COMMISSION
EUROPÉENNE

Bruxelles, le 30.6.2020
COM(2020) 271 final

ANNEX

ANNEXE

de la

proposition de décision du Conseil

concernant la position à prendre au nom de l'Union européenne au sein 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 des annexes I et II dudit accord et l'adoption de normes techniques de couplage

DÉCISION Nº 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 …

portant modification des ANNEXES I et II de l'accord et adoption de normes techniques de couplage (NTC)

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 l'«accord»), et notamment son article 3, paragraphe 7, et son article 13, paragraphe 2,

considérant ce qui suit:

(1) La décision nº 2/2019 du comité mixte du 5 décembre 2019[2] a modifié les annexes I et II de l'accord, de sorte que les conditions requises pour le couplage prévues dans ledit accord sont réunies.

(2) À la suite de l'adoption de la décision nº 2/2019 du comité mixte et conformément à l'article 21, paragraphe 3, de l'accord, les parties ont échangé leurs instruments de ratification, ayant estimé que toutes les conditions requises pour le couplage prévues dans l'accord étaient remplies.

(3) Conformément à l'article 21, paragraphe 4, de l'accord, ce dernier est entré en vigueur le 1er janvier 2020.

(4) Il convient de modifier l'annexe I de l'accord, conformément à l'article 13, paragraphe 2, dudit accord afin de garantir une transition harmonieuse dans l'attribution de la responsabilité des exploitants d'aéronefs à la Suisse pour la première fois, compte tenu des progrès accomplis dans l'établissement du couplage des registres.

(5) Afin de tenir compte des récentes évolutions et de permettre davantage de souplesse dans l'établissement du couplage des registres requis par l'accord, il y a lieu de modifier l'annexe II de l'accord, conformément à l'article 13, paragraphe 2, dudit accord, afin de prévoir la possibilité de recourir à un ensemble de technologies plus vaste mais équivalent en vue de réaliser le couplage des registres.

(6) Conformément à l'article 3, paragraphe 7, de l'accord, il convient que l'administrateur du registre suisse et l'administrateur central de l'Union élaborent des normes techniques de couplage (les «NTC») fondées sur les principes énoncés à l'annexe II de l'accord. Les NTC devraient décrire les exigences détaillées applicables à l'établissement d'une connexion fiable et sécurisée entre le journal complémentaire des transactions suisse (Swiss Supplementary Transaction Log, SSTL) et le journal des transactions de l'Union européenne (EUTL). Ces NTC devraient prendre effet une fois qu'elles ont été adoptées par décision du comité mixte.

(7) Conformément à l'article 13, paragraphe 1, de l'accord, il convient que le comité mixte arrête des lignes directrices techniques pour assurer la bonne mise en œuvre de l'accord, y compris en ce qui concerne l'établissement d'une connexion fiable et sécurisée entre le SSTL et l'EUTL. Ces lignes directrices techniques peuvent être

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

[2] JO [XXXX]

élaborées par un groupe de travail institué conformément à l'article 12, paragraphe 5, de l'accord. Le groupe de travail devrait au moins comprendre l'administrateur du registre suisse et l'administrateur central du registre de l'Union et devrait en outre assister le comité mixte dans ses fonctions conformément à l'article 13 de l'accord.

(8) Compte tenu de la nature technique des lignes directrices et de la nécessité de les adapter aux évolutions en cours, il y a lieu de soumettre au comité mixte, pour information ou approbation, le cas échéant, les lignes directrices techniques élaborées par l'administrateur du registre suisse et l'administrateur central de l'Union,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

À l'annexe I, partie B, point 17, de l'accord, le deuxième alinéa est remplacé par le texte suivant:

«Les exploitants d'aéronefs attribués à la Suisse pour la première fois après l'entrée en vigueur du présent accord passent sous la responsabilité de la Suisse après le 30 avril de l'année d'attribution, une fois que le couplage provisoire des registres est opérationnel.»

Article 2

À l'annexe II de l'accord, le quatrième alinéa est remplacé par le texte suivant:

«Les normes techniques de couplage (NTC) prévoient que les communications entre le SSTL et l'EUTL consistent en des échanges sécurisés de messages par services internet reposant sur les technologies suivantes[3] ou sur des technologies équivalentes:

- services internet utilisant SOAP (Simple Object Access Protocol),
- VPN (réseau privé virtuel) matériel;
- XML (Extensible Markup Language),
- signature numérique, et
- protocoles de synchronisation réseau.»

