Council of the
European Union

Brussels, 22 March 2024
(OR. en)

Interinstitutional File:
2024/0067 (NLE)

8159/24
ADD 1

ENV 363
CLIMA 139
ENER 155
IND 187
COMPET 368
MI 359
ECOFIN 359
TRANS 176
AELE 24
CH 7

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	20 March 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2024) 125 final
Subject:	ANNEX to the Proposal for a Council Decision on the position to be taken on behalf of the European Union in the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems as regards amending Annex II to the Agreement, the Common Operational Procedures and the Linking Technical Standards

Delegations will find attached document COM(2024) 125 final.

Encl.: COM(2024) 125 final

EUROPEAN
COMMISSION

Brussels, 20.3.2024
COM(2024) 125 final

ANNEX

ANNEX

to the

Proposal for a Council Decision

on the position to be taken on behalf of the European Union in the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems as regards amending Annex II to the Agreement, the Common Operational Procedures and the Linking Technical Standards

DECISION No 1/2024 OF THE JOINT COMMITTEE ESTABLISHED BY THE AGREEMENT BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION ON THE LINKING OF THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS of … as regards amending Annex II to the Agreement, the Common Operational Procedures and the Linking Technical Standards

THE JOINT COMMITTEE,

Having regard to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems[1] (hereinafter 'the Agreement') and in particular Article 9 and Article 13(2) thereof,

Whereas:

(1) Joint Committee Decision No 2/2019[2] provided for a provisional solution to operationalise the link between the EU ETS and the ETS of Switzerland.

(2) In its third meeting, the Joint Committee agreed on the need to analyse the cost-effectiveness of a permanent link between the Union Registry and the registry of Switzerland.

(3) In its 5th meeting, the Joint Committee agreed on the report submitted by the Working Group set up by Joint Committee Decision 1/2020[3] and 2/2020[4] and in which this Working Group analysed and recommended an approach to implement the permanent link between the Union Registry and the registry of Switzerland.

(4) To reflect the technical requirements of the permanent link between the Union Registry and the registry of Switzerland as well as to streamline the provisions of Annex II to the Agreement in the light of technological developments, Annex II to the Agreement should be amended.

(5) To ensure consistency of the Common Operational Procedures and the Linking Technical Standards with Annx II to the Agreement, those documents should also be amended.

HAS ADOPTED THIS DECISION:

Article 1

1. Annex II to the Agreement is replaced by the text in Annex I to this Decision.

2. The Common Operational Procedures referred to in Article 3(6) of the Agreement are set out in Annex II to this Decision.

3. The Linking Technical Standards referred to in Article 3(7) of the Agreement are set out in Annex III to this Decision.

Article 2

This Decision shall enter into force on the day of its adoption.

[1] OJ L 322, 7.12.2017, p. 3.

[2] OJ L 314, 29.9.2020, p. 68

[3] OJ L 226, 25.6.2021, p. 2

[4] OJ L 226, 25.6.2021, p. 16

Done in English at [Brussels][Bern], on [xx 2024].

For the Joint Committee

Secretary for the European Union	*The Chair*	*Secretary for Switzerland*

ANNEX I

‘ANNEX II

LINKING TECHNICAL STANDARDS

To operationalize the link between the EU ETS and the ETS of Switzerland, a provisional solution was implemented in 2020. As from 2023, the registry link between the two emissions trading systems will gradually develop into a permanent registry link expected to be implemented not later than 2024 that enables the functioning of the linked markets with respect to benefits from market liquidity and execution of transactions between the two linked systems in a manner that is equivalent to one market made up of two systems and which allows market participants to act as if they were in one market, subject only to individual regulatory provisions of the Parties. The Linking Technical Standards (LTS) shall specify:

– the architecture of the communication link

– the communications between the SSTL and the EUTL

– the security of data transfer

– the list of functions (transactions, reconciliation …)

– the definition of the transport layer

– the data logging requirements

– the operational arrangements (call desk, support)

– the communication activation plan and the testing procedure

– the security testing procedure.

The LTS shall specify that the administrators are to take all reasonable steps to ensure that the SSTL, the EUTL and the link are operational 24 hours a day and 7 days a week, and that any interruptions to the operation of the SSTL, the EUTL and the link are to be kept to the minimum.

The LTS shall set out additional security requirements for the Swiss registry, the SSTL, the Union registry and the EUTL and shall be documented in a ‘security management plan’. In particular, the LTS shall specify that:

– if there is a suspicion that the security of the Swiss registry, the SSTL, the Union registry or the EUTL has been compromised, both Parties shall immediately inform each other and suspend the link between the SSTL and the EUTL

– in the event of a security breach, the Parties shall commit to immediately share the information with each other. To the extent that the technical details are available, a report describing the incident (date, cause, impact, remedies) shall be shared between the Swiss registry administrator and the Union central administrator within 24 hours after a security incident is identified as a security breach.

The security testing procedure set out in the LTS shall be completed before the communication link between the SSTL and the EUTL is established, and whenever a new version or release of the SSTL or the EUTL is required.

The LTS shall provide two testing environments in addition to the production environment: a developer testing environment and an acceptance environment.

The Parties shall provide evidence through the Swiss registry administrator and the Union central administrator that an independent security assessment of their systems has been performed in the previous twelve months in accordance with the security requirements set out in the LTS. Security testing and in particular penetration testing shall be performed on all new major releases of the software in accordance with the security requirements set out in the LTS. The penetration testing shall not be performed by the software developer or by a subcontractor of the software developer.'

ANNEX II

COMMON OPERATIONAL PROCEDURES (COP)

pursuant to Article 3(6) of the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems

Procedures for permanent registry link

Table of Contents

1. GLOSSARY

Table 1-1 Acronyms and Definitions

Acronym/Term	Definition
Certificate Authority (CA)	Entity that issues digital certificates

CH	Swiss Confederation
ETS	Emissions Trading System
EU	European Union
IMT	Incident Management Team
Information Asset	A piece of information that is valuable to a company or organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LTS	Linking Technical Standards
Registry	An accounting system for allowances issued under the ETS, which keeps track of the ownership of allowances held in electronic accounts.
RFC	Request For Change
SIL	Sensitive Information List
SR	Service Request
Wiki	Website that allows users to exchange information and knowledge by adding or adapting content directly via a web browser.

2. INTRODUCTION

The Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 23 November 2017('Agreement') provides for the mutual recognition of emission allowances that can be used for compliance under the Emissions Trading System of the European Union ('EU ETS') or the Emissions Trading System of Switzerland ('ETS of Switzerland'). To operationalise the link between the EU ETS and the ETS of Switzerland, a direct link between the European Union Transaction Log (EUTL) of the Union Registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry will be established, which will enable the registry-to-registry transfer of emission allowances issued under either ETS (Article 3(2) of the Agreement). To operationalize the link between the EU ETS and the ETS of Switzerland, a provisional solution was implemented in 2020. As from 2023, the registry link between the two emissions trading systems will gradually develop into a permanent registry link expected to be implemented not later than 2024 that enables the functioning of the linked markets with respect to benefits from market liquidity and execution of transactions between the two linked systems in a manner that is equivalent to one market made up of two systems and which allows market participants to act as if they were in one market, subject only to individual regulatory provisions of the Parties. (Annex II to the Agreement).

Pursuant to Article 3(6) of the Agreement, the Swiss registry administrator and the Union central administrator shall determine common operational procedures (COP) related to technical or other matters necessary for the operation of the linking and taking into account the priorities of domestic legislation. The COP developed by the administrators shall take effect when adopted by decision of the Joint Committee.

The COP was adopted by the Joint Committee by its Decision No. 1/2020. The updated COP, as recorded in this document, will be adopted by the Joint Committee by its Decision No. 1/2024. In accordance with this Decision and requests from the Joint Committee, the Swiss registry administrator and the Union central administrator have developed and will update further technical guidelines to operationalise the link and to ensure that these are continuously adapted to technical progress and new requirements relating to the safety and security of the link and to its effective and efficient operation.

