Conseil de
l'Union européenne

Bruxelles, le 17 juin 2024
(OR. en)

10038/24
ADD 1

Dossier interinstitutionnel:
2024/0067(NLE)

ENV 530
CLIMA 207
ENER 236
IND 263
COMPET 563
MI 512
ECOFIN 586
TRANS 235
AELE 42
CH 12

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	Projet de DÉCISION DU COMITÉ MIXTE INSTITUÉ PAR L'ACCORD ENTRE L'UNION EUROPÉENNE ET LA CONFÉDÉRATION SUISSE SUR LE COUPLAGE DE LEURS SYSTÈMES D'ÉCHANGE DE QUOTAS D'ÉMISSION DE GAZ À EFFET DE SERRE en ce qui concerne la modification de l'annexe II de l'accord et des procédures opérationnelles communes et des normes techniques de couplage

PROJET DE

DÉCISION N° 1/2024
DU COMITÉ MIXTE INSTITUÉ PAR L'ACCORD
ENTRE L'UNION EUROPÉENNE
ET LA CONFÉDÉRATION SUISSE
SUR LE COUPLAGE DE LEURS SYSTÈMES D'ÉCHANGE DE QUOTAS
D'ÉMISSION DE GAZ À EFFET DE SERRE

du …

en ce qui concerne la modification de l'annexe II de l'accord
et des procédures opérationnelles communes
et des normes techniques de couplage

LE COMITÉ MIXTE,

vu l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre[1] (ci-après dénommé "accord"), et notamment son article 9 et son article 13, paragraphe 2,

[1] JO UE L 322 du 7.12.2017, p. 3.

considérant ce qui suit:

(1) La décision n° 2/2019 du comité mixte[2] a prévu une solution provisoire pour rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse.

(2) Lors de sa troisième réunion, le comité mixte est convenu de la nécessité d'analyser le rapport coût-efficacité d'un couplage permanent entre le registre de l'Union et le registre de la Suisse.

(3) Lors de cinquième réunion, le comité mixte a approuvé le rapport présenté par le groupe de travail institué par les décisions n° 1/2020[3] et n° 2/2020[4] du comité mixte. Dans ce rapport, le groupe de travail a analysé et recommandé une approche pour la mise en œuvre du couplage permanent entre le registre de l'Union et le registre de la Suisse.

---

[2] Décision n° 2/2019 du comité mixte institué par l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 5 décembre 2019 portant modification des annexes I et II de l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre [2020/1359] (JO UE L 314 du 29.9.2020, p. 68).

[3] Décision n° 1/2020 du comité mixte institué par l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 5 novembre 2020 relative à l'adoption de procédures opérationnelles communes (POC) [2021/1033] (JO UE L 226 du 25.6.2021, p. 2).

[4] Décision n° 2/2020 du comité mixte institué par l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 5 novembre 2020 portant modification des annexes I et II de l'accord et adoption de normes techniques de couplage (NTC) [2021/1034] (JO UE L 226 du 25.6.2021, p. 16).

(4) Pour tenir compte des exigences techniques relatives au couplage permanent entre le registre de l'Union et le registre de la Suisse, ainsi que pour rationaliser les dispositions de l'annexe II de l'accord à la lumière des évolutions technologiques, il convient de modifier l'annexe II de l'accord.

(5) Pour garantir la cohérence des procédures opérationnelles communes et des normes techniques de couplage avec l'annexe II de l'accord, il y a lieu de modifier ces documents également,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. L'annexe II de l'accord est remplacée par le texte figurant à l'annexe I de la présente décision.

2. Les procédures opérationnelles communes visées à l'article 3, paragraphe 6, de l'accord figurent à l'annexe II de la présente décision. Elles remplacent les procédures opérationnelles communes figurant à l'annexe de la décision n° 1/2020.

3. Les normes techniques de couplage visées à l'article 3, paragraphe 7, de l'accord figurent à l'annexe III de la présente décision. Elles remplacent les normes techniques de couplage figurant à l'annexe de la décision n° 2/2020.

Article 2

La présente décision entre en vigueur le jour de son adoption.

Fait à ..., le

Par le comité mixte

Le secrétaire pour l'Union européenne *Le président* *Le secrétaire pour la Suisse*

ANNEXE I

"ANNEXE II

NORMES TECHNIQUES DE COUPLAGE

Afin de rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse, une solution provisoire a été mise en place en 2020. À partir de 2023, le couplage des registres entre les deux systèmes d'échange de quotas d'émission prendra progressivement la forme d'un couplage permanent des registres dont la mise en œuvre est prévue pour 2024 au plus tard, et qui permettra aux marchés couplés, en ce qui concerne les bénéfices tirés de la liquidité de marché et l'exécution des transactions entre les deux systèmes couplés, de fonctionner d'une manière équivalente à un seul marché composé de deux systèmes et donnera aux acteurs du marché la possibilité d'agir comme s'il s'agissait d'un seul marché, soumis uniquement aux dispositions réglementaires individuelles des parties.

Les normes techniques de couplage précisent:

– l'architecture du lien de communication;

– les communications entre le SSTL et l'EUTL;

– la sécurité du transfert des données;

– la liste des fonctions (transactions, rapprochement, etc.);

– la définition de la couche de transport;

– les normes d'archivage des données;

– les modalités opérationnelles (service d'appel, assistance);

– le plan d'activation de communication et la procédure d'essai;

– la procédure d'essai de sécurité.

Les normes techniques de couplage prévoient que les administrateurs doivent prendre des mesures raisonnables pour s'assurer que le SSTL, l'EUTL et le lien sont opérationnels 24 heures sur 24 et 7 jours sur 7 et que les interruptions du fonctionnement du SSTL, de l'EUTL et du lien sont limitées le plus possible.

Les normes techniques de couplage énoncent des exigences supplémentaires en matière de sécurité pour le registre suisse, le SSTL, le registre de l'Union et l'EUTL et sont documentées dans un "plan de gestion de la sécurité". Les normes techniques de couplage prévoient notamment ce qui suit:

– en cas de suspicion d'atteinte à la sécurité du registre suisse, du SSTL, du registre de l'Union ou de l'EUTL, les deux parties s'informent immédiatement et suspendent immédiatement le lien entre le SSTL et l'EUTL;

– en cas de faille de sécurité, les parties s'engagent à s'échanger immédiatement les informations concernées. Dans la mesure où les détails techniques sont disponibles, un rapport décrivant l'incident (date, cause, conséquences, mesures correctives) est partagé entre l'administrateur du registre suisse et l'administrateur central de l'Union dans les 24 heures suivant la faille de sécurité.

La procédure d'essai de sécurité prévue dans les normes techniques de couplage est exécutée avant que le lien de communication entre le SSTL et l'EUTL ne soit établi et lorsqu'une nouvelle version ou édition du SSTL ou de l'EUTL est nécessaire.

Les normes techniques de couplage prévoient deux environnements d'essai en plus de l'environnement de production: un environnement d'essai développeur et un environnement d'acceptation.

Par l'intermédiaire de l'administrateur du registre suisse et de l'administrateur central de l'Union, les parties fournissent la preuve qu'une évaluation indépendante de la sécurité de leurs systèmes a été effectuée au cours des 12 derniers mois, conformément aux exigences de sécurité établies dans les normes techniques de couplage. Des essais de sécurité, et plus précisément des essais d'intrusion, sont effectués sur toutes les nouvelles versions majeures du logiciel, conformément aux exigences de sécurité énoncées dans les normes techniques de couplage. L'essai d'intrusion n'est pas effectué par le développeur du logiciel ni par un sous-traitant du développeur du logiciel.

ANNEXE II

PROCÉDURES OPÉRATIONNELLES COMMUNES (POC)
ÉTABLIES CONFORMÉMENT À L'ARTICLE 3, PARAGRAPHE 6, DE L'ACCORD
ENTRE L'UNION EUROPÉENNE ET LA CONFÉDÉRATION SUISSE
SUR LE COUPLAGE DE LEURS SYSTÈMES D'ÉCHANGE DE QUOTAS
D'ÉMISSION DE GAZ À EFFET DE SERRE

Procédures applicables au couplage permanent des registres

Table des matières

1. GLOSSAIRE 5

2. INTRODUCTION 6

2.1. Champ d'application 7

2.2. Destinataires 8

3. APPROCHE ET NORMES 8

4. GESTION DES INCIDENTS 9

4.1. Détection et enregistrement des incidents 10

4.2. Classification et support initial 11

4.3. Enquête et diagnostic 11

4.4. Résolution et rétablissement du service 12

4.5. Clôture de l'incident 13

5. GESTION DES PROBLÈMES 14

5.1. Identification et enregistrement du problème 14

5.2. Hiérarchisation des problèmes 14

5.3. Enquête et diagnostic 15

5.4. Résolution 15

5.5. Clôture du problème 15

6. EXÉCUTION DES DEMANDES 16

6.1. Introduction de la demande 16

6.2. Enregistrement et analyse de la demande 16

6.3. Approbation de la demande 16

6.4. Exécution de la demande 17

6.5. Remontée des demandes 17

6.6. Vérification de l'exécution des demandes 18

6.7. Clôture de la demande 18

7. GESTION DES CHANGEMENTS 18

7.1. Demande de changement 19

7.2. Évaluation et planification des changements 19

7.3. Approbation des changements 20

7.4. Exécution des changements 20

8. GESTION DES MISES EN PRODUCTION 20

8.1. Planification de la mise en production 21

8.2. Construction et test du package de mise en production 22

8.3. Préparation du déploiement 22

8.4. Retour en arrière de la mise en production 23

8.5. Vérification et clôture de la mise en production 23

9. GESTION DES INCIDENTS DE SÉCURITÉ 24

9.1. Catégorisation des incidents liés à la sécurité de l'information 25

9.2. Traitement des incidents liés à la sécurité de l'information 25

9.3. Caractérisation des incidents de sécurité 26

9.4. Analyse des incidents de sécurité 26

9.5. Évaluation de la gravité de l'incident de sécurité, remontée de l'incident et établissement d'un rapport 26

9.6. Rapport de réaction à un incident de sécurité 26

9.7. Suivi, renforcement des capacités et amélioration continue 27

10. GESTION DE LA SÉCURITÉ DE L'INFORMATION 28

10.1. Caractérisation des informations sensibles 28

10.2. Niveaux de sensibilité des ressources d'information 28

10.3. Désignation du propriétaire de la ressource d'information 29

10.4. Enregistrement des informations sensibles 29

10.5. Traitement des informations sensibles 30

10.6. Gestion des accès 31

10.7. Gestion des certificats/clés 32

1. GLOSSAIRE

Tableau 1-1 Sigles et définitions

Sigle/Terme	Définition
Autorité de certification (AC)	Entité chargée de délivrer des certificats numériques
CH	Confédération suisse
SEQE	Système d'échange de quotas d'émission
UE	Union européenne
IMT	Équipe de gestion des incidents
Ressource d'information	Information utile à une entreprise ou une organisation
TI	Technologies de l'information
ITIL	Bibliothèque pour l'infrastructure des technologies de l'information
ITSM	Gestion des services informatiques
NTC	Normes techniques de couplage
Registre	Système de comptabilisation des quotas délivrés au titre du SEQE, qui conserve la trace des changements de propriété des quotas détenus sur des comptes électroniques
DDC	Demande de changement
LIS	Liste d'informations sensibles
DDS	Demande de service
Wiki	Site web qui permet aux utilisateurs d'échanger des informations et des connaissances en ajoutant ou en adaptant directement des contenus au moyen d'un logiciel de navigation

2. INTRODUCTION

L'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 23 novembre 2017 (ci-après dénommé "accord") prévoit la reconnaissance mutuelle des quotas d'émission qui peuvent être utilisés à des fins de conformité dans le cadre du système d'échange de quotas d'émission de l'Union (ci-après dénommé "SEQE de l'UE") ou du système d'échange de quotas d'émission de la Suisse (ci-après dénommé "SEQE de la Suisse"). Pour rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse, un lien direct est établi entre le journal des transactions de l'Union européenne (EUTL) du registre de l'Union et le journal complémentaire des transactions suisse (SSTL) du registre suisse, ce qui permettra le transfert de registre à registre des quotas d'émission délivrés au titre de chaque SEQE (article 3, paragraphe 2, de l'accord). Afin de rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse, une solution provisoire a été mise en place en 2020. À partir de 2023, le couplage des registres entre les deux systèmes d'échange de quotas d'émission prendra progressivement la forme d'un couplage permanent des registres, dont la mise en œuvre est prévue pour 2024 au plus tard, et qui permettra aux marchés couplés, en ce qui concerne les bénéfices tirés de la liquidité de marché et l'exécution des transactions entre les deux systèmes couplés, de fonctionner d'une manière équivalente à un seul marché composé de deux systèmes et donnera aux acteurs du marché la possibilité d'agir comme s'il s'agissait d'un seul marché, soumis uniquement aux dispositions réglementaires individuelles des parties (annexe II de l'accord).

