Council of the European Union

Brussels, 6 October 2020
(OR. en)

10836/20

Interinstitutional File:
2020/0130 (NLE)

ENV 517
CLIMA 188
ENER 291
IND 136
COMPET 406
MI 334
ECOFIN 804
TRANS 398
AELE 53
CH 25

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	Draft DECISION 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 on amending Annexes I and II to the Agreement and the adoption of Linking Technical Standards (LTS)

DRAFT

DECISION No 2/2020
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 …

on amending Annexes I and II to the Agreement
and the adoption of Linking Technical Standards (LTS)

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] ('the Agreement') and in particular Article 3(7) and Article 13(2) thereof,

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

Whereas:

(1) Decision No 2/2019 of the Joint Committee of 5 December 2019[1] amended Annexes I and II to the Agreement thus fulfilling the conditions for linking set out in the Agreement.

(2) Following adoption of Decision No 2/2019 of the Joint Committee and pursuant to Article 21(3) of the Agreement, the Parties exchanged their instruments of ratification or approval, since they consider all conditions for linking as set out in the Agreement to have been fulfilled.

(3) In accordance with Article 21(4) of the Agreement, the Agreement entered into force on 1 January 2020.

(4) Annex I to the Agreement should be amended in accordance with Article 13(2) of the Agreement to ensure a smooth transition in administration of aircraft operators attributed to Switzerland for the first time by taking account of the progress made on establishing the registry link.

[1] Decision no 2/2019 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 5 December 2019 amending Annexes I and II to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems (OJ L 314, 29.9.2020, p. 68).

(5) In order to accommodate recent developments and ensure an increased level of flexibility to establish the registry link required by the Agreement, Annex II to the Agreement should be amended in accordance with Article 13(2) of the Agreement to provide for a larger, but equivalent set of technologies to set up the registry link.

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

(7) In accordance with Article 13(1) of the Agreement, the Joint Committee should agree on technical guidelines to ensure the proper implementation of the Agreement including on establishing a robust and secure connection between the SSTL and the EUTL. Technical guidelines may be developed by a working group set up pursuant to Article 12(5) of the Agreement. The working group should at least include the Swiss Registry administrator and the Union central administrator and should assist the Joint Committee in its functions under Article 13 of the Agreement.

(8) In view of the technical nature of the guidelines and the need to adapt them to ongoing developments, the technical guidelines developed by the Swiss registry administrator and the Union central administrator should be submitted to the Joint Committee for information or, where appropriate, approval,

HAS ADOPTED THIS DECISION:

Article 1

The second paragraph of point 17 in Part B of Annex I to the Agreement is hereby replaced by the following text:

'Aircraft operators attributed to Switzerland for the first time after the entry into force of this Agreement shall be administered by Switzerland after 30 April of the year of attribution and once the provisional registry link is operational.'.

Article 2

The fourth subparagraph of Annex II to the Agreement is hereby replaced by the following text:

'The LTS shall specify that the communications between the SSTL and the EUTL consist of secure exchanges of webservices messages based on the following technologies* or equivalent:

– web services using Simple Object Access Protocol (SOAP);

– hardware-based Virtual Private Network (VPN);

– XML (Extensible Markup Language);

– digital signature; and

– network time protocols.

_____

* Those technologies are currently used for establishing a connection between the Union Registry and the International Transaction Log as well as between the Swiss Registry and the International Transaction Log.'.

Article 3

The Linking Technical Standards (LTS), as annexed to this Decision, are hereby adopted.

Article 4

Herewith, a working group shall be set up pursuant to Article 12(5) of the Agreement. It shall assist the Joint Committee in ensuring the proper implementation of the Agreement including the development of technical guidelines for the implementation of the LTS.

The working group shall at least include the Swiss registry administrator and the Union central administrator.

Article 5

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

Done at Brussels, … 2020.

For the Joint Committee

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

ANNEX

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

Standards for Provisional Solution

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 under the EU ETS or the ETS of Switzerland.
CH	Swiss Confederation
CHU	Swiss general allowances (Term 'CHU2' is used as abbreviation for commitment period 2 CHU allowances)
CHUA	Swiss Aviation Allowance
COP	Common Operational Procedures jointly developed by the Parties to the Agreement to operationalise the link between the EU ETS and the ETS of Switzerland.
ETR	Emissions Trading Registry
ETS	Emissions Trading System

Acronym/Term	Definition
EU	European Union
EUA	EU General Allowance
EUAA	EU Aviation Allowance
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.

Acronym	Definition
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 monitored 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 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 operationalise the link between the EU ETS and the ETS of Switzerland, a provisional solution shall be in place by May 2020 or as soon as possible thereafter. Parties shall cooperate to replace the provisional solution with a permanent registry link as soon as possible (Annex II to the Agreement).