2.1. Scope

This document represents the common understanding between the Parties to the Agreement regarding the establishment of the procedural foundations of the link between the registries of the EU ETS and the ETS of Switzerland. While it outlines the overall procedural requirements in terms of operations, some further technical guidelines will be needed to operationalise the link.

For its proper functioning, the link will require technical specifications in order to further operationalise it. Pursuant to Article 3(7) of the Agreement, those matters are detailed in the Linking Technical Standards (LTS) document to be adopted separately by decision of the Joint Committee.

The objective of the COP is to make sure that IT services related to the operation of the link between the registries of the EU ETS and the ETS of Switzerland are delivered effectively and efficiently, especially for the fulfilling of service requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks according to international standards for IT service management.

For the permanent registry link, only the following COP will be needed, which are part of this document:

- Incident Management;
- Problem Management;
- Request Fulfilment;
- Change Management;
- Release Management;
- Security Incident Management;
- Information Security Management.

2.2. Addressees

The target audience of these COP are the EU and Swiss registry support teams.

3. Approach and Standards

The following principle applies to all COP:

- The EU and CH agree to define the COP on the basis of ITIL (Information Technology Infrastructure Library, version 4). Practices from this standard are reused and adapted to the specific needs related to the permanent registry link;
- The communication and coordination necessary for the processing of the COP between the two Parties takes place via the Registry Service Desks of the CH and EU. Tasks are always assigned within one Party;
- If there is disagreement about the handling of a COP, this will be analysed and resolved between both Service Desks. If no agreement can be reached, the finding of a joint solution is escalated to the next level.

Escalation levels	EU	CH
1st level	EU Service Desk	CH Service Desk
2nd level	EU Operations Manager	CH Registry Application Manager
3rd level	Joint Committee (which might delegate this responsibility considering Article 12(5) of the Linking Agreement)	
4th level	Joint Committee, if 3rd level is delegated	

- Each Party can determine the procedures for the operation of its own registry system, taking into account the requirements and interfaces related to these COP;
- An IT Service Management (ITSM) tool is used to support the COP, in particular Incident Management, Problem Management and Request Fulfilment, and communication between both Parties;
- In addition, the exchange of information via e-mail is allowed;
- Both Parties ensure that the information security requirements are met in accordance with the Handling Instructions.

4. INCIDENT MANAGEMENT

The objective of the Incident Management process is to return IT services to a normal service level as quickly as possible following an incident and with minimum disruption to the business.

Incident Management should also keep a record of incidents for reporting purposes and integrate with other processes to drive continuous improvement.

From a global perspective, Incident Management comprises the following activities:

- Incident detection and recording;
- Classification and initial support;
- Investigation and diagnosis;
- Resolution and recovery;
- Incident closure.

Throughout the lifecycle of an incident, the Incident Management process is responsible for the constant handling of the ownership, monitoring, tracking and communication.

4.1. Incident detection and recording

An incident can be detected by a support group, by automated monitoring tools or by technical staff performing routine surveillance.

Once detected, an incident must be recorded and assigned a unique identifier allowing for proper incident tracking and monitoring. The unique identifier of an incident is the identifier assigned in the common ticketing system by the Service Desk of the Party (either EU or CH) that raised the incident, and it has to be used in every communication related to this incident.

For all incidents, the contact point should be the Service Desk of the Party that logged the ticket.

4.2. Classification and initial support

The incident classification aims at understanding and identifying what system and/or service are affected by an incident, and to what degree. To be effective, the classification should route the incident to the correct resource on the first try, in order to speed up the incident resolution.

The classification phase should categorize and prioritize the incident according to its impact and urgency, for it to be treated according to the priority relevant time frame.

If the incident has a potential impact on the confidentiality or integrity of sensitive data, and/or an impact on the system availability, the incident shall be also declared as a security incident and then managed according to the process defined in the 'Security Incident Management' chapter of this document.

If possible, the Service Desk that logged the ticket performs an initial diagnosis. For this, the Service Desk will see if the incident is a known error. If so, then the resolution path or workaround is already known and documented.

If the Service Desk is successful in solving the incident, then it will actually close the incident at this point, as the primary purpose of Incident Management has been fulfilled (namely the fast restoration of service for the end user). If not, then the Service Desk will escalate the incident to the appropriate resolver group for further investigation and diagnosis.

4.3. Investigation and diagnosis

Incident investigation and diagnosis is applied when an incident cannot be resolved by the Service Desk as part of the initial diagnosis, and is therefore escalated appropriately. Incident escalation is a full part of the investigation and diagnosis process.

A common practice in the investigation and diagnosis phase is the attempt to recreate the incident under controlled conditions. It is important when performing incident investigation and diagnosis that the proper order of events that led up to the incident be understood.

Escalation is the recognition that an incident cannot be resolved at the current support level, and must be passed to a higher level support group or to the other Party. Escalation can follow two paths: horizontal (functional) or vertical (hierarchical).

The Service Desk that recorded and triggered the incident is responsible for escalating the incident to the appropriate resource and for tracking the overall status and assignment of the incident.

The Party to which the incident has been assigned is responsible for ensuring the requested actions are performed in a timely fashion, and for providing feedback to the Service Desk of its own Party.

4.4. Resolution and recovery

Incident resolution and recovery is performed once the incident is fully understood. Finding a resolution to an incident means that a way of rectifying the issue has been identified. The act of applying the resolution is the recovery phase.

Once the appropriate resources resolve the service failure, the incident is routed back to the relevant Service Desk that logged the incident and that Service Desk confirms with the initiator of the incident that the error has been rectified and that the incident can be closed. Findings from the processing of the incident are to be recorded for future use.

Recovery can be performed by IT support staff or by providing the end user with a set of instructions to follow.

4.5. Incident closure

Closure is the final step in the Incident Management process and takes place shortly after incident resolution.

Within the checklist of activities that need to be performed during the closure phase, the following are highlighted:

- The verification of the initial categorization that was assigned to the incident;
- The proper capture of all information surrounding the incident;
- The proper documentation of the incident and update of the knowledge base;
- The adequate communication to every stakeholder directly or indirectly affected by the incident.

An incident is formally closed once the incident closure phase has been executed by the Service Desk and communicated to the other Party.

Once an incident is closed, it is not reopened. If an incident re-occurs within a short time period then, the original incident is not re-opened, a new incident must be logged instead.

If the incident is tracked by both the EU and CH Service Desks, the final closure is the responsibility of the Service Desk that logged the ticket.

5. PROBLEM MANAGEMENT

This procedure should be followed whenever a problem is identified and therefore triggers the Problem Management process. Problem Management focuses on enhancing quality and reducing the volume of raised incidents. A problem can be the cause of one or more incidents. When an incident is reported, the objective of Incident Management is to restore the service as quickly as possible, possibly involving workarounds. When a problem is created, the objective is to investigate the root cause of the issue in order to identify a change that will ensure the problem and related incidents will not occur anymore.

5.1. Problem identification an recording

Depending on which Party initiated the ticket, either the EU or CH Service Desk will be the contact point for problem related matters.

The unique identifier of a problem is the identifier assigned by the IT Service Management (ITSM). It has to be used in every communication related to this problem.

A problem can be triggered by an incident or can be opened as a self-initiative act to fix issues discovered in the system at any point in time.

5.2. Problem Prioritization

Problems may be categorized according to their severity and priority in the same way as incidents in order to facilitate their tracking, taking the impact of the associated incidents and their frequency of occurrence into account.

5.3. Problem investigation and diagnosis

Each Party can raise a problem and the Service Desk of the initiating Party will be responsible for logging the problem, assigning it to the appropriate resource and tracking the overall status of the problem.

The resolver group to whom the problem was escalated is responsible for handling the problem in a timely fashion and communicating with the Service Desk.

Upon request, both Parties are responsible for ensuring the assigned actions are performed, and for providing feedback to the Service Desk of its own Party.