Conformément à l'article 3, paragraphe 6, de l'accord, l'administrateur du registre suisse et l'administrateur central de l'Union établissent des procédures opérationnelles communes (POC) concernant les sujets techniques ou d'une autre nature nécessaires au fonctionnement du couplage et tenant compte des priorités de la législation interne. Les POC établies par les administrateurs prennent effet une fois qu'elles ont été adoptées par décision du comité mixte.

Les POC ont été adoptées par le comité mixte en vertu de sa décision n° 1/2020. Les POC mises à jour, telles qu'elles sont décrites dans le présent document, seront adoptées par le comité mixte en vertu de sa décision n° 1/2024. Conformément à la présente décision et aux demandes du comité mixte, l'administrateur du registre suisse et l'administrateur central de l'Union ont élaboré et mettront à jour de nouvelles lignes directrices techniques visant à rendre opérationnel le couplage et à veiller à ce que celles-ci soient constamment adaptées au progrès technique et aux nouvelles exigences en matière de sécurité et de sûreté du couplage, ainsi qu'au fonctionnement efficace et efficient de celui-ci.

2.1. Champ d'application

Le présent document représente la conception commune des parties à l'accord en ce qui concerne l'établissement des procédures de base régissant le couplage entre les registres du SEQE de l'UE et du SEQE de la Suisse. Il présente les procédures générales requises pour le fonctionnement du couplage, mais des lignes directrices techniques plus détaillées seront nécessaires pour rendre ce couplage effectif.

Des spécifications techniques devront être adoptées pour que le couplage devienne véritablement opérationnel et pour en assurer le bon fonctionnement. Conformément à l'article 3, paragraphe 7, de l'accord, ces aspects sont décrits en détail dans le document relatif aux normes techniques de couplage (NTC) qui doit être adopté séparément par décision du comité mixte.

L'objectif des POC est de faire en sorte que les services informatiques liés au fonctionnement du couplage entre les registres du SEQE de l'UE et du SEQE de la Suisse soient assurés de manière efficace et efficiente, notamment pour répondre aux demandes de service, remédier aux interruptions de service, résoudre les problèmes et exécuter les opérations de routine conformément aux normes internationales en matière de gestion des services informatiques.

Pour le couplage permanent des registres, seules sont nécessaires les POC suivantes, décrites dans le présent document:

– Gestion des incidents;

– Gestion des problèmes;

– Exécution des demandes;

– Gestion des changements;

– Gestion des mises en production;

– Gestion des incidents de sécurité;

– Gestion de la sécurité de l'information.

2.2. Destinataires

Les destinataires des présentes POC sont les équipes de support du registre de l'UE et du registre suisse.

3. APPROCHE ET NORMES

Les principes suivants valent pour toutes les POC:

– l'UE et la Confédération suisse conviennent de définir les POC sur la base d'ITIL ["Information Technology Infrastructure Library" (Bibliothèque pour l'infrastructure des technologies de l'information), version 4]. Les pratiques issues de ce référentiel sont reprises et adaptées aux besoins spécifiques liés au couplage permanent des registres;

– la communication et la coordination entre les deux parties qui sont nécessaires à l'exécution des POC s'effectuent par le truchement des centres de services du registre suisse et du registre de l'UE. Les tâches sont toujours assignées au sein d'une seule partie;

– en cas de désaccord sur la manière d'aborder une POC, les deux centres de services analysent et règlent la question entre eux. Si aucun accord ne peut être trouvé, la recherche d'une solution commune est transférée au niveau supérieur;

Niveaux successifs de traitement	UE	CH
1er niveau	Centre de services de l'UE	Centre de services suisse
2e niveau	Responsable des opérations de l'UE	Gestionnaire des applications du registre suisse
3e niveau	Comité mixte (qui peut déléguer cette responsabilité en vertu de l'article 12, paragraphe 5, de l'accord)	
4e niveau	Comité mixte, si le 3e niveau est délégué	

– chaque partie est libre de déterminer les procédures applicables au fonctionnement de son propre système de registre, en tenant compte des exigences et des interfaces liées à ces POC;

– un outil de gestion des services informatiques (ITSM) est utilisé à l'appui des POC, en particulier celles relatives à la gestion des incidents, à la gestion des problèmes et à l'exécution des demandes, et pour la communication entre les parties;

– en outre, l'échange d'informations par courrier électronique est autorisé;

– les deux parties veillent à ce que les exigences en matière de sécurité de l'information soient respectées, conformément aux instructions relatives au traitement.

4. GESTION DES INCIDENTS

Le processus de gestion des incidents a pour objectif de rétablir le plus vite possible le niveau de fonctionnement normal des services informatiques après un incident et de limiter au maximum l'interruption des activités.

La gestion des incidents devrait également permettre de garder une trace des incidents pour faciliter la production de rapports, et se combiner à d'autres processus en vue d'une amélioration continue du système.

D'un point de vue global, la gestion des incidents recouvre les activités suivantes:

– détection et enregistrement des incidents;

– classification et support initial;

– enquête et diagnostic;

– résolution et rétablissement du service;

– clôture de l'incident.

Tout au long du cycle de vie de l'incident, le processus de gestion des incidents doit permettre d'assurer le traitement continu de la propriété, la surveillance, le suivi et la communication.

4.1. Détection et enregistrement des incidents

Un incident peut être détecté par un groupe de support, au moyen d'outils de suivi automatisés ou lors d'une surveillance de routine effectuée par le personnel technique.

Une fois détecté, l'incident doit être enregistré et un identificateur unique doit lui être attribué afin de permettre le suivi et la surveillance de l'incident. L'identificateur unique d'un incident est l'identificateur attribué dans le système de tickets commun par le centre de services de la partie (UE ou CH) qui a signalé l'incident; il doit figurer dans toutes les communications liées à l'incident.

Pour tous les incidents, le point de contact devrait être le centre de services de la partie qui a ouvert le ticket.

4.2. Classification et support initial

La classification des incidents vise à comprendre et à repérer quel système et/ou service est touché par un incident et dans quelle mesure. Pour être efficace, la classification doit assigner l'incident à la bonne ressource du premier coup, de façon à permettre une résolution plus rapide des incidents.

La phase de classification vise à établir le type d'incident et l'ordre de priorité de celui-ci en fonction de ses répercussions et de son degré d'urgence, afin qu'il soit traité selon les délais prescrits pour chaque niveau de priorité.

Si l'incident est susceptible de porter atteinte à la confidentialité ou à l'intégrité de données sensibles et/ou à la disponibilité du système, il est également déclaré comme un incident lié à la sécurité et traité selon la procédure définie au chapitre "Gestion des incidents de sécurité" du présent document.

Lorsque c'est possible, le centre de services qui a ouvert le ticket effectue un premier diagnostic. Pour ce faire, il vérifie si l'incident correspond à une erreur connue. Si oui, la méthode pour résoudre ou contourner le problème est déjà connue et documentée.

Si le centre de services parvient à résoudre l'incident, il clôture ce dernier à ce stade, le but premier de la gestion des incidents (soit le rétablissement rapide du service pour l'utilisateur final) ayant été atteint. S'il n'y parvient pas, il transfère l'incident au groupe de résolution approprié pour une enquête et un diagnostic plus poussés.

4.3. Enquête et diagnostic

Le processus d'enquête et de diagnostic est appliqué lorsque l'incident n'a pas pu être résolu par le centre de services dans le cadre du diagnostic initial et a donc été transféré au niveau de traitement approprié. La remontée des incidents fait partie intégrante du processus d'enquête et de diagnostic.

Une pratique courante à ce stade consiste à tenter de reproduire l'incident dans des conditions contrôlées. L'important, lorsque le processus d'enquête et de diagnostic est appliqué, est de bien comprendre dans quel ordre les événements qui ont conduit à l'incident se sont produits.

La remontée de l'incident intervient lorsqu'il apparaît que celui-ci ne peut être résolu au niveau de support actuel et doit être transféré à un groupe de support de plus haut niveau ou à l'autre partie. Cette remontée peut être horizontale (fonctionnelle) ou verticale (hiérarchique).

Le centre de services qui a enregistré l'incident et lancé la procédure de résolution est chargé de transférer l'incident à la ressource appropriée, et assure le suivi global de l'incident et son assignation.

La partie à laquelle l'incident a été transféré est chargée de veiller à l'exécution en temps utile des actions demandées et de fournir un retour d'information à son propre centre de services.

4.4. Résolution et rétablissement du service

Le processus de résolution de l'incident et de rétablissement du service est appliqué une fois que l'incident est pleinement compris. La résolution d'un incident signifie qu'on a trouvé un moyen de remédier au problème. L'application de cette solution correspond à la phase de rétablissement du service.

Une fois l'interruption de service résolue par les ressources appropriées, l'incident est renvoyé au centre de services qui a enregistré l'incident; ce dernier vérifie auprès de l'auteur du signalement de l'incident que l'erreur a été corrigée et que l'incident peut être clôturé. Les résultats du traitement de l'incident sont consignés en vue d'une utilisation future.

Le rétablissement du service peut être exécuté par le personnel de support informatique ou moyennant une série d'instructions fournies à l'utilisateur.

4.5. Clôture de l'incident

Dernière étape du processus de gestion des incidents, la clôture intervient peu après la résolution de l'incident.

La liste des opérations qui doivent être exécutées durant la phase de clôture comprend en particulier:

– la vérification de la catégorisation initiale de l'incident;

– la saisie complète de toutes les informations se rapportant à l'incident;

– la documentation complète de l'incident et la mise à jour correspondante de la base de connaissances;

– la communication d'un message approprié à chaque partie prenante directement ou indirectement concernée par l'incident.

Un incident est formellement clôturé dès l'instant où la phase de clôture a été exécutée par le centre de services et communiquée à l'autre partie.

Une fois l'incident clôturé, il n'est pas rouvert. Si le même incident survient peu de temps après, l'incident initial n'est pas rouvert, un nouvel incident doit être créé.

Si l'incident fait l'objet d'un suivi à la fois par le centre de services de l'UE et par le centre de services suisse, il incombe au centre de services qui a ouvert le ticket de clôturer définitivement l'incident.

5. GESTION DES PROBLÈMES

Il convient d'appliquer cette procédure à chaque fois qu'un problème est détecté, déclenchant ainsi le processus de gestion des problèmes. La gestion des problèmes vise essentiellement à améliorer la qualité et à réduire le nombre d'incidents signalés. Un problème peut être la cause d'un ou de plusieurs incidents. Lorsqu'un incident est signalé, l'objectif du processus de gestion des incidents est de rétablir le service dans les plus brefs délais, éventuellement à l'aide de solutions de contournement. Lorsqu'un problème est enregistré, l'objectif est d'en trouver la cause profonde afin de déterminer quel changement permettra de garantir que ce problème et les incidents qui en découlent ne se produisent plus à l'avenir.

