Distr. générale
12 août 2021
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des problèmes douaniers intéressant les transports

Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR

Deuxième session
Genève, 25-28 mai 2021
Point 6 d) de l'ordre du jour provisoire
Version 4.3 des spécifications conceptuelles, fonctionnelles et techniques du système eTIR : Spécifications techniques du système eTIR

Spécifications techniques du système eTIR

Table des matières

I. Mandat 3

II. Introduction générale 3

A. Objet 3
B. Domaine d'application 3
C. Public cible 4
D. Conditions préalables 5
E. Documents pertinents 5
F. Définitions 5
G. Abréviations 7
H. Consultation du présent document 8

III. Le système international eTIR 8

A. Principes directeurs 9
B. Architecture générale du système eTIR 10
C. Architecture détaillée du système international eTIR 17
D. Exigences techniques 20
E. Processus de développement 33
F. Processus de maintenance 44

IV. Sécurité du système eTIR 50

A. Objectifs et principes de la sécurité 50
B. Exigences relatives à la sécurité 53
C. Sécurité du système international eTIR 60
D. Security of exchanges with the eTIR international system 64
E. Security of exchanges between other eTIR stakeholders 68

V. Annexes 71

A. Conventions de notation des diagrammes 71
B. Glossaire technique 71
C. Analyse des besoins du système international eTIR en matière de capacités et d'extensibilité 74
D. Codes d'erreur 80

Liste des tableaux 86

Liste des figures 87

I. Mandat

1. À sa quatre-vingt-deuxième session (23-28 février 2020), le Comité des transports intérieurs a approuvé la création du Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR (WP.30/GE.1) (ECE/TRANS/294, par. 84[1]) et a approuvé son mandat[2] (ECE/TRANS/WP.30/2019/9 et Corr.1), sous réserve de l'accord du Comité exécutif de la Commission économique pour l'Europe (CEE). À sa réunion informelle à distance (20 mai 2020), le Comité exécutif a approuvé la création du WP.30/GE.1 jusqu'en 2022, sur la base du mandat figurant dans les documents ECE/TRANS/WP.30/2019/9 et Corr.1, tels que reproduits dans le document ECE/TRANS/294 (ECE/EX/2020/L.2, par. 5 b))[3].

2. Le mandat du Groupe dispose que celui-ci doit concentrer ses travaux sur l'élaboration d'une nouvelle version des spécifications du système eTIR, en attendant la mise en place officielle de l'Organe de mise en œuvre technique (TIB). Plus précisément, le Groupe est chargé : a) d'établir une nouvelle version des spécifications techniques du système eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications fonctionnelles du système eTIR ; b) d'établir une nouvelle version des spécifications fonctionnelles du système eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications conceptuelles du système eTIR ; c) d'élaborer des amendements aux spécifications conceptuelles du système eTIR, à la demande du Groupe de travail des problèmes douaniers intéressant les transports (WP.30).

3. On trouvera dans le présent document les parties actuellement disponibles des spécifications techniques eTIR : une introduction générale et le système international eTIR ainsi que quelques annexes.

II. Introduction générale

A. Objet

4. Les spécifications techniques du système eTIR ont pour objet de traduire les spécifications fonctionnelles du système eTIR en des exigences techniques, une architecture, des lignes directrices, des procédures et des descriptions détaillées de tous les messages échangés entre le système international eTIR et les parties prenantes eTIR.

5. Le présent document intéresse toutes les parties prenantes eTIR (autorités douanières, chaînes de garantie et titulaires) qui ont besoin de connecter leurs systèmes d'information au système international eTIR. Tous les éléments de ces spécifications doivent être considérés comme obligatoires, sauf indication contraire.

6. Le présent document sert deux objectifs : définir les aspects techniques du système international eTIR et définir sans équivoque la manière dont les informations sont échangées entre le système international eTIR et les parties prenantes eTIR.

B. Domaine d'application

7. Le présent document est divisé en cinq chapitres : la présente introduction générale, puis quatre chapitres qui portent respectivement sur le système international eTIR, la communication entre les parties prenantes eTIR et le système international eTIR, les procédures de secours techniques et enfin, les annexes et appendices. La présente section décrit le domaine d'application et le contenu de ces chapitres.

[1] Décision du Comité des transports intérieurs (ECE/TRANS/294, par. 84) : https://unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294f.pdf.

[2] Mandat du nouveau Groupe approuvé par le Comité des transports intérieurs et le Comité exécutif de la CEE.

[3] Décision du Comité exécutif (ECE/EX/2020/L.2, par. 5 b)) − https://undocs.org/fr/ECE/EX/2020/L.2.

1. Le système international eTIR

8. Le système international eTIR est la pierre angulaire de la procédure eTIR, dans la mesure où il reçoit et enregistre les informations échangées avec les autorités douanières, les chaînes de garantie et éventuellement les titulaires. Le système international eTIR a été mis au point, et il est exploité, hébergé et administré, sous les auspices de la CEE[4].

9. Ce chapitre traite en premier lieu des trois principes sélectionnés pour orienter les activités liées au développement du système international eTIR, les fondements de ces principes et leurs conséquences. Puis il présente l'architecture générale du système international eTIR[5] ainsi que son architecture détaillée, y compris ses composants et interfaces. Il présente aussi en détail les exigences techniques du système qui, sans avoir une incidence directe sur son bon fonctionnement, ont toutefois une importance capitale pour celui-ci. Les procédures de développement, y compris différentes lignes directrices et la liste des environnements informatiques et les procédures connexes, sont aussi décrites pour expliquer les méthodes suivies par la CEE aux fins du développement et de l'exploitation du système international eTIR. Enfin, la dernière section porte sur les exigences techniques liées à la sécurité de l'information et présente en détail le modèle de sécurité du système eTIR.

2. Communication entre les parties prenantes eTIR et le système international eTIR

10. Dans le cadre du système eTIR, les systèmes d'information des parties prenantes eTIR échangent des informations avec le système international eTIR.

11. On trouvera dans ce chapitre une description détaillée des exigences techniques relatives aux interfaces entre les systèmes d'information ainsi que plusieurs éléments auxquels doivent se conformer les systèmes d'information des parties prenantes eTIR. On y trouvera ensuite une description des services Web fournis par le système international eTIR et des détails techniques nécessaires à leur utilisation, puis des informations sur l'architecture et les principes de conception qui sous-tendent la mise en application des messages échangés dans le cadre de la procédure eTIR, assorties de tous les détails techniques pertinents. Enfin, ce chapitre donne des explications sur les projets d'interconnexion que doivent lancer les parties prenantes eTIR afin de connecter leurs systèmes d'information au système international eTIR.

3. Procédures de secours techniques

12. Ce chapitre présente en détail les aspects techniques des procédures de secours (déjà décrites de manière détaillée dans les spécifications fonctionnelles du système eTIR) qui doivent être suivies en cas de problème avec un ou plusieurs éléments du système eTIR.

4. Annexes et appendices

13. Ce dernier chapitre contient un glossaire technique et présente en détail les conventions de notation utilisées dans les diagrammes relatifs à l'architecture du système. Il présente également une analyse destinée à apprécier les besoins du système international eTIR s'agissant de ses capacités et de son extensibilité. Enfin, il présente la structure des fichiers XSD et les conventions employées ainsi que les listes de codes utilisées dans divers attributs des messages eTIR.

C. Public cible

14. Le présent document est établi à l'intention des services informatiques et des experts en informatique des parties prenantes eTIR désireuses d'utiliser la procédure eTIR. Il comprend, en particulier, toutes les informations nécessaires pour permettre aux parties prenantes eTIR de connecter leurs systèmes d'information au système international eTIR.

[4] Conformément au paragraphe 1 de l'article 11 de l'annexe 11 de la Convention TIR.

[5] Voir la définition du « système eTIR » dans la section I.F.

D. Conditions préalables

15. Avant de lire le présent document, il convient d'avoir assimilé les autres volets des spécifications du système eTIR, à savoir l'introduction, les concepts relatifs au système eTIR et les spécifications fonctionnelles. En outre, bien que plusieurs considérations et termes fondamentaux soient rappelés dans le présent document, il importe de bien comprendre la Convention TIR et particulièrement son annexe 11.

16. On suppose, en outre, que les lecteur(rice)s ont une bonne compréhension des notions informatiques et de la terminologie employées dans le présent document, en ce qui concerne notamment le génie logiciel. Ils(elles) doivent également connaître le fonctionnement des services Web et les protocoles SOAP et XML.

E. Documents pertinents

17. On trouvera dans le tableau suivant, à l'intention des lecteur(rice)s qui souhaitent obtenir des informations supplémentaires, la liste et la description de tous les documents qui viennent compléter le présent document.

Tableau 1
Documents pertinents

Titre	*Description*	*Version ou date*
Manuel TIR	Ce document comprend le texte complet de la Convention TIR, y compris ses annexes (à l'exception de l'annexe 11).	2018
Version récapitulative du cadre juridique du système eTIR	L'annexe I du rapport de l'AC.2 sur sa soixante-douzième session présente en détail les amendements à la Convention TIR qui ont été adoptés ainsi que le texte de la nouvelle annexe 11, qui décrit la procédure eTIR.	17 février 2020
Introduction aux documents théoriques, fonctionnels et techniques relatifs au système eTIR	Ce document présente les documents théoriques, fonctionnels et techniques relatifs à la procédure eTIR.	4.3a
Concepts relatifs au système eTIR	Ce document décrit la logique et les concepts fondamentaux qui sous-tendent la mise en œuvre du système eTIR.	4.3a
Spécifications fonctionnelles du système eTIR	Ce document a pour objet de traduire les concepts relatifs au système eTIR en des spécifications qui permettent aux développeur(se)s d'applications et aux concepteur(rice)s de messages de parfaire le système eTIR.	4.3a

F. Définitions

18. On trouvera dans le tableau ci-dessous les définitions de plusieurs termes essentiels utilisés dans le présent document.

Tableau 2
Définition de termes essentiels

Terme	*Définition*
Document d'accompagnement	Document imprimé généré électroniquement par le système douanier, après l'acceptation de la déclaration, conformément aux directives énoncées dans les spécifications techniques du système eTIR. Le document d'accompagnement peut être utilisé pour signaler les incidents survenus en cours de route et il remplace le procès-verbal de constat conformément aux dispositions de l'article 25 de la Convention TIR. Il est également utilisé dans le cadre de la procédure de secours.

Terme	*Définition*
Acteur	Voir « partie prenante eTIR ».
Renseignements anticipés rectifiés	Renseignements communiqués aux autorités compétentes du pays de départ, conformément aux spécifications du système eTIR, qui indiquent l'intention du titulaire de placer des marchandises sous couvert de la procédure eTIR.
Renseignements anticipés TIR	Renseignements communiqués aux autorités compétentes du pays dans lequel une rectification des données de la déclaration est demandée, conformément aux spécifications eTIR, qui indiquent l'intention du titulaire de rectifier les données de sa déclaration.
Bureau de douane de départ	Tout bureau de douane d'une Partie contractante où commence, pour tout ou partie du chargement, le transport TIR.
Bureau de douane de destination	Tout bureau de douane d'une Partie contractante où s'achève, pour tout ou partie du chargement, le transport TIR.
Bureau de douane d'entrée	Tout bureau de douane d'une Partie contractante par lequel un véhicule routier, un ensemble de véhicules ou un conteneur entre sur le territoire de cette Partie contractante dans le cadre d'un transport TIR.
Bureau de douane de sortie	Tout bureau de douane d'une Partie contractante par lequel un véhicule routier, un ensemble de véhicules ou un conteneur quitte le territoire de cette Partie contractante dans le cadre d'un transport TIR.
Union douanière	Une union douanière ou économique comprend deux États membres ou plus et constitue un territoire douanier unique dans le cadre de la procédure eTIR, sous réserve que ces États membres soient Parties contractantes à la Convention TIR et appliquent l'annexe 11.
Système de l'union douanière	Système central d'information d'une union douanière qui relie entre eux les systèmes douaniers nationaux de ses États membres.
Déclaration	Acte par lequel le titulaire, ou son représentant, exprime, conformément aux spécifications du système eTIR, son intention de placer des marchandises sous couvert de la procédure eTIR. Dès lors que la déclaration a été acceptée par les autorités compétentes, sur la base des renseignements anticipés TIR ou des renseignements anticipés rectifiés, et que les données correspondantes ont été transférées dans le système international eTIR, elle constitue l'équivalent juridique d'un carnet TIR accepté.
Données de la déclaration	Renseignements anticipés TIR et les renseignements anticipés rectifiés qui ont été acceptés par les autorités compétentes.
Garantie électronique	Dans le cadre de la procédure eTIR, version électronique de la garantie décrite dans la Convention TIR et matérialisée par un carnet TIR dans le régime TIR.
Système international eTIR	Système informatique conçu pour permettre l'échange électronique de données entre les acteurs de la procédure eTIR.
Procédure eTIR	Régime TIR mis en œuvre au moyen d'un échange électronique de données qui constitue l'équivalent fonctionnel du carnet TIR. Étant entendu que les dispositions de la Convention TIR s'appliquent, les dispositions propres à la procédure eTIR sont énoncées à l'annexe 11.
Services d'assistance eTIR	L'une des fonctions de la CEE est d'aider les parties prenantes eTIR à connecter leurs systèmes d'information au système international eTIR.
Spécifications du système eTIR	Spécifications conceptuelles, fonctionnelles et techniques du système eTIR, adoptées et modifiées conformément aux dispositions de l'article 5 de l'annexe 11.
Partie prenante eTIR	Entité relevant du système eTIR et utilisant la procédure eTIR décrite dans l'annexe 11 de la Convention TIR. Une partie prenante eTIR utilise ses systèmes d'information pour faire partie du système eTIR ; il peut s'agir de l'une quelconque des entités suivantes : • CEE, au moyen du système international eTIR ; • Chaînes de garantie, au moyen de leurs systèmes d'information ;

Terme	*Définition*
	• Autorités douanières, au moyen de leurs systèmes d'information ; • Titulaires, au moyen de leurs systèmes d'information.
Système eTIR	L'ensemble des parties prenantes eTIR, ainsi que leurs systèmes d'information, qui appliquent la procédure eTIR décrite dans l'annexe 11 de la Convention TIR.
Titulaires	Les titulaires de carnets TIR ne possèdent plus de carnets TIR dans le cadre de la procédure eTIR, le but étant justement de remplacer la version papier du carnet par une garantie électronique. Le terme « titulaire » est toutefois conservé dans le cadre de la procédure eTIR ; il désigne la même personne que celle qui est décrite au paragraphe o) de l'article premier de la Convention TIR.
Système douanier national	Système central d'information des autorités douanières d'une Partie contractante à la Convention TIR. Au sens de l'annexe 11, ce système doit être connecté au système international eTIR.
Prédéclaration	Données envoyées par le titulaire au bureau de douane approprié avant de présenter le véhicule routier, l'ensemble de véhicules ou le conteneur. Il peut s'agir de renseignements anticipés TIR, de renseignements anticipés rectifiés ou d'une annulation de renseignements anticipés TIR ou de renseignements anticipés rectifiés envoyés antérieurement.
Mécanisme de demande	Série de messages qui peuvent être utilisés par les parties prenantes eTIR (messages I5/I6 pour les autorités douanières et E5/E6 pour les chaînes de garantie) pour accéder aux informations stockées dans le système international eTIR concernant les garanties électroniques, les titulaires et les opérations TIR.
Organe de mise en œuvre technique	L'organe de mise en œuvre technique est chargé de contrôler les aspects techniques et fonctionnels de la mise en œuvre de la procédure eTIR, ainsi que de coordonner et de favoriser l'échange d'informations sur les questions qui relèvent de sa compétence.

G. Abréviations

19. On trouvera dans le tableau ci-dessous la liste de toutes les abréviations utilisées dans le présent document. La définition de plusieurs de ces termes et expressions se trouve dans le glossaire technique qui figure en appendice.

Tableau 3
Sigles et abréviations

Sigle/abréviation	*Description*
AC.2	Comité de gestion de la Convention TIR de 1975
BGP	Protocole de passerelle frontière
CEE	Commission économique pour l'Europe
EDIFACT	Transmission électronique des données en matière d'administration, de commerce et de transport
Go	Gigaoctet
ISO	Organisation internationale de normalisation
ICP	Infrastructure à clés publiques
ITDB	Banque de données internationale TIR
ITIL	Information Technology Infrastructure Library
Ko	Kilo-octet
Mo	Mégaoctet
OMD	Organisation mondiale des douanes

Sigle/abréviation	*Description*
ONU	Organisation des Nations Unies
PRD	PRoDuction
PRINCE2	PRojects In Controlled Environments 2
RAID	Réseau redondant de disques indépendants
SAN	Réseau de stockage
SGBD	Système de gestion de base de données
SSD	Disque à semi-conducteurs
To	Téraoctet
TIB	Organe de mise en œuvre technique
TIRExB	Commission de contrôle TIR
TOGAF	The Open Group Architecture Framework
UC	Unité centrale
UPS	Alimentation électrique non interruptible
UTC	Temps universel coordonné
UTF	Format de transformation du jeu universel de caractères codés
VCS	Système de gestion des versions
WSDL	Langage de description des services Web
XML	Langage de balisage extensible
XSD	Définition du schéma XML

H. Consultation du présent document

20. Le présent document peut être consulté sur le site Web de la CEE ainsi que sur le site Web consacré au système eTIR[6], où on trouvera les dernières versions de tous les documents relatifs au système eTIR, y compris tous les guides techniques utilisés dans le cadre des projets d'interconnexion.

