COMMISSIONE
EUROPEA

Bruxelles, 30.6.2020
COM(2020) 271 final

ANNEX

ALLEGATO

della

proposta di decisione del Consiglio

relativa alla posizione da adottare a nome dell'Unione europea in sede di comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, riguardo alla modifica degli allegati I e II dell'accordo di collegamento e all'adozione di norme tecniche di collegamento

DECISIONE N. 2/2020 DEL COMITATO MISTO ISTITUITO DALL'ACCORDO TRA L'UNIONE EUROPEA E LA CONFEDERAZIONE SVIZZERA CONCERNENTE IL COLLEGAMENTO DEI RISPETTIVI SISTEMI DI SCAMBIO DI QUOTE DI EMISSIONE DI GAS A EFFETTO SERRA

del …

relativa alla modifica dell'allegato I e II dell'accordo e delle norme tecniche di collegamento (NTC)

IL COMITATO MISTO

visto l'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione dei gas a effetto serra[1] ("l'accordo"), in particolare l'articolo 3, paragrafo 7, e l'articolo 13, paragrafo 2,

considerando quanto segue:

(1) La decisione n. 2/2019 del comitato misto, del 5 dicembre 2019[2], ha modificato gli allegati I e II dell'accordo soddisfacendo in tal modo le condizioni per il collegamento di cui all'accordo.

(2) A seguito dell'adozione della decisione n. 2/2019 del comitato misto e a norma dell'articolo 21, paragrafo 3, dell'accordo, le parti hanno scambiato i loro strumenti di ratifica, in quanto ritengono soddisfatte tutte le condizioni per il collegamento previste nell'accordo.

(3) A norma dell'articolo 21, paragrafo 4, dell'accordo, quest'ultimo è entrato in vigore il 1° gennaio 2020.

(4) È opportuno modificare l'allegato I dell'accordo conformemente all'articolo 13, paragrafo 2, dell'accordo per garantire un'agevole transizione nell'amministrazione degli operatori aerei attribuiti per la prima volta alla Svizzera, tenendo conto dei progressi compiuti nell'istituzione di tale collegamento.

(5) Per tenere conto dei recenti sviluppi e garantire un maggiore livello di flessibilità nell'istituire il collegamento dei registri richiesto dall'accordo, l'allegato II dovrebbe essere modificato conformemente all'articolo 13, paragrafo 2, dell'accordo per fornire un ventaglio più ampio ma equivalente di tecnologie per istituire il collegamento tra i registri.

(6) A norma dell'articolo 3, paragrafo 7, dell'accordo, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione dovrebbero elaborare norme tecniche di collegamento (NTC) basate sui principi di cui all'allegato II dell'accordo. Le NTC dovrebbero descrivere in dettaglio le disposizioni per l'istituzione di una connessione solida e sicura tra il libro di bordo elettronico supplementare della Svizzera (SSTL) e il catalogo delle operazioni dell'Unione europea (EUTL). Le NTC dovrebbero entrare in vigore una volta adottate con decisione del comitato misto.

(7) A norma dell'articolo 13, paragrafo 1, dell'accordo, il comitato misto dovrebbe stabilire orientamenti tecnici per garantire la corretta attuazione dell'accordo, anche per quanto riguarda l'istituzione di un collegamento solido e sicuro tra l'SSTL e l'EUTL. Gli orientamenti tecnici possono essere elaborati da un gruppo di lavoro istituito a norma dell'articolo 12, paragrafo 5, dell'accordo Del gruppo di lavoro

[1] GU L 322 del 7.12.2017, pag. 3.

[2] GU [XXXX]

dovrebbero far parte quanto meno l'amministratore del registro svizzero e l'amministratore centrale del registro dell'Unione; il gruppo di lavoro dovrebbe inoltre assistere il comitato misto nell'esercizio delle sue funzioni a norma dell'articolo 13 dell'accordo.

(8) Data la natura tecnica degli orientamenti e la necessità di adeguarli agli sviluppi in corso, gli orientamenti tecnici elaborati dall'amministratore del registro svizzero e dall'amministratore centrale dell'Unione dovrebbero essere trasmessi al comitato misto per informazione o, se del caso, approvazione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Nella parte B dell'allegato I dell'accordo, il secondo comma del punto 17 è sostituito dal testo seguente:

"Gli operatori aerei attribuiti alla Svizzera per la prima volta dopo l'entrata in vigore del presente accordo sono amministrati dalla Svizzera dopo il 30 aprile dell'anno di attribuzione e una volta che il collegamento provvisorio dei registri diventa operativo".

Articolo 2

Il quarto comma dell'allegato II dell'accordo è sostituito dal testo seguente:

"Le NTC precisano che le comunicazioni tra l'SSTL e l'EUTL costituiscono scambi sicuri di messaggi di servizi web basati sulle tecnologie seguenti[3] o su tecnologie equivalenti:

- servizi web tramite SOAP (*Simple Object Access Protocol*) o servizi web equivalenti,
- rete privata virtuale (*Virtual Private Network*) basata su hardware,
- XML - linguaggio di marcatura estensibile (*Extensible Markup Language*),
- firma digitale e
- protocolli temporali di rete (*network time protocols*)."

Articolo 3

Sono adottate le norme tecniche di collegamento (NTC) allegate alla presente decisione.

Articolo 4

A norma dell'articolo 12, paragrafo 5, dell'accordo è istituito un gruppo di lavoro. Esso assiste il comitato misto al fine di garantire la corretta attuazione dell'accordo, compresa l'elaborazione di orientamenti tecnici per l'attuazione delle NTC.

Il gruppo di lavoro comprende almeno l'amministratore del registro della Svizzera e l'amministratore centrale del registro dell'Unione

[3] Tali tecnologie sono attualmente utilizzate per stabilire un collegamento tra il registro dell'Unione e il catalogo internazionale delle operazioni, nonché tra il registro della Svizzera e il catalogo internazionale delle operazioni.

Articolo 5

La presente decisione entra in vigore il giorno dell'adozione.

Fatto in inglese a Bruxelles, il XX 2020.