5.1. Identification et enregistrement du problème

Suivant la partie qui a ouvert le ticket, le point de contact pour toutes les questions liées au problème sera le centre de services de l'UE ou de la Confédération suisse.

L'identificateur unique d'un problème est l'identificateur attribué par l'outil de gestion des services informatiques (ITSM). Cet identificateur doit figurer dans toutes les communications liées au problème.

Le processus de gestion des problèmes peut être déclenché par un incident ou être lancé délibérément pour résoudre des défaillances détectées à un niveau quelconque du système.

5.2. Hiérarchisation des problèmes

Comme les incidents, les problèmes peuvent être catégorisés en fonction de leur gravité et de leur ordre de priorité afin de faciliter leur suivi, en tenant compte de l'impact et de la fréquence des incidents liés à ces problèmes.

5.3. Enquête et diagnostic

Chaque partie peut signaler un problème, et le centre de services de cette partie est alors chargé d'enregistrer le problème, de l'assigner à la ressource appropriée et d'en assurer le suivi global.

Le groupe de résolution auquel le problème a été transféré est chargé de le traiter dans les meilleurs délais et en communiquant avec le centre de services.

Les deux parties sont chargées, sur demande, de veiller à l'exécution des actions assignées et de fournir un retour d'information à leurs centres de services respectifs.

5.4. Résolution

Le groupe de résolution auquel le problème est assigné est chargé de résoudre ce dernier et de fournir des informations pertinentes au centre de services de sa propre partie.

Les résultats du traitement du problème sont consignés en vue d'une utilisation future.

5.5. Clôture du problème

Un problème est formellement clôturé lorsqu'il a été résolu par l'application du changement. La clôture du problème est exécutée par le centre de services qui a enregistré le problème et qui a informé le centre de services de l'autre partie.

6. EXÉCUTION DES DEMANDES

Le processus d'exécution des demandes correspond au traitement de bout en bout d'une demande de service nouveau ou existant, à partir du moment où elle est enregistrée et approuvée jusqu'au moment où elle est clôturée. Les demandes de service sont généralement simples, prédéfinies, reproductibles, fréquentes, pré-approuvées et en rapport avec les procédures.

Les principales étapes à suivre sont décrites ci-après.

6.1. Introduction de la demande

Les informations relatives à une demande de service sont soumises au centre de services de l'UE ou au centre de services suisse par courrier électronique, par téléphone ou par l'intermédiaire de l'outil de gestion des services informatiques (ITSM) ou de tout autre moyen de communication reconnu.

6.2. Enregistrement et analyse de la demande

Pour toutes les demandes de service, le point de contact devrait être le centre de services de l'UE ou le centre de services suisse, selon la partie qui est à l'origine de la demande de service. Le centre de services concerné est chargé d'enregistrer et d'analyser avec la diligence requise la demande de service.

6.3. Approbation de la demande

L'agent du centre de services de la partie qui est à l'origine de la demande de service vérifie si une approbation quelconque de l'autre partie est nécessaire et, si oui, demande cette approbation. Si la demande de service n'est pas approuvée, le centre de services met à jour et clôture le dossier.

6.4. Exécution de la demande

Cette étape correspond au traitement effectif et efficace des demandes de service. Il convient d'opérer une distinction entre les cas suivants:

– l'exécution de la demande de service ne concerne qu'une des parties. Dans ce cas, cette partie émet les ordres d'exécution et coordonne l'ensemble du processus:

– l'exécution de la demande de service concerne tant l'UE que la Confédération suisse. Dans ce cas, les centres de services émettent les ordres d'exécution dans les domaines qui relèvent de leur compétence. Le traitement de la demande de service fait l'objet d'une coordination entre les deux centres de services. La responsabilité globale du processus incombe au centre de services qui a reçu et introduit la demande de service.

Une fois la demande de service exécutée, son statut doit être modifié en conséquence.

6.5. Remontée des demandes

Au besoin, le centre de services peut transférer les demandes de service pendantes à la ressource appropriée (tierce partie).

Les transferts se font vers les tierces parties respectives: le centre de services de l'UE devra passer par le centre de services suisse pour le transfert d'une demande à une tierce partie suisse, et vice versa.

La tierce partie à laquelle la demande de service a été transférée est chargée de traiter celle-ci dans les meilleurs délais et en communiquant avec le centre de services qui a transféré la demande de service.

Le centre de services qui a enregistré la demande de service est chargé du suivi global de la demande et de l'assignation d'une demande de service.

6.6. Vérification de l'exécution des demandes

Le centre de services responsable soumet le dossier de la demande de service à un dernier contrôle de qualité avant de le clôturer. Le but est de s'assurer que la demande de service a bien été traitée et que toutes les informations requises pour décrire le cycle de vie de la demande ont été fournies de manière suffisamment détaillée. En outre, les résultats du traitement de la demande sont consignés en vue d'une utilisation future.

6.7. Clôture de la demande

Si les parties auxquelles la demande de service a été assignée conviennent que celle-ci a été exécutée et que le demandeur considère que l'affaire est réglée, la demande est dite "clôturée".

Une demande de service est formellement clôturée dès l'instant où le centre de services qui a enregistré la demande de service a exécuté la phase de clôture de la demande et informé le centre de services de l'autre partie.

7. GESTION DES CHANGEMENTS

L'objectif est de faire en sorte que des méthodes et des procédures normalisées soient utilisées pour prendre en charge de manière efficace et rapide tous les changements intéressant l'infrastructure informatique, afin de réduire au minimum le nombre des incidents et leurs conséquences sur le service. Les changements de l'infrastructure informatique peuvent constituer une réponse à des problèmes ou à des exigences imposées de l'extérieur, comme des modifications de la législation, ou être mis en œuvre de manière proactive dans le cadre d'efforts visant à améliorer l'efficience et l'efficacité ou à permettre des initiatives "business" ou en rendre compte.

Le processus de gestion des changements comprend différentes étapes au cours desquelles sont enregistrées toutes les informations relatives à une demande de changement, en vue de permettre un suivi ultérieur. Ces processus garantissent que le changement sera validé et testé avant la phase de déploiement. Le processus de gestion des mises en production assure le bon déroulement du déploiement.

7.1. Demande de changement

Une demande de changement (DDC) est soumise à l'équipe de gestion des changements pour validation et approbation. Pour toutes les demandes de changement, le point de contact devrait être le centre de services de l'UE ou le centre de services suisse, en fonction de la partie qui est à l'origine de la demande. Ce centre de services sera chargé d'enregistrer la demande et de l'analyser avec la diligence requise.

Les demandes de changement peuvent avoir pour origine:

– un incident entraînant un changement;

– un problème existant qui se traduit par un changement;

– un nouveau changement demandé par un utilisateur final;

– un changement résultant d'une maintenance continue;

– une modification de la législation.

7.2. Évaluation et planification des changements

Cette étape traite des activités d'évaluation et de planification des changements. Elle comprend des activités de hiérarchisation et de planification qui visent à réduire au minimum les risques et les incidences.

Si l'exécution de la DDC concerne à la fois l'UE et la Suisse, la partie qui a enregistré la DDC vérifie l'évaluation et la planification du changement avec l'autre partie.

7.3. Approbation des changements

Toute demande de changement enregistrée doit être approuvée au niveau de traitement approprié.

7.4. Exécution des changements

L'exécution des changements fait partie de la gestion des mises en production. Les équipes de gestion des mises en production des deux parties suivent leurs propres procédures qui consistent en activités de planification et en tests. La vérification du changement intervient une fois que son exécution est achevée. Pour faire en sorte que tout se déroule comme prévu, le processus existant de gestion des changements est constamment revu et mis à jour chaque fois que nécessaire.

8. GESTION DES MISES EN PRODUCTION

Une mise en production représente un ou plusieurs changements apportés à un service informatique, réunis dans un plan de mise en production, qui doivent être autorisés, préparés, construits, testés et déployés simultanément. Une mise en production peut correspondre à la correction d'un bogue, à un changement de matériel ou d'autres composants, à des changements de logiciels, à des mises à niveau de versions d'applications, à des modifications de la documentation et/ou des processus. Le contenu de chaque mise en production est géré, testé puis déployé comme une entité unique.

La gestion des mises en production a pour but de planifier, construire, tester et valider, et de donner la capacité de fournir les services désignés, qui permettront de satisfaire les exigences des parties prenantes et de réaliser les objectifs visés. Les critères d'acceptation de tous les changements apportés au service seront définis et documentés lors de la coordination de la conception et fournis aux équipes de gestion des mises en production.

La mise en production consiste en général en un certain nombre de solutions à des problèmes et d'améliorations d'un service. Elle contient les logiciels nouveaux ou modifiés requis et tout matériel nouveau ou modifié nécessaire à l'exécution des changements approuvés.

8.1. Planification de la mise en production

La première étape du processus consiste à regrouper les changements autorisés dans des packages de mise en production et à définir l'ampleur et le contenu des mises en production. Sur la base de ces informations, le sous-processus de planification de la mise en production consiste à élaborer un calendrier pour la construction, les tests et le déploiement de la mise en production.

La planification doit définir:

– l'ampleur et le contenu de la mise en production;

– l'évaluation des risques et le profil de risque de la mise en production;

– le client/les utilisateurs concernés par la mise en production;

– l'équipe responsable de la mise en production;

– la stratégie de livraison et de déploiement;

– les ressources pour la mise en production et son déploiement.

Les deux parties s'informent mutuellement de leur planification des mises en production et de leurs fenêtres de maintenance. Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent la planification et définissent une fenêtre de maintenance commune.

8.2. Construction et test du package de mise en production

L'étape de construction et de test du processus de gestion des mises en production vise à établir les modalités d'exécution de la mise en production ou du package de mise en production, en veillant à rester dans des environnements sous contrôle avant d'apporter tout changement à la production, ainsi qu'à tester l'ensemble des changements dans tous les environnements mis en production.

Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent les plans de livraison et de tests, et notamment les aspects suivants:

– comment et à quel moment les unités de mise en production et les composants de service sont livrés;

– quels sont les délais d'exécution habituels; que se passe-t-il en cas de retard;

– comment suivre l'avancement de la livraison et obtenir une confirmation;

– les indicateurs permettant d'assurer le suivi et de déterminer la réussite du déploiement d'une mise en production;

– les cas de test courants pour les fonctionnalités et les changements concernés.

À la fin de ce sous-processus, tous les composants requis de la mise en production sont prêts à entrer dans la phase de déploiement proprement dit.

8.3. Préparation du déploiement

Le sous-processus de préparation garantit que les plans de communication sont définis correctement et que les notifications sont prêtes à être envoyées à toutes les parties prenantes et à tous les utilisateurs finals concernés, et que la mise en production est intégrée dans le processus de gestion des changements afin que tous les changements soient effectués de manière contrôlée et soient approuvés par les entités requises.

Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent les activités suivantes:

– enregistrement de la demande de changement pour programmer et préparer le déploiement dans l'environnement de production;

– création du plan d'exécution;

– approche de retour en arrière, afin de pouvoir revenir à l'état antérieur en cas d'échec d'un déploiement;

– envoi de notifications à toutes les parties concernées;

– demande d'approbation de l'exécution de la mise en production au niveau de traitement approprié.

8.4. Retour en arrière de la mise en production

Si le déploiement a échoué ou si les tests ont permis de constater que le déploiement n'a pas abouti ou n'a pas satisfait aux critères d'acceptation/de qualité convenus, les équipes de gestion des mises en production de chaque partie devront rétablir l'état antérieur. Toutes les parties prenantes concernées devront être informées, y compris les utilisateurs finals concernés/ciblés. Dans l'attente d'une approbation, le processus peut être relancé à n'importe quelle étape précédente.