5.4. Resolution

The resolver group to whom the problem is assigned is responsible for resolving the problem and providing relevant information to the Service Desk of its own Party.

Findings from the processing of the problem are to be recorded for future use.

5.5. Problem closure

A problem is formally closed once the problem is fixed by implementing the change. The problem closure phase will be carried out by the Service Desk that logged the problem and informed the Service Desk of the other Party.

6. REQUEST FULFILMENT

The Request Fulfilment Process is the end-to-end management of a request for a new or existing service from the moment it is registered and approved through to closure. Service Requests are usually small, predefined, repeatable, frequent, pre-approved, and procedural requests.

The main steps that have to be followed are outlined below:

6.1. Initiate Request

The information related to a Service Request is submitted to the EU or CH Service Desk by email, phone, or through the IT Service Management (ITSM) tool or any other agreed channel of communication.

6.2. Request Logging and Analysis

For all Service Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the Service Request. This Service Desk will be responsible for logging and analysing the Service Request with the appropriate diligence.

6.3. Request Approval

The Service Desk Agent of the Party that raised the Service Request checks if any approvals are required from the other Party and if so proceeds to obtain them. If the Service Request is not approved, the Service Desk updates and closes the ticket.

6.4. Request fulfilment

This step caters for the effective and efficient handling of Service Requests. A distinction must be made between the following cases:

- The fulfilment of the Service Request only affects one Party. In this case, this Party issues the work orders and coordinates the execution.
- The fulfilment of the Service Request affects both the EU and CH. In this case, the Service Desks issue the work orders in their area of responsibility. The processing of the Service Request fulfilment is coordinated between both Service Desks. The overall responsibility lies with the Service Desk that received and initiated the Service Request.

When the Service Request has been fulfilled, it must be placed into Resolved State.

6.5. Request Escalation

The Service Desk can escalate the outstanding Service Request to the appropriate resource (third Party) if needed.

Escalations are done to the respective third Parties, i.e. the EU Service Desk will have to go through the CH Service Desk for escalation to a CH third Party, and vice versa.

The third Party to whom the Service Request was escalated is responsible for handling the Service Request in a timely fashion and communicating with the Service Desk who escalated the Service Request.

The Service Desk that logged the Service Request is responsible for tracking the overall status and assignment of a Service Request.

6.6. Request Fulfilment Review

The responsible Service Desk submits the Service Request Record to a final quality control before it is closed. The aim is to make sure that the Service Request is actually processed and that all information required to describe the request's life-cycle is supplied in sufficient detail. In addition to this, findings from the processing of the request are to be recorded for future use.

6.7. Request Closure

If the assigned Parties agree that the Service Request has been fulfilled and the requestor considers the case resolved, the next status to be set is 'Closed'.

A Service Request is formally closed once the Service Desk that logged the Service Request has executed the request closure phase and informed the Service Desk of the other Party.

7. CHANGE MANAGEMENT

The objective is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives.

The Change Management process includes different steps that capture every detail about a Change Request for future tracking. These processes ensure that the change is validated and tested before it moves to deployment. The Release Management process is responsible for successful deployment.

7.1. Request for Change

A Request For Change (RFC) is submitted to the Change Management team for validation and approval. For all Change Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the request. This Service Desk will be responsible for logging and analysing the request with appropriate diligence.

Change Requests may originate from:

- An incident that causes a change;
- An existing problem that results in a change;
- An end user requesting for a new change;
- Change as a result of an ongoing maintenance;
- Legislative change.

7.2. Change Evaluation and Planning

This stage handles change assessment and planning activities. It includes prioritization and planning activities to minimize risk and impact.

If the implementation of the RFC affects both the EU and CH, the Party that logged the RFC verifies the change evaluation and planning with the other Party.

7.3. Change approvals

Any registered change request needs to be approved by the relevant escalation level.

7.4. Change implementation

Change implementation is handled in the Release Management process. The Release Management teams of both Parties follow their own processes that involve planning and testing. Change review happens once the implementation is completed. To ensure that everything has gone according to plan the existing Change Management process is constantly reviewed and updated wherever necessary.

8. RELEASE MANAGEMENT

A release represents one or more changes to an IT service, collected in a release plan that will have to be authorized, prepared, built, tested, and deployed together. A release may represent a bug fix, a change to hardware or other components, changes to software, upgrades of application versions, changes to documentation and/or processes. The contents of each release are managed, tested and deployed as a single entity.

Release Management aims to plan, build, test and validate, and deliver capability to provide the designed services, which will accomplish the stakeholders' requirements and deliver the intended objectives. Acceptance criteria for all changes to the service will be defined and documented during design coordination and provided to Release Management teams.

The release will typically consist of a number of problem fixes and enhancements to a service. It contains the new or changed software required and any new or changed hardware needed to implement the approved changes.

8.1. Plan the release

The first step of the process assigns authorized changes to release packages and defines the scope and content of releases. Based on this information, the Release Planning sub-process develops a schedule for building, testing and deploying the release.

Planning should define:

- Scope and content of the release;
- Risk assessment and risk profile for the release;
- Customer/users affected by the release;
- Team responsible for the release;
- Delivery and deployment strategy;
- Resources for the release and its deployment.

Both Parties inform each other about their release planning and maintenance windows. If a release affects both the EU and CH, they coordinate the planning and define a common maintenance window.

8.2. Build and Test Release Package

The build and test step of the Release Management process establishes the approach of executing the release or release package and of maintaining the controlled environments prior to changing production, as well as testing all changes in all environments released.

If a release affects both the EU and CH, they coordinate the delivery plans and tests. This includes the following aspects:

- How and when release units and service components will be delivered;
- What the typical lead times are; what happens if there is a delay;
- How to track the progress of the delivery and obtain confirmation;
- Metrics for monitoring and determining the success of the release deployment effort;
- Common test cases for relevant functionalities and changes.

At the end of this sub-process, all required release components are ready to enter the live deployment phase.

8.3. Prepare deployment

The preparation sub-process ensures that communication plans are defined correctly and notifications are ready to be sent to all stakeholders and end users impacted, and that the release is integrated with the Change Management process to ensure that all changes are performed in a controlled manner and approved by the required forums.

If a release affects both the EU and CH, they shall coordinate the following activities:

- Change Request record for scheduling and preparing deployment to Production environment;
- Create implementation plan;
- Rollback approach, so that, in case of deployment failure, the previous state can be placed back;
- Notifications sent to all necessary Parties;
- Require approval for the implementation of the release from the relevant escalation level.

8.4. Roll back the release

In case deployment has failed or testing has identified that deployment was unsuccessful or has not met the agreed acceptance/quality criteria, the Release Management teams of both Parties will need to roll back to the previous state. All necessary stakeholders will need to be informed, including impacted/targeted end users. Pending approval, the process can restart at any of the previous stages.

8.5. Review and close release

When reviewing a deployment, the following activities should be included:

- Capture feedback on customer, user and service delivery satisfaction with the deployment (collect the feedback and consider for continuously improving the service);
- Review any quality criteria that were not met;
- Check that any actions, necessary fixes and changes are complete;
- Make sure there are no capability, resource, capacity or performance issues at the end of the deployment;
- Check that any problems, known errors and workarounds are documented and accepted by the customer, end users, operational support, and other Parties impacted;
- Monitor incidents and problems caused by deployment (provide early life support to operational teams in case the release has caused an increase in volumes of work);
- Update support documentation (i.e. technical information documents);
- Formally hand over the release deployment to service operations;
- Document lessons learnt;
- Collect the release summary document from implementation teams;
- Formally close the release after verifying the Change Request record.

9. SECURITY INCIDENT MANAGEMENT

Security Incident Management is a process for handling security incidents in order to enable incident communication to potentially impacted stakeholders; incident evaluation and prioritisation; and incident response to settle any actual, suspected or potential breach of confidentiality, availability or integrity of sensitive information assets.

9.1. Information Security Incident Categorization

All incidents impacting the link between the Union Registry and the Swiss registry shall be analysed to determine a possible breach in the confidentiality, the integrity or the availability of any sensitive information recorded in the Sensitive Information List (SIL).