Per il comitato misto

Il segretario per l'Unione europea	*Il presidente*	*Il segretario per la Svizzera*

ALLEGATO

NORME TECNICHE DI COLLEGAMENTO (NTC)

a norma dell'articolo 3, paragrafo 7, dell'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra

Norma per la soluzione provvisoria

1. GLOSSARIO

Tabella 1-1: Acronimi e definizioni del settore

Acronimo/termine	Definizione
Quota di emissione	Il diritto di emettere una tonnellata di biossido di carbonio equivalente per un periodo determinato, valido unicamente per rispettare gli obblighi dell'ETS dell'UE o dell'ETS della Svizzera
CH	Confederazione svizzera
CHU	Quote generiche della Svizzera (per le quote CHU del secondo periodo di impegno si utilizza l'acronimo "CHU2")
CHUA	Quota svizzera assegnata al trasporto aereo
POC	Procedure operative comuni elaborate congiuntamente dalle parti dell'accordo per rendere operativo il collegamento tra l'ETS dell'UE e l'ETS della Svizzera
ETR (*Emissions Trading registry*)	Registro dello scambio di quote di emissione
ETS (*Emission Trading system*)	Sistema di scambio di quote di emissione
UE	Unione europea
EUA	Quota generale dell'UE
EUAA	Quota di emissione del trasporto aereo dell'UE
EUCR	Registro consolidato dell'Unione europea
EUTL	Catalogo delle operazioni dell'Unione europea
Registro	Un sistema contabile per le quote rilasciate nell'ambito dell'ETS, che tiene traccia della titolarità delle quote detenute in conti elettronici
SSTL	Libro di bordo elettronico supplementare della Svizzera

Operazione	Un processo in un registro che include il trasferimento di una quota da un conto a un altro conto
Sistema di catalogo delle operazioni	Il catalogo delle operazioni contiene la registrazione di tutte le operazioni proposte inviate da un registro all'altro registro.

Tabella 1-2 Definizioni e acronimi tecnici

Acronimo	Definizione
Crittografia asimmetrica	Utilizza chiavi pubbliche e private per cifrare e decifrare i dati.
Autorità di certificazione (AC)	Organismo che rilascia certificati digitali
Chiave crittografica	Un'informazione che determina il risultato funzionale di un algoritmo crittografico.
Decifratura	Processo inverso della cifratura.
Firma digitale	Tecnica matematica usata per convalidare l'autenticità e l'integrità di un messaggio, un software o un documento elettronico.
Cifratura	Il processo di conversione di informazioni o dati in un codice, in particolare per impedire l'accesso non autorizzato.
Immissione di file	Il processo di lettura di un file.
Firewall	Apparecchio o software per la sicurezza delle reti che monitora e controlla il traffico in entrata e in uscita in base a regole predeterminate.
Monitoraggio "Heartbeat" (strumento di diagnostica continua)	Segnale periodico generato e monitorato da hardware o software per indicare il funzionamento normale o per sincronizzare altre parti di un sistema informatico.
IPSec	Sicurezza IP. Suite di protocolli di reti che autentifica e cripta i pacchetti di dati per fornire una comunicazione cifrata sicura tra due computer su una rete IP.
Test di penetrazione	Pratica che consiste nel testare un sistema informatico, una rete o un'applicazione web per individuare le vulnerabilità in materia di sicurezza che l'autore di un attacco potrebbe sfruttare.
Processo di riconciliazione	Processo che mira a garantire la concordanza di due insiemi di registrazioni.

VPN	Rete privata virtuale (*Virtual Private Network*).
XML	Linguaggio di marcatura estensibile (*Extensible Mark-up Language*). Questo linguaggio permette ai progettisti di creare tag personalizzati, che consentono la definizione, la trasmissione, la convalida e l'interpretazione di dati tra applicazioni e tra organizzazioni.

2. INTRODUZIONE

L'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, del 23 novembre 2017 (l'"accordo"), prevede il riconoscimento reciproco delle quote di emissione che possono essere utilizzate per conformarsi al sistema di scambio di quote di emissione dell'Unione europea ("EU ETS") o al sistema di scambio di quote di emissione della Svizzera ("ETS della Svizzera"). Per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera, è opportuno stabilire un collegamento diretto tra il catalogo delle operazioni dell'Unione europea (EUTL) del registro dell'Unione e il libro di bordo elettronico supplementare della Svizzera (SSTL) del registro svizzero tale da consentire il trasferimento da un registro all'altro delle quote di emissioni rilasciate nell'ambito dei due ETS (articolo 3, paragrafo 2, dell'accordo). Per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera, nel maggio 2020 o il prima possibile dopo tale data sarà predisposta una soluzione provvisoria. Le parti cooperano per sostituire al più presto la soluzione provvisoria con un collegamento permanente dei registri (allegato II dell'accordo).

A norma dell'articolo 3, paragrafo 7, dell'accordo, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione stabiliscono norme tecniche di collegamento (NTC) basate sui principi di cui all'allegato II dell'accordo, descrivendo in dettaglio le disposizioni per l'istituzione di una connessione solida e sicura tra l'SSTL e l'EUTL. Le NTC elaborate dagli amministratori entrano in vigore una volta adottate con decisione del comitato misto.

Come indicato nel presente documento, le NTC sono adottate dal comitato misto con la decisione n. 2/2020. Conformemente alla presente decisione, il comitato misto chiede all'amministratore del registro della Svizzera e all'amministratore centrale dell'Unione di elaborare ulteriori orientamenti tecnici per rendere operativo il collegamento e di garantire che tali orientamenti siano costantemente adattati al progresso tecnico e alle nuove prescrizioni relative alla sicurezza interna ed esterna del collegamento e al suo funzionamento efficace ed efficiente.

2.1. Ambito di applicazione

Il presente documento rappresenta l'intesa comune tra le parti dell'accordo per quanto riguarda la definizione delle procedure di base del collegamento tra i registri dell'EU ETS e l'ETS della Svizzera. Descrive a grandi linee la base di riferimento per le specifiche tecniche in termini di requisiti di architettura, servizio e sicurezza, ma saranno necessari ulteriori orientamenti tecnici per rendere operativo il collegamento.

Per il corretto funzionamento del collegamento, occorreranno processi e procedure che ne rafforzino l'operatività. A norma dell'articolo 3, paragrafo 6, dell'accordo, tali aspetti sono trattati dettagliatamente in un documento separato relativo alle procedure operative comuni (POC), che deve essere adottato separatamente mediante decisione del comitato misto.

2.2. Destinatari

I destinatari del presente documento sono l'amministratore del registro svizzero e l'amministratore centrale del registro dell'Unione.

3. DISPOSIZIONI GENERALI

3.1. Architettura del collegamento di comunicazione

Lo scopo della presente sezione è fornire una descrizione dell'architettura generale per la messa in opera del collegamento tra l'UE ETS e l'ETS della Svizzera e le diverse componenti coinvolte.