8.5. Vérification et clôture de la mise en production

Lors de la vérification d'un déploiement, les actions suivantes devraient être prévues:

– obtenir un retour d'information sur la satisfaction des clients et des utilisateurs et sur la qualité du service à la suite du déploiement (recueillir le retour d'information et en tenir compte pour l'amélioration continue du service);

– examiner les critères de qualité qui n'ont pas été remplis;

– vérifier que les actions, les corrections et changements nécessaires ont été menés à terme;

– s'assurer de l'absence de problèmes d'aptitude, de ressources, de capacité ou de performance à la fin du déploiement;

– vérifier que les problèmes, les erreurs et les solutions de contournement connues sont documentés et acceptés par le client, les utilisateurs finals, le soutien opérationnel et les autres parties concernées;

– assurer un suivi des incidents et des problèmes causés par le déploiement (fournir un soutien précoce aux équipes opérationnelles si la mise en production a entraîné une augmentation de la charge de travail);

– mettre à jour la documentation de support (c'est-à-dire les documents d'information techniques);

– transférer formellement le déploiement de la mise en production à l'exploitation des services;

– consigner les enseignements tirés;

– récupérer le document récapitulatif de la mise en production auprès des équipes d'implémentation;

– clôturer formellement la mise en production après avoir vérifié l'enregistrement de la demande de changement.

9. GESTION DES INCIDENTS DE SÉCURITÉ

La gestion des incidents de sécurité est un processus de traitement des incidents de sécurité qui permet de communiquer avec les parties prenantes susceptibles d'être concernées; d'évaluer et de hiérarchiser les incidents; de réagir pour remédier à tout manquement réel, suspecté ou potentiel relatif à la confidentialité, à la disponibilité ou à l'intégrité des ressources d'information sensibles.

9.1. Catégorisation des incidents liés à la sécurité de l'information

Tous les incidents ayant une incidence sur le couplage entre le registre de l'Union et le registre suisse sont analysés afin de déterminer un éventuel manquement relatif à la confidentialité, à l'intégrité ou à la disponibilité des informations sensibles enregistrées sur la liste des informations sensibles (LIS).

Le cas échéant, l'incident doit être caractérisé en tant qu'incident lié à la sécurité de l'information, immédiatement enregistré dans l'outil de gestion des services informatiques (ITSM) et géré comme tel.

9.2. Traitement des incidents liés à la sécurité de l'information

Les incidents de sécurité sont placés sous la responsabilité du 3e niveau de traitement et la résolution des incidents sera traitée par une équipe de gestion des incidents spécialisée.

L'équipe de gestion des incidents est chargée des actions suivantes:

– effectuer une première analyse, catégoriser l'incident et évaluer sa gravité;

– coordonner les actions entre toutes les parties prenantes, y compris la documentation complète de l'analyse de l'incident, les décisions prises pour remédier à l'incident et les éventuelles faiblesses constatées;

– en fonction de la gravité de l'incident de sécurité, faire appel en temps utile au niveau de traitement approprié pour information et/ou décision.

Dans le processus de gestion de la sécurité de l'information, toutes les informations concernant les incidents sont classées au niveau le plus élevé de sensibilité de l'information et, en tout état de cause, jamais en dessous du niveau "SENSITIVE: *SEQE*".

Dans le cas d'une enquête en cours et/ou d'une faiblesse susceptible d'être exploitée et jusqu'à la résolution du problème, les informations sont classées "SPECIAL HANDLING: *ETS Critical*".

9.3. Caractérisation des incidents de sécurité

En fonction du type d'événement de sécurité, le responsable de la sécurité de l'information détermine les organismes appropriés à associer et à inclure dans l'équipe de gestion des incidents.

9.4. Analyse des incidents de sécurité

L'équipe de gestion des incidents prend contact avec toutes les organisations concernées et les membres compétents de leurs équipes, selon qu'il convient, pour examiner l'incident. L'analyse permet de déterminer l'ampleur de la perte de confidentialité, d'intégrité ou de disponibilité d'une ressource d'information et d'en évaluer les conséquences pour toutes les organisations concernées. Ensuite sont définies les mesures initiales et les mesures de suivi à prendre pour remédier à l'incident et gérer son impact ainsi que l'impact de ces mesures sur les ressources.

9.5. Évaluation de la gravité de l'incident de sécurité, remontée de l'incident et établissement d'un rapport

L'équipe de gestion des incidents évalue la gravité de tout nouvel incident de sécurité après sa caractérisation en tant que tel et entreprend l'action immédiate requise en fonction du niveau de gravité.

9.6. Rapport de réaction à un incident de sécurité

L'équipe de gestion des incidents inclut les résultats de la maîtrise de l'incident et du rétablissement du service dans le rapport de réaction à un incident lié à la sécurité de l'information. Le rapport est remis au 3^{e} niveau de traitement par courrier électronique sécurisé ou par d'autres moyens de communication sécurisée mutuellement acceptés.

La partie responsable examine les résultats de la maîtrise de l'incident et du rétablissement du service, et:

– reconnecte le registre en cas de déconnexion préalable;

– communique des informations relatives à l'incident aux équipes des registres;

– clôture l'incident.

L'équipe de gestion des incidents devrait inclure (de façon sécurisée) des détails importants dans le rapport relatif aux incidents liés à la sécurité de l'information, afin de garantir la cohérence de l'enregistrement et de la communication et de permettre une action rapide et appropriée pour maîtriser l'incident. L'équipe de gestion des incidents soumet le rapport final relatif à l'incident lié à la sécurité de l'information en temps utile après son achèvement.

9.7. Suivi, renforcement des capacités et amélioration continue

L'équipe de gestion des incidents soumettra les rapports relatifs à tous les incidents de sécurité au 3e niveau de traitement. Les rapports seront utilisés à ce niveau de traitement pour déterminer les éléments suivants:

– les points faibles dans les contrôles de sécurité et/ou l'exploitation qui doivent être renforcés;

– le besoin éventuel de renforcement de cette procédure afin d'améliorer l'efficacité de la réaction aux incidents;

– les possibilités de formation et de renforcement des capacités pour améliorer encore la résilience des systèmes de registres aux incidents liés à la sécurité de l'information, réduire le risque de futurs incidents et limiter leur impact.

10. GESTION DE LA SÉCURITÉ DE L'INFORMATION

La gestion de la sécurité de l'information vise à garantir la confidentialité, l'intégrité et la disponibilité des informations et données classifiées et des services informatiques sensibles d'une organisation. Outre les composants techniques, y compris leur conception et tests (voir NTC), les procédures opérationnelles communes suivantes sont nécessaires pour satisfaire aux exigences de sécurité requises pour le couplage permanent des registres.

10.1. Caractérisation des informations sensibles

La sensibilité d'une information est évaluée en déterminant le niveau d'impact que pourrait avoir sur l'activité (par exemple, pertes financières, dégradation de l'image, violation de la loi, etc.) une atteinte à la sécurité en rapport avec cette information.

Les ressources d'information sensibles sont caractérisées d'après l'incidence qu'elles ont sur le couplage.

Le niveau de sensibilité de ces informations est évalué au moyen de l'échelle de sensibilité applicable à ce couplage, décrite en détail dans la section "Traitement des incidents liés à la sécurité de l'information" du présent document.

10.2. Niveaux de sensibilité des ressources d'information

Lors de sa caractérisation, la ressource d'information est classée en appliquant les règles suivantes:

– l'indication d'au moins un niveau ÉLEVÉ de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource en tant que "SPECIAL HANDLING: *ETS Critical*";

– l'indication d'au moins un niveau MOYEN de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource en tant que "SENSITIVE: *ETS*";

– l'indication d'un simple FAIBLE niveau de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource de la manière suivante: "Marquage UE: SENSITIVE: *ETS Joint Procurement*; Marquage CH: LIMITED: *SEQE*".

10.3. Désignation du propriétaire de la ressource d'information

Toutes les ressources d'information devraient avoir un propriétaire attitré. Les ressources d'information du SEQE qui font partie du couplage entre l'EUTL et le SSTL ou qui y sont associées devraient figurer sur une liste d'inventaire des ressources communes, tenue à jour par les deux parties. Les ressources d'information du SEQE qui sont étrangères au couplage entre le l'EUTL et le SSTL devraient figurer sur une liste d'inventaire des ressources tenue à jour par la partie concernée.

La propriété de chaque ressource d'information faisant partie du couplage entre l'EUTL et le SSTL ou qui y est associée doit être approuvée par les parties. Le propriétaire d'une ressource d'information est responsable de l'évaluation de la sensibilité de cette ressource.

Le propriétaire doit avoir le niveau de responsabilité approprié pour la valeur de la ou des ressources attribuées. La responsabilité du propriétaire concernant la ou les ressources et l'obligation lui incombant de maintenir le niveau requis de confidentialité, d'intégrité et de disponibilité devraient faire l'objet d'un accord et d'une formalisation.

10.4. Enregistrement des informations sensibles

Toutes les informations sensibles sont enregistrées sur la liste des informations sensibles (LIS).

Le cas échéant, le regroupement d'informations sensibles qui pourraient avoir un impact plus important que celui d'une seule information est pris en compte et est enregistré sur la LIS (par exemple, ensemble d'informations stockées dans la base de données du système).

La LIS n'est pas statique. Les menaces, les vulnérabilités, la probabilité ou les conséquences des incidents de sécurité liés aux ressources peuvent changer sans préavis, et de nouvelles ressources pourraient être introduites dans le fonctionnement des systèmes de registres.

Par conséquent, la LIS doit être réexaminée régulièrement, et toute nouvelle information jugée sensible doit être immédiatement enregistrée dans la LIS.

La LIS comprend au moins, pour chaque entrée, les informations suivantes:

– la description de l'information;

– le propriétaire de l'information;

– le niveau de sensibilité;

– une mention précisant si l'information contient des données à caractère personnel;

– des informations complémentaires si nécessaire.

10.5. Traitement des informations sensibles

Lorsqu'elles sont utilisées en dehors du couplage entre le registre de l'Union et le registre suisse, les informations sensibles sont traitées conformément aux instructions de traitement.

Les informations sensibles utilisées par le couplage entre le registre de l'Union et le registre suisse sont traitées conformément aux exigences de sécurité des parties.

10.6. Gestion des accès

L'objectif de la gestion des accès est d'accorder aux utilisateurs autorisés le droit d'utiliser un service, tout en empêchant l'accès des utilisateurs non autorisés. La gestion des accès est parfois également appelée "gestion des droits" ou "gestion de l'identité".

En ce qui concerne le couplage permanent des registres et son fonctionnement, les deux parties ont besoin d'avoir accès aux éléments suivants:

– wiki: environnement de collaboration pour l'échange d'informations communes telles que la planification des mises en production;

– outil de gestion des services informatiques (ITSM) pour la gestion des incidents et des problèmes (voir chapitre 3 "Approche et normes");

– systèmes d'échange de messages: chaque partie fournit un système sécurisé d'échange de messages pour la transmission des messages contenant les données de transaction.

L'administrateur du registre suisse et l'administrateur central de l'Union veillent à ce que les accès soient à jour, et font office de points de contact pour leurs parties en ce qui concerne les activités de gestion de l'accès. Les demandes d'accès sont traitées conformément aux procédures d'exécution des demandes.

10.7. Gestion des certificats/clés

Chaque partie est responsable de la gestion de ses propres certificats/clés (génération, enregistrement, stockage, installation, utilisation, renouvellement, révocation, sauvegarde et récupération des certificats/clés). Comme indiqué dans les normes techniques de couplage (NTC), seuls sont utilisés les certificats numériques délivrés par une autorité de certification qui bénéficie de la confiance des deux parties. Le traitement et le stockage des certificats/clés doivent respecter les dispositions prévues dans les instructions de traitement.

Toute révocation et/ou tout renouvellement de certificats et de clés est coordonné par les deux parties. Les demandes d'accès sont traitées conformément aux procédures d'exécution des demandes.

L'administrateur du registre suisse et l'administrateur central de l'Union échangeront les certificats/clés par des moyens de communication sécurisés conformément aux dispositions prévues dans les instructions de traitement.

Toute vérification des certificats/clés par tout moyen entre les parties est effectuée hors bande.