Pursuant to Article 3(7) of the Agreement, the Swiss registry administrator and the Union central administrator 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, as recorded in this document is to be adopted by the Joint Committee by its Decision No 2/2020. In accordance with this Decision, the Joint Committee shall request the Swiss registry administrator and the Union central administrator to develop 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 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 its proper functioning, the link will require processes and procedures in order to further operationalise it. Pursuant to Article 3(6) of the Agreement, those matters are detailed in a separate common operational procedures (COP) document, to be adopted separately by decision of the Joint Committee.

2.2. Addressees

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

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 of the definition of the architecture of the registry link, all measures have been taken to have a robust architecture. Although the foreseen permanent registry link will be based on web services, the provisional solution will use a file exchange mechanism instead.

The technical solution uses:

– A secure message exchange transfer protocol;

– XML messages;

– XML based digital signature and encryption;

– VPN Appliance or equivalent secure data transport network.

3.1.1. Message Exchange

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

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

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

Errors and unexpected events will be 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;

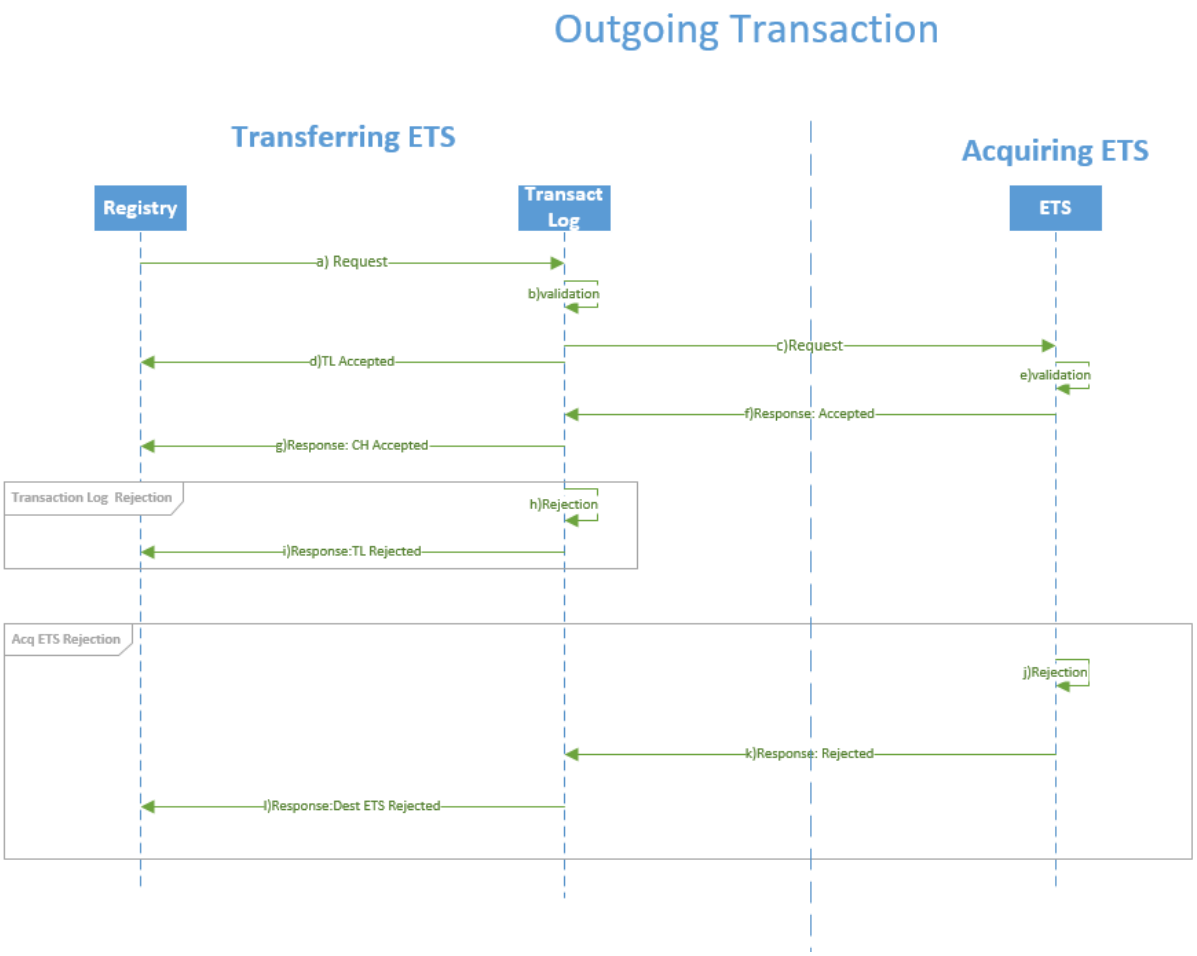
– Sequence Number.

