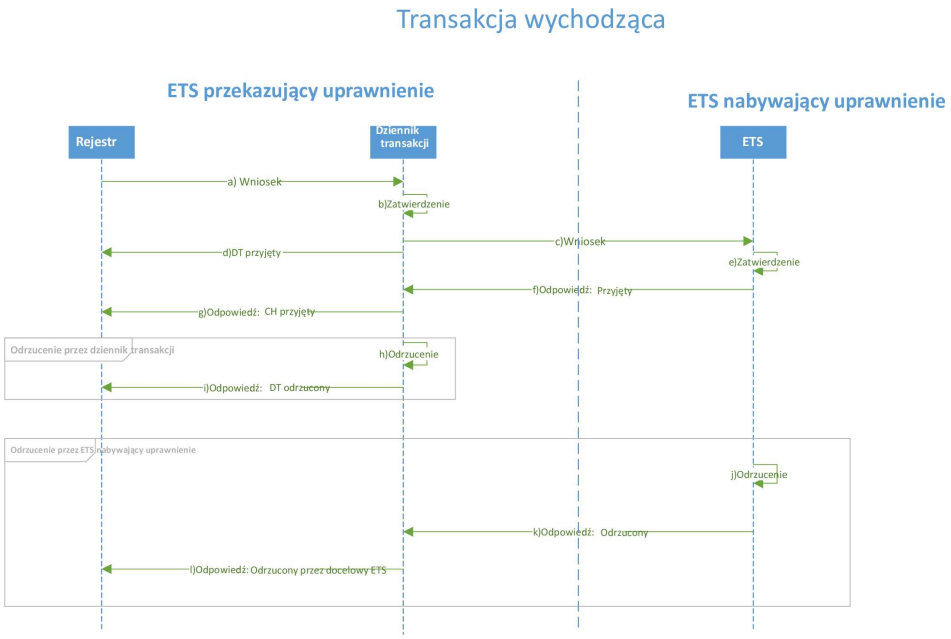
3.1.3. Okna przyjmowania

Tymczasowe rozwiązanie opiera się na wcześniej określonych oknach przyjmowania, po których następuje seria nazwanych zdarzeń. Wnioski o transakcje otrzymane za pośrednictwem powiązania będą przyjmowane wyłącznie w uprzednio ustalonych odstępach. Okna przyjmowania wiążą się ze sprawdzeniem wychodzących i przychodzących transakcji pod względem technicznym. Ponadto uzgodnienia można prowadzić codziennie i inicjować ręcznie.

Zmiany częstotliwości lub terminów każdego z tych zdarzeń będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi realizacji wniosków.

3.1.4. Przepływy wiadomości związanych z transakcją

Transakcje wychodzące



Odzwierciedla to perspektywę ETS przekazującego uprawnienie. Na powyższym schemacie sekwencji przedstawiono wszystkie przepływy szczególnych transakcji wychodzących.

Główny przepływ „transakcja zwykła” (o etapach wskazanych na rysunku powyżej):

a) w przypadku ETS przekazującego uprawnienie wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego);

b) dziennik transakcji zatwierdza wniosek o transakcję;

c) wniosek o transakcję jest wysyłany do ETS przeznaczenia;

d) odpowiedź o przyjęciu jest wysyłana do rejestru ETS pochodzenia;

e) ETS przeznaczenia zatwierdza wniosek o transakcję;

f) ETS przeznaczenia wysyła odpowiedź o przyjęciu z powrotem do dziennika transakcji ETS pochodzenia;

g) dziennik transakcji wysyła do rejestru odpowiedź o przyjęciu.

Alternatywny przepływ „odrzucenie przez dziennik transakcji" (o etapach wskazanych na rysunku powyżej, począwszy również od pkt a)):

a) w ETS pochodzenia wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego);

następnie:

b) dziennik transakcji nie zatwierdza wniosku;

c) wiadomość o odrzuceniu jest wysyłana do rejestru pochodzenia.

Alternatywny przepływ „odrzucenie przez ETS" (o etapach wskazanych na rysunku powyżej, począwszy od pkt a)):

a) w ETS pochodzenia wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego);

b) dziennik transakcji zatwierdza transakcję;

c) wniosek o transakcję jest wysyłany do ETS przeznaczenia;

d) wiadomość o przyjęciu jest wysyłana do rejestru ETS pochodzenia;

następnie:

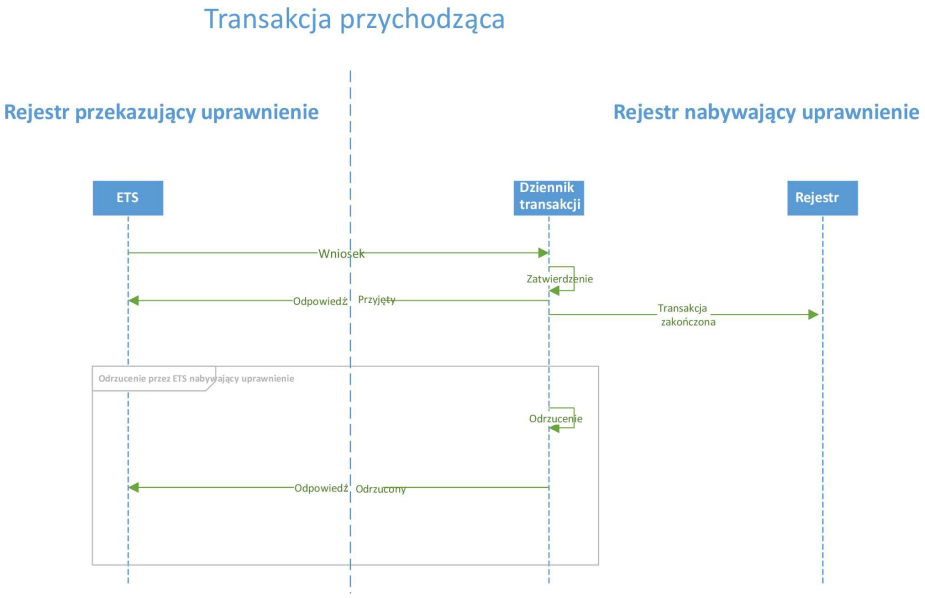
e) dziennik transakcji ETS nabywającego uprawnienie nie zatwierdza transakcji;

f) ETS nabywający uprawnienie wysyła odpowiedź odmowną do dziennika transakcji ETS przekazującego uprawnienie;

g) dziennik transakcji wysyła odmowę do rejestru.

Transakcje przychodzące

Odzwierciedla to perspektywę ETS nabywającego uprawnienie. Ten konkretny przepływ zobrazowano na kolejnym schemacie sekwencji:



Na schemacie tym przedstawiono:

1. sytuację, w której jeżeli dziennik transakcji ETS nabywającego uprawnienie zatwierdzi wniosek, to wysyła wiadomość o przyjęciu do ETS przekazującego uprawnienie oraz wiadomość „transakcja zakończona" do rejestru ETS nabywającego uprawnienie;
2. sytuację, w której jeżeli dziennik transakcji systemu nabywającego uprawnienie odmówi przyjęcia wniosku przychodzącego i wniosek ten zostanie odrzucony, wniosek o transakcję nie jest wysyłany do rejestru ETS nabywającego uprawnienie.

Protokół

Cykl wiadomości związanych z transakcją obejmuje jedynie dwie wiadomości:

— ETS przekazujący uprawnienie propozycja transakcji z ETS nabywającego uprawnienie,

— ETS nabywający uprawnienie odpowiedź na wniosek o transakcję ETS przekazującego uprawnienie: albo o przyjęciu, albo odrzuceniu (w tym powód odrzucenia):

  — przyjęty: transakcja zostaje zakończona,

  — odrzucony: transakcja zostaje przerwana.

Status transakcji

— status transakcji w ETS przekazującym uprawnienie zostanie ustawiony na „proponowana" po wysłaniu wniosku,

— status transakcji w ETS nabywającym uprawnienie zostanie ustawiony na „proponowana" po otrzymaniu wniosku i w czasie jego rozpatrywania,

— status transakcji w ETS nabywającym uprawnienie zostanie ustawiony na „zakończona"/„przerwana" po przetworzeniu propozycji. ETS nabywający uprawnienie wyśle wówczas odpowiednią wiadomość o przyjęciu/odrzuceniu,

— status transakcji w ETS przekazującym uprawnienie zostanie ustawiony na zakończona/przerwana po otrzymaniu i przetworzeniu wiadomości o przyjęciu/odrzuceniu,

— w przypadku nieotrzymania odpowiedzi, status transakcji w ETS przekazującym uprawnienie pozostanie ustawiony jako proponowana,

— status transakcji w ETS nabywającym uprawnienie zostanie ustawiony na „przerwana" jeżeli jakakolwiek transakcja pozostanie jako „proponowana" dłużej niż 30 minut.

Incydenty związane z transakcjami będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi zarządzania incydentami.

3.2. *Bezpieczeństwo przesyłania danych*

Przekazywane dane będą podlegać czterem poziomom bezpieczeństwa:

1) kontroli dostępu do sieci: zapora sieciowa i warstwa połączenia międzysieciowego;
2) szyfrowaniu na poziomie przesyłania: VPN lub równoważna sieć bezpiecznego przesyłania danych;
3) szyfrowaniu na poziomie sesji: protokół bezpiecznego przekazywania wymiany wiadomości;
4) szyfrowaniu na poziomie aplikacji: szyfrowanie treści i podpisywanie w formacie XML.

3.2.1. Zapora sieciowa i połączenie międzysieciowe

Powiązanie ustanawia się za pośrednictwem sieci zabezpieczonej sprzętową zaporą sieciową. Zaporę sieciową konfiguruje się za pomocą reguł w taki sposób, aby wyłącznie „zarejestrowani" klienci mogli połączyć się z serwerem VPN.