III. Le système international eTIR

21. Le présent chapitre décrit tous les aspects techniques du système international eTIR ; on y trouvera les informations nécessaires pour comprendre comment ce système est mis en œuvre, administré, hébergé et tenu à jour et comment il doit fonctionner sur le plan technique.

22. Le niveau de détail dépend des aspects traités ; ainsi, il se peut que certains détails techniques fassent défaut, et ce pour deux motifs :

- Étant donné que le présent document est accessible publiquement, certains détails techniques ont été omis intentionnellement, pour des raisons de sécurité. Bien que la CEE ait conscience que la sécurité par l'opacité[7] ne devrait pas constituer la seule mesure de sécurité en place, elle souhaite éviter de divulguer trop d'informations, sous peine de mettre en péril la sécurité du système eTIR. Les Parties contractantes désireuses d'en apprendre davantage sur ces détails supplémentaires peuvent prendre contact avec le Secrétaire TIR pour organiser une visite d'étude dans les locaux de la CEE ;
- Certains aspects relatifs aux produits, infrastructures ou bibliothèques logiciels ou matériels utilisés, ainsi que certains éléments propres à leur mise en œuvre, évoluent fréquemment au gré des rapides progrès technologiques. La CEE devrait avoir toute latitude pour effectuer les modifications qui s'imposent compte tenu de l'évolution des impératifs techniques (concernant, par exemple, les capacités, l'extensibilité et le

[6] Voir etir.org/documentation.
[7] Voir en.wikipedia.org/wiki/Security_through_obscurity.

fonctionnement) sans avoir à fournir une version actualisée des spécifications techniques.

23. Sachant que plusieurs détails techniques ne sont pas mentionnés dans le présent document, la CEE souhaite rester transparente et faire la preuve de son professionnalisme auprès des Parties contractantes en présentant dans le détail ses modalités de travail, ses principes directeurs et ses procédures.

A. Principes directeurs

1. Introduction

24. Les principes décrits dans la présente section définissent les règles générales de base et les valeurs fondamentales qui orientent les décisions prises au sujet des aspects techniques du système international eTIR (qu'il s'agisse, par exemple, de sa conception, de son hébergement, de sa gestion ou encore de sa maintenance). La démarche suivie pour définir ces trois principes est fondée sur la norme TOGAF[8], qui permet d'exprimer les principes d'une architecture logicielle.

2. Principe 1 : Sécurité de l'information

a) Énoncé

25. Les informations stockées dans le système international eTIR sont considérées comme étant confidentielles et peuvent être consultées en tout temps, bien qu'uniquement par les parties prenantes habilitées, au moyen de messages eTIR qui doivent être authentifiés et sécurisés.

b) Fondements

26. Les articles 7 et 8 de l'annexe 11 de la Convention TIR énoncent des prescriptions relatives à l'authentification et à l'intégrité des données.

27. Les articles 11 et 12 de l'annexe 11 de la Convention TIR énoncent des prescriptions relatives à la mise à disposition et à l'intégrité des données.

c) Conséquences

28. La confidentialité, l'intégrité, la mise à disposition et la non-répudiation des informations échangées (données en transit) entre le système international eTIR et les parties prenantes eTIR et enregistrées dans le système international eTIR (données au repos) doivent être garanties.

29. Les informations échangées et enregistrées dans le système international eTIR sont classées comme confidentielles conformément aux dispositions de la circulaire du Secrétaire général intitulée « Informations sensibles ou confidentielles : classification et maniement »[9] et les politiques et mesures pertinentes s'appliquent.

3. Principe 2 : Haut degré de fiabilité et de qualité

a) Énoncé

30. Le développement et la maintenance du système international eTIR doivent suivre des normes de haute fiabilité et de haute qualité, et ces normes doivent être continuellement révisées et améliorées.

b) Fondements

31. Un haut degré de fiabilité permet de réduire au minimum les coûts afférents au développement, au fonctionnement et à la maintenance du système international eTIR.

[8] Voir la norme TOGAF ® v9.2 : pubs.opengroup.org/architecture/togaf9-doc/arch/chap20.html.
[9] Voir undocs.org/fr/st/sgb/2007/6.

32. Un haut degré de fiabilité permet de réduire au minimum les ressources que doivent engager les parties prenantes eTIR pour mettre au point, exploiter et maintenir l'interconnexion entre leurs systèmes d'information et le système international eTIR.

c) Conséquences

33. Il convient d'adopter les pratiques optimales ayant fait leurs preuves dans le secteur des technologies de l'information pour développer, exploiter et tenir à jour le système international eTIR.

34. Les nouvelles tendances constatées dans le secteur des technologies de l'information devraient être régulièrement évaluées pour trouver le moyen d'améliorer continuellement le développement, le fonctionnement et la maintenance du système international eTIR.

4. Principe 3 : Facilité de connexion pour les parties prenantes eTIR

a) Énoncé

35. Le système international eTIR doit être conçu et la documentation pertinente doit être élaborée de manière à faciliter l'interconnexion avec les parties prenantes eTIR, y compris la mise à jour vers les nouvelles versions.

b) Fondements

36. La facilité de connexion permet de réduire au minimum les ressources que doivent engager les parties prenantes eTIR pour mettre en place, exploiter et maintenir l'interconnexion entre leurs systèmes d'information et le système international eTIR.

37. La facilité de connexion permet de réduire au minimum les coûts engagés par les services d'assistance eTIR pour aider les Parties contractantes à connecter leur système douanier national au système international eTIR.

c) Conséquences

38. Le système international eTIR, ses interfaces et les documents qui s'y rapportent doivent reposer, dans la mesure du possible, sur des normes mondialement reconnues.

39. La documentation nécessaire doit être produite, en plus des spécifications eTIR, pour orienter et accompagner les parties prenantes eTIR dans leurs projets d'interconnexion.

40. Grâce à l'expérience acquise et aux données reçues en retour dans le cadre de l'assistance prêtée aux parties prenantes eTIR aux fins de leurs projets d'interconnexion, des améliorations supplémentaires devraient être apportées pour perfectionner continuellement la documentation et l'aide fournies par les services d'assistance eTIR.

B. Architecture générale du système eTIR

1. Introduction

41. On trouvera dans la présente section des informations sur l'architecture technique générale du système eTIR et, en particulier, sur les interactions entre les systèmes d'information des différents acteurs de la procédure eTIR. Y figure également un aperçu détaillé des systèmes d'information de chaque acteur, y compris les interfaces et les messages échangés.

42. Les diagrammes de la présente section suivent le modèle de notation ArchiMate[10] qui est décrit dans l'annexe IV.A du présent document.

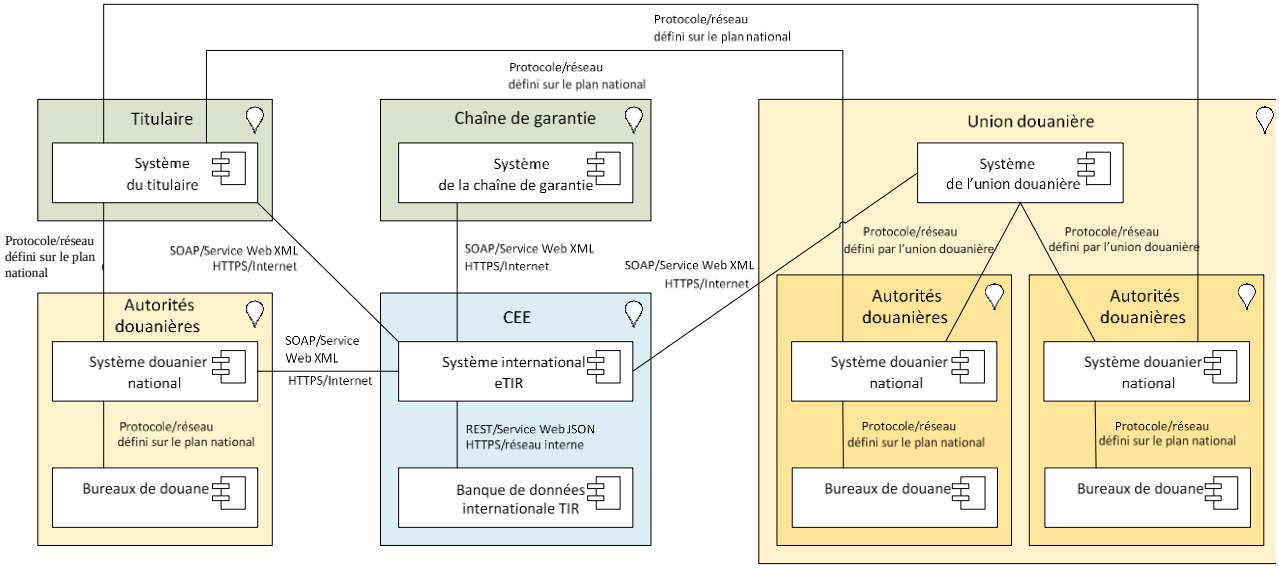
2. Aperçu

43. Le système eTIR est constitué par l'interconnexion entre les systèmes d'information des différents acteurs de la procédure eTIR : les autorités douanières, les titulaires, les chaînes

[10] Spécifications ArchiMate®, version 3.0.1. Voir : pubs.opengroup.org/architecture/archimate3-doc/.

de garantie et la CEE. L'architecture technique globale présentée dans la figure ci-dessous illustre l'interconnexion entre les systèmes d'information de tous les acteurs, y compris dans le cas des unions douanières. Celles-ci pourraient tirer parti des connexions et des systèmes d'information qu'elles ont déjà mis en place pour leur propre usage[11].

Figure I
Architecture technique globale du système eTIR



44. On trouvera dans les sections suivantes plus de détails sur les systèmes d'information de chaque acteur, en particulier les interfaces et les messages échangés. Afin d'éviter les répétitions, les interfaces entre deux systèmes d'information ne sont présentées en détail que dans la section concernant l'acteur qui est à l'origine de la plupart des transactions.

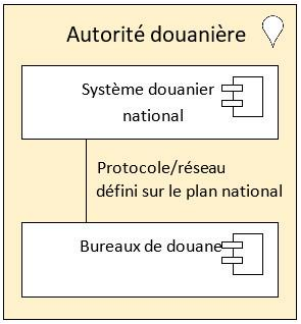
3. Autorités douanières

45. Les autorités douanières se servent de systèmes d'information pour gérer les procédures douanières telles que l'importation, l'exportation et le transit. La conception et l'architecture de ces systèmes d'information étant l'apanage exclusif des autorités douanières compétentes, elles peuvent varier fortement d'une Partie contractante à une autre. On suppose que les bureaux de douane sont connectés avec le système central d'information des autorités douanières, dénommé ci-après « système douanier national ».

46. Afin de mettre en œuvre correctement les dispositions de l'annexe 11 de la Convention TIR et d'adapter leurs systèmes d'information à la procédure eTIR, les autorités douanières doivent connecter leur système douanier national au système international eTIR. Dans le cadre de la procédure eTIR, les principaux acteurs côté douanes sont les agents des douanes (situés dans les bureaux de douane) qui traitent les transports TIR. S'il est nécessaire que tous les bureaux de douane habilités à traiter des transports TIR dans le cadre de la procédure eTIR soient connectés au système douanier national concerné, les modalités de connexion relèvent de chaque autorité douanière. De même, les interfaces utilisateur qu'utilisent les agents des douanes pour traiter la procédure eTIR sont conçues et mises en œuvre par chaque autorité douanière.

[11] Comme cela est suggéré dans la note explicative au paragraphe 2 de l'article 3 de l'annexe 11 de la Convention TIR.

Figure II
Interactions entre les systèmes douaniers nationaux et les bureaux de douane



47. Les agents des douanes échangent des informations avec le système international eTIR par l'intermédiaire de leur système douanier national, au moyen des messages suivants :

- « I1 − Accepter la garantie » (pour accepter la garantie affectée à une opération TIR) associé à la réponse « I2 − Résultats de l'acceptation de la garantie » ;
- « I5 − Demander des informations sur la garantie » (pour demander des informations relatives à une garantie existante) associé à la réponse « I6 − Résultats de la demande d'informations sur la garantie » ;
- « I7 − Enregistrer les données de la déclaration » (pour enregistrer les données d'une déclaration relative à une opération TIR) associé à la réponse « I8 − Résultats de l'enregistrement des données de la déclaration » ;
- « I9 − Lancer l'opération TIR » (pour commencer une opération TIR) associé à la réponse « I10 − Résultats du lancement de l'opération TIR » ;
- « I11 − Achever l'opération TIR » (pour achever une opération TIR) associé à la réponse « I12 − Résultats de l'achèvement de l'opération TIR » ;
- « I13 − Apurer l'opération TIR » (pour apurer une opération TIR) associé à la réponse « I14 − Résultats de l'apurement de l'opération TIR » ;
- « I17 − Refuser le lancement d'une opération TIR » (pour refuser le lancement d'une opération TIR) associé à la réponse « I18 − Résultats du refus du lancement d'une opération TIR ».

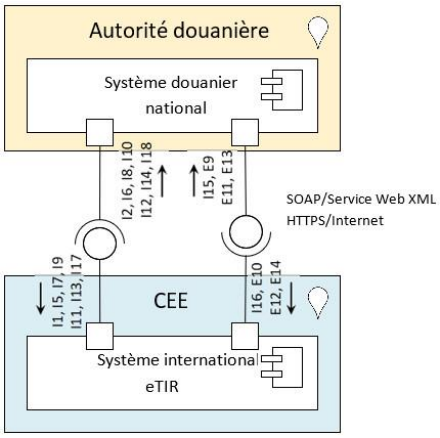
48. En outre, le système international eTIR peut notifier au système douanier national des événements particuliers relatifs à une opération de transport TIR, au moyen du message de demande « I15 − Notifier les services douaniers » associé à la réponse « I16 − Confirmation de la notification aux services douaniers ».

49. Enfin, le système international eTIR peut faire suivre aux autorités douanières compétentes des informations fournies par le titulaire concernant les renseignements anticipés TIR et les renseignements anticipés rectifiés[12], au moyen des messages suivants :

- « E9 − Renseignements anticipés TIR » (pour recevoir les renseignements anticipés TIR envoyés par le titulaire par l'intermédiaire du système international eTIR) associé à la réponse « E10 − Résultats pour les renseignements anticipés TIR » ;
- « E11 − Renseignements anticipés rectifiés » (pour recevoir les renseignements anticipés rectifiés envoyés par le titulaire par l'intermédiaire du système international eTIR) associé à la réponse « E12 − Résultats pour les renseignements anticipés rectifiés » ;
- « E13 − Annuler les renseignements anticipés » (pour recevoir les informations relatives à l'annulation de renseignements anticipés TIR ou de renseignements anticipés rectifiés envoyés antérieurement) associé à la réponse « E14 − Résultats de l'annulation des renseignements anticipés ».

[12] Conformément aux paragraphes 2 et 3 de l'article 6 de l'annexe 11 de la Convention TIR.

Figure III
Interactions entre le système douanier national et le système international eTIR



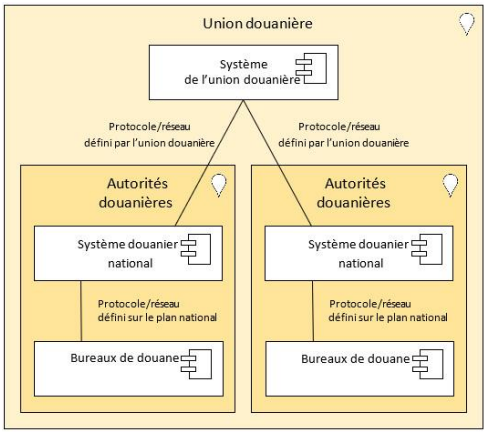
50. Ces messages (I1, I2, I5, I6, I7, I8, I9, I10, I11, I12, I13, I14, I15, I16, I17, I18, E9, E10, E11, E12, E13 et E14) sont transmis par l'intermédiaire d'un protocole HTTPS via Internet au moyen de services Web SOAP et les données sont transférées au format XML.

4. Unions douanières

51. Une union douanière peut avoir mis en place un système pour faciliter les échanges d'informations entre les systèmes douaniers nationaux de ses États membres. La conception et l'architecture de ces systèmes étant l'apanage exclusif des unions douanières concernées, elles peuvent varier d'une union douanière à une autre.

52. Afin de mettre en œuvre correctement les dispositions de l'annexe 11 de la Convention TIR et d'adapter leurs systèmes d'information à la procédure eTIR, les États membres d'une union douanière peuvent vouloir connecter leurs systèmes douaniers nationaux au système international eTIR par l'intermédiaire du système de l'union douanière. En pareil cas, le système de l'union douanière transmet les messages pertinents aux destinataires appropriés et peut éventuellement jouer aussi un rôle de convertisseur si les messages échangés entre le système de l'union douanière et un système douanier national ne sont pas conformes aux spécifications eTIR.

Figure IV
Interactions entre le système de l'union douanière et les systèmes douaniers nationaux



53. Dans le reste du présent document, on considérera que l'interface entre le système international eTIR et le système d'une union douanière est le même qu'entre le système international eTIR et un système douanier national, sauf indication contraire.