ANNEXE III

NORMES TECHNIQUES DE COUPLAGE (NTC)
ÉTABLIES CONFORMÉMENT À L'ARTICLE 3, PARAGRAPHE 7, DE L'ACCORD
ENTRE L'UNION EUROPÉENNE ET LA CONFÉDÉRATION SUISSE
SUR LE COUPLAGE DE LEURS SYSTÈMES D'ÉCHANGE DE QUOTAS
D'ÉMISSION DE GAZ À EFFET DE SERRE

Normes applicables au couplage permanent des registres

Table des matières

1. GLOSSAIRE 4

2. INTRODUCTION 6

2.1. Champ d'application 7

2.2. Destinataires 7

3. DISPOSITIONS GÉNÉRALES 8

3.1. Architecture du lien de communication 8

3.1.1. Échange de message 8

3.1.2. Message XML – Haut niveau de description 9

3.1.3. Fenêtres d'ingestion 9

3.1.4. Flux des messages de transaction 10

3.2. Sécurité du transfert des données 15

3.2.1. Pare-feu et interconnexion des réseaux 15

3.2.2. VPN (Réseau privé virtuel – *Virtual Private Network*) 16

3.2.3. Mise en œuvre de l'IPsec 16

3.2.4. Protocole de transfert sécurisé pour l'échange de messages 17

3.2.5. Signature et cryptage XML 17

3.2.6. Clés cryptographiques 17

3.3. Liste des fonctions dans le cadre du couplage 18

3.3.1. Transactions "business" 18

3.3.2. Protocole de rapprochement 19

3.3.3. Message de test 20

3.4. Exigences relatives à l'enregistrement des données 20

3.5. Prescriptions opérationnelles 22

4. DISPOSITIONS PERMETTANT DE GARANTIR LA DISPONIBILITÉ 23

4.1. Conception garantissant la disponibilité de la communication 23

4.2. Plan d'initialisation, de communication, de réactivation et de test 24

4.2.1. Tests des infrastructures TIC en interne 25

4.2.2. Tests de communication 26

4.2.3. Tests du système complet (de bout en bout) 26

4.2.4. Tests de sécurité 26

4.3. Environnements de validation/de test 27

5. DISPOSITIONS RELATIVES À LA CONFIDENTIALITÉ ET À L'INTÉGRITÉ 28

5.1. Infrastructure destinée aux tests de sécurité 29

5.2. Dispositions relatives à la suspension et à la réactivation du couplage 30

5.3. Dispositions relatives aux failles de sécurité 31

5.4. Lignes directrices relatives aux tests de sécurité 31

5.4.1. Logiciels 31

5.4.2. Infrastructure 32

5.5. Dispositions en matière d'évaluation des risques 32

1. GLOSSAIRE

Tableau 1-1 Sigles et définitions "business"

Sigle/Terme	Définition
Quota	Droit d'émettre une tonne équivalent dioxyde de carbone au cours d'une période donnée, valable uniquement aux fins du respect des exigences du SEQE de l'une ou l'autre des entités.
CH	Confédération suisse.
CHU	Type de quota fixe, également appelé CHU2 (en référence à la deuxième période d'engagement du protocole de Kyoto), émis par la CH.
CHUA	Quota suisse pour le secteur de l'aviation.
POC	Procédures opérationnelles communes. Procédures élaborées conjointement par les parties à l'accord afin de rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse.
ETR	Registre des échanges de quotas d'émission.
SEQE	Système d'échange de quotas d'émission.
UE	Union européenne.
EUA	Quota général de l'UE.
EUAA	Quota de l'UE pour le secteur de l'aviation.
EUCR	Registre consolidé de l'Union européenne.
EUTL	Journal des transactions de l'Union européenne.
Registre	Système de comptabilisation des quotas délivrés au titre du SEQE, qui conserve la trace des changements de propriété des quotas détenus sur des comptes électroniques.
SSTL	Journal complémentaire des transactions suisse.
Transaction	Processus d'inscription au registre comportant le transfert d'un quota d'un compte à un autre.
Système de journal des transactions	Le journal des transactions contient un enregistrement de chacune des transactions proposées d'un registre à l'autre.

Tableau 1-2 Sigles et définitions techniques

Sigle	Définition
Cryptographie asymétrique	Cryptographie utilisant des clés publiques et privées pour crypter et décrypter les données.
Autorité de certification (AC)	Entité chargée de délivrer des certificats numériques.
Clé cryptographique	Information qui détermine le résultat fonctionnel d'un algorithme de cryptage.
Décryptage	Processus inverse du processus de cryptage.
Signature numérique	Technique mathématique utilisée pour valider l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique.
Cryptage	Processus consistant à convertir des informations ou des données en un code, notamment en vue d'empêcher l'accès non autorisé.
Ingestion de fichier	Processus de lecture d'un fichier.
Pare-feu	Appareil ou logiciel de sécurisation du réseau qui surveille et contrôle le trafic entrant dans le réseau ou sortant de celui-ci selon des règles prédéfinies.
Surveillance des signaux de présence (*heartbeat*)	Signal périodique généré et surveillé par du matériel ou un logiciel et qui indique que le fonctionnement est normal ou qui permet la synchronisation avec d'autres parties d'un système informatique.
IPSec	IP SECurity. Suite de protocoles réseau qui authentifie et crypte les paquets de données afin de permettre la communication sécurisée cryptée entre deux ordinateurs sur un réseau IP (protocole Internet).
Tests d'intrusion	Mise à l'essai d'un système informatique, d'un réseau informatique ou d'une application web afin de détecter les failles de sécurité qu'un attaquant pourrait exploiter.
Processus de rapprochement	Processus visant à garantir la concordance de deux séries d'enregistrements.
VPN	Réseau privé virtuel (Virtual Private Network).
XML	Extensible Mark-up Language. Ce langage informatique permet aux concepteurs de créer des balises personnalisées et de définir, transmettre, valider et interpréter des données issues de différentes applications et organisations.

2. INTRODUCTION

L'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 23 novembre 2017 (ci-après dénommé "accord") prévoit la reconnaissance mutuelle des quotas d'émission qui peuvent être utilisés à des fins de conformité dans le cadre du système d'échange de quotas d'émission de l'Union (ci-après dénommé "SEQE de l'UE") ou du système d'échange de quotas d'émission de la Suisse (ci-après dénommé "SEQE de la Suisse"). Afin de rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse, un lien direct sera établi entre le journal des transactions de l'Union européenne (EUTL) du registre de l'Union et le journal complémentaire des transactions suisse (SSTL) du registre suisse, ce qui permettra le transfert de registre à registre des quotas d'émission délivrés au titre de chaque SEQE (article 3, paragraphe 2, de l'accord). Afin de rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE de la Suisse, une solution provisoire a été mise en place en 2020. À partir de 2023, le couplage des registres entre les deux systèmes d'échange de quotas d'émission prendra progressivement la forme d'un couplage permanent des registres dont la mise en œuvre est prévue pour 2024 au plus tard, et qui permettra aux marchés couplés, en ce qui concerne les bénéfices tirés de la liquidité de marché et l'exécution des transactions entre les deux systèmes couplés, de fonctionner d'une manière équivalente à un seul marché composé de deux systèmes et donnera aux acteurs du marché la possibilité d'agir comme s'il s'agissait d'un seul marché, soumis uniquement aux dispositions réglementaires individuelles des parties (annexe II de l'accord).

Conformément à l'article 3, paragraphe 7, de l'accord, l'administrateur du registre suisse et l'administrateur central de l'Union élaborent des normes techniques de couplage (NTC) fondées sur les principes énoncés à l'annexe II, décrivant les exigences détaillées applicables à l'établissement d'une connexion fiable et sécurisée entre le SSTL et l'EUTL. Les NTC établies par les administrateurs prennent effet une fois qu'elles ont été adoptées par décision du comité mixte.

Les NTC ont été adoptées par le comité mixte en vertu de sa décision n° 2/2020. Les NTC mises à jour, telles qu'elles sont décrites dans le présent document, seront adoptées par le comité mixte en vertu de sa décision n° 1/2024. Conformément à la présente décision et aux demandes du comité mixte, l'administrateur du registre suisse et l'administrateur central de l'Union ont élaboré et mettront à jour de nouvelles lignes directrices techniques visant à rendre opérationnel le couplage et à veiller à ce que celles-ci soient constamment adaptées au progrès technique et aux nouvelles exigences en matière de sécurité et de sûreté du couplage, ainsi qu'au fonctionnement efficace et efficient de celui-ci.

2.1. Champ d'application

Le présent document représente la conception commune des parties à l'accord en ce qui concerne l'établissement des bases techniques pour le couplage entre les registres du SEQE de l'UE et du SEQE de la Suisse. Quoiqu'il jette les bases des spécifications techniques relatives aux exigences en matière d'architecture, de service et de sécurité, des orientations détaillées supplémentaires seront nécessaires afin de rendre le couplage opérationnel.

Pour assurer le bon fonctionnement du couplage, des processus et des procédures devront être mis en place pour le rendre opérationnel. Conformément à l'article 3, paragraphe 6, de l'accord, ces aspects sont décrits en détail dans un document relatif aux procédures opérationnelles communes (POC) qui doit être adopté séparément par décision du comité mixte.

2.2. Destinataires

L'administrateur du registre suisse et l'administrateur central de l'Union sont destinataires du présent document.

3. DISPOSITIONS GÉNÉRALES

3.1. Architecture du lien de communication

La présente section a pour objet la description de l'architecture générale pour la mise en œuvre du couplage entre le SEQE de l'UE et le SEQE de la Suisse ainsi que des différentes composantes qui y participent.

La sécurité étant un élément essentiel pour la définition de l'architecture du couplage des registres, toutes les mesures ont été prises afin de disposer d'une architecture fiable. Le couplage permanent des registres fait appel à un mécanisme d'échange de fichiers qui met en œuvre une connexion sécurisée employant un système d'espace d'air virtuel.

La solution technique est la suivante:

– un protocole de transfert sécurisé pour l'échange de messages;

– des messages XML;

– une signature numérique et un cryptage XML;

– un VPN.

3.1.1. Échange de messages

La communication entre le registre de l'Union et le registre suisse repose sur un mécanisme d'échange de messages par des canaux sécurisés. Chaque bout dispose de son propre référentiel de messages reçus.

Les deux parties conservent un journal des messages reçus, ainsi que les détails relatifs au traitement.

Les erreurs ou un statut inattendu doivent être signalés, sous la forme d'alertes, et les équipes de support devraient prendre contact entre elles.

Les erreurs et les imprévus sont traités dans le respect des procédures opérationnelles établies dans le processus de gestion des incidents des POC.

3.1.2. Message XML – Haut niveau de description

Un message XML contient l'un des éléments suivants:

– une ou plusieurs demandes de transaction et/ou une ou plusieurs réponses de transaction;

– une opération/une réponse relevant du processus de rapprochement;

– un message de test.

Chaque message contient un en-tête comportant les éléments suivants:

– système SEQE source;

– numéro de séquence.