Article 3

Les normes techniques de couplage (NTC) annexées à la présente décision sont adoptées.

Article 4

Un groupe de travail est institué en vertu de l'article 12, paragraphe 5, de l'accord. Il assiste le comité mixte afin de garantir la bonne application de l'accord, et en particulier l'élaboration de lignes directrices techniques pour la mise en œuvre des NTC.

Le groupe de travail comprend au moins l'administrateur du registre suisse et l'administrateur central du registre de l'Union.

[3] Ces technologies sont actuellement utilisées pour établir une connexion entre le registre de l'Union et le relevé international des transactions ainsi qu'entre le registre suisse et le relevé international des transactions.

Article 5

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

Fait à Bruxelles, en langue anglaise, le XX 2020.

Par le comité mixte

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

ANNEXE

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

Norme relative à une solution provisoire

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 établies au titre du SEQE de l'UE ou du SEQE suisse.
CH	Confédération suisse
CHU	Quotas généraux suisses (le terme «CHU2» est utilisé comme abréviation pour les quotas CHU de la deuxième période d'engagement)
CHUA	Quota suisse pour le secteur de l'aviation
POC	Procédures opérationnelles communes élaborées conjointement par les parties à l'accord afin de rendre opérationnel le lien entre le SEQE de l'UE et le SEQE 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 l'«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 le «SEQE de l'UE») ou du système d'échange de quotas d'émission de la Suisse (ci-après le «SEQE suisse»). Pour rendre opérationnel le couplage entre le SEQE de l'UE et le SEQE 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 suisse, une solution provisoire doit être mise en place d'ici mai 2020 ou dès que possible après cette date. Les parties doivent coopérer afin de remplacer dès que possible la solution provisoire par un couplage permanent des registres (annexe II de l'accord).

Conformément à l'article 3, paragraphe 7, de l'accord, l'administrateur du registre suisse et l'administrateur central du registre 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 décrites dans le présent document doivent être adoptées par le comité mixte en vertu de sa décision nº 2/2020. Par la présente décision, le comité mixte charge l'administrateur du registre suisse et l'administrateur central de l'Union d'élaborer de nouvelles lignes directrices techniques visant à rendre opérationnel le couplage et de veiller à ce que ces lignes directrices soient constamment adaptées au progrès technique et aux nouvelles exigences en matière de sécurité et de sûreté du couplage, ainsi qu'à un 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 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.

À cette fin et pour assurer un fonctionnement adéquat, des processus et des procédures devront être mises en place. 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 du registre de l'Union sont destinataires du présent document.

3. DISPOSITIONS GENERALES

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 suisse ainsi que des différentes composantes qui y participent.

La sécurité étant un élément essentiel pour la définition de l'architecture, toutes les mesures ont été prises afin de disposer d'une architecture fiable. Alors que le couplage permanent des registres sera fondé sur des services internet, dans la solution provisoire, il sera plutôt fait appel à un mécanisme d'échange de fichiers.

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 réseau de transport de données sécurisé à l'aide d'un routeur VPN ou équivalent.

3.1.1. Échange de messages

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

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

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

Les erreurs et les imprévus seront 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:

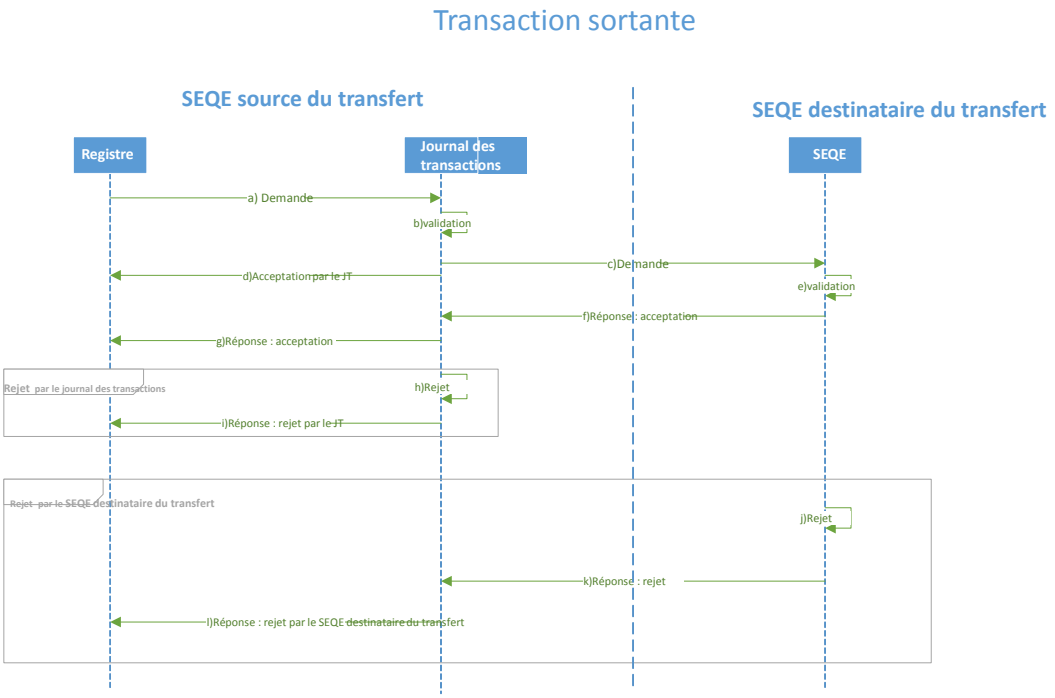
- Système SEQE source;
- Numéro de séquence.

3.1.3. Fenêtres d'ingestion

La solution provisoire 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 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 ils 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

Cette section est présentée sous l'angle du SEQE source du transfert. Le diagramme de séquence ci-dessus décrit l'ensemble des flux spécifiques aux transactions sortantes.

Flux principal d'une «transaction normale» (les étapes sont indiquées 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 «Journal des transactions rejetées» [les étapes sont indiquées dans le schéma ci-dessus, à partir du point a)]:

(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).

Ensuite:

(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» [les étapes sont indiquées dans le schéma ci-dessus, à partir du point a)]:

(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.

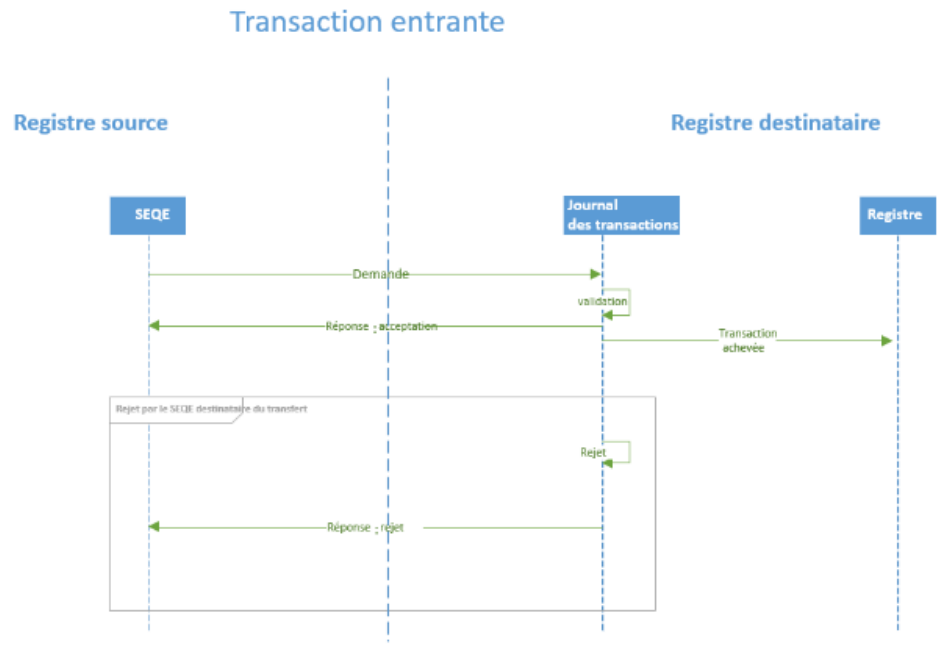
Ensuite:

(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



Cette section est présentée 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 SEQE destinataire du transfert, le statut d'une transaction restant en «proposé» («proposed») pendant plus de 30 minutes passera à «arrêté» («terminated»).