3.2.2. Wirtualna sieć prywatna (VPN)

Wszelka komunikacja między stronami jest zabezpieczana z wykorzystaniem technologii bezpiecznego przesyłania danych. W przypadku wirtualnej sieci prywatnej (VPN) infrastruktura powinna opierać się na urządzeniach sprzętowych lub wirtualnych. Technologie VPN zapewniają możliwość „tworzenia korytarza" przez sieć taką jak internet z jednego punktu do drugiego, zabezpieczającego wszelką komunikację. Przed stworzeniem korytarza VPN wydawany jest certyfikat elektroniczny dla punktu końcowego potencjalnego klienta, co pozwala klientowi na dostarczenie potwierdzenia tożsamości w trakcie negocjowania połączenia. Każda ze stron jest odpowiedzialna za zainstalowanie certyfikatu w swoim punkcie końcowym VPN. Korzystając z certyfikatu elektronicznego, każdy końcowy serwer VPN uzyska dostęp do centrum certyfikacji w celu negocjowania danych uwierzytelniających. Podczas procesu tworzenia korytarza negocjowane jest szyfrowanie, zapewniające, aby wszelka komunikacja za pośrednictwem korytarza była zabezpieczona.

Punkty końcowe klienta VPN konfiguruje się, aby na stałe utrzymać korytarz VPN w celu umożliwienia niezawodnej, dwustronnej komunikacji między stronami w czasie rzeczywistym w dowolnym momencie.

Każde inne równoważne rozwiązanie musi być zgodne z powyższymi zasadami.

3.2.3. Wdrażanie IPSec

W przypadku korzystania z rozwiązania VPN, stosowanie protokołu IPSec celem utworzenia międzylokacyjnej infrastruktury VPN zapewni międzylokacyjne uwierzytelnianie, integrację i szyfrowanie danych. Konfiguracje IPSec w VPN zapewniają właściwe uwierzytelnianie między dwoma punktami końcowymi połączenia VPN. Strony zidentyfikują i uwierzytelnią zdalnego klienta za pośrednictwem połączenia IPSec, korzystając z certyfikatów elektronicznych wydanych przez centrum certyfikacji i uznawanych przez drugi koniec.

IPSec zapewnia również integralność danych wszelkiej komunikacji prowadzonej za pośrednictwem korytarza VPN. Pakiety danych są skracane i podpisywane z wykorzystaniem informacji uwierzytelniających ustanowionych przez VPN. Poufność danych jest zapewniana w podobny sposób – poprzez umożliwienie szyfrowania IPSec.

3.2.4. Protokół bezpiecznego przekazywania wymiany wiadomości

Tymczasowe rozwiązanie opiera się na wielu warstwach szyfrowania służących bezpiecznej wymianie danych między stronami. Oba systemy i ich różne środowiska są wzajemnie powiązane na poziomie sieci za pomocą korytarzy VPN lub równoważnych sieci bezpiecznego przesyłania danych. Na poziomie aplikacji pliki są przekazywane z wykorzystaniem protokołu bezpiecznego przekazywania wymiany wiadomości na poziomie sesji.

3.2.5. Szyfrowanie i podpisywanie w formacie XML

W ramach plików XML podpisywanie i szyfrowanie odbywa się na dwóch poziomach. Każdy wniosek o transakcję, odpowiedź na wniosek o transakcję oraz komunikat dotyczący uzgodnienia są elektronicznie podpisywane indywidualnie.

Na drugim etapie każdy element podrzędny elementu „wiadomość" jest indywidualnie szyfrowany.

Ponadto, jako trzeci etap i w celu zapewnienia integralności i niezaprzeczalności całej wiadomości, wiadomość będąca elementem podstawowym jest podpisywana elektronicznie. Skutkuje to wysokim poziomem zabezpieczenia danych opartych na formacie XML. Przy technicznym wdrożeniu przestrzega się norm ustanowionych przez konsorcjum World Wide Web.

Aby odszyfrować i zweryfikować wiadomość proces jest wykonywany w odwrotnej kolejności.

3.2.6. Klucze kryptograficzne

Do celów szyfrowania i podpisywania stosowana będzie kryptografia wykorzystująca klucz publiczny.

W szczególnym przypadku IPSec korzysta się z certyfikatu elektronicznego wydanego przez centrum certyfikacji i uznawanego przez obie strony. To centrum certyfikacji weryfikuje tożsamość posiadacza certyfikatu i wydaje certyfikaty, które są wykorzystywane do niepodważalnej identyfikacji organizacji i ustanowienia kanałów bezpiecznej transmisji danych między stronami.

Z kluczy kryptograficznych korzysta się do podpisywania i szyfrowania kanałów komunikacji i plików z danymi. Publiczne certyfikaty są elektronicznie wymieniane między stronami z wykorzystaniem bezpiecznych kanałów i weryfikowane w sposób pozapasmowy. Procedura ta stanowi integralną część procesu zarządzania bezpieczeństwem informacji określonego we wspólnych procedurach operacyjnych.