Poiché la sicurezza è un elemento fondamentale per la definizione dell'architettura, sono state adottate tutte le misure per disporre di un'architettura solida. Il futuro collegamento permanente tra i registri si baserà su servizi web, la soluzione provvisoria utilizzerà invece un meccanismo per lo scambio di file.

La soluzione tecnica utilizza:

- un protocollo di trasferimento sicuro per lo scambio di messaggi;
- messaggi XML;
- la firma digitale e la cifratura basate su XLM;
- un dispositivo VPN o una rete di trasporto di dati sicura equivalente.

3.1.1. Scambio di messaggi

La comunicazione tra il registro dell'Unione e il registro svizzero si baserà su un meccanismo di scambio di messaggi attraverso canali protetti. Ciascun ETS disporrà del proprio archivio dei messaggi ricevuti.

Entrambe le parti conservano un registro dei messaggi ricevuti, unitamente ai dettagli relativi al trattamento.

Occorre segnalare gli errori o gli stati non previsti, come gli avvisi, e le squadre di sostegno dovrebbero attivarsi per interagire.

Gli errori e gli eventi imprevisti saranno trattati nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.1.2. Messaggio XML – Descrizione di alto livello

Un messaggio XML contiene uno degli elementi seguenti:

- una o più richieste di operazioni e/o una o più risposte a operazioni;
- un'operazione/una risposta relativa alla procedura di conciliazione;
- un messaggio di prova.

Ciascun messaggio contiene un'intestazione che riporta:

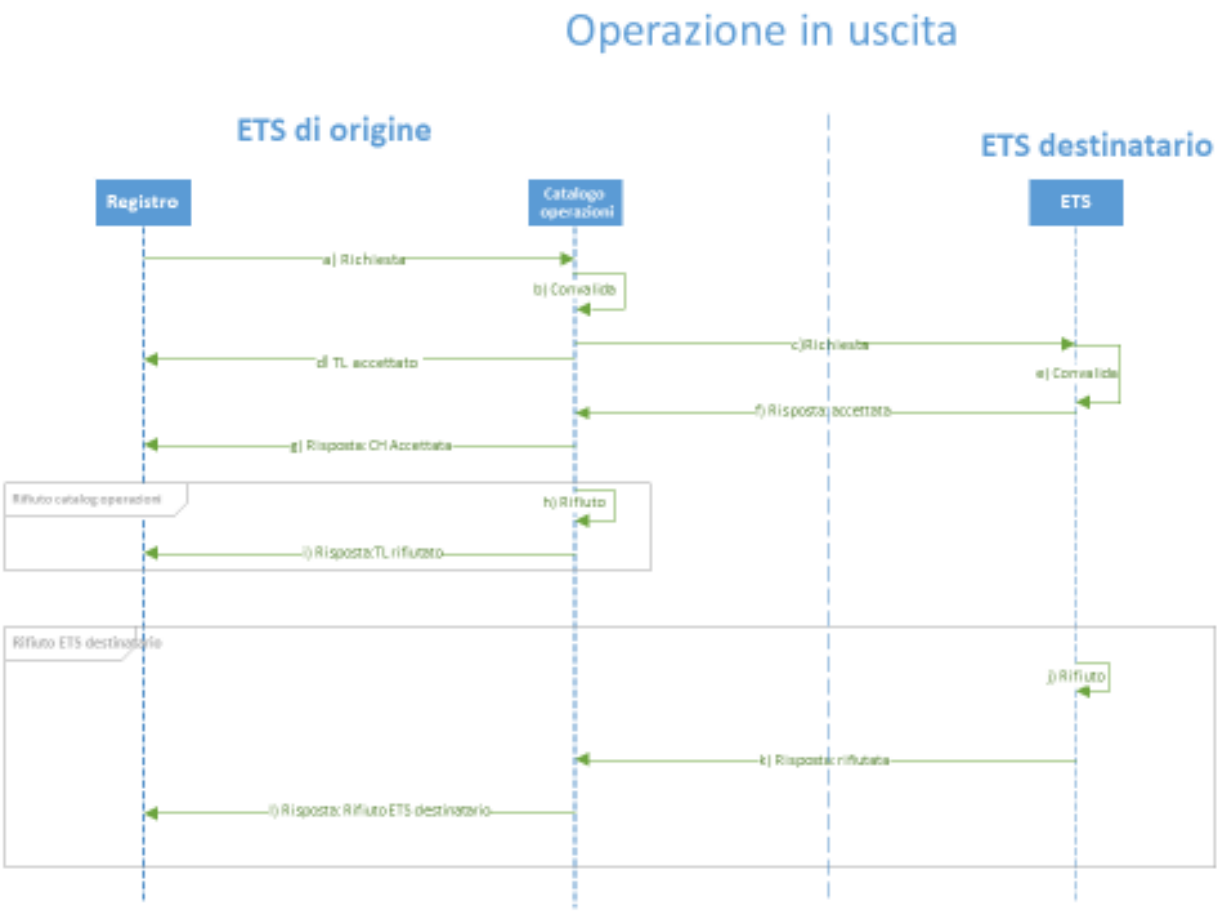
- il sistema ETS da cui proviene (ETS di origine);
- il numero di sequenza.

3.1.3. Finestre di immissione

La soluzione provvisoria si basa su finestre predefinite di immissione, seguite da una serie di eventi designati. Le richieste di operazioni ricevute attraverso il collegamento possono essere immesse solo a intervalli prestabiliti e comprendono una convalida tecnica per le operazioni in entrata e in uscita. Inoltre, le riconciliazioni possono essere effettuate su base giornaliera e possono essere avviate manualmente.

Le modifiche nella frequenza/tempistica di tutti questi eventi saranno trattate nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.1.4. Flussi di messaggi delle operazioni



Operazioni in uscita

Queste operazioni riflettono il punto di vista dell'ETS di origine. Il grafico della sequenza illustra tutti i flussi specifici di operazioni in uscita.

Flusso principale "Operazione normale" (le cui fasi sono indicate nel grafico di cui sopra):

(a) Nell'ETS di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta terminati tutti i tempi di attesa di lavoro (24 ore, se del caso).

(b) Il catalogo delle operazioni convalida la richiesta di operazione.

(c) La richiesta di operazione è inviata all'ETS destinatario.

(d) La risposta di accettazione è inviata al registro ETS di origine.