If so, the incident shall be characterized as an information security incident, immediately registered in the IT Service Management (ITSM) tool and managed as such.

9.2. Information Security Incident Handling

Security Incidents are placed under the responsibility of the 3rd escalation level and resolution of the incidents will be dealt with by a dedicated Incident Management Team (IMT).

The IMT is responsible for:

- Carrying out a first analysis, categorizing and rating the severity of the incident;
- Coordinating actions between all the stakeholders including the full documentation of the incident analysis, the decisions taken to tackle the incident and any possible identified weaknesses;
- Depending on the severity of the security incident, escalating the incident in a timely manner to the appropriate level for information and/or a decision.

In the Information Security Management process, all information regarding incidents is classified at the highest level of sensitivity of the information, but in any case not lower than SENSITIVE: *ETS*.

For an on-going investigation and/or a weakness that could be exploited, and until its remediation, the information is classified as SPECIAL HANDLING: *ETS Critical*.

9.3. Security Incident Identification

Based on the security event type, the information security officer determines appropriate organizations to be involved and to be part of the IMT.

9.4. Security Incident Analysis

The IMT liaises with all involved organizations and the relevant members of their teams, as appropriate, to review the incident. During the analysis, the extent of an asset's confidentiality, integrity or availability loss is identified and consequences for all affected organizations are assessed. Next, initial and follow-up actions to resolve the incident and manage its impact, including the resource impact of these actions, are defined.

9.5. Security Incident Severity assessment, Escalation and Reporting

The IMT shall assess the severity of any new security incident after its characterization as a security incident and shall start immediate required action according to the severity of the incident.

9.6. Security Response Reporting

The IMT includes incident containment and recovery results in the information security incident response report. The report is provided to the 3rd escalation level using secure email or other mutually accepted means of secure communication.

The responsible Party reviews the containment and recovery results and:

- Reconnects the registry in case of prior disconnection;
- Provides incident communications to the registry teams;
- Closes the incident.

The IMT should include – in a secure manner - relevant details in the information security incident report in order to ensure consistent recording and communication and to enable prompt and appropriate action to contain the incident. Following its completion, the IMT provides the information security incident final report in due course.

9.7. Monitoring, Capacity Building and Continuous Improvement

The IMT will provide reports for all security incidents to the 3rd escalation level. The reports will be used by this escalation level to determine the following:

- Weak points in security controls and/or operation that need to be strengthened;
- A possible need to enhance this procedure to improve the effectiveness of the response to incidents;
- Training and capacity building opportunities to further strengthen the information security resilience of registry systems, reduce the risk of future incidents and minimize their impact.

10. INFORMATION SECURITY MANAGEMENT

Information Security Management aims to ensure the confidentiality, integrity and availability of an organization's classified information, data and IT services. In addition to the technical components including their design and testing (see LTS), the following common operational procedures are necessary to fulfil the security requirements for the permanent registry link.

10.1. Sensitive information identification

The sensitivity of a piece of information is assessed by determining the level of impact on the business (e.g. financial losses, image degradation, law infringement…) a security breach related to this information could have.

The sensitive information assets shall be identified on the basis of their impact on linking.

The level of sensitivity of this information shall be assessed according to the sensitivity scale applicable for this linking and detailed in the 'Information Security Incident Handling' section of this document.

10.2. Sensitivity levels of Information Assets

Upon its identification, the information asset is classified by applying the following rules:

- The identification of at least a single HIGH confidentiality, integrity or availability level classifies the asset as SPECIAL HANDLING: *ETS Critical*;
- The identification of at least a single MEDIUM confidentiality, integrity or availability level classifies the asset as SENSITIVE: *ETS*;
- The identification of only LOW confidentiality, integrity or availability levels classifies the asset as Marking EU**:** SENSITIVE: *ETS Joint Procurement.* Marking CH: LIMITED: ETS.

10.3. Assignment of Information Assets Owner

All information assets should have an assigned owner. Information assets of the ETS, belonging to or in conjunction with the link between the EUTL and the SSTL should be included in a joint asset inventory list, maintained by both Parties. Information assets of the ETS outside the link between the EUTL and the SSTL should be included in an asset inventory list, maintained by the respective Party.

Ownership of each information asset belonging to or in conjunction with the link between the EUTL and the SSTL is to be agreed to by the Parties. The owner of an information asset is responsible for assessing its sensitivity.

The owner should have a level of seniority that is appropriate to the value of the assigned asset(s). The owner's responsibility for the asset(s) and his or her obligation to maintain the required level of confidentiality, integrity and availability should be agreed and formalized.

10.4. Registration of sensitive Information

All sensitive information shall be registered in the Sensitive Information List (SIL).

Where relevant, the aggregation of sensitive information that could lead to a higher impact than the impact of one single piece of information shall be taken into account and registered in the SIL (e.g. a set of information stored in the system database).

The SIL is not static. Threats, vulnerabilities, likelihood or consequences of security incidents related to the assets may change without any indication and new assets might be introduced into the operation of registry systems.

Therefore, the SIL shall be reviewed regularly and any new information identified as sensitive shall be immediately registered into the SIL.

The SIL shall contain at least the following information for each entry:

- Description of the information
- Information owner
- Sensitivity level
- Indication if the information includes personal data
- Additional information if required

10.5. Handling of sensitive Information

When processed outside the link between the Union Registry and Swiss Registry, sensitive information shall be handled in accordance with the Handling Instructions.

Sensitive information processed by link between the Union Registry and Swiss Registry shall be handled in accordance with the Security requirements by the Parties.

10.6. Access Management

The objective of Access Management is to grant authorized users the right to use a service, while preventing access to non-authorized users. Access Management is sometimes also referred to as 'Rights Management' or 'Identity Management'.

For the permanent registry link and its operation, both Parties need access to the following components:

- Wiki: A collaboration environment for the exchange of common information, such as release planning;
- IT Service Management (ITSM) Tool for incident and problem management (see chapter 3, 'Approach and Standards');
- Message exchange system: each Party shall provide a secure message exchange transfer system for the transmission of the messages containing the transaction data.

The Swiss registry administrator and the Union central administrator ensure that accesses are up-to-date and act as contact points for their Parties for access management activities. Access requests are handled according to the Request Fulfilment procedures.

10.7. Certificate/Key Management

Each Party is responsible for its own certificate/key management (generation, registration, storage, installation, usage, renewal, revocation, backup and recovery of certificates/keys). As outlined in the Linking Technical Standards (LTS), only digital certificates issued by a Certificate Authority (CA) trusted by both Parties shall be used. The handling and storage of certificates/keys must follow the provisions set in the Handling Instructions.

Any revocation and/or renewal of certificates and keys shall be coordinated by both Parties. This takes place according to the Request Fulfilment procedures.

The Swiss registry administrator and the Union central administrator will exchange certificates/keys via secure means of communication according to the provisions laid down in the Handling Instructions.

Any verification of certificates/keys in any means between the Parties will take place out of band.

ANNEX III

LINKING TECHNICAL STANDARDS (LTS)

pursuant to Article 3(7) of the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems

Standard for permanent registry link

Table of Contents

1. GLOSSARY

Table 1-1 Business Acronyms and Definitions

Acronym/Term	Definition
Allowance	An allowance to emit one tonne of carbon dioxide equivalent during a specified period, which shall be valid only for the purposes of meeting the requirements of the ETS of either entity.
CH	Swiss Confederation
CHU	Stationary allowance type, also called CHU2 (referring to Commitment Period 2 of the Kyoto Protocol), issued by CH
CHUA	Swiss Aviation Allowance
COP	Common Operational Procedures. Commonly developed procedures to operationalise the link between the EU ETS and the ETS of Switzerland.
ETR	Emissions trading registry
ETS	Emissions Trading System
EU	European Union
EUA	EU general allowance
EUAA	EU Aviation Allowance

Acronym/Term	Definition
EUCR	European Union Consolidated Registry
EUTL	European Union Transaction Log
Registry	An accounting system for allowances issued under the ETS, which keeps track of the ownership of allowances held in electronic accounts.
SSTL	Swiss Supplementary Transaction Log
Transaction	A process in a registry that includes the transfer of an allowance from one account to another account.
Transaction log system	The transaction log contains a record of each proposed transaction sent from one Registry to the other.