3.3. *Wykaz funkcji w ramach powiązania*

Powiązanie określa system przesyłania szeregu funkcji realizujących procesy biznesowe wynikające z umowy. Powiązanie obejmuje również specyfikację procesu uzgadniania oraz wiadomości testowych, które umożliwią wdrożenie monitorowania pulsu.

3.3.1. Transakcje handlowe

Z perspektywy handlowej powiązanie uwzględnia cztery (4) rodzaje wniosków o transakcję.

— Przekazanie z zewnątrz:

  — po wejściu w życie powiązania ETS unijne i szwajcarskie uprawnienia będą zamienne i tym samym ich przekazanie między stronami będzie w pełni możliwe,

— wysłanie przekazania za pośrednictwem powiązania będzie obejmowało rachunek przekazującego w ETS oraz rachunek nabywającego w drugim ETS,

— przekazanie może obejmować dowolną liczbę czterech (4) rodzajów uprawnień:

— szwajcarskich uprawnień do emisji ogólnych (CHU);

— szwajcarskich uprawnień do emisji lotniczych (CHUA);

— unijnych uprawnień do emisji ogólnych (EUA);

— unijnych uprawnień do emisji lotniczych (EUAA).

— Przydział międzynarodowy:

operatorzy statku powietrznego administrowani za pośrednictwem jednego ETS mający obowiązki wobec drugiego ETS oraz uprawnieni do otrzymania bezpłatnych uprawnień od tego drugiego ETS otrzymają bezpłatne uprawnienia do emisji lotniczych od tego drugiego ETS w drodze transakcji przydziału międzynarodowego.

— Cofnięcie przydziału międzynarodowego:

transakcja ta będzie miała miejsce w przypadku, w którym przydział bezpłatnych uprawnień do rachunku posiadania operatora statku powietrznego w ramach drugiego ETS będzie musiał zostać cofnięty w całości.

— Zwrot nadmiernego przydziału:

podobny do cofnięcia, ale w przypadku gdy przydział nie musi być w pełni cofnięty i konieczne jest zwrócenie do przydzielającego ETS jedynie uprawnień przydzielonych w nadmiarze.

3.3.2. Protokół uzgadniania

Uzgodnienia będą mieć miejsce dopiero po zamknięciu okien przyjmowania, zatwierdzania i przetwarzania wiadomości.

Uzgodnienia stanowią integralną część środków służących zachowaniu bezpieczeństwa i spójności powiązania. Obie strony ustalą dokładne terminy uzgodnień przed sporządzeniem harmonogramu. Zaplanowane codzienne uzgodnienia mogą się odbywać, jeżeli obie strony wyrażą na nie zgodę. Będzie wykonywane co najmniej jedno zaplanowane uzgodnienie po każdym przeprowadzeniu przyjęcia.

W każdym przypadku każda ze stron może w dowolnym momencie zainicjować ręczne uzgodnienie.

Zmiany terminów i częstotliwości zaplanowanych uzgodnień będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi realizacji wniosków.

3.3.3. Wiadomość testowa

Przewiduje się wiadomość testową w celu testowania łączności typu koniec-koniec. Wiadomość będzie zawierać dane, które wskażą, że jest to wiadomość testowa, i po otrzymaniu jej przez drugi koniec zostanie przesłana na nią odpowiedź.

3.4. *Standardy usług sieciowych*

Usługi sieciowe nie będą wykorzystywane w ramach tymczasowego rozwiązania. Warto jednak zauważyć, że układ i format wiadomości XML pozostaną w dużym stopniu niezmienione. Dzięki wprowadzeniu stałego powiązania rejestrów w przyszłości, usługi sieciowe powinny umożliwić wymianę wiadomości XML w czasie rzeczywistym.

3.5. *Konkretna definicja usług sieciowych*

Sekcja ta nie ma zastosowania do tymczasowego rozwiązania. Jak wspomniano w poprzedniej sekcji, usługi sieciowe będą wykorzystywane dopiero w ramach przyszłego stałego powiązania rejestrów.

3.6. *Wymogi rejestracji danych*

Aby wesprzeć konieczność zachowywania przez obie strony odpowiednich i spójnych informacji oraz zapewnić narzędzia do wykorzystania w procesie uzgadniania służące do usunięcia niespójności, obie strony będą prowadzić cztery (4) rodzaje dzienników danych:

— dzienniki transakcji,

— dzienniki uzgadniania,

— archiwum wiadomości,

— ścieżki audytu wewnętrznego.

Wszelkie dane w tych dziennikach muszą być przechowywane przez okres co najmniej trzech (3) miesięcy do celów rozwiązywania problemów, a ich dalsze zachowanie będzie zależeć od obowiązującego prawa na każdym końcu na potrzeby przeprowadzenia audytu. Pliki dziennika starsze niż trzy (3) miesiące można zarchiwizować w bezpiecznej lokalizacji w niezależnym systemie informatycznym, o ile ich wyszukanie lub uzyskanie do nich dostępu będzie możliwe w rozsądnym czasie.