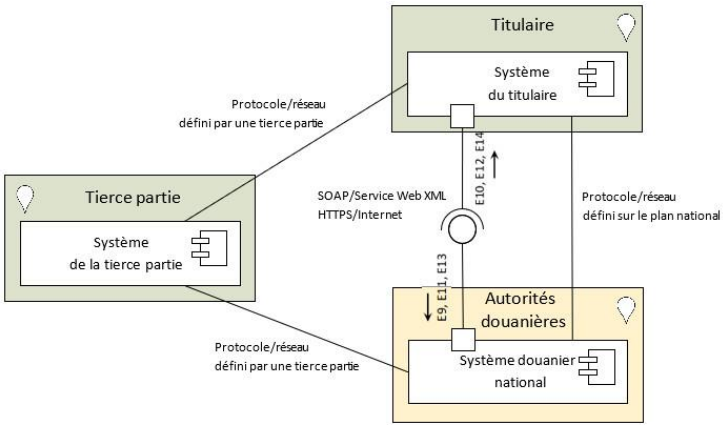
5. Titulaires

54. Les titulaires sont tenus de soumettre au bureau de douane de départ les renseignements anticipés TIR relatifs à l'opération de transport TIR qu'ils souhaitent lancer.

Ils ont toujours la possibilité d'annuler des renseignements anticipés TIR envoyés antérieurement et de soumettre de nouveaux renseignements anticipés TIR. Dès que la déclaration est acceptée par le bureau de douane de départ, le titulaire peut envoyer des « renseignements anticipés rectifiés » au prochain bureau de douane d'entrée ou de départ pour demander la modification de la déclaration. Il peut alors annuler des renseignements anticipés rectifiés envoyés antérieurement, tant que ces renseignements n'ont pas encore été acceptés par les autorités douanières.

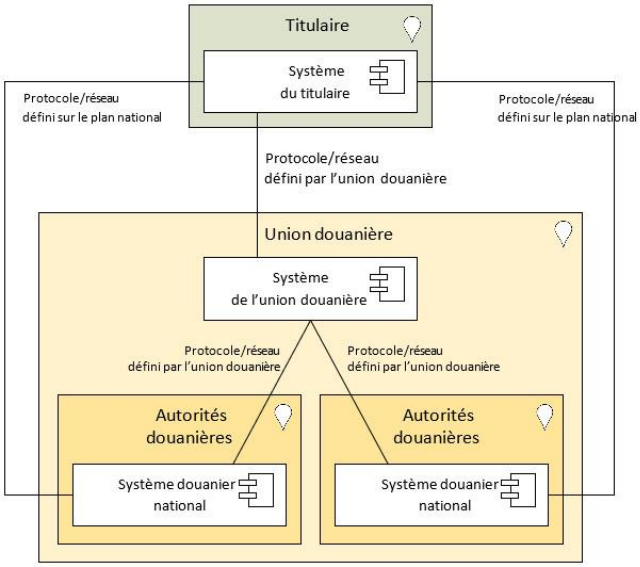
55. Il existe plusieurs moyens électroniques pour soumettre ces informations aux autorités douanières : depuis un portail Web administré par les autorités douanières, au moyen de services Web conformément aux spécifications eTIR, depuis un portail Web administré par une tierce partie, etc. Chaque autorité douanière est tenue de publier la liste complète des moyens possibles pour soumettre ces informations[13]. Tous les moyens électroniques employés doivent transmettre les informations voulues au moyen des messages eTIR adaptés, à savoir : E9, E11 et E13.

Figure V
Interactions possibles entre le système du titulaire et le système douanier national



56. Dans le cas des unions douanières, également, les titulaires peuvent soumettre des informations de prédéclaration aux autorités douanières compétentes des États membres qui en font partie. En plus des moyens déjà présentés en détail dans le paragraphe précédent, un portail supplémentaire peut aussi exister au niveau de l'union douanière.

Figure VI
Interactions entre le système du titulaire et le système d'une union douanière

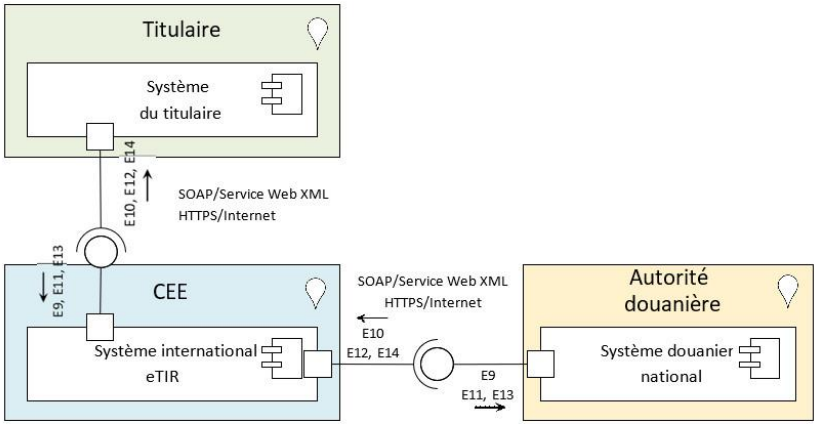


[13] Conformément au paragraphe 4 de l'article 6 de l'annexe 11 de la Convention TIR.

57. Enfin, les titulaires peuvent toujours soumettre au bureau de douane compétent des informations de prédéclaration par l'intermédiaire du système international eTIR[14], en utilisant les messages suivants :

- « E9 − Renseignements anticipés TIR » (pour envoyer les renseignements anticipés TIR au bureau de douane de départ par l'intermédiaire du système international eTIR) associé à la réponse « E10 − Résultats pour les renseignements anticipés TIR » ;
- « E11 − Renseignements anticipés rectifiés » (pour envoyer les renseignements anticipés rectifiés au bureau de douane compétent par l'intermédiaire du système international eTIR) associé à la réponse « E12 − Résultats pour les renseignements anticipés rectifiés » ;
- « E13 − Annuler les renseignements anticipés » (pour envoyer au bureau de douane compétent des informations relatives à des renseignements anticipés TIR ou à des renseignements anticipés rectifiés par l'intermédiaire du système international eTIR) associé à la réponse « E14 − Résultats de l'annulation des renseignements anticipés ».

Figure VII
Interactions entre le système du titulaire et le système douanier national via le système international eTIR



58. Ces messages (E9, E10, E11, E12, E13 et E14) sont transmis par l'intermédiaire d'un protocole HTTPS via Internet au moyen de services Web SOAP et les données sont transférées au format XML.

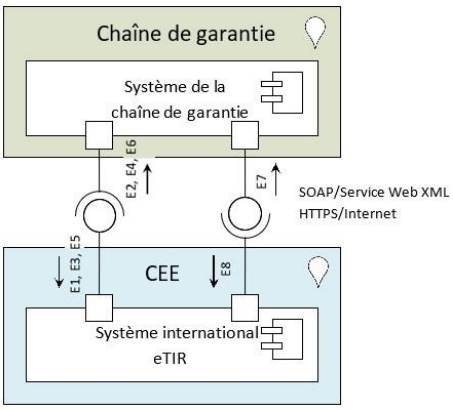
6. Chaînes de garantie

59. Les chaînes de garantie administrent les systèmes d'information utilisés pour la gestion des garanties électroniques et l'échange des données nécessaires avec le système international eTIR, au moyen des messages suivants :

- « E1 − Enregistrer la garantie » (pour enregistrer une nouvelle garantie) associé à la réponse « E2 − Résultats de l'enregistrement de la garantie » ;
- « E3 − Annuler la garantie » (pour annuler une garantie existante) associé à la réponse « E4 − Résultats de l'annulation de la garantie » ;
- « E5 − Demander des informations sur la garantie » (pour demander toutes les informations relatives à une garantie existante) associé à la réponse « E6 − Résultats de la demande d'informations sur la garantie » ;
- « E7 − Notifier la chaîne de garantie » (pour que des événements particuliers relatifs à une garantie existante soient notifiés aux chaînes de garantie par le système international eTIR) associé à la réponse « E8 − Confirmation de la notification à la chaîne de garantie ».

[14] Conformément aux paragraphes 2 et 3 de l'article 6 de l'annexe 11 de la Convention TIR.

Figure VIII
Interactions entre la chaîne de garantie et le système international eTIR



60. Ces messages (E1, E2, E3, E4, E5, E6, E7 et E8) sont transmis par l'intermédiaire d'un protocole HTTPS via Internet au moyen de services Web SOAP et les données sont transférées au format XML.

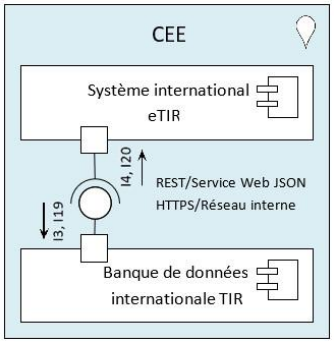
7. Commission économique pour l'Europe

61. La CEE administre deux systèmes d'information : le système international eTIR et la Banque de données internationale TIR (ITDB). Le système international eTIR est la pierre angulaire du système eTIR et a pour fonction principale de recevoir, de valider, d'enregistrer et d'envoyer les données échangées entre les différents acteurs pendant les transports TIR conformément à la procédure eTIR. L'ITDB est un système d'information mis au point sous les auspices de la TIRExB et a pour principale fonction, dans le cadre du système eTIR, de gérer la liste des titulaires de carnets TIR agréés et la liste des bureaux de douane habilités à réaliser des opérations TIR.

62. Pour ce qui est du traitement des renseignements reçus au moyen des messages eTIR, le système international eTIR interroge l'ITDB (le cas échéant) pour :

- Vérifier l'agrément d'un titulaire en utilisant le message de demande « I3 − Obtenir des informations sur le titulaire » associé à la réponse « I4 − Informations sur le titulaire » ;
- Vérifier l'existence du bureau de douane en utilisant le message de demande « I19 − Vérifier les bureaux de douane » associé à la réponse « I20 − Validation des bureaux de douane ».

Figure IX
Interactions entre le système international eTIR et l'ITDB



63. Ces messages (I3, I4, I19 et I20) sont transmis par l'intermédiaire d'un protocole HTTPS via le réseau sécurisé du centre informatique qui héberge chacun des deux systèmes d'information, au moyen de services Web RESTful et les données sont transférées au format JSON.

C. Architecture détaillée du système international eTIR

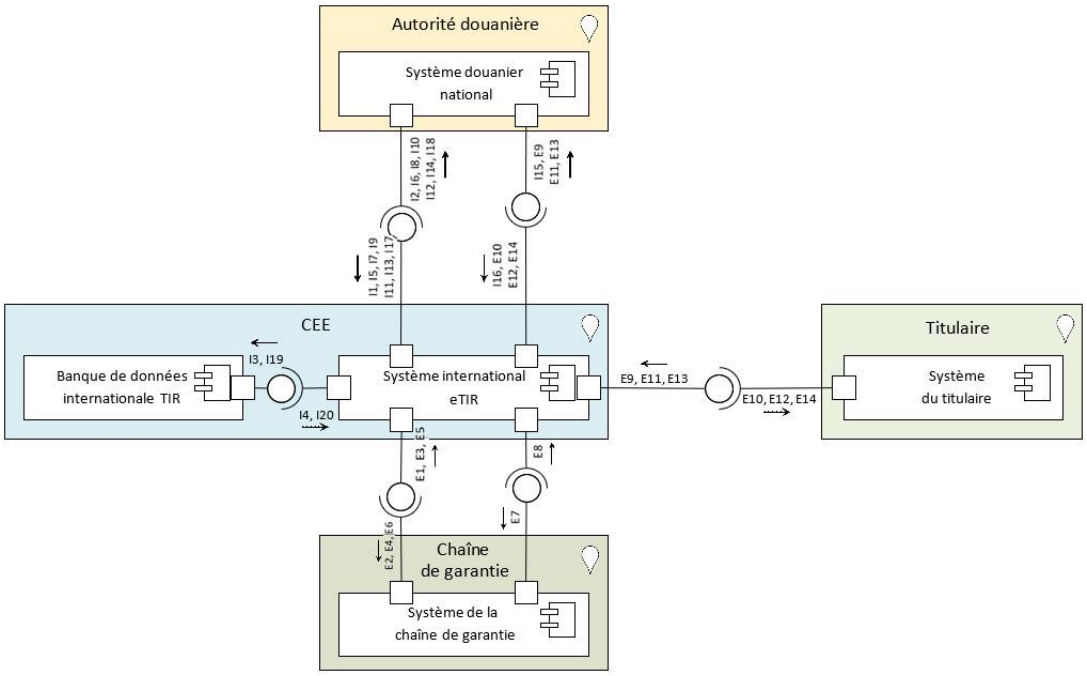
1. Introduction

64. La présente section décrit les éléments logiciels et matériels de l'architecture du système international eTIR. Afin que son contenu reste neutre en ce qui concerne les technologies, elle ne contient pas d'informations sur les produits, les infrastructures ou les bibliothèques utilisés pour mettre en œuvre les fonctions nécessaires aux composants. En effet, compte tenu de l'évolution rapide de la technologie, la CEE se tiendra continuellement informée quant aux options disponibles et effectuera des modifications quand elle le jugera nécessaire afin que les composants du système international eTIR puissent continuer de fonctionner normalement et se développer suffisamment afin de pouvoir, dans le temps, fournir les capacités nécessaires et satisfaire aux normes d'exploitation (voir la section suivante concernant les exigences techniques).

2. Interfaces avec les parties prenantes eTIR

65. Les interfaces entre le système international eTIR et les autres parties prenantes eTIR sont déjà présentées en détail dans la section précédente. La figure ci-après résume toutes ces interfaces, en précisant les codes correspondant aux messages pertinents et le flux de l'information.

Figure X
Interfaces du système international eTIR



3. Lieux de stockage

66. Les messages sont traités par le système international eTIR et les éléments qui les composent sont enregistrés en trois lieux différents :

- Tous les messages sortants et entrants sont intégralement enregistrés dans le **journal eTIR**, le but étant de conserver les données nécessaires à la non-répudiation et de pouvoir fournir aux Parties contractantes les informations éventuellement demandées ;
- Les données extraites des messages sont enregistrées dans la **base de données eTIR** afin de pouvoir être interrogées par le mécanisme de demande et à des fins statistiques ;
- Si des « documents joints » ou des « certificats d'agrément » sont inclus dans les messages (ce qui peut être le cas pour les messages E6, E9, I6, I7 et I15), ils sont

extraits et sauvegardés en tant que fichiers dans les **documents eTIR**, un système de fichiers distinct centralisé et sécurisé.

4. Architecture logicielle

67. Le système international eTIR repose sur les composants logiciels suivants :

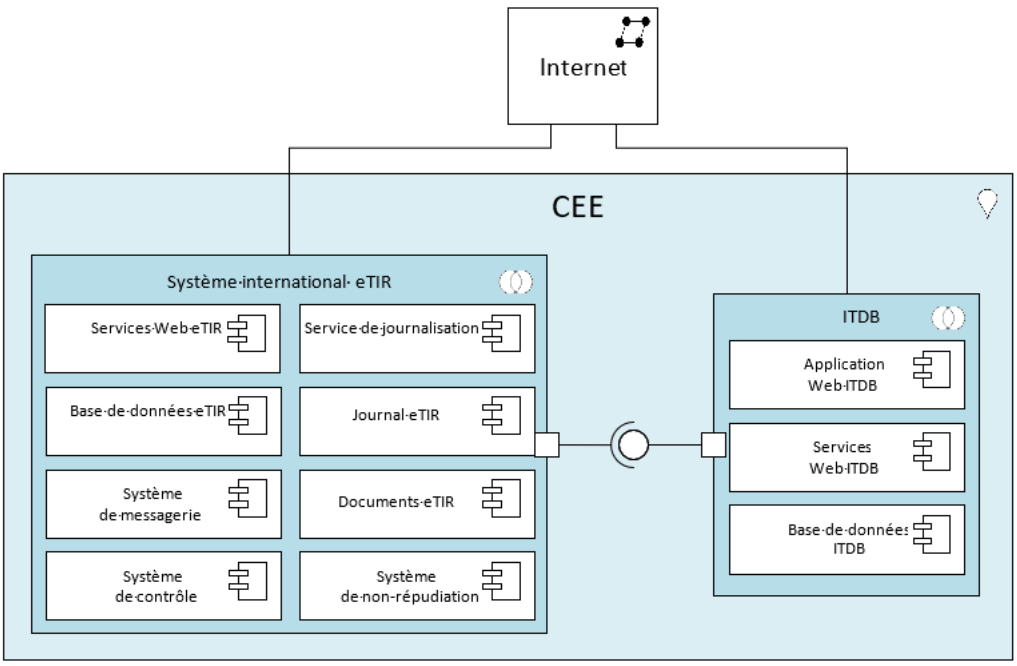
- Les **services Web eTIR**, où les messages sont reçus, validés, traités, enregistrés et envoyés, constituent le cœur du système international eTIR ;
- Le **service de journalisation** sert à enregistrer tous les messages envoyés et reçus par le système international eTIR, ainsi que toutes les informations enregistrées par ses autres composants, infrastructures et bibliothèques logiciels.

68. Le système international eTIR repose aussi sur les systèmes suivants :

- Le **système de messagerie** sert à envoyer des messages par courrier électronique aux parties prenantes eTIR à des occasions particulières, principalement durant une procédure de secours ;
- Le **système de contrôle** sert à surveiller les ressources et le fonctionnement des serveurs virtuels, ainsi que la disponibilité et le fonctionnement des services du système international eTIR ;
- Le **système de non-répudiation** permet d'extraire les données stockées dans les journaux eTIR, de les indexer et de mettre à disposition une interface utilisateur accessible exclusivement aux administrateurs informatiques de la CEE. Cette interface utilisateur permet d'interroger les journaux pour trouver un message donné (au moyen de son « identifiant message » unique) ou un couple de messages demande/réponse, et de fournir aux Parties contractantes toutes les informations voulues à des fins de vérification[15].