3.1.3. Fenêtres d'ingestion

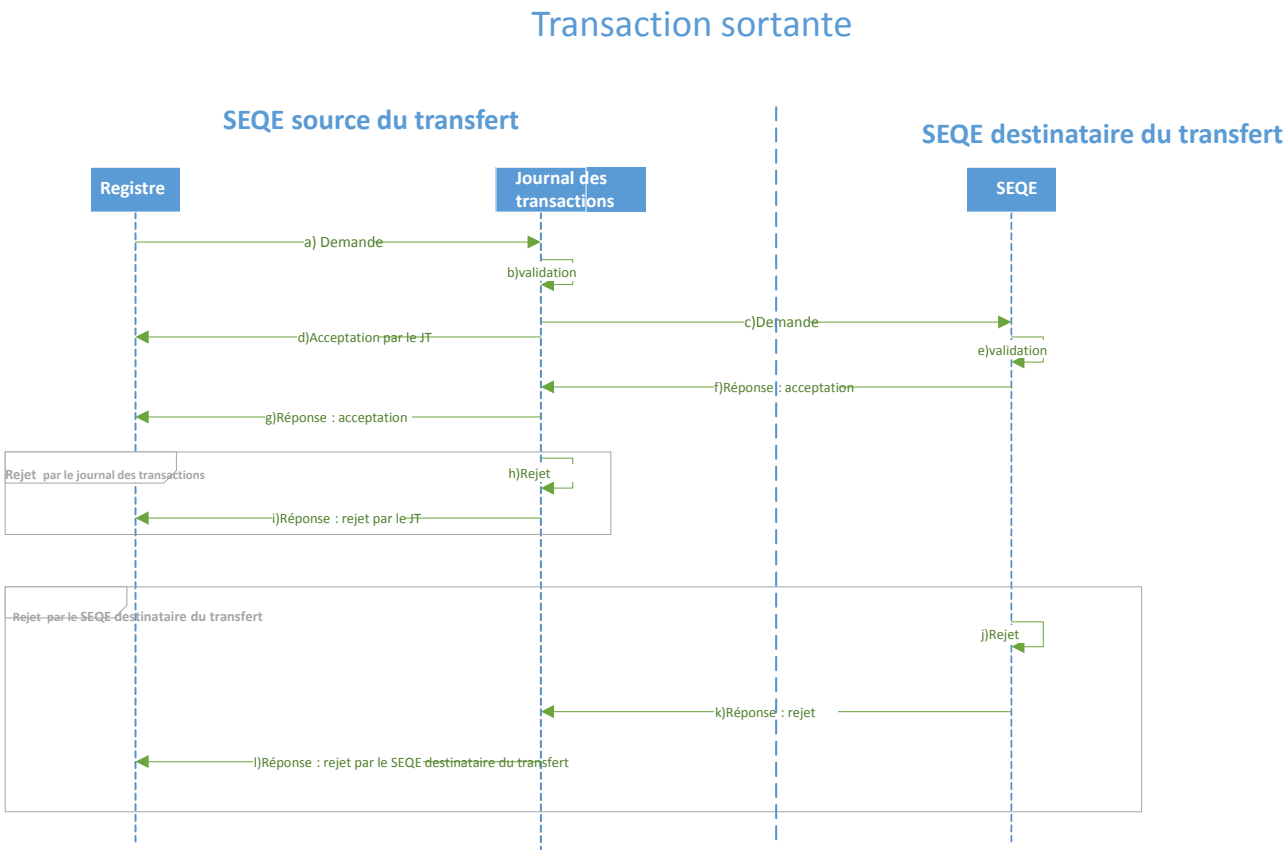
Le couplage permanent des registres repose sur des fenêtres prédéfinies destinées à l'ingestion qui sont suivies par une série d'événements nommés. Les demandes de transaction reçues via le lien ne seront ingérées qu'à intervalles prédéfinis et les fenêtres d'ingestion feront l'objet d'une validation technique, tant à l'entrée qu'à la sortie. En outre, des rapprochements peuvent être effectués quotidiennement et être déclenchés manuellement.

Les modifications apportées à la fréquence de ces événements et/ou au calendrier selon lequel ceux-ci ont lieu seront effectuées dans le respect des procédures opérationnelles établies dans le processus d'exécution des demandes des POC.

3.1.4. Flux des messages de transaction

Transactions sortantes

Le schéma ci-dessous est présenté sous l'angle du SEQE source du transfert. Le flux de données est représenté dans le diagramme de séquence suivant:



Le flux principal est composé des étapes suivantes (comme dans le schéma ci-dessus):

a) dans le SEQE source du transfert, la demande de transaction est envoyée du registre vers le journal des transactions, lorsque tous les délais "business" sont écoulés (délai de 24 heures, le cas échéant);

b) le journal des transactions valide la demande de transaction;

c) la demande de transaction est envoyée au SEQE destinataire;

d) la réponse d'acceptation est alors envoyée au registre du SEQE source;

e) le SEQE destinataire valide la demande de transaction;

f) le SEQE destinataire renvoie la réponse d'acceptation au journal des transactions du SEQE source;

g) le journal des transactions envoie la réponse d'acceptation au registre.

Autre flux "Rejet par le journal des transactions" (comme dans le schéma ci-dessus, à partir du point a) dans le flux principal]:

a) dans le système source, la demande de transaction est envoyée du registre vers le journal des transactions, lorsque tous les délais "business" sont écoulés (délai de 24 heures, le cas échéant);

b) le journal des transactions ne valide pas la demande;

c) le message de rejet est envoyé au registre source.

Autre flux "Rejet par le SEQE" (comme dans le schéma ci-dessus, à partir du point d) dans le flux principal]:

a) dans le SEQE source, la demande de transaction est envoyée du registre vers le journal des transactions lorsque tous les délais "business" sont écoulés (délai de 24 heures, le cas échéant);

b) le journal des transactions valide la transaction;

c) la demande de transaction est envoyée au SEQE destinataire;

d) le message d'acceptation est envoyé au registre du SEQE source;

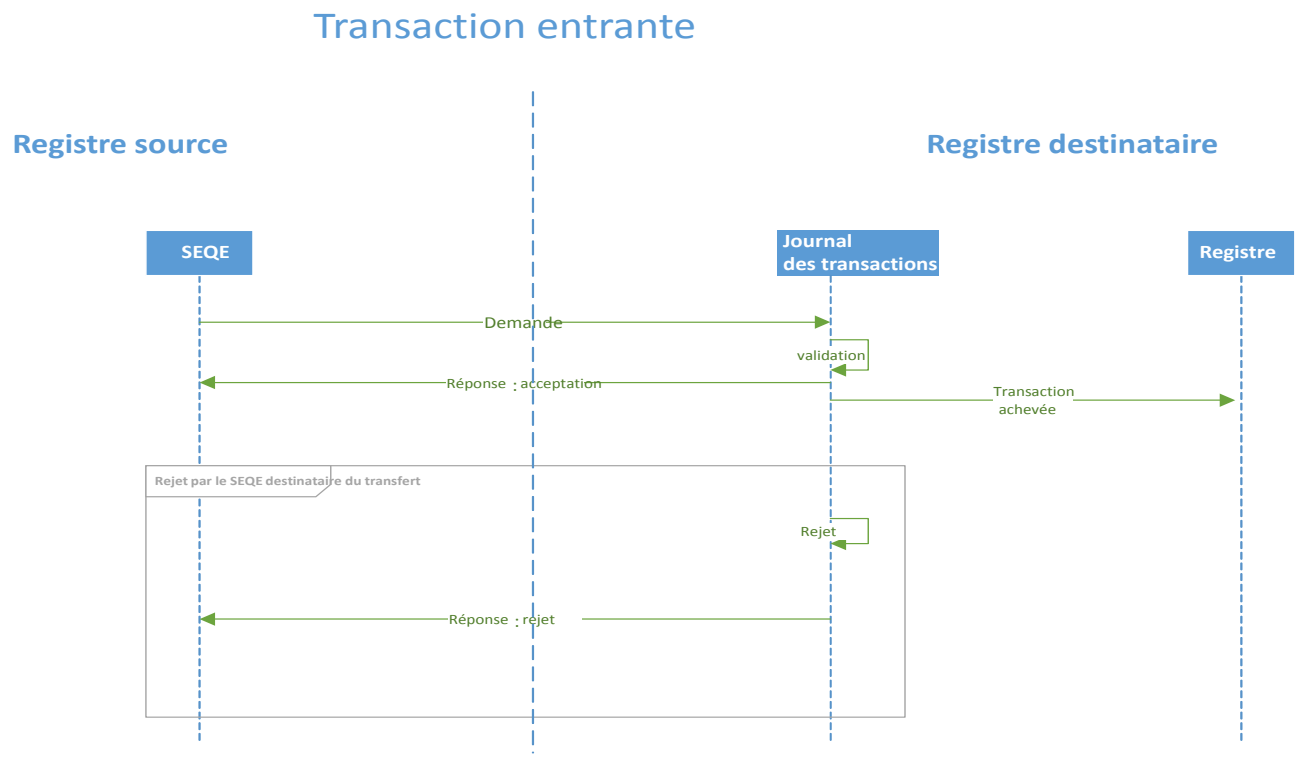
e) le journal des transactions du SEQE destinataire du transfert ne valide pas la transaction;

f) le SEQE destinataire du transfert envoie la réponse de rejet au journal des transactions du SEQE source du transfert;

g) Le journal des transactions communique le rejet au registre.

Transactions entrantes

Le schéma ci-dessous est présenté sous l'angle du SEQE destinataire du transfert. Le flux de données est représenté dans le diagramme de séquence suivant:



Le diagramme illustre ce qui suit:

1) lorsque le journal des transactions du SEQE destinataire du transfert valide la demande, il envoie le message d'acceptation au SEQE source du transfert ainsi qu'un message "transaction achevée" au registre du SEQE destinataire;

2) lorsqu'une demande entrante est rejetée par le journal des transactions destinataire, la demande de transaction n'est pas envoyée au registre du SEQE destinataire.

Protocole

Le cycle des messages de transaction ne comporte que deux messages:

– proposition de transaction SEQE → source du transfert SEQE destinataire du transfert;

– réponse de transaction SEQE → destinataire du transfert SEQE source du transfert: soit acceptation, soit rejet (raison du rejet incluse):

  – acceptation: la transaction est achevée;

  – rejet: la transaction est arrêtée.

Statut des transactions

– Le statut de la transaction du SEQE source du transfert sera "proposé" ("proposed") au moment de l'envoi de la demande.

– Le statut des transactions du SEQE destinataire du transfert sera "proposé" ("proposed") au moment de la réception de la demande ainsi que pendant le traitement de cette dernière.

– Le statut des transactions du SEQE destinataire du transfert sera "achevé/arrêté" ("completed/terminated") à l'issue du traitement de la proposition. Le SEQE destinataire du transfert enverra alors le message d'acceptation/de rejet correspondant.

– Le statut de la transaction du SEQE source du transfert sera "achevé/arrêté" ("completed/terminated") lorsque le message d'acceptation/de rejet sera reçu et pendant le traitement de ce dernier.

– En ce qui concerne le SEQE source du transfert, le statut de la transaction restera "proposé" ("proposed") tant qu'aucune réponse ne sera reçue.

– Dans le statut de la transaction du SEQE destinataire du transfert, le statut d'une transaction sera "arrêté" ("terminated") si une transaction reste en "proposé" ("proposed") pendant plus de 30 minutes.

Les incidents liés aux transactions seront traités dans le respect des procédures opérationnelles établies dans le processus de gestion des incidents des POC.

3.2. Sécurité du transfert des données

Les données en transit sont protégées par quatre niveaux de sécurité:

1) contrôle d'accès au réseau: pare-feu et couche d'interconnexion des réseaux;

2) cryptage au niveau "transport": VPN;

3) cryptage au niveau "session": protocole de transfert sécurisé pour l'échange de messages;

4) cryptage au niveau "application": signature XML et cryptage XML du contenu.

3.2.1. Pare-feu et interconnexion des réseaux

Le lien est établi au moyen d'un réseau protégé par un pare-feu matériel. Le pare-feu est configuré selon des règles en vertu desquelles seuls les clients "enregistrés" peuvent se connecter au serveur VPN.

3.2.2. VPN (Réseau privé virtuel – Virtual Private Network)

Toutes les communications entre les parties sont protégées au moyen d'une technologie de réseau privé virtuel (VPN). Les technologies VPN permettent de transporter les informations d'un point à un autre à travers un canal sécurisé ("tunnel") créé sur un réseau comme l'Internet, ce qui protège l'ensemble des communications. Avant que le tunnel VPN ne soit créé, un certificat numérique est émis vers un point de terminaison du client potentiel, ce qui permet à ce dernier de faire la preuve de son identité au cours de la phase de négociation de la connexion. Chaque partie est responsable de l'installation du certificat à son point de terminaison VPN. Chaque terminaison du serveur VPN aura accès, au moyen de certificats numériques, à une autorité centrale pour les négociations portant sur ses identifiants d'authentification. Lors du processus de création du tunnel, le cryptage fait l'objet de négociations, ce qui garantit la protection de l'ensemble des communications transitant par le tunnel.