Dzienniki transakcji

Zarówno podsystem EUTL, jak i podsystem SSTL, obejmuje wdrożenie dzienników transakcji.

Dokładniej rzecz ujmując, w dziennikach transakcji będzie rejestrowana każda propozycja transakcji wysyłana do drugiego ETS. Każdy zapis zawiera wszystkie pola treści transakcji oraz późniejszy wynik transakcji (odpowiedź ETS otrzymującego propozycję). W dziennikach transakcji będą rejestrowane również transakcje przychodzące, a także odpowiedzi wysyłane do ETS pochodzenia.

Dzienniki uzgadniania

Dziennik uzgadniania zawiera zapis każdego komunikatu dotyczącego uzgodnienia wymienionego między obydwiema stronami, w tym identyfikator uzgodnienia, znacznik czasowy i wynik uzgodnienia: status uzgodnienia „przyjęte" lub „rozbieżne". W ramach tymczasowego rozwiązania komunikaty dotyczące uzgodnienia stanowią integralną część wymienianych wiadomości.

Obie strony rejestrują każdy wniosek i odpowiedź w dzienniku uzgadniania. Chociaż informacje zamieszczane w dzienniku uzgadniania nie są udostępniane bezpośrednio jako część samego uzgodnienia, dostęp do tych informacji może być konieczny, aby rozstrzygnąć niespójności.

Archiwum wiadomości

Wymaga się, aby obie strony archiwizowały kopie wymienianych danych (pliki XML), wysyłanych i otrzymywanych oraz fakt, czy dane te lub wiadomości XML miały odpowiedni format.

Archiwum ma służyć głównie do celów przeprowadzania audytu – posiadania dowodu tego, co zostało wysłane drugiej stronie i od niej otrzymane. W tym kontekście wraz z plikami należy archiwizować również powiązane z nimi certyfikaty.

Pliki te dostarczą także dodatkowych informacji na potrzeby rozwiązywania problemów.

Ścieżki audytu wewnętrznego

Dzienniki te są określane i stosowane przez strony we własnym zakresie.

3.7. *Wymogi operacyjne*

Wymiana danych między obydwoma systemami w ramach tymczasowego rozwiązania nie jest w pełni niezależna, co oznacza, że do uruchomienia powiązania wymaga operatorów i procedur.

4. **Przepisy dotyczące dostępności**

4.1. *Opracowywanie dostępności komunikacji*

Architekturę tymczasowego rozwiązania stanowią zasadniczo infrastruktura z zakresu technologii informacyjno-komunikacyjnych i oprogramowanie, które umożliwiają komunikację między ETS Szwajcarii i EU ETS. Zapewnienie wysokiego poziomu dostępności, integralności i poufności tego przepływu danych staje się zatem podstawowym aspektem, który należy uwzględnić przy opracowywaniu tymczasowego rozwiązania i stałego powiązania rejestrów. W przypadku projektu, w którym infrastruktura z zakresu technologii informacyjno-komunikacyjnych, niestandardowe oprogramowanie oraz procesy odgrywają integralną rolę, należy wziąć pod uwagę wszystkie trzy elementy, aby opracować odporny system.

Odporność infrastruktury z zakresu technologii informacyjno-komunikacyjnych

Podstawowe elementy architektoniczne szczegółowo opisano w rozdziale niniejszego dokumentu dotyczącym przepisów ogólnych. Po stronie infrastruktury z zakresu technologii informacyjno-komunikacyjnych tymczasowe powiązanie ustanawia odporną sieć VPN (lub równoważną) tworzącą zabezpieczone korytarze komunikacji, za pośrednictwem których odbywa się bezpieczna wymiana wiadomości. Inne elementy infrastruktury są konfigurowane w wysokiej dostępności lub opierają się na mechanizmach rezerwowych.

Odporność niestandardowego oprogramowania

Niestandardowe moduły oprogramowania zwiększają odporność poprzez ponawianie próby nawiązania komunikacji z drugim końcem przez określony czas, jeżeli z jakiegoś powodu jest on niedostępny.

Odporność usługi

W ramach tymczasowego rozwiązania wymiana danych między stronami odbywa się we wcześniej określonych przedziałach czasowych przez cały rok. Niektóre z etapów niezbędnych podczas uprzednio zaplanowanej wymiany danych wymagają ręcznej interwencji operatorów systemu lub administratorów rejestru. Biorąc ten aspekt pod uwagę oraz w celu zwiększenia dostępności i powodzenia wymiany:

— w procedurach operacyjnych przewidziano znaczne okna czasowe na przeprowadzenie każdego etapu,

— moduły oprogramowania tymczasowego rozwiązania realizują asynchroniczną komunikację,

— automatyczny proces uzgadniania wykryje, jeżeli na którymś końcu wystąpiły problemy z przyjęciem plików z danymi,

— procesy monitorowania (infrastruktura z zakresu technologii informacyjno-komunikacyjnych i moduły niestandardowego oprogramowania) są rozpatrywane w ramach procedur zarządzania incydentami i uruchamiają te procedury (jak określono w dokumencie na temat wspólnych procedur operacyjnych). Procedury służące ograniczeniu czasu potrzebnego na przywrócenie normalnego funkcjonowania po wystąpieniu incydentów są niezbędne, aby zapewnić wysokie współczynniki dostępności.