69. Le diagramme ci-dessous présente l'architecture logicielle du système international eTIR. Les interfaces exploitées et utilisées par le système international eTIR ne sont pas représentées puisqu'elles sont déjà énumérées et décrites dans les sections précédentes.

Figure XI
Architecture logicielle du système international eTIR



[15] Conformément au paragraphe 3 de l'article 12 de l'annexe 11 de la Convention TIR.

70. Les exigences techniques des composants logiciels du système international eTIR sont énumérées dans la section suivante. Les composants logiciels de l'ITDB ne sont énumérés qu'à titre d'information, dans la mesure où ils sont gérés par la CEE, sous les auspices de la TIRExB.

5. Architecture des systèmes

71. L'entité des Nations Unies qui héberge le système international eTIR (ci-après l'entité d'hébergement) dispose de son propre centre de données situé dans un complexe de l'ONU ; elle bénéficie donc des privilèges et immunités consacrés par la Charte des Nations Unies[16] et exposés plus en détail dans la Convention sur les privilèges et immunités des Nations Unies[17].

72. L'entité d'hébergement emploie une batterie de serveurs virtuels pour fournir les serveurs qui constituent les divers composants du système international eTIR ; actuellement, à chaque nœud de réseau correspond un server virtuel. La CEE envisage d'utiliser, dans un avenir proche, des conteneurs et des méthodes d'orchestration de conteneurs pour mieux répondre aux exigences relatives à l'extensibilité du système international eTIR tout en maintenant les coûts d'hébergement à un niveau acceptable.

73. Le système international eTIR est conçu et mis en œuvre de sorte à limiter les points uniques de défaillance afin que les objectifs de disponibilité du système (présentés en détail dans la section suivante) soient remplis. Cette architecture permet, en outre, d'intervenir sur les composants système sans avoir à mettre le système international eTIR à l'arrêt. Il est particulièrement important d'assurer la maintenance régulière du système, par exemple, en remplaçant le matériel défectueux, en actualisant les composants logiciels et en appliquant les correctifs logiciels nécessaires.

74. Le système international eTIR repose sur les composants système suivants (les exigences techniques correspondantes sont énumérées dans la section suivante) :

- Les **services Web eTIR** constituent le cœur du système international eTIR, où les messages sont reçus, validés, traités, enregistrés et envoyés. Il comprend plusieurs nœuds de serveur Web frontal auxquels l'équilibreur de charge distribue les messages ;
- La **base de données eTIR** constitue le principal lieu de stockage et comprend un système de gestion de bases de données (SGBD) en cluster qui utilise plusieurs nœuds de serveurs virtuels et un stockage sur disque à haute performance ;
- Le **journal eTIR** est le lieu de stockage dans lequel les informations enregistrées sont transférées quotidiennement ; il comprend un serveur virtuel pourvu d'un espace disque suffisant pour stocker toutes les informations du journal ;
- Les **documents eTIR** constituent le lieu de stockage dans lequel les documents joints sont sauvegardés ; il comprend un serveur virtuel pourvu d'un espace disque suffisant pour stocker tous les documents.

75. Le système international eTIR repose aussi sur les composants système externes suivants :

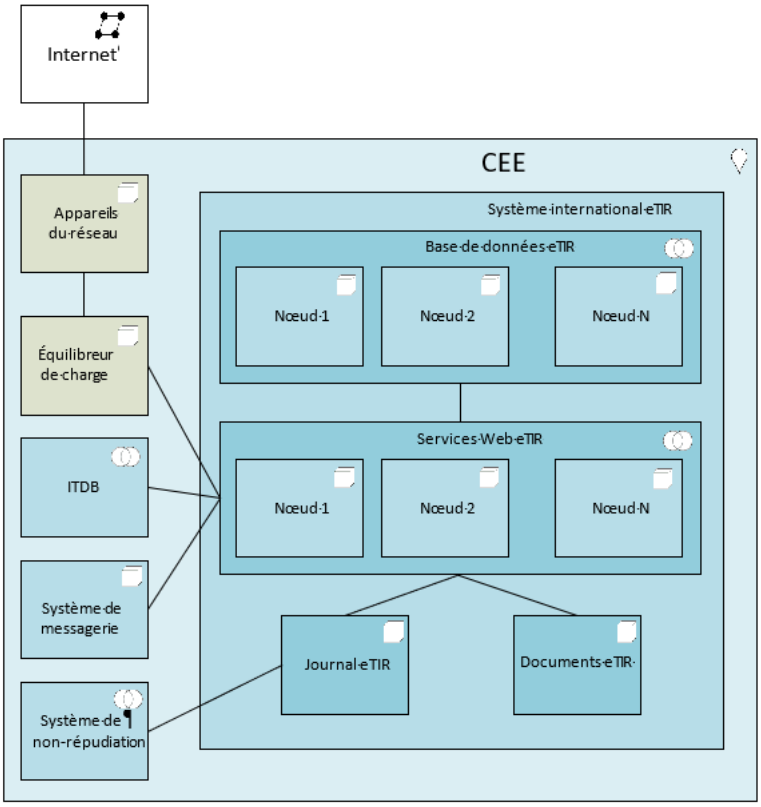
- L'**ITDB** dispose de sa propre architecture système pour satisfaire à ses objectifs de disponibilité. En cas d'indisponibilité de l'ITDB, le système international eTIR suit une procédure de secours décrite plus loin dans le présent document ;
- Le **système de messagerie** est fourni par l'entité d'hébergement et comprend un serveur virtuel réservé exclusivement à l'envoi de messages électroniques. Le système international eTIR utilise principalement ce système externe en cas de procédure de secours ;

[16] Voir un.org/fr/about-us/un-charter.
[17] Voir treaties.un.org/doc/Treaties/1946/12/19461214%2010-17%20PM/Ch_III_1p.pdf.

- Le **système de non-répudiation** est un système externe de gestion qui n'est pas directement nécessaire au bon fonctionnement du système international eTIR et qui ne comprend donc qu'un serveur virtuel unique.

76. Le diagramme suivant représente l'architecture du système international eTIR.

Figure XII
Architecture du système international eTIR



77. Le scénario type suivant illustre un échange d'informations typique entre les composants du système. Un message entrant envoyé par une partie prenante eTIR par Internet atteint en premier lieu les appareils du réseau de l'entité d'hébergement (routeur BGP et pare-feu). Puis le message est transféré à l'équilibreur de charge, qui le fait suivre au nœud approprié des services Web eTIR (serveur Web frontal), lequel valide et traite le message. Ce serveur Web stocke ensuite les données pertinentes dans la base de données eTIR, dans le journal eTIR et, le cas échéant, dans les documents eTIR. Enfin, il établit le message de réponse et l'envoie à la partie prenante eTIR qui a initialement envoyé le message de demande. Par souci de clarté, les systèmes additionnels liés au routage réseau et à la sécurité ne sont pas représentés sur ce diagramme (routeurs, commutateurs, pare-feu, système de détection des intrusions, système de prévention des intrusions, etc.).

D. Exigences techniques

1. Introduction

78. La présente section décrit les exigences techniques − ou non fonctionnelles − auxquelles le système international eTIR doit se conformer. Les exigences techniques sont des critères qui peuvent être utilisés pour juger dans quelle mesure un système est efficace et remplit sa fonction. Ces critères, aussi importants que les exigences fonctionnelles, conditionnent l'architecture et les principes de conception du système.

79. Chacune des sous-sections suivantes décrit les exigences relatives à un critère non fonctionnel particulier. Ces exigences peuvent être de nature qualitative (par exemple, le code source doit être versionné avec Git) ou quantitative (par exemple, le système international

eTIR doit être accessible 24 heures sur 24 et 365 jours par an). Par souci de clarté, un identifiant unique est affecté à chaque exigence.

80. Pour être à même d'apprécier dans quelle mesure les exigences quantitatives sont remplies, on doit disposer d'indicateurs. Sous réserve qu'ils puissent être divulgués sans danger pour la sécurité du système, ceux-ci peuvent être communiqués périodiquement au TIB pour information.

81. Étant donné que le système international eTIR repose sur l'échange de messages par l'intermédiaire de services Web et qu'il n'est pas prévu qu'une quelconque interface utilisateur soit développée pour le système (sauf à des fins internes propres à son administration), les critères suivants ne sont pas applicables et ne seront donc pas décrits : accessibilité, compatibilité et utilisabilité.

82. Plusieurs objectifs quantitatifs seront régulièrement évalués par la CEE et communiqués au TIB, avec des propositions visant à combler les éventuelles déficiences et à mieux cibler les objectifs. Le TIB décidera alors s'il convient de mettre en œuvre ces propositions ou de les recommander à l'AC.2.

83. Enfin, lorsque des produits, logiciels, infrastructures et bibliothèques utilisés pour répondre aux exigences sont mentionnés, la CEE se réserve le droit de modifier sa sélection ultérieurement dans l'intérêt du système eTIR, sous réserve que cette décision n'entraîne pas de coûts supplémentaires. Les informations relatives à cette nouvelle sélection éventuelle seront communiquées au TIB et la version suivante des spécifications du système eTIR actualisée en conséquence.

2. Disponibilité

84. Le système international eTIR est disponible quand il est pleinement accessible et utilisable par ses utilisateurs habilités (CEE et toutes les parties prenantes eTIR connectées au système).

85. La disponibilité du système international eTIR est vitale pour le bon fonctionnement de l'ensemble du système dès son lancement, et le sera d'autant plus lorsque le nombre de transports TIR réalisés dans le cadre de la procédure eTIR augmentera. Les tableaux ci-dessous décrivent les éléments tant qualitatifs que quantitatifs des exigences relatives à la disponibilité. Plusieurs d'entre eux seront intégrés à l'accord de prestation de services à signer avec l'entité des Nations Unies sélectionnée pour héberger le système (ci-après l'entité d'hébergement).

Tableau 4
Exigences qualitatives relatives à la disponibilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AV.1	Les opérations normales de maintenance des composants logiciels et matériels du système international eTIR sont exécutées de manière transparente, le service restant disponible.	Concevoir le système international eTIR de manière à éviter les points de défaillance uniques, en utilisant plusieurs serveurs Web frontaux pour équilibrer la charge de travail, en formant des clusters de bases de données, en dupliquant des composants d'application, et éventuellement en utilisant des serveurs mandataires à haute disponibilité ou des méthodes d'orchestration de conteneurs

Tableau 5
Exigences quantitatives relatives à la disponibilité

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
AV.2	Disponibilité générale du système international eTIR	Héberger le système international eTIR dans une entité de l'ONU qui offre ce niveau de disponibilité, en précisant ce	24 heures par jour, tous les jours de l'année

		point dans l'accord de prestation de services.	
AV.3	Pourcentage de temps de disponibilité du système international eTIR	Les opérations normales de maintenance des composants logiciels et matériels du système international eTIR sont réalisées de manière transparente, le service restant disponible. Les problèmes informatiques sont rapidement décelés et sont traités selon des procédures normalisées et un mécanisme de remontée de l'information.	Plus de 99 % (à savoir une durée maximale d'indisponibilité de 3 j, 15 h, 39 m et 29 s par an)
AV.4	Temps maximal d'indisponibilité continue du système international eTIR en cas de problème majeur	Un suivi des services, des composants logiciels et des serveurs virtuels est mis en place et configuré en concertation avec l'entité d'hébergement. Les procédures sont arrêtées et établies dans l'accord de prestation de services.	4 heures en semaine et 24 heures pendant les week-ends, par incident

86. Quand le système international eTIR commencera à être utilisé en production, à la suite de l'analyse des mesures collectées et des informations communiquées en retour par les parties prenantes eTIR, la CEE ou le TIB voudront peut-être proposer d'améliorer les valeurs cibles des exigences AV.3 et AV.4 pour accroître la disponibilité du service. Dans ce cas, la CEE pourra soumettre au TIB une proposition visant à améliorer les valeurs cibles susmentionnées, en précisant les éventuelles incidences budgétaires.

3. Sauvegarde

87. Une sauvegarde est une copie des données eTIR faite et stockée en un lieu distinct et sécurisé de manière à pouvoir restaurer ces données en cas de perte.

88. Pour que les exigences soient remplies, chaque emplacement de stockage (à savoir la base de données eTIR, les journaux eTIR et les documents eTIR) sera sauvegardé. Les exigences présentées dans le tableau ci-dessous seront intégrées à l'accord de prestation de services à signer avec l'entité d'hébergement.

Tableau 6
Exigences relatives aux copies de sauvegarde

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
BK.1	Fréquence des copies de sauvegarde des données du système eTIR	Les informations stockées dans la base de données eTIR, les journaux eTIR et les documents eTIR sont copiées deux fois par jour et stockées en un lieu sécurisé.	12 heures
BK.2	Délai maximal de restauration des données sauvegardées en cas de perte de données	Les procédures de restauration des données sont définies et établies dans l'accord de prestation de services, en concertation avec l'entité d'hébergement. Des tests sont régulièrement réalisés.	6 heures

89. Quand le système international eTIR commencera à être utilisé en production, la CEE ou le TIB voudront peut-être proposer d'améliorer les valeurs cibles des exigences BK.1 et BK.2. Dans ce cas, la CEE pourra soumettre au TIB une proposition visant à améliorer les valeurs cibles susmentionnées, en précisant les éventuelles incidences budgétaires.

4. Capacité et extensibilité

90. En ce qui concerne la gestion des capacités, il convient de prendre en considération deux éléments : la capacité de traitement du système (sa capacité de traitement des messages entrants et des réponses à envoyer) et le stockage des divers éléments d'information reçus. L'extensibilité du système international eTIR s'entend de sa capacité à traiter une charge de travail croissante dès lors qu'on y ajoute des ressources.

91. Les chiffres présentés dans le tableau ci-dessous sont fondés sur une analyse réalisée pour apprécier les besoins en ce qui concerne la capacité et l'extensibilité du système international eTIR, qu'on trouvera dans l'annexe V.C. Comme indiqué dans les conclusions de cette analyse, la qualité des estimations et prévisions relatives à la capacité de traitement et au volume des données est fonction des différentes suppositions sur lesquelles elles reposent. Le système international eTIR n'étant pas encore en service, cette analyse manque de données en conditions réelles. C'est pourquoi les exigences relatives à la capacité et à l'extensibilité du système eTIR ne devraient être prises en compte dans sa conception que pour les deux premières années, puisqu'il est très probable que plusieurs suppositions devront être corrigées à la lumière des données obtenues en conditions réelles, ce qui modifiera le résultat des calculs ainsi que les prévisions pour les années suivantes.

Tableau 7
Exigences relatives à la capacité et à l'extensibilité

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
CP.1	Nombre maximal de messages à traiter	Un composant stocke les messages entrants dans une file d'attente. Plusieurs serveurs Web frontaux extraient les messages de la file d'attente pour qu'ils puissent être traités dans le délai d'attente maximal.	2021 : 12 messages par minute 2022 : 78 messages par minute 2023 : 270 messages par minute 2024 : 570 messages par minute 2025 : 1 200 messages par minute
CP.2	Espace de stockage maximal affecté aux journaux eTIR	Les journaux eTIR sont enregistrés directement sur les serveurs Web frontaux. Ils sont déplacés tous les jours vers un emplacement centralisé et sécurisé, pourvu d'une capacité de stockage suffisante pour regrouper toutes les données qu'ils contiennent.	2021 : 371 Go par an 2022 : 1,2 To par an 2023 : 4,9 To par an 2024 : 17,1 To par an 2025 : 36,1 To par an
CP.3	Espace de stockage maximal affecté à la base de données eTIR	En fonction des données reçues et des résultats des mesures régulières des performances, seules les données les plus récentes (des six derniers mois, par exemple) pourraient être conservées dans la base de données en cluster (les données plus anciennes étant régulièrement transférées dans une base de données secondaire) pour que la taille de la base (principale) n'entrave pas son fonctionnement.	2021 : 1,4 Go par an 2022 : 4,3 Go par an 2023 : 17,9 Go par an 2024 : 62,6 Go par an 2025 : 133,3 Go par an
CP.4	Espace de stockage maximal affecté aux documents eTIR	Les documents eTIR ne sont pas stockés dans la base de données, mais dans un système de fichiers centralisé et sécurisé, pourvu d'une capacité de stockage suffisante pour les regrouper tous.	2021 : 100 Go par an 2022 : 315 Go par an 2023 : 1,3 To par an 2024 : 4,6 To par an 2025 : 9,8 To par an

92. Comme indiqué dans les conclusions de l'analyse présentée dans l'annexe V.C, la CEE doit réaliser la même analyse six mois après que le système international eTIR aura été mis en production, afin de soumettre au TIB une version révisée des valeurs cibles susmentionnées, ainsi qu'une éventuelle proposition de budget.

5. Gestion de la configuration

93. La gestion de la configuration est le suivi de tous les éléments de configuration du système international eTIR. Un élément de configuration est une ressource informatique ou un ensemble de ressources informatiques qui peuvent dépendre d'autres processus ou être liées à d'autres processus informatiques (par exemple, code source, fichiers de configuration, procédures, documentation interne, etc.).

94. Disposer d'un nombre approprié de mesures et de procédures liées à la gestion de la configuration est la seule solution viable et efficace pour assurer le développement et la maintenance d'un grand système d'information tel que le système international eTIR, et la CEE veillera à ce que les exigences techniques ci-après soient correctement prises en compte.