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»: réseau de transport de données sécurisé à l'aide d'un routeur VPN ou équivalent.

(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 transport sécurisé des données. Dans le cas d'un VPN, l'infrastructure devrait être basée sur un dispositif virtuel ou matériel. 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 le tunnel reste ouvert en permanence, afin de permettre à tout moment une communication fiable, bidirectionnelle et en temps réel entre les parties.

Toute autre solution équivalente doit respecter les principes susmentionnés.

3.2.3. Mise en œuvre de l'IPsec

En cas de recours à une solution VPN, 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

La solution provisoire 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 ou de réseaux équivalents

de transport sécurisé de données. 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, 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. Un rapprochement programmé sera toutefois exécuté au minimum après chaque processus d'ingestion de données.

Néanmoins, chaque partie peut à tout moment procéder 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. Normes applicables aux services internet

Les services internet ne seront pas utilisés dans le cadre de la solution provisoire. Il convient toutefois de signaler que le format des messages XML restera globalement inchangé. Lorsque le couplage permanent des registres sera mis en place, les services internet devraient permettre l'échange de messages XML en temps réel.

3.5. Définition spécifique des services internet

La présente section ne s'applique pas à la solution provisoire. Comme indiqué dans la section précédente, les services internet seront utilisés uniquement dans le cadre du futur couplage permanent des registres.

3.6. 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 cadre de la solution provisoire, les messages de rapprochement font partie intégrante des messages échangés.

Les deux parties enregistrent chaque demande et la réponse à celle-ci 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.

3.7. Prescriptions opérationnelles

L'échange de données entre les deux systèmes n'est pas totalement autonome dans le cadre de la solution provisoire: des opérateurs et des procédures sont nécessaires à la mise en œuvre du couplage.

4. DISPOSITIONS PERMETTANT DE GARANTIR LA DISPONIBILITE

4.1. Conception garantissant la disponibilité de la communication

Fondamentalement, l'architecture de la solution provisoire consiste en une infrastructure et un logiciel TIC qui permettent la communication entre le SEQE 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 de la solution provisoire et 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 provisoire, un réseau VPN résilient (ou équivalent) 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 permettent de renforcer 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 de la solution provisoire, les échanges de données entre les parties ont lieu dans des plages horaires prédéfinies tout au long de l'année. 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 importantes pour l'exécution de chaque étape.
- Les modules logiciels de la solution provisoire 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 de la solution provisoire doivent 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 la solution provisoire 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:

4.2.1. Test des infrastructures TIC en interne

Il est prévu que ces tests soient réalisés et/ou vérifiés par chacune des parties 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

Chacune des parties doit amorcer séparément le test et celui-ci doit se conclure en coopération avec 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 (ou du réseau de transport sécurisé équivalent) 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 deux parties à chaque bout, selon les instructions figurant dans les sections «Lignes directrices en matière de tests de sécurité» et «Dispositions en matière d'évaluation des risques».

Ce n'est qu'après que les quatre phases/blocs se sont conclus par un résultat prévisible que le lien provisoire 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 provisoire 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 (ou du réseau équivalent), 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 au VPN, il en existe deux configurations, prévues pour deux environnements différents: une pour l'environnement PROD et une autre pour ACC et TEST.

5. DISPOSITIONS RELATIVES A LA CONFIDENTIALITE ET A L'INTEGRITE

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, mais 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 que définis dans la section «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 que défini dans la section «Architecture du lien de communication») doit faire l'objet d'un test de sécurité.

L'infrastructure de test doit être séparée de l'infrastructures de production tant au niveau «réseau» qu'au niveau «infrastructure» et permettre l'exécution des tests de sécurité 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 deux parties s'informent 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 (maintenance,...), donc planifiées;
- raisons de sécurité (ou pannes de l'infrastructure informatique), donc 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 sera prise conformément aux 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 «Lignes directrices en matière de tests de sécurité» et «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 «SEQE Critique» 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 ne soit pas 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 «SEQE Critique», conformément aux instructions de traitement.