Les points de terminaison du client VPN doivent être configurés de manière à ce que le tunnel reste ouvert en permanence, afin de permettre à tout moment une communication fiable, bidirectionnelle et en temps réel entre les parties.

En règle générale, l'Union européenne utilise les services télématiques transeuropéens sécurisés entre administrations (s-TESTA) comme réseau IP privé. Ce réseau convient donc également pour le couplage permanent des registres.

3.2.3. Mise en œuvre de l'IPsec

L'utilisation du protocole IPSec en vue de la mise en place de l'infrastructure VPN de liaison de site à site permettra l'authentification, l'intégrité et le cryptage des données de site à site. Les configurations VPN incluant des protocoles IPsec garantissent une authentification appropriée entre deux points de terminaison d'une connexion VPN. Les parties identifieront et authentifieront le client distant par l'intermédiaire de la connexion IPSec au moyen de certificats numériques fournis par une autorité de certification reconnue par l'autre bout.

L'IPsec garantit également l'intégrité des données pour l'ensemble des communications transitant par le tunnel VPN. Les paquets de données sont soumis à un processus de hachage et de signature utilisant les informations d'authentification déterminées par le VPN. La confidentialité des données est assurée de même par le cryptage IPSec.

3.2.4. Protocole de transfert sécurisé pour l'échange de messages

Le couplage permanent des registres repose sur de multiples couches de cryptage permettant l'échange sécurisé de données entre les parties. Les deux systèmes et leurs environnements respectifs sont interconnectés au niveau "réseau" au moyen de tunnels VPN. Au niveau "application", les fichiers sont transférés au moyen d'un protocole de transfert sécurisé pour l'échange de messages.

3.2.5. Signature et cryptage XML

Dans les fichiers XML, la signature et le cryptage interviennent à deux niveaux. À chaque demande de transaction, la réponse de transaction et le message de rapprochement reçoivent chacun une signature numérique.

Dans un deuxième temps, chaque sous-élément de l'élément "message" est crypté séparément.

En outre, dans un troisième temps, pour garantir l'intégrité et la non-répudiation de l'ensemble du message, l'élément racine du message est signé numériquement. Il en résulte un haut niveau de protection des données embarquées XML. La mise en œuvre technique respecte les normes du World Wide Web Consortium.

Pour décrypter et vérifier le message, le même processus est suivi dans l'ordre inverse.

3.2.6. Clés cryptographiques

La cryptographie à clé publique sera utilisée pour le cryptage et la signature.

Dans le cas spécifique d'IPSec, un certificat numérique émis par une autorité de certification (AC) bénéficiant de la confiance des deux parties est utilisé. Après vérification de l'identité du titulaire du certificat, cette AC émet des certificats qui sont utilisés pour identifier formellement une organisation et établir des canaux sécurisés de communication des données entre les parties.

Les clés cryptographiques sont utilisées pour la signature et le cryptage des canaux de communication et des fichiers de données. Les certificats publics sont échangés sous forme numérique entre les parties par l'intermédiaire de canaux sécurisés et vérifiés hors bande. Cette procédure fait partie intégrante du processus de gestion de la sécurité de l'information des POC.

3.3. Liste des fonctions dans le cadre du couplage

Le couplage comprend les spécifications du système de transmission pour une série de fonctions qui mettent en œuvre les processus "business" découlant de l'accord. Le couplage intègre les spécifications en ce qui concerne le processus de rapprochement et les messages de test qui permettront la mise en œuvre d'un système de surveillance par signaux de présence.

3.3.1. Transactions "business"

D'un point de vue "business", dans le cadre du couplage, il est prévu quatre (4) types de demandes de transaction:

– transferts externes:

  – après l'entrée en vigueur du couplage des SEQE, les quotas de l'UE et les quotas suisses deviennent fongibles, et, partant, totalement transférables d'une partie à l'autre;

  – un transfert dans le cadre du couplage fera intervenir un compte source du transfert pour l'un des SEQE et un compte destinataire du transfert pour l'autre SEQE;

– le transfert peut porter sur n'importe quelle quantité des quatre (4) types de quotas suivants:

– quotas généraux suisses (CHU);

– quotas suisses pour le secteur de l'aviation (CHUA);

– quotas généraux de l'UE (EUA);

– quotas de l'UE pour le secteur de l'aviation (EUAA);

– allocation internationale:

les exploitants d'aéronefs relevant d'un SEQE qui ont des obligations à l'égard de l'autre SEQE et qui peuvent prétendre à une allocation de quotas à titre gratuit dans le cadre de ce second SEQE se verront attribuer gratuitement des quotas du secteur de l'aviation au titre du second SEQE au moyen de la transaction "allocation internationale";

– annulation de l'allocation internationale:

cette transaction sera effectuée dans le cas où il y a lieu d'annuler en totalité les quotas alloués à titre gratuit qui ont été versés sur compte de dépôt d'exploitant d'aéronefs au titre de l'autre SEQE;

– Reversement de l'allocation excédentaire:

comparable à l'annulation, mais dans le cas où l'allocation ne doit pas être intégralement annulée et où seuls les quotas alloués en surplus doivent être reversés au SEQE au titre duquel ils ont été alloués.

3.3.2. Protocole de rapprochement

Les rapprochements ne seront effectués qu'après fermeture des fenêtres relatives à l'ingestion, à la validation et au traitement des messages.

Les rapprochements font partie intégrante des mesures garantissant la sécurité et la cohérence du couplage. Les deux parties conviendront du calendrier exact du rapprochement avant d'établir formellement sa programmation. Un rapprochement peut être programmé quotidiennement si les deux parties en conviennent. Au minimum, au moins un rapprochement programmé sera exécuté après chaque processus d'ingestion de données.

Dans tous les cas, l'une ou l'autre partie peut procéder à tout moment à des rapprochements manuels.

Les modifications apportées au calendrier et à la fréquence des rapprochements programmés seront effectuées dans le respect des procédures opérationnelles établies dans le processus d'exécution des demandes des POC.

3.3.3. Message de test

Un message de test est prévu pour tester la communication de bout en bout. Ce message contient des données qui permettent de l'identifier en tant que message de test, et une réponse est envoyée par l'autre bout dès sa réception.

3.4. Exigences relatives à l'enregistrement des données

Afin de répondre au besoin des deux parties de préserver l'exactitude et la cohérence des informations, et afin de fournir des outils utilisables lors du processus de rapprochement pour éliminer les incohérences, quatre (4) types de journaux de données doivent être tenus par chacune des parties:

– journaux des transactions;

– journaux des rapprochements;

– archive de messages;

– journaux des audits internes.

Toutes les données de ces journaux devront être conservées durant au moins trois (3) mois aux fins de la résolution de problèmes et leur conservation ultérieure à des fins d'audit dépendra du droit applicable à chaque bout. Les fichiers-journaux datant de plus de trois (3) mois peuvent être archivés dans un système informatique indépendant sécurisé, à la condition qu'ils puissent être retrouvés ou qu'on puisse y accéder dans un délai raisonnable.

Journaux des transactions

Les journaux des transactions sont mis en œuvre dans les sous-systèmes EUTL et SSTL.

Plus précisément, les journaux des transactions enregistreront chacune des transactions proposées à l'autre SEQE. Chaque enregistrement contient l'ensemble des champs relatif au contenu de la transaction ainsi qu'au résultat qui s'ensuit (la réponse envoyée par le SEQE qui reçoit la demande). Les journaux des transactions enregistreront également les transactions entrantes et la réponse envoyée au SEQE source du transfert.

Journaux des rapprochements

Le journal des rapprochements enregistre chacun des messages de rapprochement échangés entre les parties, notamment l'identifiant, l'horodatage et le résultat du rapprochement: statut du rapprochement "Pass" (réussite) ou "Discrepancies" (divergences). Dans le couplage permanent des registres, les messages de rapprochement font partie intégrante des messages échangés et sont par conséquent stockés de la manière décrite dans la section "Archive de messages".

Les deux parties consignent chaque demande et sa réponse dans le journal des rapprochements. Bien que les informations contenues dans le journal des rapprochements ne soient pas directement partagées dans le cadre du processus de rapprochement proprement dit, il peut s'avérer nécessaire d'avoir accès à ces informations pour supprimer les incohérences.

Archive de messages

Les deux parties sont tenues d'archiver une copie des données échangées (les fichiers XML), envoyées et reçues, ainsi que l'information indiquant si le format de ces messages XML est correct ou non.

La principale raison d'être de l'archivage est l'audit, le but étant de disposer de preuves de ce qui a été envoyé et reçu par les deux parties. À cette fin, les certificats doivent également être archivés avec les fichiers correspondants.

Ces fichiers fourniront également des informations supplémentaires aux fins de la résolution de problèmes.

Journaux des audits internes

Ces journaux sont définis et utilisés par chaque partie séparément.

3.5. Prescriptions opérationnelles

L'échange de données entre les deux systèmes n'est pas totalement autonome dans le cadre du couplage permanent des registres. Cela signifie que des opérateurs et des procédures sont nécessaires pour rendre le couplage opérationnel. Plusieurs rôles et outils sont détaillés à cette fin dans le cadre de ce processus.

4. DISPOSITIONS PERMETTANT DE GARANTIR LA DISPONIBILITÉ

4.1. Conception garantissant la disponibilité de la communication

Fondamentalement, l'architecture du couplage permanent des registres consiste en une infrastructure et un logiciel TIC qui permettent la communication entre le SEQE de la Suisse et le SEQE de l'UE. Garantir des niveaux élevés de disponibilité, d'intégrité et de confidentialité pour ce flux de données est dès lors un aspect essentiel qui doit être pris en compte dans la conception du couplage permanent des registres. Étant donné qu'il s'agit d'un projet dans lequel l'infrastructure TIC, le logiciel sur mesure et les processus jouent un rôle essentiel, il doit être tenu compte de ces trois éléments pour concevoir un système résilient.

Résilience de l'infrastructure TIC

Le chapitre " Dispositions générales" du présent document détaille les blocs de construction de l'architecture. En ce qui concerne l'infrastructure TIC, dans le cadre du couplage permanent des registres, un réseau VPN résilient est mis en place et crée des tunnels de communication sécurisés par l'intermédiaire desquels les messages peuvent être échangés de manière sécurisée. D'autres éléments d'infrastructure sont configurés en haute disponibilité et/ou disposent de mécanismes de secours.

Résilience des logiciels sur mesure

Les modules logiciels sur mesure renforcent la résilience car ils tentent, pendant une durée donnée, de rétablir la communication avec l'autre bout lorsque, pour une raison quelconque, ce service n'est pas disponible.

Résilience des services

Dans le cadre du couplage permanent des registres, les échanges de données entre les parties ont lieu à des intervalles prédéfinis. Certaines des étapes requises pour les échanges de données préprogrammés exigent l'intervention manuelle des opérateurs du système et/ou des administrateurs des registres. Afin de prendre en compte cet aspect et d'accroître la disponibilité et le succès des échanges:

– les procédures opérationnelles prévoient des fenêtres temporelles pour l'exécution de chaque étape;

– les modules logiciels du couplage permanent des registres mettent en œuvre une communication asynchrone;

– le processus de rapprochement automatique détecte si des problèmes sont survenus lors de l'ingestion des fichiers de données à l'un des bouts;

– les processus de surveillance (infrastructure TIC et modules logiciels sur mesure) sont pris en compte dans les procédures de gestion des incidents et déclenchent certaines procédures en la matière (comme défini dans le document relatif aux procédures opérationnelles). Ces procédures qui visent à réduire le temps du retour à la normale à la suite d'incidents sont essentielles pour garantir des taux élevés de disponibilité.