Tableau 8
Exigences relatives à la gestion de la configuration

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
CM.1	Le code source de tous les modules du système international eTIR devrait être versionné au moyen d'un système de gestion des versions (VCS) afin que cette ressource puisse être exploitée efficacement.	Le code source de tous les modules du système international eTIR est versionné au moyen du système Git et il est hébergé dans des locaux de l'ONU.
CM.2	Toutes les modifications relatives à la base de données eTIR devraient être versionnées au moyen d'un VCS afin que cette ressource puisse être exploitée efficacement.	Toutes les modifications relatives à la base de données eTIR sont versionnées au moyen des systèmes Liquibase et Git et sont hébergées dans des locaux de l'ONU.
CM.3	Toutes les ressources liées à la documentation du système eTIR devraient être versionnées au moyen d'un VCS afin que cette ressource puisse être exploitée efficacement.	Toutes les ressources liées à la documentation du système eTIR sont versionnées au moyen d'un VCS différent en fonction de leur nature, et elles sont hébergées dans des locaux de l'ONU.
CM.4	Toutes les ressources liées à la documentation interne du système eTIR devraient être versionnées et être accessibles à la CEE, au moyen d'un logiciel de collaboration, pour que les connaissances puissent être mises en commun efficacement et la productivité améliorée.	Toutes les ressources liées à la documentation interne du système eTIR sont versionnées, et sont accessibles à la CEE au moyen d'un système de gestion des connaissances qui sert de plateforme sécurisée et versionnée de collaboration, laquelle est hébergé dans des locaux de l'ONU.
CM.5	Tous les bogues signalés, ajouts demandés et autres points à examiner doivent être enregistrés, traités et enfin réglés au moyen d'un système de suivi, afin que les points signalés par toutes les parties prenantes eTIR soient correctement évalués et traités avec le niveau de priorité approprié.	Tous les bogues signalés, ajouts demandés et autres points à examiner sont enregistrés, traités et enfin réglés au moyen d'un système de suivi hébergé dans des locaux de l'ONU.

6. Conservation des données

95. La conservation des données concerne les politiques liées à la gestion des données et dossiers persistants, destinées à satisfaire aux exigences juridiques et commerciales relatives à l'archivage des données, dont celles énoncées dans l'annexe 11. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la conservation des données dans le cadre du système international eTIR.

Tableau 9
Exigences relatives à la conservation des données

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
RE.1	Disponibilité des informations stockées dans le système international eTIR	Les informations stockées dans la base de données eTIR, les journaux eTIR et les documents eTIR sont sauvegardées quotidiennement, et des copies supplémentaires sont conservées sur des bandes stockées en un lieu distinct,	10 ans[18]

[18] Conformément au paragraphe 1 de l'article 12 de l'annexe 11 de la Convention TIR.

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
		sécurisé et résistant à la plupart des sinistres.	
RE.2	Récupération des informations demandées par les Parties contractantes à des fins de vérification[19]	Les procédures de récupération sont définies et établies dans l'accord de prestation de services, en concertation avec l'entité d'hébergement.	Délai maximal de trois jours pour récupérer les informations

7. Reprise après sinistre

96. La reprise après sinistre repose sur un ensemble de politiques, d'outils et de procédures propices à la reprise ou au maintien du système international eTIR à la suite d'un sinistre naturel ou anthropique. Axée sur les systèmes informatiques ou les technologies qui sous-tendent certaines fonctions essentielles, elle peut donc être considérée comme un sous-ensemble de la planification de la continuité des opérations.

97. Généralement, la reprise après sinistre, dans le contexte de laquelle on suppose que le site principal est irrécupérable (au moins pour un certain temps), comprend l'ensemble des processus qu'il convient de suivre pour rétablir les services sur un site secondaire. Dans le domaine d'application de la version 4.3 des spécifications du système eTIR, on suppose que seul un site secondaire de type intermédiaire est à disposition à des fins de reprise, principalement pour des raisons de coûts.

98. Un site de secours intermédiaire offre le matériel et les circuits de données nécessaires à une reprise rapide des opérations. Le matériel est généralement préconfiguré et prêt pour qu'on y installe les applications appropriées à l'appui des opérations de l'entité concernée. Néanmoins, s'il est prévu que ce site secondaire soit utilisé parce que le site principal n'est plus disponible en raison d'un sinistre, il sera toujours nécessaire d'installer et de configurer tous les composants logiciels sur les serveurs du site de secours intermédiaire. En outre, les données temps réel du site principal ne sont pas copiées en temps réel sur ce type de site secondaire, mais uniquement à des intervalles périodiques.

99. Les sinistres ont d'importantes conséquences dans la mesure où ils peuvent mettre le système international eTIR à l'arrêt pendant une période inhabituellement longue (probablement de plus d'une journée). La probabilité qu'un sinistre se produise est toutefois extrêmement faible. Le risque encouru est mince dans le cadre de la version 4.3 des spécifications du système eTIR, puisque le nombre de transports TIR réalisés selon la procédure eTIR sera d'abord faible, puis augmentera progressivement à mesure que de plus en plus de Parties contractantes connecteront leurs systèmes douaniers nationaux au système international eTIR. En outre, les procédures de secours décrites dans les spécifications fonctionnelles du système eTIR constituent une mesure d'atténuation de ce risque.

100. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la reprise après sinistre pour le système international eTIR.

Tableau 10
Exigences relatives à la reprise après sinistre

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
DR.1	Délai de reprise des activités[20] dans le système international eTIR à la suite d'un sinistre	Établir un plan de reprise après sinistre assorti de toutes les procédures détaillant comment remettre sur pied le système international eTIR, et tester ce plan régulièrement.	48 heures

[19] Conformément au paragraphe 3 de l'article 12 de l'annexe 11 de la Convention TIR.
[20] Délai qui devrait suffire à rétablir le service informatique en cas de sinistre.

DR.2	Objectif de point de reprise[21] des activités dans le système international eTIR	Envoyer régulièrement et de manière sécurisée des copies des données eTIR vers le site de secours intermédiaire. Exécuter des tests de reprise.	4 heures

101. Quand la mise en production du système international eTIR aura commencé, la CEE ou le TIB voudront peut-être proposer d'améliorer les valeurs cibles des exigences DR.1 et DR.2. Dans ce cas, la CEE pourra soumettre au TIB une proposition visant à améliorer les valeurs cibles susmentionnées, en précisant les éventuelles incidences budgétaires.

8. Tolérance de panne

102. La tolérance de panne est la propriété qui permet à un système de continuer à fonctionner normalement en cas de défaillance (un ou plusieurs dysfonctionnements) de certains de ses composants. L'architecture et l'infrastructure des systèmes d'information modernes prennent en compte les dysfonctionnements techniques typiques des composants tels que les disques durs et les connexions réseau, ou les coupures d'électricité, et peuvent offrir une tolérance de panne qui est transparente pour les utilisateurs finaux.

103. Les exigences énoncées dans le tableau ci-dessous offrent un premier niveau de secours technique qui ne nécessite pas d'activation par les parties prenantes eTIR. Ces exigences sont principalement remplies par l'infrastructure de base et elles seront intégrées à l'accord de prestation de services à signer avec l'entité d'hébergement.

Tableau 11
Exigences relatives à la tolérance de panne

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
FT.1	Gérer correctement le dysfonctionnement d'un serveur physique, qui peut être imputable au matériel (unité centrale, mémoire, carte mère, disque dur, carte réseau, etc.), pour éviter que le système international eTIR devienne indisponible.	Au moyen d'une infrastructure fondée sur une batterie de serveurs virtuels dépendant de plusieurs serveurs physiques qui gèrent l'échange à chaud de machines virtuelles, pour atténuer les conséquences de ce type de dysfonctionnement, et d'une architecture fondée sur une grappe de serveurs, pour éviter les points de défaillance uniques.
FT.2	Gérer correctement le dysfonctionnement du matériel utilisé pour le stockage (disque dur ou disque à semi-conducteurs (SSD)), pour éviter que le système international eTIR devienne indisponible	Au moyen d'une infrastructure fondée sur un réseau de stockage (SAN) utilisant un réseau redondant de disques indépendants (RAID), et d'une architecture fondée sur une grappe de serveurs, pour éviter les points de défaillance uniques.
FT.3	Gérer correctement la perte de connexion à Internet, pour éviter que le système international eTIR devienne indisponible	Au moyen d'une double connexion à Internet par l'intermédiaire de deux fournisseurs.
FT.4	Gérer correctement les coupures d'électricité pour éviter que le système international eTIR devienne indisponible	Au moyen de baies d'alimentation électrique non interruptible et de générateurs d'urgence à essence pour alimenter le centre de données, avec une réserve d'essence suffisante pour maintenir le service jusqu'au rétablissement de l'alimentation électrique, qui permettra de reconstituer la réserve.

9. Internationalisation et localisation

104. L'internationalisation et la localisation sont des moyens d'adapter un logiciel à différentes langues, particularités régionales et exigences techniques d'une région donnée. L'internationalisation consiste à concevoir une application de manière qu'elle puisse être

[21] Période cible maximale pendant laquelle des données (échanges) d'un service informatique peuvent être perdues en cas de perturbation.

adaptée à différentes langues et régions sans qu'il s'impose d'apporter des modifications informatiques. La localisation consiste à adapter un logiciel internationalisé à une région ou une langue particulière en traduisant le texte et en ajoutant des composants spécifiques à la région concernée.

105. Étant donné que le système international eTIR n'a pas d'interface utilisateur, les exigences relatives à l'internationalisation sont limitées aux messages eTIR et à la manière dont les données sont stockées aux différents emplacements prévus à cet effet. Plusieurs démarches ont été suivies pour limiter les besoins en matière de localisation :

- La plupart des attributs des messages eTIR utilisent des listes de codes. Ces listes énumèrent en détail tous les codes qui peuvent être affectés à un attribut, ce qui facilite le transfert d'informations d'un système à un autre, puisque tous les systèmes exploitent la même série de listes de codes. En outre, cette méthode évite d'avoir à traduire des valeurs, qui n'ont donc pas à être localisées ;
- Les nombres sont exprimés au moyen de schémas fixes qui sont clairement définis dans le fichier de définition du schéma XML (XSD) des messages eTIR. Cette approche élimine toute ambiguïté potentielle liée aux séparateurs décimaux et aux séparateurs de milliers ;
- Les dates sont aussi exprimées à l'aide de schémas spécifiques correspondant soit à une date, soit à une date et une heure, compte tenu d'un décalage pour le temps universel coordonné (UTC) ;
- Les champs de texte sont limités au minimum et utilisés dans la plupart des cas pour représenter des mots qui ne sont généralement pas traduits, tels que des identifiants, des noms propres et des adresses. Quelques champs de texte sont utilisés pour contenir des phrases dans une langue donnée ; le sous-attribut « Langue, codée » peut alors servir à définir la langue des valeurs stockées dans ces champs.

106. On trouvera dans le tableau ci-dessous la liste des exigences relatives à l'internationalisation et à la localisation.

Tableau 12
Exigences relatives à l'internationalisation et à la localisation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
IL.1	Les messages eTIR devraient pouvoir gérer des valeurs de type texte en anglais, en français et en russe.	Les messages eTIR échangés dans SOAP/XML sont encodés en UTF-8, et le type de contenu est « application/ soap+xml ».
IL.2	La base de données eTIR devrait pouvoir stocker des valeurs de type texte (provenant des messages eTIR) en anglais, en français et en russe.	La base de données eTIR est encodée en UTF-8.
IL.3	Les journaux eTIR devraient pouvoir stocker la totalité des messages eTIR à mesure qu'ils sont reçus.	Les fichiers stockés dans les journaux eTIR sont encodés en UTF-8.
IL.4	Les documents eTIR devraient permettre de stocker les pièces jointes en diverses langues en plus de l'anglais, du français et du russe.	Les fichiers stockés parmi les documents eTIR sont encodés en UTF-8.
IL.5	La langue des valeurs de type texte dans les messages eTIR devrait pouvoir être identifiée.	Les valeurs de type texte sont accompagnées du sous-attribut « Langue, codée », qui utilise une liste de codes pour spécifier le nom de la langue.

10. Interopérabilité

107. L'interopérabilité est la capacité qu'un système, dont les interfaces sont détaillées de manière exhaustive, a ou aura de fonctionner de manière pleinement compatible avec d'autres systèmes, sur le plan soit de la mise en œuvre, soit de l'accès.

108. Le système eTIR repose sur la communication entre machines, déclenchée par des événements donnés. C'est pourquoi les interfaces entre les différentes parties prenantes eTIR doivent être clairement définies, ce qui facilite l'interconnexion entre les systèmes. De plus, et dans le même but, les interfaces devraient être fondées sur des normes reconnues mondialement.

Tableau 13
Exigences relatives à l'interopérabilité

Identifiant	*Description et objectifs*	*Comment satisfaire à l'exigence*
IT.1	Le modèle de données eTIR devrait être harmonisé avec un modèle de données reconnu mondialement afin de faciliter la connexion entre le système international eTIR et les systèmes d'information des autres parties prenantes eTIR.	Le modèle de données eTIR est pleinement harmonisé avec celui de l'Organisation mondiale des douanes (OMD). Des demandes de mise à jour des données sont soumises par la CEE afin d'adapter continuellement le modèle de données de l'OMD aux besoins de la procédure eTIR.
IT.2	Le format et les spécifications techniques des messages eTIR suivent des lignes directrices strictes aux fins de l'interopérabilité dans le cadre de l'échange électronique de messages entre les systèmes d'information.	Les spécifications relatives aux messages eTIR suivent les lignes directrices de l'OMD sur les schémas XML. Des essais de conformité sont en outre exécutés automatiquement à titre de vérification.
IT.3	Les informations échangées dans les messages eTIR sont normalisées autant que possible pour faciliter leur traitement par toutes les parties prenantes eTIR.	Les attributs des messages eTIR reposent autant que possible sur des listes de codes issues de normes reconnues (UN/EDIFACT et ISO).
IT.4	Les parties prenantes eTIR devraient disposer de suffisamment de temps pour effectuer la migration vers la nouvelle version des spécifications du système eTIR tout en continuant d'utiliser la version actuelle.	Le système international eTIR sera capable de recevoir, de traiter et d'envoyer des messages eTIR en utilisant simultanément deux versions des spécifications du système eTIR : la version actuelle et la version suivante, proposée à toutes les parties prenantes eTIR pendant une période de migration donnée, dont les détails seront fournis dans les procédures de gestion des mises à jour.

11. Maintenabilité

109. La maintenabilité s'entend de la facilité avec laquelle on peut assurer la maintenance d'un produit afin, notamment, de corriger des défauts[22], satisfaire à de nouvelles exigences, faciliter la future maintenance et s'adapter au changement.

110. L'un des écueils classiques du génie logiciel et de la gestion des applications est de sous-estimer la nécessité d'investir continuellement des sommes d'argent raisonnables dans la maintenance et la mise à jour des systèmes d'information, afin de ne pas avoir à payer des sommes très importantes pour assurer la réécriture complète du code lorsque le système n'a pas été maintenu correctement dans le temps.

111. Le secteur informatique a aussi conscience qu'une part importante du coût total de possession (typiquement entre 50 % et 80 %) d'un système d'information, au cours de son cycle de vie, est dépensée pendant la phase de maintenance. Il importe donc de prendre les mesures préventives appropriées pour faire en sorte que les coûts de maintenance d'un système d'information restent à un niveau raisonnable, tout en veillant à satisfaire à l'ensemble des exigences relatives à la maintenabilité.

112. Il convient en particulier de prendre des mesures pour éviter de constituer une dette technique. La dette technique est un concept propre au développement informatique qui rend

[22] Voir la définition du terme « défaut » dans le glossaire technique.

compte des coûts de modifications additionnelles imputables à une mauvaise décision, qui, si elle porte ses fruits à court terme, fait croître les coûts de maintenance à long terme. À l'instar de la dette monétaire, en cas de défaut de remboursement de la dette technique, des « intérêts » peuvent s'accumuler, ce qui complique d'autant plus l'adaptation aux évolutions futures.

113. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la maintenabilité.

Tableau 14
Exigences relatives à la maintenabilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
MT.1	Il ne doit pas y avoir de dette technique au niveau des langages, infrastructures et bibliothèques de programmation utilisés pour développer le système international eTIR.	Les dernières versions stables des langages, infrastructures et bibliothèques de programmation utilisés pour développer le système international eTIR sont régulièrement passées en revue et des mises à jour régulièrement planifiées. Les nouvelles tendances sont examinées périodiquement, et les mesures appropriées sont prises pour effectuer des migrations afin d'adopter de meilleures solutions avant qu'un composant devienne obsolète.
MT.2	Il ne doit pas y avoir de dette technique au niveau du code source du système international eTIR.	Un outil d'analyse statique de code est utilisé pour mesurer l'indice de maintenabilité du code source et on s'emploie régulièrement à réduire le nombre des problèmes décelés par cet outil. On exécute aussi régulièrement des activités de réécriture du code, afin de réduire l'*entropie logicielle*[23] de ce dernier.
MT.3	Les connaissances sont intégrées afin de tenir à jour et d'améliorer le système international eTIR	La documentation interne du système international eTIR est gérée au moyen d'un système de gestion des connaissances, à savoir une plateforme sécurisée et versionnée pour la collaboration entre les membres de la CEE. Un coordonnateur informatique a notamment pour mission de veiller à ce qu'une documentation suffisante (comprenant des procédures d'exploitation normalisées) soit établie et tenue à jour dans le cadre du système de gestion des connaissances, afin de réduire les risques afférents au remplacement du personnel et à la concentration des responsabilités[24].