(e) L'ETS destinatario convalida la richiesta di operazione.

(f) L'ETS destinatario invia la risposta di accettazione al catalogo delle operazioni dell'ETS di origine.

(g) Il catalogo delle operazioni invia la risposta di accettazione al registro.

Flusso alternativo "Rifiuto del catalogo delle transazioni" (le cui fasi sono indicate nel grafico, partendo dalla lettera a)):

(a) Nel sistema di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta trascorsi tutti i tempi di attesa di lavoro (24 ore, se del caso).

In seguito:

(b) Il catalogo delle operazioni non convalida la richiesta

(c) Il messaggio di rifiuto è inviato al registro di origine.

Flusso alternativo "Rifiuto da parte dell'ETS" (le cui fasi sono indicate nel grafico, partendo dalla lettera a)):

(a) Nell'ETS di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta trascorsi tutti i tempi di attesa di lavoro (24 ore, se del caso).

(b) Il catalogo delle operazioni convalida l'operazione.

(c) La richiesta di operazione è inviata all'ETS destinatario.

(d) Il messaggio di accettazione è inviato al registro dell'ETS di origine.

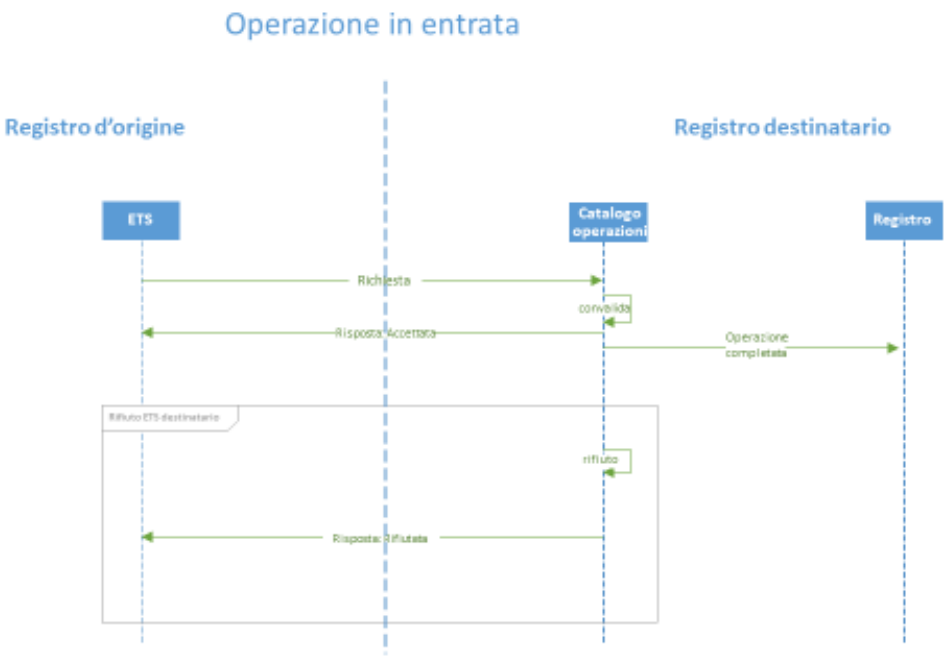
In seguito:

(e) Il catalogo delle operazioni dell'ETS destinatario non convalida l'operazione.

(f) L'ETS destinatario invia la risposta di rifiuto al catalogo delle operazioni dell'ETS di origine.

(g) Il catalogo delle operazioni trasmette il rifiuto al registro.

Operazioni in entrata



Queste operazioni riflettono il punto di vista dell'ETS destinatario. Il flusso specifico è illustrato nel seguente grafico della sequenza:

Il grafico indica:

1. Quando il catalogo delle operazioni dell'ETS destinatario convalida la richiesta, invia il messaggio di accettazione all'ETS di origine e un messaggio "operazione completata" al registro dell'ETS destinatario.
2. Quando una richiesta in entrata viene rifiutata nel catalogo delle operazioni del destinatario, la richiesta di operazione non è inviata al registro dell'ETS destinatario.

Protocollo

Il ciclo dei messaggi delle operazioni comporta solo due messaggi:

- Proposta di operazione dall'ETS di origine → all'ETS destinatario.
- Risposta dell'ETS destinatario→ all'ETS di origine circa l'operazione: accettata o rifiutata (includendo il motivo del rifiuto).
  - Accettata: l'operazione è completata.
  - Rifiutata: l'operazione è interrotta.

Status delle operazioni

- Lo status dell'operazione dell'ETS di origine sarà impostato su "proposto" ("*proposed*") al momento dell'invio della richiesta.
- Lo status dell'operazione dell'ETS destinatario sarà impostato su "proposto" ("*proposed*") al momento del ricevimento della richiesta e nel corso del suo trattamento.
- Lo status dell'operazione dell'ETS destinatario sarà impostato su "completato/interrotto" ("*completed/terminated*") al termine del trattamento della proposta. L'ETS destinatario invierà quindi il messaggio di accettazione/rifiuto corrispondente.
- Lo status dell'operazione dell'ETS di origine sarà impostato su "completato/interrotto" ("*completed/terminated*") quando il messaggio di accettazione/rifiuto viene ricevuto e nel corso del suo trattamento.
- Nell'ETS di origine lo statuto dell'operazione rimane "proposto" (*proposed*) fino a quando non arriva una risposta.
- L'ETS destinatario imposterà su "interrotta" (*terminated*) qualsiasi operazione che risulti "proposta" per oltre 30 minuti.

Gli incidenti relativi alle operazioni saranno trattati nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.2. Sicurezza del trasferimento dei dati

I dati in transito sono soggetti a quattro livelli di sicurezza:

(1) Controllo dell'accesso alla rete: firewall e strato dell'interconnessione di rete.

(2) Cifratura a livello di trasporto: una VPN o una rete di trasporto di dati sicura equivalente.

(3) Cifratura a livello di sessione: protocollo di trasferimento sicuro per lo scambio di messaggi.

(4) Cifratura a livello di applicazione: firma e cifratura XLM del contenuto.

3.2.1. Firewall e interconnessione della rete

Il collegamento è stabilito mediante una rete protetta da un firewall hardware. Il firewall è configurato secondo norme che permettono unicamente ai clienti "registrati" di effettuare collegamenti con il server VPN.