Table 1-2 Technical Acronyms and Definitions

Acronym	Definition
Asymmetric cryptography	Uses public and private keys to encrypt and decrypt data.
Certificate Authority (CA)	Entity that issues digital certificates.
Cryptographic key	A piece of information that determines the functional output of a cryptographic algorithm.
Decryption	Reverse process of encryption.
Digital signature	A mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access.
File ingestion	The process of reading a file.
Firewall	Network security appliance or software that monitors and controls incoming and outgoing network traffic based on predetermined rules.
Heartbeat monitoring	Periodic signal generated and monitor by hardware or software to indicate normal operation or to synchronize other parts of a computer system.
IPSEC	IP SECurity. Network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
Penetration testing	Practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit
Reconciliation process	Process of ensuring that two sets of records are in agreement.
VPN	Virtual Private Network.
XML	Extensible Mark-up Language. It allows designers to create their own customised tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organisations.

2. INTRODUCTION

The Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 23 November 2017 (“Agreement”) provides for the mutual recognition of emission allowances that can be used for compliance under the Emissions Trading System of the European Union (“EU ETS”) or the Emissions Trading System of Switzerland (“ETS of Switzerland”). To operationalise the link between the EU ETS and the ETS of Switzerland, a direct link between the European Union Transaction Log (EUTL) of the Union Registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry shall be established, which will enable the registry-to-registry transfer of emission allowances issued under either ETS (Article 3(2) of the Agreement). To operationalize the link between the EU ETS and the ETS of Switzerland, a provisional solution was implemented in 2020. As from 2023, the registry link between the two emissions trading systems will gradually develop into a permanent registry link expected to be implemented not later than 2024 that enables the functioning of the linked markets with respect to benefits from market liquidity and execution of transactions between the two linked systems in a manner that is equivalent to one market made up of two systems and which allows market participants to act as if they were in one market, subject only to individual regulatory provisions of the Parties (Annex II of the Agreement).

Pursuant to Article 3(7) of the Agreement, the Swiss registry administrator and the central administrator of the Union Registry shall develop Linking Technical Standards (LTS) based on the principles set out in Annex II to the Agreement, describing the detailed requirements for establishing a robust and secure connection between the SSTL and the EUTL. The LTS developed by the administrators shall take effect when adopted by a decision of the Joint Committee.

The LTS was adopted by the Joint Committee by its Decision No. 2/2020. The updated LTS, as recorded in this document, will be adopted by the Joint Committee by its Decision No. 1/2024. In accordance with this Decision and requests from the Joint Committee, the Swiss registry administrator and the Union central administrator have developed and will update further technical guidelines to operationalise the link and to ensure that these are continuously adapted to technical progress and/or new requirements relating to the safety and security of the link and to its effective and efficient operation.

2.1. Scope

This document represents the common understanding between the Parties to the Agreement regarding the establishment of the technical foundations of the link between the registries of the EU ETS and the ETS of Switzerland. While it outlines the baseline for the technical specifications in terms of architectural, service and security requirements, some further detailed guidance will be needed to operationalise the link.

For the proper functioning, the link will require processes and procedures in order to further operationalise the link. Pursuant to Article 3(6) of the Agreement, those matters are detailed in a separate common operational procedures (COP) document, adopted by decision of the Joint Committee.

2.2. Addressees

This document is addressed to the Swiss registry administrator and the central administrator of the Union Registry.

3. General Provisions

3.1. Architecture of the communication link

The purpose of this section is to provide a description of the general architecture of the operationalisation of the link between the EU ETS and the ETS of Switzerland and the different components involved in it.

Security being a key part for the definition of the architecture, all measures have been taken to have a robust architecture. The permanent registry link uses a file exchange mechanism, as implementation of a secure Air Gap connection.

The technical solution uses:

- A secure message exchange transfer protocol.
- XML messages.
- XML based digital signature and encryption.
- VPN.

The following figure provides an overall view of the permanent registry link's architecture:

3.1.1. Message exchange

The communication between the Union Registry and the Swiss registry is based on a message exchange mechanism through secured channels. Each end counts on its own repository of received messages.

Both Parties keep a log of the messages received, together with the processing details.

Errors or unexpected status are to be reported, as alerts, and human contact between the support teams should take place.

Errors and unexpected events are handled in observance of the operational procedures laid down in the incident management process of the COP.

3.1.2. XML Message - High level description

An XML Message contains one of the following:

- One or several Transaction Requests and/or one or several Transaction Responses;
- One operation/response related to reconciliation;
- One Test message.

Every message contains a header with:

- Originating ETS system;
- Sequence Number.

3.1.3. Ingestion windows

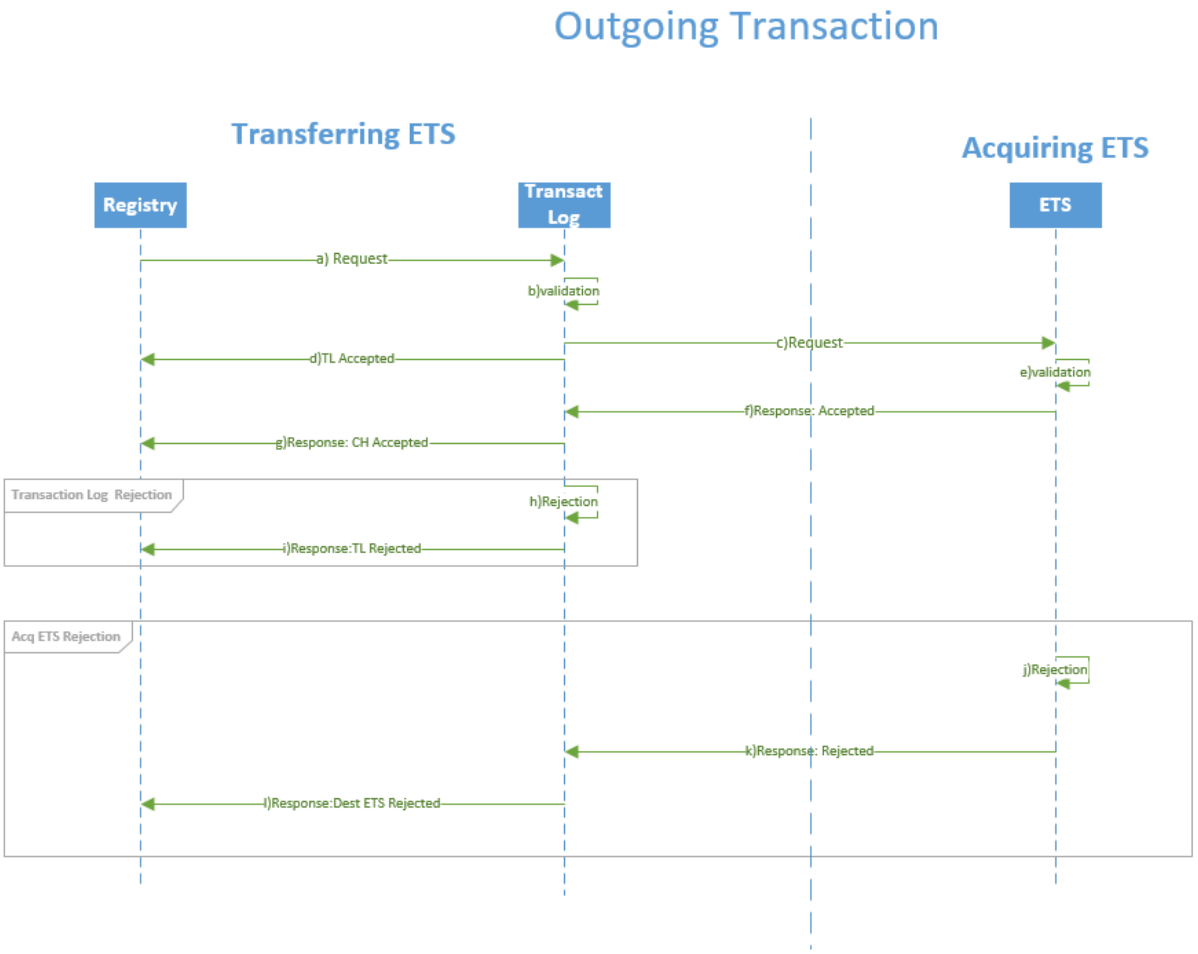
The permanent registry link is based on predefined ingestion windows that are followed by a set of named events. Transaction requests received through the link will only be ingested at predefined intervals, and includes a technical validation for outgoing and incoming transactions. In addition, reconciliations may run in a daily basis and can be triggered manually.