12. Performance

114. La performance est une indication numérique des possibilités maximales ou optimales du matériel, du logiciel, du système ou du processus technique servant à exécuter une tâche donnée. Dans le cas du système international eTIR, les exigences portent sur les délais de réponse et la capacité de traitement.

115. Les exigences relatives à la capacité de traitement du système international eTIR sont déjà présentées en détail dans la section consacrée à la capacité, à savoir les exigences CP.1 et CP.2. Les exigences relatives aux délais de réponse sont présentées en détail dans le tableau ci-dessous sur la performance quantitative, et d'autres exigences relatives à la performance sont énumérées dans le tableau suivant sur la performance qualitative.

[23] Voir la définition dans le glossaire technique.

[24] Risques liés à la concentration des responsabilités : risques encourus par une entité qui dépend fortement d'une personne en particulier pour son bon fonctionnement.

Tableau 15
Exigences quantitatives relatives à la performance

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
PE.1	Délai moyen de réponse aux messages courts (10 Ko au maximum), tel que mesuré par l'envoyeur entre l'envoi du message de demande et la réception du message de réponse	Le système international eTIR est bien conçu et exempt d'insuffisances logiques ou techniques susceptibles de perturber son fonctionnement. La gestion de la base de données eTIR, l'écriture d'informations dans les journaux eTIR et la connexion à l'ITDB sont optimisées.	1 seconde
PE.2	Délai maximal de réponse aux messages courts (10 Ko au maximum), tel que mesuré par l'envoyeur entre l'envoi du message de demande et la réception du message de réponse	Un nombre suffisant de nœuds est prévu pour permettre aux composants logiciels des services Web eTIR de traiter toutes les demandes. Un nombre suffisant de nœuds est prévu pour permettre à la base de données eTIR de traiter toutes les demandes.	10 secondes
PE.3	Délai maximal de réponse tel que mesuré par l'envoyeur entre l'envoi du message de demande et la réception du message de réponse	La taille maximale des messages eTIR est fixée à 20 Mo. La connexion Internet du système international eTIR dispose d'une bande passante élevée (plus de 100 mégabits par seconde).	Délai d'attente fixé à 60 secondes

Tableau 16
Exigences qualitatives relatives à la performance

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
PE.4	Les indicateurs de performance du système international eTIR devraient faire l'objet d'un suivi pour déceler tout problème éventuel.	Des indicateurs de performance sont enregistrés à différents points essentiels lors de la réception, du traitement et de l'enregistrement d'un message de demande et de l'envoi d'un message de réponse. Ces indicateurs font l'objet d'un suivi afin que l'alerte soit donnée et que la CEE mène son enquête si les valeurs mesurées dépassent certaines limites.
PE.5	Les indicateurs de performance du système international eTIR restent stables ou s'améliorent dans le temps.	On utilise un outil de test de charge pour exécuter des tests automatisés lorsque le système international eTIR est mis à jour. Cet outil permet de vérifier qu'aucun élément ne risque d'entraîner une régression appréciable.

13. Fiabilité

116. La fiabilité s'entend de la capacité qu'a un système d'information de traiter les erreurs d'exécution et les entrées invalides. Cette notion englobe également l'ensemble des pratiques suivies pour que les objectifs de qualité soient atteints. L'optimisation de la fiabilité du système international eTIR est au cœur du deuxième principe directeur suivi par la CEE.

117. Aux fins de la réalisation de cet objectif, ainsi que de la bonne qualité d'ensemble du système international eTIR, les pratiques suivantes sont mises en place à titre préventif :

- Des lignes directrices ont été établies par la CEE concernant le développement, le déploiement, le fonctionnement et la maintenance du système international eTIR. Ces lignes directrices constituent un ensemble de règles et de pratiques communes qui garantissent des résultats prévisibles et de bonne qualité ;

- Des procédures strictes de versionnement sont appliquées pour qu'on puisse savoir à quel besoin saisi dans le système de suivi correspond chacune des modifications apportées au code source du système international eTIR ainsi qu'à la structure et au contenu de la base de données eTIR ;
- Le code source est réexaminé pour faire baisser la probabilité que des artéfacts indésirables (défauts) s'y trouvent et pour contrôler le respect des lignes directrices relatives au codage ;
- Toutes les modifications apportées au code source (pour introduire une fonction ou pour corriger un défaut) sont accompagnées de tests automatisés appropriés pour vérifier qu'aucun élément ne risque de faire régresser le code ;
- Le code source est régulièrement vérifié au moyen d'un outil d'analyse statique afin de déterminer plusieurs indicateurs liés à la maintenabilité, la fiabilité, la sécurité, la couverture de code et la duplication de code. Les problèmes repérés par cet outil sont traités par la CEE dans le but de répondre aux objectifs de qualité (seuils de qualité) fixés au préalable ;
- Une chaîne d'intégration continue a été mise en place pour exécuter automatiquement plusieurs opérations pendant le développement du système international eTIR, afin de garantir un haut niveau de fiabilité et de qualité.

118. En plus des pratiques préventives, la pratique réactive ci-dessous a été mise en place pour qu'il soit possible de déceler et de régler les problèmes le plut tôt possible :

- Le système de surveillance suit en continu plusieurs indicateurs et indices associés aux composants logiciels et matériels du système international eTIR pour déceler tout problème et communiquer l'alerte appropriée afin qu'il soit réglé rapidement (en fonction de son degré de gravité).

119. On trouvera dans les tableaux ci-dessous la liste des exigences relatives à la fiabilité.

Tableau 17
Exigences quantitatives relatives à la fiabilité

Identifiant	*Description*	*Comment atteindre l'objectif*	*Valeur cible*
RL.1	Nombre des erreurs de la gravité la plus élevée détectées par l'outil d'analyse statique, et restant à corriger	Vérifier régulièrement le code source au moyen de l'outil d'analyse statique et corriger toute erreur, en donnant la priorité aux erreurs les plus graves.	0 (toutes les erreurs de ce type doivent être corrigées)
RL.2	Nombre des erreurs de gravité normale détectées par l'outil d'analyse statique, et restant à corriger	Introduire la vérification du code source au moyen de l'outil d'analyse statique dans la chaîne d'intégration continue, pour donner rapidement des informations en retour et améliorer les méthodes de travail.	Moins de 150
RL.3	Pourcentage de code source fonctionnel couvert par les tests automatisés (couverture de code)	Passer le code en revue et appliquer des lignes directrices pour le développement, de sorte que toutes les modifications du code source s'accompagnent d'un nombre approprié de tests automatisés.	Plus de 60 %
RL.4	Pourcentage de code source dupliqué (duplication de code)	Passer régulièrement le code en revue pour éviter la duplication.	Moins de 3 %

120. La CEE révisera régulièrement les cibles fixées pour les exigences quantitatives de fiabilité énumérées dans le tableau ci-dessus afin d'améliorer continuellement la qualité générale du code source du système international eTIR.

Tableau 18
Exigences qualitatives relatives à la fiabilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
RL.5	Toutes les modifications du code source sont apportées de manière à faire baisser la probabilité que des erreurs soient introduites.	La CEE applique des lignes directrices et des pratiques optimales spécifiques dans le développement du système international eTIR. L'exécution de tests automatisés permet de signaler immédiatement toute régression introduite. Les commits qui ne dépassent pas les seuils de qualité déterminés sont rejetés.
RL.6	Toutes les modifications du code source sont liées à un besoin, ce qui permet de garantir une bonne traçabilité.	Le VCS utilisé pour le code source et le système de suivi sont interconnectés. On peut trouver le point lié à un commit particulier dans le VCS et tous les commits doivent faire référence à un point.
RL.7	Il s'agit d'éliminer, dans les procédures de développement, autant de tâches redondantes, manuelles et sources d'erreurs que possible.	Mettre en place une chaîne d'intégration continue qui soulage les informaticiens des tâches secondaires et permette de leur donner rapidement des informations en retour sur la qualité de la modification qu'ils apportent au code source.

14. Réutilisabilité

121. La réutilisabilité consiste à utiliser d'une manière ou d'une autre des ressources existantes dans le processus de développement d'un logiciel. Ces ressources sont des produits et des sous-produits du cycle de développement du logiciel et comprennent le code, les composants logiciels, les suites de tests, les conceptions et la documentation.

122. Le but principal de la réutilisabilité est d'arrêter de « réinventer la roue ». Dans le génie logiciel moderne, et grâce aux langages de programmation orientés objet, il est aisé de réutiliser des composants logiciels existants. En outre, cette approche est pertinente, non seulement pour les composants logiciels, mais aussi pour les méthodes et les infrastructures, puisqu'elle est fondée sur une abondance d'expériences et de bonnes pratiques. On trouvera ci-après la liste de celles qui ont servi au développement du système eTIR :

- Gestion de projet : Le secrétariat de l'ONU a sélectionné la méthode de gestion de projet PRINCE2® (PRojects IN Controlled Environments), que la CEE a adaptée pour l'appliquer à la gestion de ses projets ;
- Architecture d'entreprise : La CEE utilise plusieurs éléments de l'infrastructure TOGAF® (The Open Group Architecture Framework) pour ses besoins en matière d'architecture ;
- Développement de logiciels : La CEE suit une méthode agile pour le développement et la maintenance du système international eTIR et elle applique plusieurs pratiques DevOps ;
- Gestion des services : La CEE utilise plusieurs éléments de la bibliothèque ITIL® (Information Technology Infrastructure Library) pour ses procédures en lien avec les services d'assistance eTIR et ses relations avec l'entité de l'ONU hébergeant le système international eTIR ;
- Conscience des risques pour la sécurité : La CEE utilise plusieurs éléments du projet OWASP® (Open Web Application Security Project) pour se tenir informée des dernières menaces et des pratiques optimales les plus récentes.

123. Dans la plupart des cas, il est préférable de sélectionner un élément à réutiliser plutôt que d'en développer un soi-même. En effet, si les fonctions satisfont aux exigences, il est généralement plus rapide et moins coûteux de procéder de la sorte. Lorsqu'il est question d'un composant ou d'un produit logiciel, il peut s'agir soit d'un logiciel open source, soit d'un logiciel protégé. Il convient de prendre en compte dans le processus de décision les

paramètres suivants : le coût total de possession (y compris la formation et l'assistance), la maturité et la viabilité de la solution informatique, les avantages et les inconvénients.

124. On trouvera dans le tableau ci-dessous l'exigence applicable en matière de réutilisabilité.

Tableau 19
Exigence relative à la réutilisabilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
RU.1	Il s'agit de réutiliser des méthodes, infrastructures, logiciels et matériels existants pour économiser du temps et obtenir de meilleurs résultats	Dans le cas d'un nouveau besoin, ou pendant l'évaluation régulière des éléments réutilisés, la CEE cherche des solutions et applique son approche de prise de décisions pour choisir l'option optimale.

15. Sécurité

125. Tous les éléments et les exigences techniques liés à la sécurité du système international eTIR sont décrits dans le chapitre intitulé « Sécurité du système eTIR », qu'on trouvera plus loin dans le présent document.

E. Processus de développement

1. Introduction

126. La présente section décrit les processus suivis par les informaticiens de la CEE pour développer le système international eTIR afin que les Parties contractantes à la Convention TIR et les autres parties prenantes eTIR puissent appréhender correctement ces aspects. Faire preuve de transparence au sujet de ces processus permet également à toutes les parties prenantes eTIR de suggérer des propositions d'améliorations, l'objectif ultime étant de disposer d'un système eTIR plus performant à long terme.

2. Lignes directrices générales

127. Les informaticiens ont pris le temps de préparer, de discuter et d'adopter leurs propres lignes directrices internes, qui portent sur tous les éléments du développement et de la maintenance du système international eTIR. Ces lignes directrices sont fondées sur les pratiques optimales et éprouvées du secteur informatique et sur l'expérience acquise par les informaticiens. Elles ne sont cependant pas gravées dans le marbre, et les experts s'efforceront en permanence de recenser les possibilités de les améliorer. Ce point est particulièrement important dans un domaine de compétence tel que les technologies de l'information et de la communication, qui évolue très rapidement.

128. Les trois principes directeurs énoncés au début du présent document éclairent et guident les informaticiens dans leur travail d'élaboration et d'amélioration des lignes directrices, ainsi que dans tous les processus décisionnels.

129. Lorsqu'ils prennent une décision technique sur tout aspect lié au système international eTIR, les informaticiens appliquent les meilleures pratiques habituelles en matière de prise de décisions. Ils consacrent le temps nécessaire à l'étude des nouvelles tendances, des approches et des éventuels produits. Ils définissent ensuite les options envisageables et répertorient leurs avantages et inconvénients respectifs, ce qui permet de prendre une décision et de sélectionner la meilleure option. Les décisions sont documentées, ainsi que le raisonnement qui a conduit à ces choix, afin de conserver la mémoire institutionnelle.

130. Enfin, les informaticiens tiennent compte du principe de Pareto[25] dans leur prise de décisions afin de déterminer l'équilibre optimal entre les avantages qu'il est possible d'obtenir et le temps nécessaire pour y parvenir. Ce principe est généralement vérifié lorsqu'il

[25] Voir fr.wikipedia.org/wiki/Pareto_principe.

est appliqué au génie logiciel, et il devient encore plus pertinent quand il s'agit de s'assurer que les fonds sont dépensés à bon escient en période de situation économique difficile.

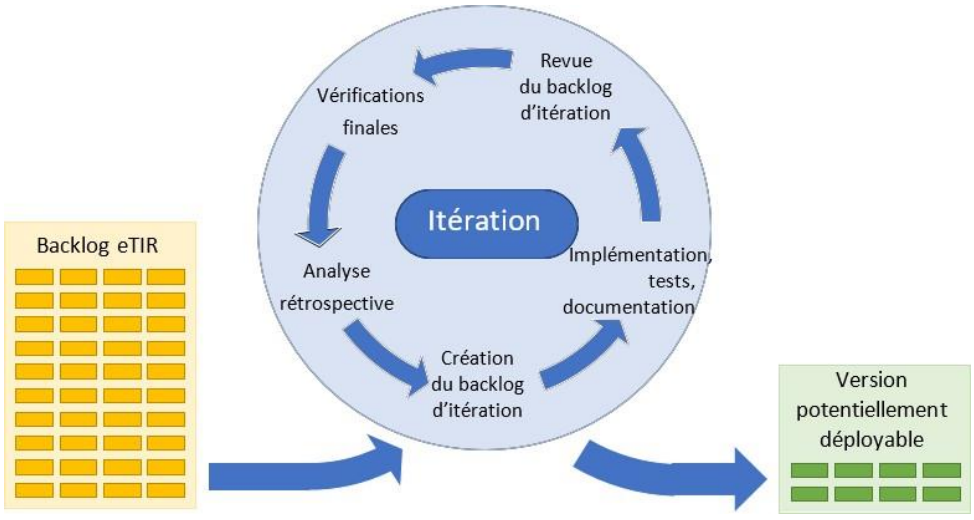
3. Méthode de développement

131. Le succès du développement d'un système d'information d'envergure tel que le système international eTIR passe par la mise en œuvre d'une méthode de gestion de projet informatique. Dans la courte − mais intense − histoire de l'informatique, plusieurs paradigmes et modèles ont été proposés et largement testés (par exemple, les méthodes de prototypage, en cascade, en V, agiles, incrémentales, etc.). La rédaction en 2001 du Manifeste agile (Manifeste pour le développement agile de logiciels)[26] et de ses 12 principes, qui découlent de plusieurs nouvelles méthodes agiles (telles que l'eXtreme Programming et Scrum), a constitué une avancée majeure. Depuis lors, de nombreux projets informatiques ont été menés en recourant aux méthodes agiles, qui augmentent les chances de succès de ces entreprises complexes.

132. La CEE a choisi d'utiliser une méthode agile proche de Scrum et Kanban pour développer le système international eTIR. Cette approche est axée sur les objectifs suivants : développer des logiciels utiles et fonctionnels, être capable de répondre rapidement aux changements, assurer un haut niveau de qualité et, surtout, satisfaire les utilisateurs.

133. Le travail à faire est décomposé en tâches, qui sont placées dans une liste d'attente appelée « backlog eTIR ». Le développement se fait par cycles d'itérations de plusieurs semaines. Au début de chaque itération, les informaticiens sélectionnent dans le backlog eTIR un ensemble de tâches à traiter, qui forment le backlog d'itération. Les activités d'implémentation, de test et de documentation menées pendant le cycle d'itération portent sur ces tâches, qui sont ensuite passées en revue vers la fin du cycle afin de définir la portée définitive de l'itération (il est en effet possible de retirer de l'itération plusieurs tâches non terminées). La dernière étape du cycle consiste à vérifier la qualité de l'itération, dont le résultat constitue une version potentiellement déployable du système.

Figure XIII
Développement par itération



134. Sachant que le système international eTIR doit être développé en une seule fois, puis exploité et maintenu de manière adéquate pendant une durée indéterminée, la CEE a également choisi d'adopter plusieurs pratiques du mouvement DevOps, qui visent à prévenir les problèmes pouvant survenir lors du passage de la phase de développement à la phase opérationnelle du projet. Ces pratiques, détaillées ci-après, sont les suivantes : investir dans l'automatisation des tests, s'appuyer sur l'intégration continue, analyser les indicateurs et mener des analyses rétrospectives non culpabilisantes.

[26] Voir agilemanifesto.org/iso/fr/manifesto.html.