4.2. Plan d'initialisation, de communication, de réactivation et de test

L'ensemble des différents éléments intervenant dans l'architecture du couplage permanent des registres doit être soumis avec succès à des tests individuels et collectifs afin de vérifier que les niveaux "infrastructure TIC" et "système d'information" de la plateforme sont prêts. Ces tests opérationnels sont une condition préalable et impérative chaque fois que le couplage permanent des registres doit passer du statut "suspendu" ("suspended") au statut "opérationnel" sur la plateforme.

L'activation du statut opérationnel du lien exige donc qu'un plan de test prédéfini ait été exécuté avec succès, ce qui permet de s'assurer qu'un ensemble de tests en interne ont été exécutés au préalable pour chaque registre et que la connectivité a été validée de bout en bout avant de commencer à soumettre des transactions en production entre les deux parties.

Le plan de test devrait mentionner la stratégie de test globale et comporter des détails relatifs à l'infrastructure de test. En particulier, pour chacun des éléments de chaque bloc de test, il faut disposer des éléments suivants:

– des critères et des outils de test;

– des rôles assignés en vue de l'exécution du test;

– des résultats escomptés (positifs et négatifs);

– du programme du test;

– de l'enregistrement des exigences relatives aux résultats des tests;

– de la documentation relative à la résolution de problèmes;

– des dispositions relatives à la remontée des incidents.

Le processus des tests d'activation du statut opérationnel pourrait être subdivisé en quatre (4) blocs ou phases conceptuels indiqués ci-dessous.

4.2.1. Tests des infrastructures TIC en interne

Il est prévu que ces tests soient réalisés et/ou vérifiés séparément par des administrateurs des registres à chaque bout.

Chaque élément de l'infrastructure TIC à chaque bout doit être testé séparément. Cette prescription vaut pour chaque composante de l'infrastructure. Ces tests peuvent être exécutés automatiquement ou manuellement mais ils doivent permettre de confirmer que chaque élément de l'infrastructure est opérationnel.

4.2.2. Tests de communication

Ces tests sont amorcés individuellement par l'une ou l'autre partie et leur achèvement requiert la coopération de l'autre bout.

Une fois que chacun des différents éléments est opérationnel, les canaux de communication entre les deux registres doivent être mis à l'essai également. À cette fin, chaque partie vérifie que l'accès à Internet fonctionne, que les tunnels VPN sont mis en place et qu'une connectivité IP de site à site est établie. L'accessibilité des éléments d'infrastructure locaux et distants et la connectivité IP devraient ensuite être confirmées à l'autre bout.

4.2.3. Tests du système complet (de bout en bout)

Il est prévu que ces tests soient exécutés à chaque bout et que les résultats soient communiqués à l'autre partie.

Une fois que les canaux de communication et chacune des composantes des deux registres ont été testés, une série de transactions et de rapprochements simulés, représentatifs de l'ensemble des fonctions à mettre en œuvre dans le cadre du lien, est préparée à chaque bout.

4.2.4. Tests de sécurité

Ces tests sont censés être effectués et/ou déclenchés par les administrateurs des registres à chaque bout, selon les instructions figurant dans les sections 5.4 "Lignes directrices en matière de tests de sécurité" et 5.5 "Dispositions en matière d'évaluation des risques".

Ce n'est qu'après que les quatre phases/blocs se sont conclus par des résultats prévisibles que le couplage permanent des registres peut être considéré comme opérationnel.

Ressources destinées aux tests

Chaque partie s'appuie sur des ressources spécifiques destinées aux tests (logiciels et matériels spécifiques aux infrastructures TIC) et développe des fonctions de test à intégrer dans son propre système afin de soutenir la validation manuelle et continue de la plateforme. Des procédures de test manuelles, entreprises séparément par chacune des parties ou en coopération, peuvent être exécutées à tout moment par les administrateurs des registres. L'activation du statut opérationnel est un processus manuel en lui-même.

Il est également prévu que la plateforme effectue des contrôles automatiques à intervalles réguliers. Ces contrôles visent à accroître la disponibilité de la plateforme par la détection précoce d'éventuels problèmes au niveau de l'infrastructure ou au niveau logiciel. Ce plan de surveillance de la plateforme est constitué de deux éléments:

– surveillance des infrastructures TIC: les infrastructures seront surveillées aux deux bouts par les prestataires de services d'infrastructure TIC. Les tests automatiques porteront sur les différents éléments de l'infrastructure ainsi que sur la disponibilité des canaux de communication;

– surveillance des applications: les modules logiciels du couplage permanent des registres mettront en œuvre une surveillance de la communication du système au niveau "application" (manuellement et/ou à intervalles réguliers) qui permettra de tester la disponibilité de bout en bout du couplage en simulant certaines des transactions.

4.3. Environnements de validation/de test

L'architecture du registre de l'Union et du registre suisse comprend les trois environnements suivants:

– production (PROD): cet environnement contient les données réelles et traite des transactions réelles;

– validation (*Acceptance* – ACC): cet environnement contient des données représentatives, fictives ou anonymisées. Il s'agit de l'environnement dans lequel les opérateurs du système des deux parties valident les nouvelles mises en production;

– test (TEST): cet environnement contient des données représentatives, fictives ou anonymisées. Son accès est limité aux administrateurs des registres et il est destiné à la réalisation de tests d'intégration par les deux parties.

Exception faite du VPN, les trois environnements sont totalement indépendamment les uns des autres, ce qui signifie que le matériel, les logiciels, les bases de données, les environnements virtuels, les adresses IP et les ports sont configurés de manière indépendante les uns des autres et fonctionnent indépendamment également.

Quant à la configuration du VPN, la communication entre les trois environnements doit être totalement indépendante, ce qui est garanti par l'utilisation des s-TESTA.

5. DISPOSITIONS RELATIVES À LA CONFIDENTIALITÉ ET À L'INTÉGRITÉ

Les mécanismes et les procédures de sécurité prévoient l'application du principe du double regard pour les opérations effectuées dans le cadre du couplage du registre de l'Union et du registre suisse. Le principe du double regard s'applique chaque fois que nécessaire. Toutefois, il pourrait ne pas s'appliquer à toutes les actions entreprises par les administrateurs des registres.

Les exigences en matière de sécurité sont prises en compte et abordées dans le plan de gestion de la sécurité, qui inclut également des processus liés au traitement des incidents de sécurité à la suite d'éventuelles failles de sécurité. La partie opérationnelle de ces processus est décrite dans les POC.

5.1. Infrastructure destinée aux tests de sécurité

Chaque partie s'engage à mettre en place une infrastructure destinée aux tests de sécurité (au moyen de l'ensemble commun de logiciels et de matériel utilisés pour détecter les vulnérabilités lors des phases de développement et d'exploitation):

– distincte de l'environnement de production;

– dans laquelle la sécurité est analysée par une équipe indépendante des équipes chargées du développement et de l'exploitation du système.

Chaque partie s'engage à effectuer des analyses statiques et dynamiques.

Dans le cas d'une analyse dynamique (comme des tests d'intrusion), les deux parties s'engagent à limiter d'ordinaire les évaluations aux environnements de test et de validation (tels qu'ils sont définis dans la section 4.3 "Environnements de validation/de test"). Ce principe admet des exceptions qui doivent faire l'objet d'une approbation par les deux parties.

Avant d'être déployé dans l'environnement de production, chaque module logiciel du lien (tel qu'il est défini dans la section 3.1 "Architecture du lien de communication") doit faire l'objet d'un test de sécurité.

L'infrastructure de test doit être séparée de l'infrastructure de production tant au niveau "réseau" qu'au niveau "infrastructure". Il s'agit de l'infrastructure de test, où les tests de sécurité sont nécessaires au contrôle de la conformité au regard des exigences en matière de sécurité.

5.2. Dispositions relatives à la suspension et à la réactivation du lien

En cas de suspicion d'atteinte à la sécurité du registre suisse, du SSTL, du registre de l'Union ou de l'EUTL, les parties s'informent immédiatement et suspendent immédiatement le lien entre le SSTL et l'EUTL.

Les procédures relatives au partage de l'information, à la décision de suspension et à la décision de réactivation font partie du processus d'exécution des demandes des POC.

Suspensions

La suspension du couplage des registres conformément à l'annexe II de l'accord peut advenir pour les raisons suivantes:

– raisons administratives (par exemple, maintenance), qui sont planifiées;

– raisons de sécurité (ou pannes de l'infrastructure informatique), qui sont non planifiées.

En cas d'urgence, chaque partie informera l'autre partie et suspendra unilatéralement le couplage des registres.

S'il est décidé de suspendre le couplage des registres, chaque partie veillera alors à ce que le lien soit interrompu au niveau "réseau" (par le blocage des connexions entrantes et sortantes, en tout ou en partie).

La décision de suspension du couplage des registres, qu'elle soit planifiée ou non, sera prise selon la procédure de gestion des changements ou selon la procédure de gestion des incidents de sécurité des POC.

Réactivation de la communication

La décision de réactivation du couplage des registres sera prise de la manière détaillée dans les POC et, en tout état de cause, pas avant que les procédures de test de sécurité n'aient été exécutées avec succès, comme indiqué dans les sections 5.4 "Lignes directrices en matière de tests de sécurité" et 4.2 "Plan d'initialisation, de communication, de réactivation et de test".

5.3. Dispositions relatives aux failles de sécurité

Une faille de sécurité est un incident de sécurité susceptible de porter atteinte à la confidentialité et à l'intégrité d'informations sensibles et/ou à la disponibilité du système qui les traite.

Les informations sensibles sont recensées sur la liste des informations sensibles et peuvent être traitées dans le système ou dans toute partie y afférente.

Sauf indication contraire, les informations directement liées à la faille de sécurité seront considérées comme sensibles, marquées "SPECIAL HANDLING: *ETS Critical*" et traitées conformément aux instructions de traitement.

Toute faille de sécurité sera traitée conformément au chapitre "Gestion des incidents de sécurité" des POC.

5.4. Lignes directrices relatives aux tests de sécurité

5.4.1. Logiciels

Les tests de sécurité, notamment, le cas échéant, les tests d'intrusion, doivent être exécutés au minimum pour toute nouvelle mise en production majeure du logiciel, conformément aux exigences de sécurité établies dans les NTC aux fins de l'évaluation de la sécurité du couplage ainsi que des risques correspondants.

Si aucune mise en production majeure n'est intervenue aux cours des 12 derniers mois, un test de sécurité doit être exécuté sur le système en place en tenant compte de l'évolution des menaces informatiques survenue au cours des 12 derniers mois.

Les tests de sécurité du couplage des registres doivent être effectués dans l'environnement de validation et, si nécessaire, dans l'environnement de production, en coordination avec les deux parties et avec leur accord mutuel.

Les tests des applications internet respecteront les normes ouvertes internationales telles que celles établies par l'OWASP (*Open Web Application Security Project*).

5.4.2. Infrastructure

Les infrastructures qui prennent en charge le système de production doivent être régulièrement scrutées (au moins une fois par mois) en vue de détecter d'éventuelles vulnérabilités auxquelles il conviendra de remédier, le cas échéant, selon le même principe que celui défini dans la section précédente, au moyen d'une base de données actualisée relative aux vulnérabilités.

5.5. Dispositions en matière d'évaluation des risques

Si des tests d'intrusion doivent être effectués, ils doivent être inclus dans les tests de sécurité.

Chaque partie peut confier à une société spécialisée la réalisation des tests de sécurité, à condition que la société en question:

– possède les compétences et l'expérience requises en matière de tests de sécurité de ce type;

– ne rende pas directement compte au développeur et/ou à la partie contractante, ne participe pas au développement des logiciels du couplage et ni ne soit un sous-traitant du développeur;

– ait signé un accord de non-divulgation l'engageant à respecter la confidentialité des résultats et à traiter ces derniers comme relevant du niveau "SPECIAL HANDLING: *ETS Critical*", conformément aux instructions de traitement.