Changes in the frequency and/or timing of any of these events will be handled in observance of the operational procedures laid down in the request fulfilment process of the COP.

3.1.4. Transaction Message Flows

Outgoing transactions

This reflects the point of view of the transferring ETS. The specific flow is depicted in the following sequence diagram:



Main flow shows the following steps (as in drawing above):

(a) On the transferring ETS, the transaction request is sent from the registry to the Transaction log, once all the business delays are over (24 hours delay, where applicable).

(b) Transaction log validates the transaction request.

(c) The transaction request is sent to the destination ETS.

(d) The acceptance response is sent to the originating ETS' registry.

(e) The destination ETS validates the transaction request.

(f) The destination ETS sends the acceptance response back to the originating ETS' Transaction log.

(g) The Transaction log sends the acceptance response to the registry.

Alternative flow “Transaction Log Rejection” (as in drawing above, starting from (a) in main flow):

(a) In the originating system, the transaction request is sent from the registry to the Transaction log, once all the business delays are over (24 hours delay, where applicable).

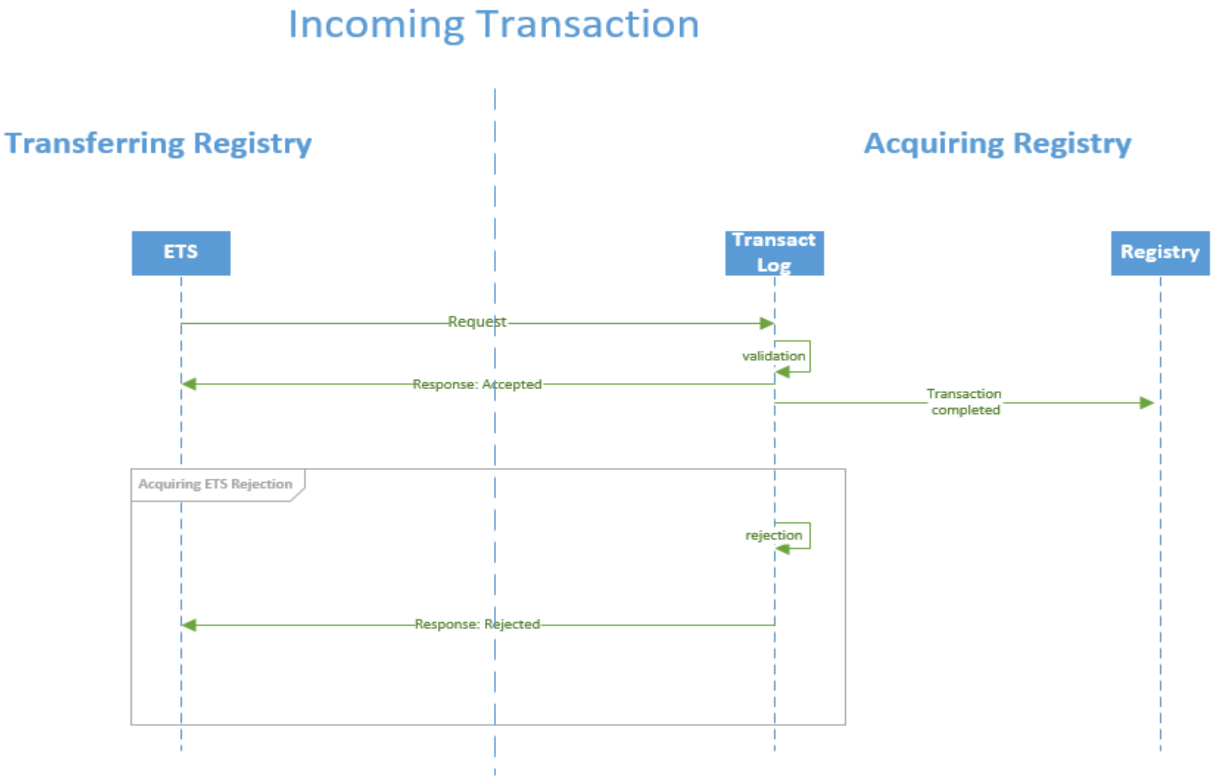
(b) Transaction log does not validate the request

(c) Rejection message is sent to the originating registry.

Alternative flow “ETS Rejection” (as in drawing above, starting from (d) in main flow):

(a) In the originating ETS, the transaction request is sent from the registry to the Transaction log, once all the business delays are over (24 hours delay, where applicable).
(b) Transaction log validates the transaction.
(c) The transaction request is sent to the destination ETS.
(d) The acceptance message is sent to the originating ETS’ registry.
(e) The acquiring ETS’ Transaction log does not validate the transaction.
(f) Acquiring ETS sends the refusal response to the transferring ETS’ Transaction log.
(g) Transaction log send the refusal to the registry.

Incoming Transactions



This reflects the point of view of the acquiring ETS. The specific flow is depicted in the following sequence diagram:

The diagram shows:

(1) When the acquiring ETS’ Transaction log validates the request, it sends the acceptance message to the Transferring ETS and a ‘transaction completed’ message to the acquiring ETS’ registry.

(2) When an incoming request is refused on the acquiring Transaction log and it is refused, the transaction request is not sent to the acquiring ETS’ registry.

Protocol

The transaction message cycle involves only two messages:

- Transferring ETS → Acquiring ETS Transaction Proposal.
- Acquiring ETS → Transferring ETS Transaction Response: Either Accepted or Rejected (including the reason for rejection).
  - Accepted: Transaction is completed.
  - Rejected: Transaction is terminated.

Transaction status

- Transferring ETS transaction status will be set to ‘proposed’ when the request is sent.
- Acquiring ETS transaction status will be set to ‘proposed’ when the request is received and while it is being treated.
- Acquiring ETS transaction status will be set to ‘completed’/’terminated’, when the proposal is processed. Acquiring ETS will then send the corresponding acceptance/rejection message.
- Transferring ETS transaction status will be set to completed/terminated when the acceptance/rejection is received and processed.
- In the Transferring ETS the transaction status will remain as proposed if no response is received.
- Acquiring ETS will set to ‘terminated’ any transaction staying as proposed for more than 30 minutes.

Incidents related to transactions will be handled in observance of the operational procedures laid down in the incident management process of the COP.

3.2. Data Transfer Security

The data in transit will be subject to four levels of security:

(1) Network access control: Firewall and network interconnection layer.

(2) Transport level encryption: VPN.

(3) Session level encryption: Secure message exchange transfer protocol.

(4) Application level encryption: XML Content encryption and signature.

3.2.1. Firewall and Network Interconnection

The link shall be established over a network protected by a hardware-based firewall. The firewall shall be configured with rules such that only “registered” clients can make connections to the VPN server.