3.2.2. Rete privata virtuale (virtual private network - VPN)

Tutte le comunicazioni tra le parti sono protette mediante una tecnologia di trasporto di dati sicura Nel caso di una rete privata virtuale (VPN), l'infrastruttura dovrebbe essere basata su dispositivi hardware o virtuali. Le tecnologie VPN consentono di trasportare informazioni da un punto ad un altro attraverso un canale sicuro (tunnel) su una rete, come l'Internet, proteggendo l'insieme delle comunicazioni. Prima della creazione del tunnel VPN, un certificato digitale è rilasciato a un endpoint del potenziale cliente, consentendo a quest'ultimo di fornire la prova della sua identità durante la negoziazione della connessione. Ciascuna parte è responsabile dell'installazione del certificato nel proprio endpoint VPN. Utilizzando certificati digitali, ogni endpoint del server VPN avrà accesso ad un'autorità centrale per negoziare le credenziali di autenticazione. Durante il processo di creazione del tunnel, viene negoziata la cifratura, il che garantisce la protezione di tutte le comunicazioni che transitano nel tunnel.

Gli endpoint VPN del cliente sono configurati in modo che il tunnel resti sempre aperto al fine di consentire in qualsiasi momento una comunicazione affidabile, bidirezionale e in tempo reale tra le parti.

Qualsiasi altra soluzione equivalente deve rispettare i principi summenzionati.

3.2.3. Attuazione dell'IPSec

Quando si ricorre ad una soluzione VPN, l'utilizzo del protocollo IPSec per istituire l'infrastruttura VPN da sito a sito consentirà l'autenticazione, l'integrità dei dati e la cifratura dei dati da sito a sito. Le configurazioni VPN IPSec garantiscono un'adeguata autenticazione tra due endpoint in un collegamentoVPN. Le parti individueranno e autenticheranno il cliente remoto tramite la connessione IPSec utilizzando i certificati digitali forniti da un'autorità di certificazione riconosciuta dall'altro ETS.

L'IPsec garantisce inoltre l'integrità dei dati di tutte le comunicazioni che transitano nel tunnel VPN. I pacchetti di dati sono sottoposti alla tecnica crittografica *hash* e firmati utilizzando le informazioni di autenticazione determinate dalla VPN. Anche la riservatezza dei dati è garantita mediante la cifratura IPSec.

3.2.4. Protocollo di trasferimento sicuro per lo scambio di messaggi.

La soluzione provvisoria ricorre ad una cifratura a più livelli che consente lo scambio sicuro di dati tra le parti. I due sistemi e i loro diversi ambienti sono interconnessi a livello di rete mediante tunnel VPN o reti di trasporto di dati sicure equivalenti. A livello di applicazione i file cono trasferiti mediante un protocollo di trasferimento sicuro a livello di sessione.

3.2.5. Firma e cifratura XLM

Nei file XML, la firma e la cifratura sono effettuate su due livelli. Tutte le richieste di operazione, le risposte di operazione e i messaggi di riconciliazione sono firmati elettronicamente.

In una seconda fase, ogni sottoelemento dell'elemento "messaggio" è criptato separatamente.

Inoltre, nella terza fase, per garantire l'integrità e la non disconoscibilità dell'intero messaggio, l'elemento radice del messaggio è firmato elettronicamente. Ne consegue un elevato livello di protezione dei dati XML incorporati. L'esecuzione tecnica rispetta le norme del Consorzio mondiale del Web (W3C).

Per decifrare e verificare il messaggio, si segue lo stesso processo in ordine inverso.

3.2.6. Chiavi crittografiche

Per la cifratura e la firma si utilizzerà la crittografia a chiave pubblica.

Nel caso specifico dell'IPSec, viene utilizzato un certificato digitale rilasciato da un'autorità di certificazione (AC) ritenuta affidabile da entrambe le parti. L'AC in questione verifica l'identità e rilascia certificati che sono utilizzati per identificare formalmente un'organizzazione e istituire canali sicuri di comunicazione di dati tra le parti.

Le chiavi crittografiche sono usate per firmare e criptare canali di comunicazione e file di dati. Le parti si scambiano per via elettronica, attraverso canali protetti, i certificati pubblici che vengono verificati fuori banda. Questa procedura è parte integrante del processo di gestione della sicurezza delle informazioni delle POC.

3.3. Elenco delle funzioni nell'ambito del collegamento

Il collegamento comprende le specifiche del sistema di trasmissione per una serie di funzioni che attuano i processi "business" derivanti dall'accordo. Il collegamento include anche le specifiche per il processo di riconciliazione e i messaggi di prova che consentiranno l'attuazione di un sistema di monitoraggio *heartbeat*.

3.3.1. Operazioni "business"

Dal punto di vista "business", nell'ambito del collegamento sono previsti quattro (4) tipi di richieste di operazioni:

- Trasferimenti esterni:
  - Dopo l'entrata in funzione del collegamento dei sistemi ETS, le quote dell'UE e le quote della Svizzera sono fungibili e dunque totalmente trasferibili tra le parti.
  - Un trasferimento effettuato tramite il collegamento presuppone un conto di origine su un ETS e un conto destinatario sull'altro ETS.
  - Il trasferimento può riguardare qualsiasi quantità dei quattro (4) tipi di quote:
    - Quote generiche della Svizzera (CHU)
    - Quote assegnate al trasporto aereo della Svizzera (CHUA)
    - Quote generiche dell'UE (EUA)
    - Quote assegnate al trasporto aereo UE (EUAA)
- Assegnazione internazionale:

  Gli operatori aerei amministrati da un ETS che hanno degli obblighi nei confronti dell'altro ETS e hanno il diritto di ricevere quote a titolo gratuito da questo secondo ETS, riceveranno gratuitamente quote di trasporto aereo da quest'ultimo, mediante un'operazione di assegnazione internazionale.

- Annullamento di un'assegnazione internazionale:

  Questa operazione viene effettuata qualora occorra annullare l'insieme delle quote assegnate a titolo gratuito versate sul conto di deposito di un operatore aereo dall'altro ETS.

- Restituzione di quote in eccesso:

  Procedura analoga a quella dell'annullamento, ma in cui non occorre annullare tutte le quote assegnate poiché devono essere restituite all'ETS che le ha assegnate solo le quote in eccesso.

3.3.2. Protocollo di riconciliazione

Le riconciliazioni avvengono unicamente solo dopo la chiusura delle finestre per l'immissione, la convalida e il trattamento dei messaggi.