4.2. *Plan dotyczący inicjowania, komunikacji, ponownej aktywacji oraz testów*

Wszystkie poszczególne elementy związane z architekturą tymczasowego rozwiązania muszą przejść serię indywidualnych i wspólnych testów, aby potwierdzić, że platforma na poziomie infrastruktury z zakresu technologii informacyjno-komunikacyjnych oraz systemu informacyjnego jest gotowa. Przeprowadzenie tych testów operacyjnych jest obowiązkowym warunkiem wstępnym za każdym razem, gdy platforma zmienia status tymczasowego rozwiązania z zawieszonego na funkcjonujący.

Aktywacja statusu powiązania, który oznacza funkcjonowanie, wymaga zatem wykonania uprzednio określonego planu testów z powodzeniem. Musi to potwierdzić, że przed rozpoczęciem składania wniosków o transakcje dotyczące produkcji między obydwiema stronami, każdy rejestr przeprowadził najpierw szereg wewnętrznych testów, a następnie zatwierdził łączność koniec-koniec.

W planie testów należy wskazać ogólną strategię testów oraz podać szczegółowe informacje na temat infrastruktury testowania. W szczególności w odniesieniu do każdego elementu we wszystkich blokach testów plan ten musi obejmować:

— kryteria i narzędzia testu,

— role przypisane do przeprowadzenia testu,

— oczekiwane wyniki (pozytywne i negatywne),

— program testu,

— rejestrację wymogów w zakresie wyników testu,

— dokumentację rozwiązywania problemów,

— postanowienia dotyczące eskalacji.

Jako proces, testy dotyczące aktywacji statusu oznaczającego funkcjonowanie można podzielić na cztery (4) konceptualne bloki lub etapy.

4.2.1. Testy wewnętrznej infrastruktury z zakresu technologii informacyjno-komunikacyjnych

Testy te mają być przeprowadzone lub poddane kontroli indywidualnie przez obie strony na każdym końcu.

Wszystkie elementy infrastruktury z zakresu technologii informacyjno-komunikacyjnych na każdym końcu muszą być przetestowane indywidualnie. Obejmuje to każdy pojedynczy komponent infrastruktury. Testy te można wykonać automatycznie lub ręcznie, ale muszą one zweryfikować, czy każdy element infrastruktury funkcjonuje.

4.2.2. Testy komunikacji

Testy te są inicjowane indywidualnie przez którąkolwiek ze stron, a zakończenie testów wymaga współpracy z drugim końcem.

Gdy poszczególne elementy funkcjonują, należy przetestować kanały komunikacji między obydwoma rejestrami. W tym celu każda strona weryfikuje, czy dostęp do internetu działa, czy ustanowiono kanały VPN (lub równoważnej sieci bezpiecznego przesyłania) oraz czy istnieje międzylokacyjne połączenie IP. Następnie należy potwierdzić drugiemu końcowi, że elementy infrastruktury lokalnej i zdalnej oraz połączenie IP są możliwe do osiągnięcia.

4.2.3. Testy całego systemu (koniec-koniec)

Testy te wykonuje się na każdym końcu, a wyniki muszą być udostępnione drugiej stronie.

Po przetestowaniu kanałów komunikacji i wszystkich poszczególnych komponentów obu rejestrów każdy koniec przygotowuje serię symulowanych transakcji i uzgodnień reprezentatywnych dla wszystkich funkcji, które mają zostać wdrożone w ramach powiązania.

4.2.4. Testy bezpieczeństwa

Testy te mają być przeprowadzone lub zainicjowane przez obie strony na każdym końcu, jak wyszczególniono w sekcji 5.4 „Wytyczne testowania bezpieczeństwa" oraz 5.5 „Przepisy dotyczące oceny ryzyka".

Tymczasowe powiązanie można uznać za posiadające status oznaczający funkcjonowanie, dopiero gdy wszystkie cztery etapy/bloki zakończą się przewidywalnymi wynikami.

Zasoby testowania

Każda strona polega na określonych zasobach testowania (konkretnej infrastrukturze oprogramowania i sprzętu z zakresu technologii informacyjno-komunikacyjnych) i opracowuje funkcje testowania w swoich odnośnych systemach w celu wsparcia ręcznego i nieustannego sprawdzania platformy. Administratorzy rejestru mogą przeprowadzić ręczne indywidualne lub wspólne procedury testowania w dowolnym momencie. Aktywacja statusu oznaczającego funkcjonowanie sama w sobie jest procesem ręcznym.