3.1.3. Ingestion Windows

The provisional solution 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. Ingestion windows include a technical validation for outgoing and incoming transactions. In addition, reconciliations may run on 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 sequence diagram above depicts all the specific outgoing transaction flows.

Main flow 'Normal Transaction' (with steps indicated in the 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' (with steps indicated in the drawing above, starting equally from (a)):

(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).

Followed by:

(b) Transaction log does not validate the request;

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

Alternative flow 'ETS Rejection' (with steps indicated in the drawing above, starting from (a)):

(a) In the originating ETS, the transaction request is sent from the registry to the Transaction log, once all 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.

Followed by:

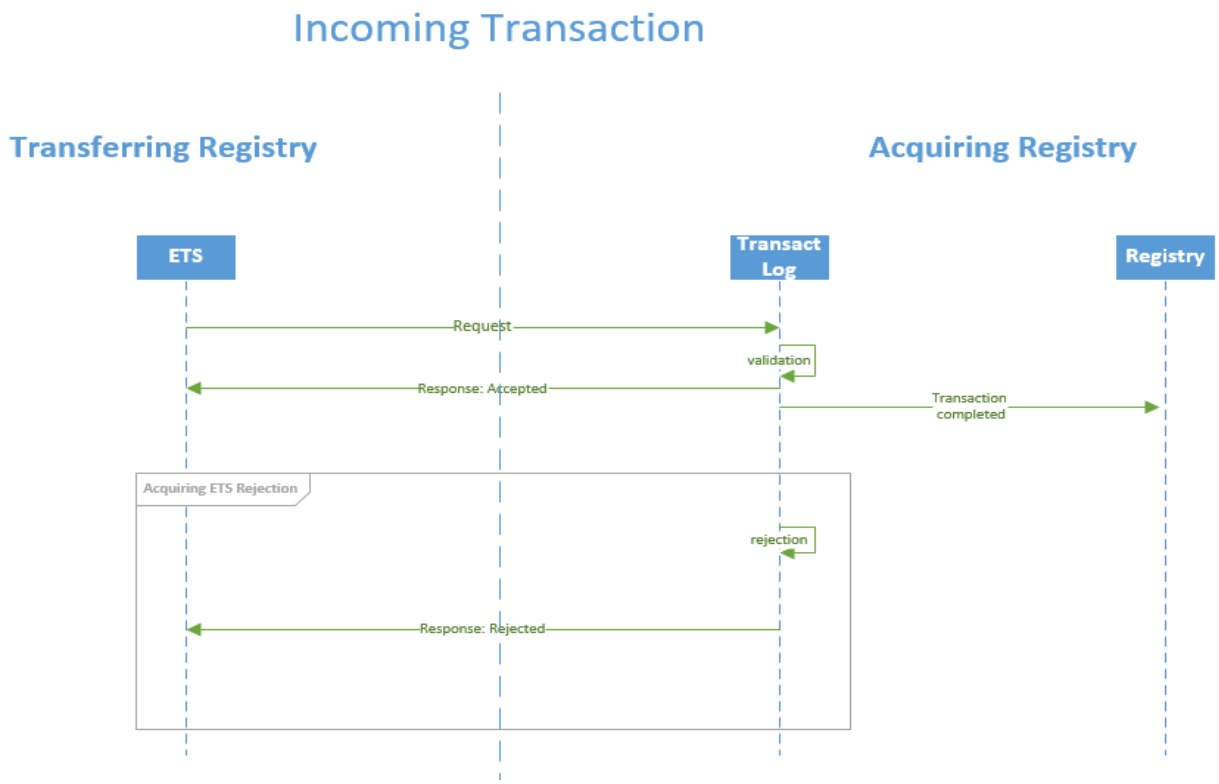
(e) The acquiring ETS Transaction log does not validate the transaction;

(f) Acquiring ETS sends the refusal response to the transferring ETS Transaction log;

(g) Transaction log send the refusal to the registry.

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

Incoming Transactions



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 transaction status will be set to 'terminated' if any proposed transaction stays in the 'proposed' state 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 or equivalent secure data transport network;

(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 a secure data transport technology. In the case of a Virtual Private Network (VPN), the infrastructure should be based on hardware or virtual appliances. 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.

Any other equivalent solution shall be compliant with the abovementioned principles.

3.2.3. IPSec Implementation

In case of using a VPN solution, 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 provisional solution 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 or equivalent secure data transport networks. 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 a 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 the identity of the certificate holder and issues certificates which are used to positively identify an organisation and set up 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 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 have 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 a minimum, at least one scheduled reconciliation will be executed after each ingestion takes place.