Le riconciliazioni sono parte integrante delle misure di sicurezza e di coerenza del collegamento. Le parti concorderanno l'esatta tempistica delle riconciliazioni prima di stabilire un calendario. Con l'accordo di entrambe le parti si possono effettuare riconciliazioni giornaliere programmate. Tuttavia, dopo ciascuna immissione sarà effettuata almeno una riconciliazione programmata.

Ciascuna parte può comunque procedere in qualsiasi momento a riconciliazioni manuali.

Le modifiche della tempistica e della frequenza delle riconciliazioni programmate saranno trattate nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.3.3. Messaggio di prova

Per verificare la comunicazione *end-to-end* è previsto un messaggio di prova. Il messaggio conterrà dati che lo identificheranno come messaggio di prova e una volta pervenuto all'altro ETS questi invierà una risposta

3.4. Norme per i servizi web

Nella soluzione provvisoria non saranno utilizzati servizi web. È opportuno notare, tuttavia, che la forma e il formato dei messaggi XML rimarranno in gran parte immutati. Con l'introduzione del collegamento permanente dei registri in futuro, i servizi web dovrebbero consentire lo scambio di messaggi XML in tempo reale.

3.5. Definizione specifica dei servizi web

Questa sezione non riguarda la soluzione provvisoria. Come indicato nella sezione precedente, i servizi web saranno utilizzati solo nel futuro collegamento permanente dei registri.

3.6. Requisiti relativi alla registrazione dei dati

Per rispondere all'esigenza di entrambe le parti di garantire l'accuratezza e la coerenza delle informazioni e per fornire loro strumenti da utilizzare nel processo di riconciliazione per eliminare le incoerenze, entrambe le parti conservano quattro (4) tipi di registrazioni di dati:

- cataloghi delle operazioni;
- cataloghi delle riconciliazioni;
- archivio dei messaggi;

- cataloghi degli audit interni.

Tutti i dati di questi cataloghi dovranno essere conservati almeno per tre (3) mesi ai fini della risoluzione di problemi; la loro ulteriore conservazione ai fini di audit dipenderà invece dalla legge applicabile a ciascun ETS. I file dei cataloghi che risalgono a più di tre (3) mesi possono essere archiviati in un sistema informatico indipendente sicuro, a condizione che possano essere recuperati o vi si possa accedere entro un termine ragionevole.

Cataloghi delle operazioni

I cataloghi delle operazioni sono attuati nei sottosistemi EUTL e SSTL.

Più specificamente, i cataloghi delle operazioni registrano ogni operazione proposta inviata all'altro ETS. Ciascuna registrazione contiene tutti i campi relativi al contenuto dell'operazione e al suo risultato (la risposta dell'ETS destinatario). I cataloghi delle operazioni registrano le operazioni in entrata e le risposte inviate all'ETS di origine.

Cataloghi delle riconciliazioni

Il catalogo delle riconciliazioni contiene la registrazione di tutti i messaggi di riconciliazione scambiati tra le due parti, ivi compresi l'identificatore, la marcatura temporale e il risultato della riconciliazione: Status della riconciliazione "Superata" (*Pass*) o "Discrepanze" (*Discrepancies*). Nella soluzione provvisoria i messaggi di riconciliazione fanno parte integrante dei messaggi scambiati.

Entrambe le parti registrano le singole richieste e le relative risposte nel catalogo delle riconciliazioni. Anche se le informazioni contenute in questo catalogo non sono condivise direttamente nell'ambito della procedura di conciliazione vera e propria, l'accesso a tali informazioni potrebbe essere necessario per eliminare le incoerenze.

Archivio dei messaggi

Entrambe le parti sono tenute ad archiviare una copia dei dati scambiati (file XLM), inviati e ricevuti, indicando se il formato di questi messaggi XLM è corretto.

Questo archivio è utilizzato principalmente a fini di audit, per disporre di una prova di quello che è stato inviato e ricevuto da entrambe le parti. In quest'ottica, insieme ai file, occorre archiviare anche i relativi certificati.

Questi file forniscono inoltre informazioni aggiuntive ai fini della soluzione di eventuali problemi.

Catalogo degli audit interni

Questi cataloghi sono predisposti e utilizzati da ciascuna parte separatamente.

3.7. Requisiti operativi

Nella soluzione provvisoria lo scambio di dati tra i due sistemi non è totalmente autonomo: sono infatti necessari operatori e procedure per rendere operativo il collegamento.

4. DISPOSIZIONI RELATIVE ALLA DISPONIBILITÀ

4.1. Progettazione della disponibilità delle comunicazioni

Fondamentalmente l'architettura della soluzione provvisoria consiste in un'infrastruttura TIC e un software che consentono la comunicazione tra l'ETS della Svizzera e l'EU ETS. Garantire livelli elevati di disponibilità, integrità e riservatezza per questo flusso di dati diventa un aspetto essenziale di cui tenere conto nella progettazione della soluzione provvisoria e del

collegamento permanente dei registri. Trattandosi di un progetto nel quale l'infrastruttura TIC, il software personalizzato e i processi svolgono un ruolo fondamentale, per progettare un sistema resiliente occorre tenere conto di questi tre elementi.

Resilienza dell'infrastruttura TIC

Il capitolo sulle disposizioni generali del presente documento descrive in dettaglio gli elementi costitutivi dell'architettura. Per quanto riguarda l'infrastruttura TIC, nell'ambito del collegamento provvisorio, è stata istituita una rete VPN resiliente (o una rete equivalente) che crea dei tunnel di comunicazione sicuri mediante i quali i messaggi possono essere scambiati in modo sicuro. Altri elementi dell'infrastruttura sono configurati in alta disponibilità e/o sono dotati di meccanismi di riserva.

Resilienza dei software personalizzati

I moduli software personalizzati consentono di potenziare la resilienza in quanto, per un determinato periodo di tempo, tentano di ristabilire la comunicazione con l'altro ETS quando, per un motivo qualsiasi, questo servizio non è disponibile.