Podobnie przewidziano, że platforma dokonuje automatycznych kontroli w regularnych odstępach czasu. Kontrole te służą zwiększeniu dostępności platformy poprzez wczesne wykrywanie potencjalnych problemów z infrastrukturą lub oprogramowaniem. Ten program monitorowania platformy składa się z dwóch elementów:

— monitorowania infrastruktur z zakresu technologii informacyjno-komunikacyjnych: infrastruktura na obu końcach będzie monitorowana przez dostawców usług infrastrukturalnych z zakresu technologii informacyjno-komunikacyjnych. Automatyczne testy będą obejmować poszczególne elementy infrastruktury oraz dostępność kanałów komunikacji,

— monitorowanie aplikacji: moduły oprogramowania tymczasowego powiązania będą realizować monitorowanie komunikacji systemowej na poziomie aplikacji (albo ręcznie, albo w regularnych odstępach czasu), które przetestuje dostępność powiązania między końcami poprzez symulację niektórych transakcji za pośrednictwem powiązania.

4.3. *Środowisko akceptacyjne/testowe*

Architektura rejestru Unii i rejestru Szwajcarii składa się z następujących trzech środowisk:

— produkcyjnego: środowisko to przechowuje rzeczywiste dane i przetwarza rzeczywiste transakcje,

— akceptacyjnego: środowisko to zawiera nierzeczywiste lub zamaskowane, reprezentatywne dane. Jest to środowisko, w którym operatorzy systemów obu stron zatwierdzają nowe wersje,

— testowego: środowisko to zawiera nierzeczywiste lub zamaskowane, reprezentatywne dane. Środowisko to ogranicza się do administratorów rejestru i służy do przeprowadzania testów integracyjnych przez obie strony.

Z wyjątkiem VPN (lub równoważnej sieci) te trzy środowiska są w pełni niezależne od siebie, co oznacza, że sprzęt, oprogramowanie, bazy danych, środowiska wirtualne, adresy IP i porty są ustanawiane i funkcjonują niezależnie od siebie.

Jeżeli chodzi o strukturę VPN, jest ona ustanawiana w dwóch różnych środowiskach, jednym produkcyjnym i drugim niezależnym akceptacyjno-testowym.

5. **Przepisy dotyczące poufności i integralności**

W ramach mechanizmów i procedur bezpieczeństwa przewidziano dwuosobową metodę (zasadę czworga oczu) odnoszącą się do operacji odbywających się za pośrednictwem powiązania między rejestrem Unii i rejestrem Szwajcarii. Tę dwuosobową metodę stosuje się w razie potrzeby. Może ona jednak nie mieć zastosowania do wszystkich kroków podejmowanych przez administratorów rejestrów.

Wymogi bezpieczeństwa rozważa się i uwzględnia w planie zarządzania bezpieczeństwem, który obejmuje również procesy związane z obsługą incydentów dotyczących bezpieczeństwa w następstwie ewentualnego naruszenia bezpieczeństwa. Operacyjną część tych procesów opisano we wspólnych procedurach operacyjnych.

5.1. *Infrastruktura testowania bezpieczeństwa*

Każda strona angażuje się w ustanowienie infrastruktury testowania bezpieczeństwa (korzystając ze wspólnego zestawu sprzętu i oprogramowania wykorzystywanego do wykrywania luk na etapie opracowywania i funkcjonowania):

— oddzielonej od środowiska produkcyjnego,

— w ramach której bezpieczeństwo jest analizowane przez zespół niezależny od opracowywania i funkcjonowania systemu.

Każda strona zobowiązuje się do przeprowadzenia zarówno analizy statycznej, jak i dynamicznej.

W przypadku analizy dynamicznej (takiej jak testy penetracyjne) obie strony zobowiązują się do ograniczenia ocen zazwyczaj do środowiska testowego i akceptacyjnego (jak określono w sekcji 4.3 „Środowisko akceptacyjne/testowe"). Odstępstwa od tej polityki podlegają wyrażeniu zezwolenia przez obie strony.

Przed wdrożeniem w środowisku produkcyjnym każdy moduł oprogramowania łącza (jak określono w sekcji 3.1 „Architektura łącza komunikacyjnego") testuje się pod względem bezpieczeństwa.

Infrastruktura testowa musi być oddzielona od infrastruktury produkcyjnej zarówno na poziomie sieci, jak i na poziomie infrastrukturalnym. Testy bezpieczeństwa wymagane w celu sprawdzenia zgodności z wymogami bezpieczeństwa są przeprowadzane w ramach infrastruktury testowej.

5.2. *Przepisy dotyczące zawieszenia i ponownej aktywacji powiązania*

Jeżeli istnieje podejrzenie, że bezpieczeństwo rejestru Szwajcarii, SSTL, rejestru Unii lub EUTL zostało naruszone, którakolwiek ze stron natychmiast informuje drugą stronę i zawiesza powiązanie między SSTL i EUTL.