3.2.2. Virtual Private Network (VPN)

All communications between the Parties shall be protected using virtual private network (VPN) technology. VPN technologies provide the ability to "tunnel" through a network like the Internet from one point to another, protecting all communications. Prior to the creation of the VPN tunnel, a digital certificate is issued to a prospective client end-point, allowing the client to provide proof of identity during the negotiation of the connection. Each Party is responsible for installing the certificate into its VPN end-point. Using digital certificates, each end VPN server will access a central authority to negotiate authentication credentials. During the tunnel creation process, encryption is negotiated, ensuring that all communications through the tunnel are protected.

The client VPN end-points shall be configured to maintain the VPN tunnel permanently, in order to allow reliable, two-way, real-time communication between the Parties at all times.

Generally, the European Union is using the Secure Trans European Services for Telematics between Administrations (STESTA) as private IP-based network. Therefore, this network is also suitable for the permanent registry link.

3.2.3. IPSec Implementation

The use of the IPSec protocol to form the site-to-site VPN infrastructure will provide for site-to-site authentication, data integrity, and data encryption. IPSec VPN configurations ensure proper authentication between two end-points in a VPN connection. The Parties will identify and authenticate the remote client via the IPSec connection using a digital certificates provided by a Certificate Authority recognised by the other end.

IPSec also ensures data integrity of all communications passed through the VPN tunnel. Data packets are hashed and signed using the authentication information established by the VPN. Confidentiality of the data is assured likewise by enabling IPSec encryption.

3.2.4. Secure message exchange transfer protocol

The permanent registry link relies on multiple encryption layers to securely exchange data between the Parties. Both systems and their different environments are interconnected at the network level by means of VPN tunnels. At the application level files are transferred using a secure message exchange transfer protocol at session level.

3.2.5. XML Encryption and signature

Within XML files, signing and encryption occurs at two levels. Every transaction request, transaction response and reconciliation message is digitally signed individually.

In a second step, every sub element of the '*message'* element is individually encrypted.

In addition, as third step and to ensure the integrity and non-repudiation of the whole message, the root element message is digitally signed. This results in a high level of protection for the XML embedded data. The technical implementation observes the World Wide Web Consortium standards.

To decrypt and verify the message, the process is followed in reverse order.

3.2.6. Cryptographic Keys

Public key cryptography will be used for encryption and signing.

For the specific case of IPSec, a digital certificate issued by a Certificate Authority (CA) trusted by both Parties shall be used. This CA verifies identity and issues certificates which are used to positively identify an organisation and setup secure data communications channels between the Parties.

Cryptographic keys are used for signing and encrypting communication channels and data files. The public certificates are digitally exchanged by the Parties using secure channels and verified out of band. This procedure is an integral part of the Information Security Management process of the COP.

3.3. List of Functions under the link

The link specifies the transmission system for a series of functions that implement the business processes derived from the Agreement. The link also includes the specification for the reconciliation process and for the test messages that will allow the implementation of a heartbeat monitoring.

3.3.1. Business transactions

From the business perspective, the link contemplates four (4) types of Transaction Requests:

- External transfer:
  - After entry into force of the ETS linking, EU and CH allowances are fungible, and thus fully transferrable, between the Parties.
  - A transfer sent through the link will involve a transferring account on an ETS and acquiring account on the other ETS.
  - The transfer can include any amount of the four (4) types of allowances:
    - Swiss general allowances (CHU)
    - Swiss aviation allowances (CHUA)
    - EU general allowances (EUA)
    - EU aviation allowances (EUAA)
- International Allocation:

Aircraft Operators administered by one ETS with obligations on the other ETS and entitled to receive free allowances from that second ETS, will receive free aviation allowances, from the second ETS, by means of the international allocation transaction.

- Reversal of International Allocation:

This transaction will happen in the case that free allowances allocated to an aircraft operator holding by the other ETS has to be reversed in total.

- Return of Excess Allocation:

Similar to the reversal, but where the allocation does not need to be fully reversed, and only the over allocated allowances have to be returned to the allocating ETS.

3.3.2. Reconciliation protocol

Reconciliations will only take place after the windows for messages ingestion, validation and processing are closed.

Reconciliations are an integral part of the security and consistency measures of the linking. Both Parties will agree on the exact timing of reconciliation before creating any schedule. A daily scheduled reconciliation can take place if agreed by both Parties. At least a scheduled reconciliation will be executed however after the ingestion takes place.

Either Party can nevertheless initiate manual reconciliations at any time.

> Changes in the timing and frequency of the scheduled reconciliation will be handled in observance of the operational procedures laid down in the request fulfilment process of the COP.

3.3.3. Test message

A test message is foreseen to test end-to-end communication. The message will contain data that will identify it as a test and will be answered upon reception by the other end.

3.4. Data Logging Requirements

To support the need for both Parties to maintain accurate and consistent information, and to provide tools for use in the reconciliation process to resolve inconsistencies, four (4) types of data logs shall be maintained by both Parties:

- Transaction logs;
- Reconciliation logs;
- Message archive;
- Internal audit logs.

All data in these logs shall be maintained at least during three (3) months for the purposes of troubleshooting and their further retention will depend on the applicable law at each end for the purpose of auditing. Log files older than three (3) months may be archived into a secure location in an independent IT system, as long as it can be retrieved or accessed within a reasonable period.

Transaction logs

Both EUTL and SSTL subsystems are Transaction log implementations. Tied out between both ETS systems.

More specifically, the Transaction logs will keep a record of each proposed transaction sent to the other ETS. Each record contains all the fields of the transaction content and the subsequent outcome of the transaction (the response of the receiving ETS). The Transaction logs will also keep a record for the incoming transactions as well as the response sent to the originating ETS.

Reconciliation logs

The Reconciliation Log contains a record of each reconciliation message exchanged between both Parties, including the reconciliation id, the timestamp and the result of the reconciliation: Reconciliation status “Pass” or “Discrepancies”. In the permanent registry link reconciliation messages are an integral part of the messages exchanged and are therefore stored as described in ‘Message archive’ section.

Both Parties shall log each request and its response in the Reconciliation Log. Although information in the Reconciliation Log is not shared directly as part of the Reconciliation itself, access to this information may be necessary in order to resolve inconsistencies.

Message archive

Both Parties are required to archive a copy of the exchanged data (the XML files), sent and received, and whether those or XML messages were correct in their format or not.

The main purpose of the archive is for auditing, to have an evidence of what was sent and received to and from the other Party. In that sense, along with the files, the related certificates need to be archived as well.

These files will also provide additional information for troubleshooting.

Internal Audit Log

These logs are defined and used by each Party on its own.

3.5. Operational Requirements

The exchange of data between both systems is not fully autonomous in the permanent registry link, this is it requires operators and procedures to operationalise the link. Several roles and tools are detailed to this end in this process.

4. AVAILABILITY PROVISIONS

4.1. Communication Availability design

The architecture for the permanent registry link is fundamentally an ICT infrastructure and software that allows the communication between the ETS of Switzerland and the ETS of the EU. Ensuring high levels of availability, integrity and confidentiality of this flow of data becomes then an essential aspect to consider in the design of the permanent registry link. Being a project in where the ICT infrastructure, the custom made software, and the processes play an integral role, all three elements have to be taken into account in order to design a resilient system.

ICT infrastructure resilience

General provisions chapter to this document detail the architectural building blocks. On the ICT infrastructure side, the permanent registry link sets up a resilient VPN network that creates secure communication tunnels over which secure message exchanges can take place. Other infrastructure elements are configured in high-availability and/or count on fall-back mechanisms.

Custom Software resilience

The custom developed software modules enhance the resilience by retrying the communication for a given period of time with the other end if due to any reason is not available.

Service resilience

In the permanent registry link, data exchanges between Parties occur at predefined intervals. Some of the steps required in the prescheduled data exchanges require manual intervention by system operators and/or registry administrators. Taking this aspect into account, and in order to increase the availability and success of the exchanges:

- The operational procedures foresee time windows to perform each step.
- The software modules for the permanent registry link implement asynchronous communication.
- The automatic reconciliation process will detect if there were issues in the ingestion of data files at either end.
- Monitoring processes (ICT infrastructure and custom software modules) are considered into and trigger Incident Management procedures (as defined in the common operational procedures document). Those procedures that aim at reducing the time to restore normal operation following incidents are essential to ensure high availability ratios.