4. Lignes directrices relatives au développement

135. Les directives sur le codage normalisé et l'abondante littérature informatique[27] sur le sujet constituent le fondement des lignes directrices relatives au développement. Le système international eTIR repose sur la technologie Java, et les informaticiens utilisent un environnement de développement intégré moderne et reconnu qui leur permet de programmer efficacement dans ce langage et dans l'écosystème qui lui est associé. Cet environnement permet également d'intégrer certaines lignes directrices relatives au développement (accès au système de gestion de version, outil d'analyse statique du code et règles de formatage du code).

136. Les informaticiens utilisent le système de gestion de version Git et appliquent les pratiques optimales habituelles associées à ce produit. Les modifications apportées au code source sont régulièrement enregistrées et publiées dans le répertoire central, ce qui permet de les partager avec tous les développeurs et d'éviter les pertes de données en cas de dysfonctionnement d'un poste de travail. Les développements importants sont généralement réalisés sur des branches séparées. Enfin, la publication des modifications du code dans le répertoire central nécessite des étapes préalables (détaillées dans les sections suivantes) afin de garantir la qualité de chaque contribution.

5. Lignes directrices relatives à la journalisation

137. Le service de journalisation du système international eTIR est très important, car il produit les données nécessaires au système de non-répudiation et à la génération des indicateurs permettant de surveiller la santé globale du système. Comme l'expliquent les pratiques DevOps, ces indicateurs (ou critères mesurables) sont le seul moyen pour les informaticiens de surveiller le fonctionnement du système, d'être alertés en cas d'anomalie et, par conséquent, de pouvoir résoudre efficacement un problème avant même d'être contactés par les utilisateurs finaux.

138. Le service de journalisation génère plusieurs fichiers, qui ont chacun une fonction propre. Chaque événement enregistré dans un fichier de journalisation est accompagné d'informations sur la date et l'heure à laquelle il s'est produit et sur sa gravité potentielle :

- **Messages eTIR** : la totalité du contenu des messages entrants et sortants est sauvegardée dans un fichier afin de conserver l'ensemble des suites de messages (fils) échangés entre le système international eTIR et les systèmes d'information qui lui sont connectés. Ces données sont ensuite utilisées par le système de non-répudiation et peuvent être récupérées sur demande par les Parties contractantes à la Convention TIR ;
- **Base de données** : toutes les requêtes adressées à la base de données sont enregistrées dans un fichier, ainsi que le temps nécessaire pour y répondre. Cela permet de mesurer en permanence la performance du traitement de ces requêtes et de fournir aux informaticiens les indicateurs dont ils ont besoin pour identifier et supprimer les éventuels goulets d'étranglement et pour mieux planifier les besoins en matière d'extension ;
- **ITDB :** toutes les demandes adressées à l'interface de la Banque de données internationale TIR (ITDB) sont sauvegardées dans un fichier, ainsi que le temps nécessaire pour y répondre. Cela permet de mesurer en permanence la performance du traitement de ces demandes et de fournir aux informaticiens les indicateurs dont ilsont besoin pour optimiser cette interface ;
- **Application** : tous les événements qui se produisent dans le module des services Web eTIR sont enregistrés dans un fichier afin d'en conserver un historique complet, qui est utilisé par le système de surveillance pour alerter en temps réel sur tout problème majeur survenant dans le système international eTIR. Ces données sont également utilisées dans le cadre des enquêtes afin d'identifier la cause première d'un problème.

[27] En particulier les publications de Kent Beck, Martin Fowler et Robert C. Martin.

6. Lignes directrices relatives aux tests

139. Les tests sont un élément essentiel du génie logiciel. L'histoire de l'informatique montre invariablement que la probabilité de voir échouer les projets logiciels est nettement plus élevée si l'on n'accorde pas l'attention nécessaire à cet élément. Les tests peuvent être exécutés manuellement ou automatiquement. Dans le cas d'un test manuel, le testeur exécute une séquence d'actions prédéfinies pour interagir avec le système d'information à tester et compare les résultats obtenus avec les résultats attendus. Si ces résultats correspondent, le test est réussi ; dans le cas contraire, c'est un échec. Les tests manuels constituent la démarche la plus évidente qu'un ingénieur logiciel puisse immédiatement entreprendre pour vérifier si la partie du logiciel qui vient d'être développée fonctionne comme prévu. Cependant, le principal inconvénient des tests manuels est que leur mise en œuvre requiert l'intervention d'une personne, ce qui est coûteux et source d'erreurs. De plus, ils ne vérifient l'état du système qu'au moment où ils sont exécutés et leur résultat (succès ou échec) n'est donc plus pertinent lorsque les conditions changent (mise à jour du code source, mise à jour des paramètres de l'environnement, etc.).

140. Les pratiques actuelles dans le domaine du génie logiciel reconnaissent que les tests manuels ne sont plus suffisants pour assurer la fiabilité et la qualité du système d'information en cours de développement. Comme l'expliquent les pratiques DevOps connexes, il est maintenant nécessaire d'automatiser les tests pour qu'ils soient systématiquement exécutés lors d'événements spécifiques récurrents (lorsque les conditions changent, comme mentionné ci-dessus), afin qu'aucune régression ne soit introduite. En effet, lorsqu'ils mettent en œuvre de nouvelles fonctionnalités ou corrigent des défauts dans le code source, les ingénieurs risquent toujours de générer des effets secondaires indésirables (par exemple, des défauts). Afin de résoudre ce problème inhérent au génie logiciel, il est nécessaire de procéder à des tests automatisés pour vérifier toutes les modifications apportées au code source. Il importe de garder à l'esprit que le temps consacré à la mise en œuvre de tests automatisés est toujours payant. En effet, l'absence de tests automatisés entraîne une nette augmentation du nombre de défauts, et le temps qu'il faut consacrer à les étudier et à les corriger est nettement supérieur au temps de mise en œuvre de ces tests. En outre, les problèmes réguliers que rencontrent les utilisateurs en raison de ces défauts peuvent engendrer des frustrations et nuire gravement à la réputation de l'entité responsable du système.

141. Il existe plusieurs types de tests automatisés, qui ont leurs propres caractéristiques et se complètent les uns les autres :

- **Tests unitaires** : tests permettant de vérifier qu'une partie du logiciel (appelée « unité ») répond aux spécifications et se comporte comme prévu. Dans les langages de programmation orientés objets comme Java, l'unité est souvent une interface entière, par exemple une classe, mais il peut aussi s'agir d'une méthode. L'objectif des tests unitaires est de tester séparément les différentes parties du programme et demontrer qu'elles fonctionnent correctement. Un test unitaire fournit un contrat strict et écrit que la portion de code doit strictement respecter. Les tests unitaires sont généralement rapides à mettre en œuvre puis à exécuter ;
- **Tests d'intégration** : tests permettant de vérifier que les différents modules du logiciel fonctionnent correctement une fois intégrés ensemble. L'objectif des tests d'intégration est d'évaluer la conformité d'un système aux exigences fonctionnelles énoncées. Ils sont menés après les tests unitaires et avant les tests de validation. Les intrants des tests d'intégration sont les modules testés individuellement ; ces modules sont regroupés en agrégats, et testés conformément au plan de test d'intégration ; le résultat (extrant) des tests de validation est le système intégré, qui est prêt à subir les tests de validation ;
- **Tests de performance** : tests permettant de vérifier qu'un système logiciel répond aux exigences de performance. Cette famille de tests comprend également les tests de charge, qui mesurent les performances du logiciel lorsqu'il est soumis à un nombre élevé de requêtes. Ce type de tests est important pour vérifier que les performances du logiciel ne se dégradent pas au fil du temps, en particulier lorsque de nouvelles fonctionnalités sont ajoutées ;
- **Tests de validation** : tests permettant de vérifier qu'un système logiciel répond aux

spécifications et qu'il remplit l'objectif prévu. Ces tests sont généralement les plus complexes et les plus coûteux à implémenter et à mettre à jour, car ils impliquent de simuler les actions effectuées par les utilisateurs finaux sur l'interface utilisateur du système. Dans le cadre spécifique du système international eTIR, il n'y a pas d'interface utilisateur, car les données sont échangées automatiquement avec les systèmes d'information des autres parties prenantes eTIR, à l'aide des messages eTIR. Cette approche permet d'effectuer des tests de validation de manière très simple et très efficace, car chaque message de demande (dans le cadre du test) déclenche l'envoi d'un message de réponse qui permet de s'assurer que le système se comporte comme prévu ;

- **Tests de conformité** : tests analogues aux tests de validation et comportant, dans le cadre du système eTIR, des essais de simulation permettant de garantir qu'un ensemble représentatif de transports TIR est correctement géré, grâce à l'envoi et à laréception d'une séquence spécifique de messages eTIR qui sont vérifiés afin de validerdes scénarios complets. Ces tests peuvent également porter sur le système d'information d'une partie prenante TIR, ou bien en inclure plusieurs pour mieux reproduire des transports TIR effectués selon la procédure eTIR.

142. Lorsqu'ils écrivent des tests automatisés, les ingénieurs doivent également s'assurer que la plupart (sinon la totalité) des lignes pertinentes du code source sont couvertes et validées. Ils doivent en particulier vérifier que les tests couvrent tous les chemins d'exécution du code source (cette pratique et les indicateurs qui y sont associés sont appelés « couverture des branches »). Les ingénieurs doivent non seulement veiller à ce que la couverture du code soit appropriée, mais aussi à ce que les assertions utilisées pour valider le code source soient adaptées et exhaustives, faute de quoi les tests ne remplissent pas leur objectif.

143. Comme évoqué ci-dessus, le seul moyen durable de développer et de maintenir un système d'information est d'assurer une bonne couverture de code, si bien que les informaticiens ont intégré cet objectif et les pratiques connexes dans les processus de développement. Lorsqu'une nouvelle fonction est mise en œuvre, il est nécessaire d'écrire le nombre approprié de tests unitaires et de tests de validation pour atteindre l'objectif de couverture du code. Lorsqu'un défaut est corrigé, un ou plusieurs tests doivent être écrits pour éviter que le même problème ne se reproduise.

7. Analyse statique du code

144. L'analyse statique du code consiste à évaluer automatiquement la qualité du code source d'un logiciel sans exécuter ce dernier. Cette évaluation est effectuée par un outil intégrant des règles de programmation et des pratiques optimales, dont la plupart ont été définies au fil des ans par la communauté mondiale des experts en informatique. L'analyse statique du code constitue un moyen très efficace de procéder à un premier contrôle de la qualité du code source et un excellent complément aux revues de code ciblées effectuées manuellement par les informaticiens.

145. Si les experts en informatique sont convaincus de l'utilité de ce type d'outil automatisé, ils sont également conscients qu'il est nécessaire d'examiner conjointement la pertinence de plusieurs règles, compte tenu du contexte spécifique du système international eTIR. Ils configurent donc les règles et leurs niveaux d'exigence afin de les adapter au mieux à ce contexte.

146. Une analyse statique du code est régulièrement menée sur l'ensemble du code source du système international eTIR. Les informaticiens tirent également parti de l'intégration de cette capacité dans l'environnement de développement qu'ils utilisent pour programmer, ce qui leur donne immédiatement des informations en retour sur la qualité du code qu'ils écrivent.

147. L'objectif est d'augmenter progressivement la qualité du code source et de la maintenir à un niveau très élevé tout au long de son cycle de vie. Cela améliore la fiabilité et la maintenabilité du code source et, en fin de compte, fait gagner du temps aux informaticiens, ce qui accroît leur productivité. Cet objectif est mis en œuvre en deux phases, à savoir augmenter progressivement la qualité du code source et la maintenir à un niveau élevé.

148. Au cours de la première phase, les informaticiens fixent des seuils de qualité[28] peu élevés dans l'outil d'analyse statique du code et corrigent autant de problèmes que nécessaire pour atteindre ces objectifs. Les seuils sont ensuite progressivement relevés, et les informaticiens continuent de se pencher sur la résolution des problèmes afin d'atteindre les nouveaux objectifs. Lorsque les informaticiens estiment, en tenant également compte du principe de Pareto, que les seuils de qualité ont atteint un niveau suffisant[29], la deuxième phase peut commencer.

149. Au cours de la deuxième phase, l'objectif est de poursuivre les efforts de développement et de maintenance du système international eTIR, tout en respectant les seuils de qualité. Il est possible de mettre en place des mesures supplémentaires pour avertir les informaticiens lorsque la mise à jour du code source entraîne le non-respect de l'un de ces seuils de qualité, afin qu'ils puissent immédiatement étudier le problème et le résoudre.

8. Processus d'intégration continue

150. Dans le domaine du génie logiciel, l'intégration continue consiste à fusionner plusieurs fois par jour les copies de travail de tous les développeurs sur une ligne principale partagée. Cette pratique n'est pas nouvelle (elle date des années 1990) et a été continuellement affinée et étendue pour aboutir aux pratiques DevOps actuelles, connues sous le nom d'intégration et déploiement continus (CI/CD). Les informaticiens ont choisi de se concentrer sur l'intégration continue pour commencer ; une fois le niveau de maturité approprié atteint, ils pourront envisager d'adopter également le déploiement continu, qui nécessite des bases solides.

151. La définition actuelle de l'intégration continue rend compte de l'automatisation de toutes les étapes associées à l'intégration et à la vérification des modifications du code source d'un logiciel. L'intégration continue consiste à exécuter tous les tests automatisés sur une version du logiciel qui vient d'être créée et déployée et qui contient les dernières modifications enregistrées dans le système de gestion de version (VCS), ce qui permet aux développeurs de logiciels d'obtenir rapidement des informations en retour sur la qualité du code qu'ils envoient au VCS. L'intégration continue soulage les développeurs des tâches secondaires et sources d'erreurs associées à la création, au test et au déploiement d'une nouvelle version du logiciel, afin qu'ils puissent se concentrer sur leur véritable valeur ajoutée : livrer des fonctionnalités aux clients.

152. Les informaticiens ont mis en place un processus d'intégration continue (ou « pipeline d'intégration continue »), qui se présente sous la forme d'un outil spécialisé dans lequel plusieurs actions sont définies et configurées pour être exécutées de manière séquentielle et automatisée chaque fois qu'une modification du code est enregistrée dans le système de gestion de version. Les étapes correspondantes sont les suivantes :

a) **Création** : le processus d'intégration continue détecte qu'une modification (*commit*) a été enregistrée dans le système de gestion de version, récupère la dernière version du code source et crée les nouveaux composants logiciels concernés par la modification ;

b) **Première phase de test** : des tests unitaires et des tests d'intégration automatisés sont ensuite exécutés sur les composants logiciels qui viennent d'être créés, afin de vérifier que la modification du code n'a entraîné aucune régression ;

c) **Déploiement dans l'environnement de tests d'intégration système (SIT)**[30] : les nouveaux composants logiciels sont déployés dans l'environnement de tests d'intégrationsystème en tant qu'instance pleinement fonctionnelle du système international eTIR ;

d) **Deuxième phase de test** : des tests de validation automatisés sont ensuite exécutés sur la nouvelle instance du système international eTIR pour continuer à vérifier,

[28] Un seuil de qualité est un objectif quantitatif portant sur un critère particulier, par exemple : « Moins de 10 problèmes critiques » ou « Plus de 40 % du code source couvert par des tests ».

[29] Comme précisé dans les Exigences relatives à la fiabilité du système international eTIR.

[30] Voir la section suivante pour plus d'informations.

au niveau le plus élevé, que la modification du code n'a entraîné aucune régression.

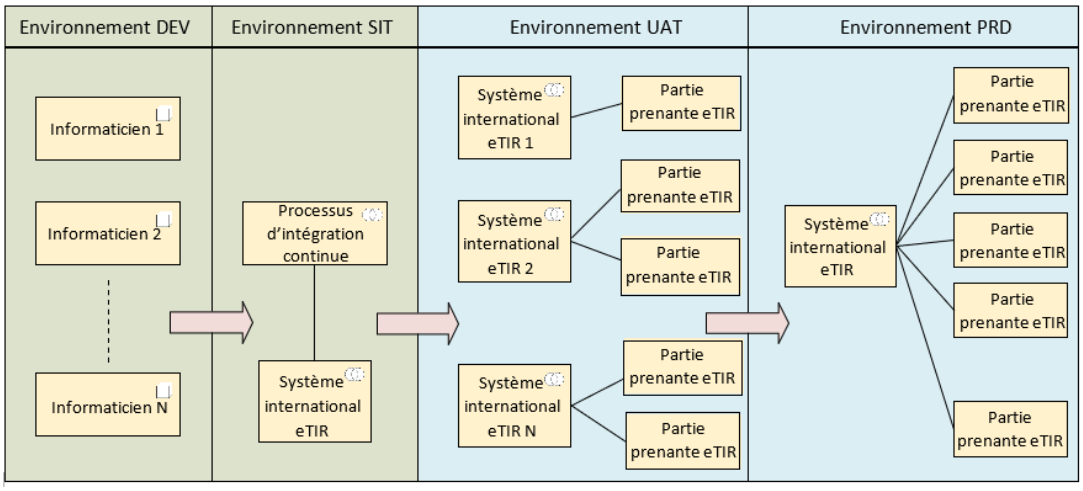
153. Si une erreur survient à l'une des étapes (par exemple, en cas d'échec ne serait-ce que d'un seul test), le processus d'intégration continue s'arrête et une notification d'échec est envoyée aux informaticiens sur leur plateforme de collaboration. Le temps d'exécution pour l'ensemble des étapes ne doit pas dépasser trente minutes afin que l'informaticien qui enregistre une modification dans le système de gestion de version obtienne rapidement des informations en retour. Le processus d'intégration continue associe plusieurs des pratiques optimales décrites ci-dessus et constitue un excellent moyen d'assurer la fiabilité du système eTIR et d'augmenter la productivité des informaticiens.