Procedury dotyczące udostępnienia informacji, decyzji o zawieszeniu i decyzji o ponownej aktywacji są częścią procesu realizacji wniosku w ramach wspólnych procedur operacyjnych.

Zawieszenia

Zawieszenie powiązania rejestrów zgodnie z załącznikiem II do umowy może mieć miejsce ze względu na:

— planowane powody administracyjne (np. konserwacja),

— nieplanowane powody związane z bezpieczeństwem (lub awarię infrastruktury informatycznej).

W sytuacji awaryjnej każda ze stron poinformuje drugą i jednostronnie zawiesi powiązanie rejestrów.

W przypadku podjęcia decyzji o zawieszeniu powiązania rejestrów, każda strona w związku z tym zapewni, aby powiązanie zostało przerwane na poziomie sieci (poprzez zablokowanie części lub wszystkich połączeń przychodzących i wychodzących).

Decyzja o zawieszeniu powiązania rejestrów, planowanym lub nieplanowanym, zostanie podjęta zgodnie z procedurą zarządzania zmianą lub procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji określoną we wspólnych procedurach operacyjnych.

Ponowna aktywacja komunikacji

Decyzja o ponownej aktywacji powiązania rejestrów zostanie podjęta w sposób określony we wspólnych procedurach operacyjnych i w żadnym wypadku nie nastąpi przed zakończeniem z powodzeniem procedur testowania bezpieczeństwa wyszczególnionych w sekcji 5.4 „Wytyczne testowania bezpieczeństwa" oraz 4.2 „Plan dotyczący inicjowania, komunikacji, ponownej aktywacji oraz testów".

5.3. *Przepisy dotyczące naruszenia bezpieczeństwa*

Naruszenie bezpieczeństwa uznaje się za incydent związany z bezpieczeństwem mający wpływ na poufność i integralność informacji szczególnie chronionych lub dostępność przetwarzającego je systemu.

Informacje szczególnie chronione określono w wykazie informacji szczególnie chronionych i można je przetwarzać w systemie lub dowolnej powiązanej części systemu.

Informacje bezpośrednio związane z naruszeniem bezpieczeństwa zostaną uznane za szczególnie chronione, oznaczone jako „KRYTYCZNY poziom ochrony w ETS" i przetworzone zgodnie z instrukcjami przetwarzania, o ile nie ustanowiono inaczej.

Każde naruszenie bezpieczeństwa będzie rozwiązywane zgodnie z rozdziałem wspólnych procedur operacyjnych dotyczącym zarządzania incydentami związanymi z bezpieczeństwem informacji.

5.4. *Wytyczne dotyczące testowania bezpieczeństwa*

5.4.1. Oprogramowanie

Testowanie bezpieczeństwa, w tym w stosownych przypadkach testy penetracyjne, przeprowadza się przynajmniej na wszystkich głównych nowo wydanych wersjach oprogramowania zgodnie z wymogami bezpieczeństwa określonymi w normach technicznych powiązania, aby ocenić bezpieczeństwo powiązania i związane z nim ryzyko.

Jeżeli w ciągu ostatnich 12 miesięcy nie wydano głównej wersji, testowanie bezpieczeństwa przeprowadza się na obecnym systemie, biorąc pod uwagę rozwój zagrożeń dla cyberbezpieczeństwa, który nastąpił na przestrzeni ostatnich 12 miesięcy.

Testowania bezpieczeństwa powiązania rejestrów dokonuje się w środowisku akceptacyjnym i – jeżeli jest to wymagane – w środowisku produkcyjnym oraz przy koordynacji i wzajemnym porozumieniu obu stron.

Testowanie aplikacji sieciowej odbędzie się z zachowaniem międzynarodowych standardów otwartych, takich jak standardy opracowane przez Projekt Bezpieczeństwa Aplikacji Sieci Otwartej (OWASP).

5.4.2. Infrastruktura

Infrastruktura wspierająca system produkcji jest regularnie poddawana przeglądowi pod kątem luk (co najmniej raz w miesiącu), a wykryte luki zostają usunięte. Testy przeprowadza się zgodnie z metodą opisaną w sekcji 5.4.1, przy użyciu aktualnej bazy danych dotyczącej luk.

5.5. *Przepisy dotyczące oceny ryzyka*

Jeżeli stosowane są testy penetracyjne, muszą one zostać uwzględnione w testowaniu bezpieczeństwa.

Każda strona może udzielić zamówienia na przeprowadzenia testowania bezpieczeństwa specjalizującemu się w tym przedsiębiorstwu, o ile przedsiębiorstwo to:

— ma kwalifikacje i doświadczenie w zakresie takiego testowania bezpieczeństwa,

— nie odpowiada bezpośrednio przed twórcą ani jego wykonawcą i nie jest zaangażowane w opracowywanie oprogramowania powiązania ani nie jest podwykonawcą twórcy,

— podpisało umowę poufności celem zachowania poufności wyników i przetwarzania ich na poziomie „KRYTYCZNY poziom ochrony w ETS" zgodnie z instrukcjami przetwarzania.