In any case, either Party can 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 provided for to test end-to-end communication. The message will contain data that will identify the message as a test and will be answered upon reception by the other end.

3.4. Standards for Web Services

Web services will not be used in the provisional solution. It is worth noting however that the shape and format of XML messages will remain unchanged to a great extent. With the introduction of the permanent registry link in the future, web services should allow the exchange of XML messages in real-time.

3.5. Web Services Specific Definition

This section is not applicable for the provisional solution. As mentioned in the previous section, web services will only be used in the future permanent registry link.

3.6. 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 they can be retrieved or accessed within a reasonable period.

Transaction Logs

Both EUTL and SSTL subsystems contain Transaction log implementations.

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 provisional solution reconciliation messages are an integral part of the messages exchanged.

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 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.

3.7. Operational Requirements

The exchange of data between both systems is not fully autonomous in the provisional solution, this means it requires operators and procedures to operationalise the link.

4. AVAILABILITY PROVISIONS

4.1. Communication Availability Design

The architecture for the provisional solution is fundamentally an ICT infrastructure and software that allows the communication between the ETS of Switzerland and the EU ETS. Ensuring high levels of availability, integrity and confidentiality of this flow of data therefore becomes an essential aspect to consider in the design of the provisional solution and the permanent registry link. Being a project in which 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

The general provisions chapter of this document details the architectural building blocks. On the ICT infrastructure side, the provisional linking sets up a resilient VPN network (or equivalent) 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, it is not available.

Service resilience

In the provisional solution, data exchanges between Parties occur at predefined timeslots throughout the year. 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 significant time windows to perform each step;

– The software modules for the provisional solution 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 in, 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 provisional solution 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 provisional solution 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 test first, followed by end-to-end connectivity validation prior to beginning 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 into 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 both Parties 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 are triggered individually by either Party and concluding the tests requires the cooperation of 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 (or equivalent secure transport network) 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 at 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 both Parties at each end and as detailed in sections 5.4, 'Security Testing Guidelines', and 5.5, 'Risk Assessment Provisions'.

Only after each of the four phases/blocks have ended with a predictable results can the provisional link 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 in 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 provided for 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 communication channels.

– Application monitoring: the provisional 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 registry of Switzerland 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 is meant to be used to perform integration tests by both Parties.

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

As for the VPN layout, this is set up in two different environments, one for PROD, another independent one for ACC and TEST.

5. CONFIDENTIALITY AND INTEGRITY PROVISIONS

Security Mechanisms and Procedures provide for a two-person method (4-eye principle) for operations occurring in the link between the Union Registry and the Swiss registry. The two-person method 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 also includes 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 to 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 to performing both static and dynamic analysis.

In the case of dynamic analysis (like penetration testing), both Parties commit to restricting the evaluations ordinarily to the test and acceptance environments (as defined in section 4.3, 'Acceptance/Testing environments'). Exceptions to this policy are subject to the approval of both Parties.

Before being deployed in the production environment, every software module of the link (as defined in section 3.1, 'Architecture of the communication link') shall be security tested.

Testing infrastructure must be separated at both network and infrastructure levels from the production infrastructure. The security tests required to check compliance with security requirements are carried out within the testing infrastructure.

5.2. Link Suspension and Reactivation Provisions

Where there is a suspicion that the security of the registry of Switzerland, the SSTL, the Union registry or the EUTL has been compromised, either Party shall immediately inform the other and suspend the link between the SSTL and the EUTL.

The procedures for information sharing, for a decision to suspend and for a 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 the Agreement may happen due to:

– Administrative reasons (for example, maintenance), which are planned;

– Security reasons (or IT infrastructure breakdowns), which are unplanned.

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

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

The decision to suspend the registry link, whether it is planned or unplanned, will be taken in accordance with the Change Management or Security Incident Management procedure of the COP.

Communication Reactivation

A decision to reactivate the registry link will be taken in the manner detailed in the COP and in any case not before the successful completion of the security testing procedures as detailed in sections 5.4, 'Security testing guidelines', and 4.2, 'Initialisation, Communication, Re-activation and Testing Plan'.

5.3. Security Breach Provisions

A security breach is considered to be 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 of the system.

Information directly related to the security breach will be considered to be sensitive, marked 'ETS CRITICAL' and handled in accordance with the handling instructions, unless specified otherwise.

Every security breach will be handled in accordance with 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, security testing shall be performed on the current system, taking into account 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 the 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 shall be fixed. Testing is performed according to the method outlined in section 5.4.1, using an 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 a subcontractor of the developer;

– Has signed Non-Disclosure Agreement to keep the results confidential and to handle them at the 'ETS CRITICAL' level in accordance with handling instructions.