Resilienza dei servizi

Nella soluzione provvisoria, gli scambi di dati tra le parti avvengono a intervalli predefiniti nel corso dell'anno. Alcune delle fasi necessarie per gli scambi di dati preprogrammati richiedono l'intervento manuale dei gestori dei sistemi e/o degli amministratori dei registri. Tenendo conto di questo aspetto e per aumentare la disponibilità e l'adeguato svolgimento degli scambi:

- le procedure operative prevedono finestre temporali significative per l'esecuzione di ogni tappa.
- I moduli software per la soluzione provvisoria attuano una comunicazione asincrona.
- Il processo automatico di riconciliazione individuerà eventuali problemi nell'immissione dei file di dati nei due ETS.
- I processi di monitoraggio (infrastruttura TIC e moduli software personalizzati) sono considerati nelle procedure di gestione degli incidenti e attivano queste procedure (definite nel documento relativo alle procedure operative comuni). Le procedure volte a ridurre il tempo necessario per ripristinare il normale funzionamento a seguito di incidenti sono fondamentali per garantire tassi di disponibilità elevati.

4.2. Piano di attivazione, comunicazione, riattivazione e prove

Tutti i diversi elementi dell'architettura della soluzione provvisoria devono superare una serie di prove individuali e collettive destinate a verificare che la piattaforma è pronta a livello dell'infrastruttura TIC e del sistema di informazione. Questi test operativi costituiscono una condizione preliminare obbligatoria ogni volta che la soluzione provvisoria passa dallo status "sospeso" (*suspended*) allo status "operativo" (*operational*).

L'attivazione dello status operativo del collegamento presuppone l'adeguata esecuzione di un piano di prove predefinito. Ciò consente di verificare che per ciascun registro è stata effettuata dapprima una serie di prove interne, seguita dalla convalida della connettività *end-to-end*, prima di iniziare a trasmettere operazioni vere e proprie tra le due parti.

Il piano delle prove dovrebbe menzionare la strategia di prove generale e informazioni dettagliate sull'infrastruttura per le prove. In particolare, per ciascun elemento di ogni blocco di prova occorre disporre degli elementi seguenti:

- i criteri e gli strumenti di prova;
- i ruoli assegnati in vista dell'esecuzione delle prove;
- i risultati attesi (positivi e negativi);
- il calendario delle prove;
- la registrazione dei requisiti relativi ai risultati delle prove;
- la documentazione relativa alla risoluzione dei problemi;
- le disposizioni relative ai livelli successivi di intervento.

Il processo delle prove di attivazione dello status operativo potrebbe essere suddiviso in quattro (4) blocchi o fasi concettuali:

4.2.1. Prove dell'infrastruttura TIC in interno

Queste prove devono essere eseguite e/o verificate individualmente da entrambe le parti nel proprio ETS.

Ogni elemento delle infrastrutture TIC degli ETS deve essere testato individualmente. Ciò vale anche per ogni singola componente dell'infrastruttura. Queste prove possono essere eseguite automaticamente o manualmente ma devono consentire di verificare che ogni elemento dell'infrastruttura è operativo.

4.2.2. Prove di comunicazione

Queste prove devono essere avviate da ciascuna parte individualmente e devono concludersi in cooperazione con l'altra parte.

Una volta resi operativi i singoli elementi, i canali di comunicazione tra i due registri devono essere testati. A tal fine, ciascuna parte verifica che l'accesso a Internet funzioni, che siano predisposti i tunnel VPN (o altre reti di trasporto sicure equivalenti) e che sia stabilita la connettività IP da sito a sito. L'accessibilità degli elementi di infrastruttura locali e remoti e la connettività IP dovrebbero quindi essere confermati all'altro ETS.

4.2.3. Prove sull'intero sistema (end-to-end)

Queste prove devono essere effettuate da ogni ETS e i risultati devono essere comunicati all'altra parte.

Una volta testati i canali di comunicazione e ciascuna singola componente di entrambi i registri, ciascun ETS deve predisporre una serie di operazioni simulate e di riconciliazioni che siano rappresentative di tutte le funzioni da attuare nell'ambito del collegamento.

4.2.4. Prove di sicurezza

Queste prove devono essere effettuate e/o attivate da entrambe le parti nel proprio ETS seguendo le indicazioni di cui alle sezioni "Linee guida in materia di prove di sicurezza" e "Disposizioni in materia di valutazione dei rischi".

Solo dopo la fine delle quattro fasi/blocchi con esiti prevedibili, si può ritenere che il collegamento provvisorio sia operativo.

Risorse destinate alle prove

Ciascuna parte si avvale di risorse specifiche destinate alle prove (software e hardware specifici delle infrastrutture TIC) e mette a punto funzioni di prova nel proprio sistema al fine di agevolare la convalida manuale e continua della piattaforma. Le procedure di prova manuali, effettuate separatamente o in cooperazione, possono essere eseguite in qualsiasi momento dagli amministratori dei registri. L'attivazione dello status operativo è un processo manuale in sé.

È previsto inoltre che la piattaforma effettui controlli automatici a intervalli regolari che mirano ad incrementare la disponibilità della piattaforma individuando rapidamente eventuali problemi a livello di infrastruttura o di software. Il piano di monitoraggio della piattaforma è costituito da due elementi:

- monitoraggio delle infrastrutture TIC: in entrambi gli ETS l'infrastruttura sarà monitorata dai fornitori di servizi di infrastruttura TIC. Le prove automatiche riguarderanno i diversi elementi dell'infrastruttura e la disponibilità dei canali di comunicazione.
- Monitoraggio delle applicazioni: i moduli software del collegamento provvisorio effettueranno il monitoraggio del sistema di comunicazione a livello di applicazione (manualmente e/o a intervalli regolari) che consentirà di verificare la disponibilità *end-to-end* del collegamento simulando alcune operazioni.

4.3. Ambienti di accettazione/prova

L'architettura del registro dell'Unione e del registro della Svizzera prevede i tre ambienti seguenti:

- produzione (PROD): questo ambiente contiene dati reali e tratta operazioni effettive.
- Accettazione (ACC): questo ambiente contiene dati rappresentativi, fittizi o anonimizzati. Si tratta dell'ambiente in cui i gestori dei sistemi di entrambe le parti convalidano i nuovi rilasci di versioni.
- Prova (TEST): questo ambiente contiene dati rappresentativi, fittizi o anonimizzati. L'accesso è limitato agli amministratori dei registri e l'ambiente è destinato ad essere utilizzato da entrambe le parti per effettuare prove di integrazione.

Ad eccezione della VPN (o di una rete equivalente), i tre ambienti sono totalmente indipendenti l'uno dall'altro: l'hardware, il software, le basi di dati, gli ambienti virtuali, gli indirizzi IP e le porte sono configurati e funzionano in modo indipendente gli uni dagli altri.

La VPN è caratterizzata da due configurazioni per due ambienti diversi, una per l'ambiente PROD, e un'altra indipendente per gli ambienti ACC e TEST.