4.2. Initialisation, Communication re-activation and testing plan

All different elements involved in the architecture of the permanent registry link shall pass a series of individual and collective tests in order to confirm the platform is ready at ICT infrastructure and information system level. These operational tests are a compulsory prerequisite each time the platform transitions the permanent registry link from suspended to operational status.

The operational status activation of the link requires then the successful execution of a predefined test plan. This shall confirm that each registry has performed a set of internal tests first, followed by end-to-end connectivity validation prior to begin the submission of production transactions between both Parties.

The test plan should mention the overall test strategy and details about the testing infrastructure. In particular, for each element in every test block it should include:

- The test criteria and tools;
- The roles assigned to perform the test;
- The expected results (positive and negative);
- Test schedule;
- The logging of test results requirements;
- Troubleshooting documentation;
- Escalation provisions.

As a process, the operational status activation tests could be split in four (4) conceptual blocks or phases:

4.2.1. Internal ICT infrastructure tests

These tests are meant to be performed and/or checked individually by Registry administrators at each end.

Every element of ICT infrastructure at each end shall be tested individually. This includes every single component of the infrastructure. These tests can be executed automatically or manually but shall verify that every element of the infrastructure is operational.

4.2.2. Communication tests

These tests shall start individually at each Party and conclude in cooperation with the other end.

Once individual elements are operational, the communication channels between both registries needs to be tested. To this end, each Party shall verify that Internet access works, the VPN tunnels are established, and there is site-to-site IP connectivity. Reachability of the local and remote infrastructure elements and IP connectivity should then be confirmed to the other end.

4.2.3. Full system (end-to-end) tests

These tests are meant to be executed at each end and results shall be shared with the other Party.

Once communication channels and each individual component of both registries have been tested, each end shall prepare a series of simulated transactions and reconciliation that are representative of all functions to be implemented under the link.

4.2.4. Security tests

These tests are meant to be performed and/or triggered by Registry administrators at each end and as detailed in sections 'Security Testing Guidelines' and 'Risk Assessment provisions'.

Only after each of the four phases/blocks have ended with a predictable results, the permanent registry link can be considered in operational status.

Testing resources

Each Party shall count on specific testing resources (specific ICT infrastructure software and hardware) and shall develop testing functions into their respective systems in order to support the manual and continuous validation of the platform. Manual individual or cooperative testing procedures can be executed at any time by registry administrators. Operational status activation is a manual process in itself.

It is likewise foreseen that the platform performs automatic checks at regular intervals. Those checks are aimed at increasing the availability of the platform by detecting early potential infrastructure or software issues. This platform monitoring plan is composed of two elements:

- ICT infrastructures monitoring: at both ends the infrastructure will be monitored by the ICT infrastructure service providers. The automatic tests will cover the different infrastructure elements and the availability of the communication channels.
- Application monitoring: the permanent registry linking software modules will implement system communication monitoring at application level (either manually and/or at regular intervals) that will test the end-to-end availability of the linking by simulating some of the transactions over the link.

4.3. Acceptance/Testing environments

The architecture of the Union Registry and the Swiss registry consist of the following three environments:

- Production (PROD): This environment holds the real data and processes real transactions.
- Acceptance (ACC): This environment contains non-real or anonymised, representative data. It is the environment where system operators by both Parties validate new releases.
- Test (TEST): This environment contains non-real or anonymised, representative data. This environment is limited to registry administrators and meant to be used to perform integration tests by both Parties.

Except for the VPN, the three environments are fully independent of each other, meaning hardware, software, databases, virtual environments, IP-addresses, ports are set up and operate independently of each other.

As for the VPN layout, communication between the three environments has to be fully independent, which is ensured by using STESTA.

5. CONFIDENTIALITY AND INTEGRITY PROVISIONS

Security Mechanisms and Procedures foresee a two person-role (4-eye principle) for operations occurring in the link between the Union Registry and the Swiss registry. The two person-role shall apply whenever necessary, however, it might not apply to all steps, undertaken by Registry Administrators.

The security requirements are considered and addressed in the security management plan, which includes likewise processes related to the handling of security incidents following an eventual security breach. The operational part of these processes is described in the COP.

5.1. Security Testing Infrastructure

Each Party commits in setting up a security testing infrastructure (by using the common set software and hardware used in the detection of vulnerabilities at development and operation phases):

- Separated from the production environment;
- Where security is analysed by a team independent from the development and the operation of the system.

Each Party commits performing both static and dynamic analysis.

In the case of dynamic analysis (like penetration testing), both Parties commit to restrict the evaluations ordinarily to the test and acceptance environments (as defined in ‘Acceptance/Testing environments’ section). Exceptions to this policy are subject to approval of both Parties.

Before being deployed in the production environment, every software module of the link (as defined in the ‘Architecture of the communication link’ section) shall be security tested.

Testing infrastructure must be separated at both network and infrastructure levels from the production one and allow to carry out the security tests required to check compliance with security requirements.

5.2. Link Suspension and Reactivation Provisions

In case, there is a suspicion that the security of the Swiss registry, the SSTL, the Union registry or the EUTL has been compromised, both Parties shall immediately inform each other and suspend the link between the SSTL and the EUTL.

> The procedures for information sharing, decision to suspend and decision to reactivate are part of the Request Fulfilment process of the COP.

Suspensions

Suspension of the registry link in accordance with the Annex II of Agreement may happen due to:

- Administrative reasons (maintenance,….), and therefore planned;
- Security reasons (or IT infrastructure breakdowns), and therefore unplanned.

In case of emergency, either Party will inform the other Party and suspend unilaterally the registry link.

If decision is made to suspend the registry link, then each Party will therefore ensure the link is interrupted at network level (by blocking parts or all incoming and outgoing connections).

> The decision of suspending the registry link, whether it is planned or unplanned, will be taken according to the Change Management or Security Incident Management procedure of the COP.

Communication Reactivation

Decision to reactivate will be taken as detailed in the COP and in any case not before successful completion of the security testing procedures as detailed in ‘Security testing guidelines’ and ‘Initialisation, Communication re-activation and testing plan’ sections.

5.3. Security Breach Provisions

A security breach is considered as a Security Incident impacting the confidentiality and the integrity of any sensitive information and/or the availability of the system handling them.

Sensitive information is identified in the Sensitive Information List and may be handled in the system or in any related part.

Information directly related to the security breach will be considered as sensitive, marked “SPECIAL HANDLING: *ETS Critical*” and handled according to the handling instructions, unless specified otherwise.

Every security breach will be handled according to the Security Incident Management chapter of the COP.

5.4. Security Testing Guidelines

5.4.1. Software

Security testing, including penetration testing if applicable, shall be performed at least on all new major releases of the software in accordance with the security requirements set out in the LTS in order to assess the security of the linking and the related risks.

If no major release has been produced in the last 12 months, a security testing shall be performed on the current system considering the cyber threat evolution that occurred in the last 12 months.

Security testing of the registry link shall be done in the acceptance environment and, if required, in the production environment and with coordination and mutual agreement of both Parties.

Web application testing will observe international open standards such as the ones developed by the Open Web Application Security Project (OWASP).

5.4.2. Infrastructure

The infrastructure supporting the production system shall be regularly scanned against vulnerabilities (at least once a month) and detected vulnerabilities fixed in the same principle as defined in the previous section using up-to-date vulnerability database.

5.5. Risk Assessment provisions

If penetration testing is applicable it must be included in the security testing.

Each Party may contract a specialized company for the performance of security testing, provided this company:

- Has the skills and the experience of such security testing;
- Is not reporting directly to the developer and/or its contractor and is neither involved in the development of the software of the link nor being a subcontractor of the developer;
- Has signed Non-Disclosure Agreement to keep the results confidential and to handle them at the “SPECIAL HANDLING: ETS Critical” level in accordance with the handling instructions.