5. DISPOSIZIONI IN MATERIA DI RISERVATEZZA E INTEGRITÀ

I meccanismi e le procedure di sicurezza si basano sul "principio dei quattro occhi" per le operazioni effettuate nell'ambito del collegamento tra il registro dell'Unione e il registro svizzero. Questo principio si applica ogniqualvolta sia necessario, ma non per forza a tutte le azioni intraprese dagli amministratori dei registri.

I requisiti di sicurezza sono esaminati e trattati nel piano di gestione della sicurezza, che comprende anche i processi relativi alla gestione degli incidenti di sicurezza a seguito di un'eventuale violazione della sicurezza. La parte operativa di questi processi è descritta nelle POC.

5.1. Infrastruttura per le prove di sicurezza

Ciascuna parte si impegna a predisporre un'infrastruttura destinata alle prove di sicurezza (avvalendosi dell'insieme comune di software e hardware utilizzati per individuare le vulnerabilità nella fase di sviluppo e funzionamento):

- separata dall'ambiente di produzione;
- in cui la sicurezza è analizzata da un'équipe indipendente dallo sviluppo e dal funzionamento del sistema.

Le parti si impegnano ad effettuare analisi sia statiche che dinamiche.

Nel caso di analisi dinamiche (come i test di penetrazione), entrambe le parti si impegnano di norma a limitare le valutazioni agli ambienti di prova e di accettazione (definiti nella sezione "Ambienti di accettazione/prova"). Le eventuali deroghe sono soggette all'approvazione di entrambe le parti.

Prima di essere utilizzato nell'ambiente di produzione, ogni modulo di software del collegamento (definito nella sezione "Architettura del collegamento di comunicazione") è sottoposto a prove di sicurezza.

L'infrastruttura per le prove deve essere separata sia a livello di rete che di infrastruttura dal livello di produzione e deve consentire di effettuare le prove di sicurezza necessarie per verificare la conformità ai requisiti di sicurezza.

5.2. Disposizioni relative alla sospensione e alla riattivazione del collegamento

Se si sospetta che la sicurezza del registro svizzero, dell'SSTL, del registro dell'Unione o dell'EUTL sia stata compromessa, entrambe le parti si informano reciprocamente e immediatamente e sospendono il collegamento tra l'SSTL e l'EUTL.

Le procedure per la condivisione delle informazioni, la decisione di sospendere e la decisione di riattivare fanno parte del processo per il soddisfacimento delle richieste delle POC.

Sospensioni

La sospensione del collegamento dei registri conformemente all'allegato II dell'accordo può avvenire per:

- ragioni amministrative (manutenzione, ...) programmate;
- ragioni di sicurezza (o guasti dell'infrastruttura IT) non previste.

In caso di emergenza, ciascuna parte informa l'altra parte e sospende unilateralmente il collegamento dei registri.

Se si decide di sospendere il collegamento dei registri, ciascuna parte provvederà a interrompere il collegamento a livello di rete (bloccando in parte o in toto le connessioni in entrata e in uscita).

La decisione di sospendere il collegamento dei registri, sia essa programmata o no, sarà adottata conformemente alla procedura per la gestione delle modifiche o alla procedura per

la gestione degli incidenti di sicurezza delle POC.

Riattivazione della comunicazione

La decisione di riattivazione sarà presa come specificato nelle POC e, in ogni caso, non prima di aver portato a termine con successo le procedure riguardanti prove di sicurezza, come specificato nelle sezioni "Linee guida in materia di prove di sicurezza" e "Piano di attivazione, comunicazione, riattivazione e prove".

5.3. Disposizioni in materia di violazioni della sicurezza

Una violazione della sicurezza è considerata un incidente di sicurezza che incide sulla riservatezza e l'integrità delle informazioni riservate e/o sulla disponibilità del sistema di trattamento di tali informazioni.

Le informazioni riservate sono identificate nell'elenco delle informazioni riservate e possono essere trattate nel sistema o in qualsiasi parte ad esso correlata.

Le informazioni direttamente connesse alla violazione della sicurezza saranno considerate riservate, contrassegnate come "informazioni ETS riservatissime" (*ETS Critical*) e trattate secondo le istruzioni di trattamento, salvo diversamente specificato.

Tutte le violazioni della sicurezza saranno gestite nel rispetto delle procedure di cui al capitolo "Gestione degli incidenti di sicurezza" delle POC.

5.4. Linee guida in materia di prove di sicurezza

5.4.1. Software

Le prove di sicurezza, compresi gli eventuali test di penetrazione, devono essere eseguite quanto meno per tutti i nuovi principali rilasci di versioni del software, conformemente alle disposizioni in materia di sicurezza definiti nelle NTC, al fine di valutare la sicurezza del collegamento e i relativi rischi.

Se negli ultimi 12 mesi non è stato effettuato nessun rilascio importante di nuove versioni, è necessario effettuare prove di sicurezza sul sistema attuale, tenuto conto dell'evoluzione delle minacce informatiche verificatesi negli ultimi 12 mesi.

Le prove di sicurezza del collegamento del registro saranno effettuate nell'ambiente di accettazione e, se necessario, nell'ambiente di produzione, in coordinamento e con l'accordo di entrambe le parti.

Le prove sulle applicazioni web saranno eseguite conformemente agli standard aperti internazionali come quelli messi a punto dall'OWASP (*Open Web Application Security Project*).

5.4.2. Infrastruttura

Le infrastrutture alla base del sistema di produzione devono essere controllate periodicamente (almeno una volta al mese) al fine di individuare eventuali vulnerabilità cui occorrerà porre rimedio secondo il principio definito nella sezione precedente, utilizzando una base di dati aggiornata relativa alle vulnerabilità.

5.5. Disposizioni in materia di valutazione dei rischi

Se occorre effettuare test di penetrazione, questi devono essere inclusi nelle prove di sicurezza.

Ogni parte può affidare a una società specializzata l'esecuzione di prove di sicurezza, a condizione che questa:

- vanti competenze e esperienza nel settore;
- non faccia riferimento direttamente allo sviluppatore e/o al suo contraente, e non sia coinvolta nello sviluppo del software del collegamento né sia una subappaltatrice dello sviluppatore;
- abbia firmato un accordo di non divulgazione con cui si impegna a garantire la riservatezza dei risultati e a trattarli al livello di "informazioni ETS riservatissime" (*ETS Critical*) conformemente alle istruzioni di trattamento.