9. Environnements

154. S'inspirant des meilleures pratiques actuelles du secteur informatique, les informaticiens ont créé et configuré quatre environnements différents pour développer et gérer le système international eTIR dans les meilleures conditions. L'un des défis à relever s'agissant de la gestion de plusieurs environnements consiste à limiter les différences entre eux afin d'éviter l'apparition de défauts associés à un environnement donné. Tous les informaticiens mettent en place et suivent des procédures de développement spécifiques afin de limiter la probabilité d'occurrence de ce type de défauts.

155. La figure ci-dessous illustre les différents environnements, qui sont décrits dans les paragraphes suivants.

Figure XIV
Environnements du système international eTIR



156. **Environnement de développement (DEV)** : chaque informaticien dispose de son propre poste de travail sur lequel il peut développer et tester une copie locale du système international eTIR sans interférer avec le travail des autres. Une fois qu'une modification du code a été préparée et testée, l'informaticien l'enregistre dans le VCS afin qu'elle soit automatiquement déployée et testée dans l'environnement de tests d'intégration système (SIT) par le processus d'intégration continue.

157. **Environnement de tests d'intégration système (SIT)** : environnement interne qui sert d'emplacement temporaire dans lequel le processus d'intégration continue crée, déploie et teste automatiquement les nouvelles instances du système international eTIR. Une fois qu'un ensemble de modifications du code a été validé dans cet environnement, les informaticiens peuvent décider de créer et de déployer la dernière version du système international eTIR dans l'environnement de tests d'acceptation utilisateur (UAT).

158. **Environnement de tests d'acceptation utilisateur (UAT)** : les parties prenantes eTIR peuvent accéder à cet environnement pour effectuer des tests dans le cadre de leurs projets d'interconnexion. Plusieurs copies du système international eTIR sont disponibles et chaque partie prenante eTIR a accès à une ou plusieurs de ces instances. Les tests de conformité du système international eTIR et des systèmes d'information des parties prenantes eTIR sont également effectués dans l'environnement UAT. Une fois qu'une version du

système international eTIR a été testée de manière approfondie dans l'environnement UAT, elle peut être transférée dans l'environnement d'exploitation (PRD).

159. **Environnement d'exploitation (PRD)** : il abrite une instance unique du système international eTIR, à laquelle seules les parties prenantes eTIR qui ont achevé leur projet d'interconnexion peuvent accéder. Cet environnement « réel » est le seul qui est utilisé pour effectuer des transports TIR selon la procédure eTIR.

10. Lignes directrices relatives aux bases de données

160. La base de données eTIR fait appel à un système de gestion de base de données (SGBD) pour enregistrer les informations transmises dans les messages eTIR. Ce composant constitue le cœur du système international eTIR, et il convient d'apporter le plus grand soin à son développement et à sa maintenance.

161. La structure de la base de données eTIR est héritée des projets pilotes eTIR, et les informaticiens ont répertorié plusieurs possibilités d'amélioration et d'optimisation dont la mise en œuvre progressive est prévue. Les informaticiens utilisent un outil spécialisé, Liquibase, pour suivre, gérer et appliquer les changements de schéma (structure) de la base de données. Cette bibliothèque permet également de gérer les modifications des données maîtres et des données de référence stockées dans la base de données.

162. Dans le cadre du système eTIR, les « données maîtres et de référence » désignent les données relatives aux parties et aux rôles et les données utilisées pour classer les données traitées et stockées provenant des messages eTIR (par exemple, les identités des parties prenantes eTIR, les codes de pays, les types de garanties, la classification des marchandises, etc.). Ces données changent rarement et doivent être gérées méticuleusement.

163. Cet outil permet également de vérifier facilement quelles modifications ont été appliquées aux différentes copies de la base de données eTIR, que l'on retrouve dans tous les environnements énumérés dans la section précédente. Ceci est important pour garantir qu'une modification récente du schéma ou des données maîtres et de référence est appliquée de manière cohérente dans tous les environnements, conformément aux procédures de gestion des versions appropriées.

11. Gestion des tâches

164. L'un des principes fondamentaux de la méthode agile adoptée est une gestion des tâches définie et efficace. Dans ce contexte, une tâche peut être une demande de fonction, une demande de changement ou la notification d'un défaut. Toutes les modifications apportées au modèle de données eTIR, au code source ou à la documentation du système international eTIR doivent d'abord être enregistrées dans le système de suivi de la CEE. Ceci est essentiel pour assurer une bonne traçabilité de tous les changements et permet de vérifier que seules des modifications autorisées sont appliquées.

165. Lorsqu'un informaticien enregistre une tâche dans le système de suivi, il s'assure que tous les renseignements nécessaires sont fournis afin que tout autre informaticien soit en mesure de comprendre ce qui doit être fait. Il s'agit également d'un moyen d'assurer la pérennité de la mémoire institutionnelle indépendamment de l'éventuelle rotation du personnel au sein de la CEE.

166. Les experts en informatique se sont mis d'accord sur une série d'activités qui doivent être menées au cours des différentes phases du cycle de vie d'une tâche pour que celle-ci puisse être considérée comme achevée. C'est ce qui s'appelle la « définition de fini ». Les noms des phases correspondent aux différents états d'une tâche.

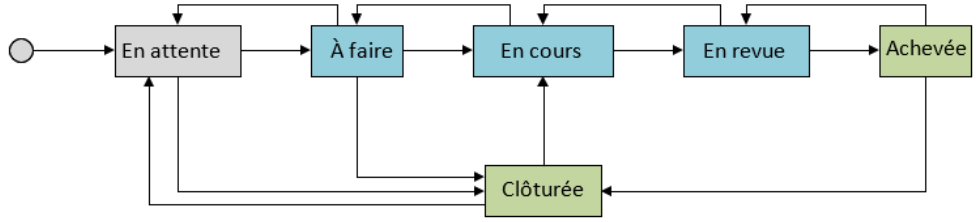
- **Définition de fini (DOD)** : liste des conditions ou critères d'acceptation[31] qui doivent être satisfaits pour qu'une tâche soit considérée comme achevée. L'objectif est de garantir en permanence un niveau approprié de qualité et de fiabilité du système. Le temps consacré à ces activités est toujours payant, car il permet d'éviter d'introduire de défauts dans l'environnement PRD. Réduire le nombre de défauts

[31] Les conditions et les critères d'acceptation sont définis plus loin dans la section.

limite les efforts et le stress liés au dépannage et préserve la réputation de la CEE.

167. Une nouvelle tâche se voit attribuer l'état « En attente », qui indique son appartenance au backlog (liste d'attente) eTIR ; une priorité lui est également affectée. Les tâches sont les lots de travail élémentaires qui sont assignés aux informaticiens par le coordinateur informatique après avoir été ajoutés dans le backlog d'itération. La figure suivante illustre le cycle de vie d'une tâche et les différents états par lesquels elle passe ; ces états sont décrits ci-après.

Figure XV
Cycle de vie des tâches



- **En attente** : la tâche a été répertoriée et enregistrée dans le système de suivi, mais n'a pas encore été sélectionnée pour être exécutée ;

- **À faire** : la tâche a été sélectionnée pour être menée à bien pendant une itération et est assignée à un informaticien, qui doit accomplir les étapes associées à la phase « À faire » de la DOD (voir ci-dessous) ;

- **En cours** : la tâche est en cours de traitement par l'informaticien, qui doit accomplir les étapes associées à la phase « En cours » de la DOD ;

- **En revue** : la tâche est examinée par un autre informaticien, qui vérifie plusieurs aspects liés à l'assurance qualité en suivant toutes les étapes associées à la phase « Revue » de la DOD ;

- **Achevée** : la tâche est achevée (mise en œuvre et revue) et elle sera validée par les informaticiens lors des réunions régulières où toutes les tâches déployées dans l'environnement PRD sont définitivement clôturées ;

- **Clôturée** : la tâche est clôturée soit parce qu'elle est « Achevée » (et prête à être déployée), soit parce qu'elle est « En attente » ou « À faire » et qu'il n'est pas prévu de la corriger ou qu'elle fait double emploi avec une autre tâche.

168. Selon la DOD, les objectifs clefs et les critères d'acceptation des différentes phases sont les suivants :

- **À faire** : la tâche est décrite de manière suffisamment détaillée et est accompagnée de suffisamment d'informations pour que tout informaticien soit en mesure de comprendre ce qui doit être fait, et une première estimation du temps nécessaire est fournie ;

- **En cours** : la modification nécessaire est entièrement effectuée sur toutes les ressources informatiques appropriées (modèle de données eTIR, code source et documentation). Toutes les exigences en matière de qualité et de fiabilité sont satisfaites (y compris les vérifications effectuées par le processus d'intégration continue et l'outil d'analyse statique) et toutes les lignes directrices applicables sont respectées ;

- **En revue** : les résultats des tâches effectuées au cours de la phase « En cours » sont vérifiés par un autre informaticien, en particulier ceux des tests portant sur la couverture du code source qui a été mis à jour.

12. Lignes directrices relatives à la documentation

169. La CEE gère trois types de documents relatifs au système international eTIR. Le premier correspond aux spécifications eTIR, dont les procédures d'amendement sont décrites à l'article 5 de l'annexe 11 de la Convention TIR.

170. Le second correspond à la documentation interne dont la CEE a besoin pour assurer correctement le développement, le fonctionnement et la maintenance du système international eTIR. Cette documentation est constituée et mise à jour par les experts de la CEE et est gérée au moyen d'un système de gestion des connaissances sécurisé, qui permet de garder la trace des différentes versions (versionnage) afin d'assurer la pérennité de la mémoire institutionnelle. La documentation interne contient des informations confidentielles portant notamment sur :

- Le développement : lignes directrices, documentation technique, formation, documentation des parties prenantes, procédures d'exploitation normalisées connexes, etc. ;

- La gestion : gestion de l'équipe, notes de réunion, procédures d'exploitation normalisées connexes, etc. ;

- Les opérations : connexion avec les Parties contractantes, environnements, service d'assistance eTIR, procédures d'exploitation normalisées connexes, etc.

171. Le troisième correspond à la documentation produite par la CEE afin de permettre aux parties prenantes eTIR de connecter leurs systèmes d'information au système international eTIR. Ces documents sont publiés sur le site Web eTIR[32]. Ils sont élaborés en complément des spécifications eTIR afin de faciliter les projets d'interconnexion et de tirer parti de l'expérience acquise dans le cadre de ces projets. Ils permettent à la CEE de clarifier en permanence divers aspects du système eTIR de manière plus fréquente et plus souple. Tous ces documents sont toujours entièrement conformes à l'annexe 11 et à la version des spécifications eTIR sur laquelle ils reposent.

13. Gestion des numéros de version

172. La CEE gère le code source du système international eTIR et les modifications appliquées au schéma et aux « données maîtres et de référence » de la base de données eTIR au moyen d'un système de gestion de version (VCS). Le VCS sélectionné par la CEE est Git, dont le répertoire central est hébergé sur une plateforme interne et sécurisée.

173. Les informaticiens appliquent les pratiques optimales habituelles associées à Git, notamment celles établies par DevOps. En principe, ils enregistrent et publient fréquemment les modifications qu'ils apportent au code dans le répertoire central, après avoir effectué tous les tests localement pour vérifier que ces modifications n'entraîneront pas d'erreurs pendant le processus d'intégration continue. Chaque modification enregistrée (*commit*) ne doit concerner qu'une seule tâche, et le commentaire qui lui est associé doit clairement mentionner la tâche en question et décrire la teneur des changements.

174. Des branches sont créées et utilisées dans plusieurs cas, par exemple pour travailler sur une fonction complexe qui ne peut pas être immédiatement enregistrée dans la branche principale. Une fois la fonction terminée et testée, cette branche est alors fusionnée avec la branche principale. Une branche est également créée chaque fois qu'une version du système international eTIR est transférée dans l'environnement PRD, conformément aux lignes directrices de gestion des versions. Des balises sont également créées lorsqu'une nouvelle version du système international eTIR est déployée dans l'environnement UAT ou dans l'environnement PRD.

175. S'agissant du numéro de version du système international eTIR, la CEE a choisi une approche qui fait appel aux trois numéros suivants :

- **Numéro de version principal** : il est incrémenté lorsqu'une modification majeure

[32] Voir etir.org/documentation

est apportée à l'interface de programmation d'applications (API) qui permet aux parties prenantes eTIR de se connecter au système international eTIR. Il peut également être incrémenté lorsqu'un changement important est apporté au système international eTIR sans que l'API soit modifiée ;

- **Numéro de version secondaire** : il est incrémenté dans tous les cas autres que ceux qui concernent le numéro de version principal ou le numéro de version du correctif. Lorsque le numéro de version principal est incrémenté, le numéro de version secondaire est remis à 0 ;

- **Numéro de version du correctif** : il n'est utilisé que lorsqu'un ou plusieurs correctifs doivent être appliqués à une version qui est déjà déployée dans l'environnement PRD, et qu'on ne veut pas créer une nouvelle version du système international eTIR.

176. Les numéros de version principal et secondaire ainsi que le numéro de version du correctif, s'il existe, sont toujours mis à jour simultanément sur tous les composants logiciels du système international eTIR. Le numéro de version se présente comme suit : XX.YY.ZZ, XX étant le numéro de version principal, YY le numéro de version secondaire et ZZ le numéro de version du correctif (qui n'est pas indiqué s'il est égal à 0). On trouvera ci-après deux exemples de numéro de version du système international eTIR :

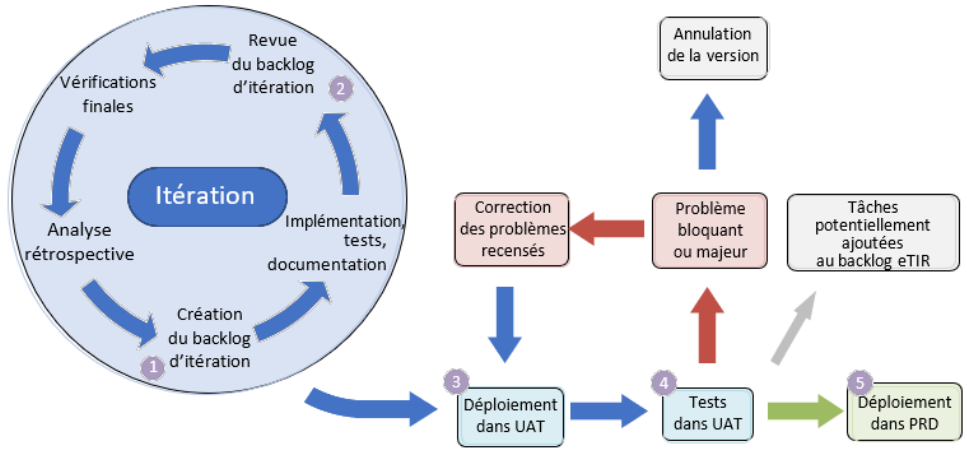
- **Système international eTIR 4.15**, où 4 est le numéro de version principal et 15 le numéro de version secondaire (cas fréquent) ;

- **Système international eTIR 4.15.1**, où 4 est le numéro de version principal, 15 le numéro de version secondaire et 1 le numéro de la version du correctif (cas rare).

13. Gestion des versions

177. La gestion des versions désigne le processus de gestion, de planification, de programmation et de contrôle mis en œuvre pour créer un logiciel ; ce processus se déroule dans différents environnements et comprend différentes étapes, y compris les tests et le déploiement des versions du logiciel. Dans le cadre du système international eTIR, il s'agit du processus illustré à la figure IV et dont les étapes sont décrites ci-dessous.

Figure XVI
Processus de gestion des versions



a) **Création du backlog d'itération** : les informaticiens sélectionnent dans le backlog eTIR (liste d'attente) les tâches à traiter pendant l'itération et définissent le numéro de la nouvelle version du logiciel. Le numéro de chaque version est unique et obligatoire si la version doit être déployée dans les environnements UAT ou PRD ;

b) **Revue du backlog d'itération** : les informaticiens vérifient quelles tâches sont considérées comme « achevées » et modifient soit la durée de l'itération, soit la liste des tâches à traiter pendant celle-ci. À la fin de cette phase, toutes les tâches sont

terminées, testées et documentées et les seuils de qualité sont respectés dans l'environnement SIT. Les notes de version, qui expliquent les changements apportés par la nouvelle version, sont préparées ;

c) **Déploiement dans l'environnement UAT** : les parties prenantes eTIR qui utilisent les instances du système international eTIR sont préalablement informées de ce déploiement. La nouvelle version est ensuite déployée dans toutes les instances du système international eTIR, et les bases de données eTIR correspondantes sont réinitialisées. Les notes de version sont communiquées aux parties prenantes eTIR ;

d) **Test dans l'environnement UAT** : la nouvelle version est ensuite testée dans l'environnement UAT par les parties prenantes eTIR pendant une période dont la durée est fixée d'un commun accord par toutes les parties. Les experts déterminent s'il est nécessaire ou non de procéder de nouveau aux tests de conformité. Tout problème constaté est signalé au service d'assistance eTIR qui l'enregistre et le classe dans une catégorie. Si un ou plusieurs problèmes bloquants ou majeurs sont découverts, soit ils sont corrigés, soit la version est annulée et une nouvelle version du logiciel est préparée, dont la liste de tâches inclut en priorité les problèmes à résoudre. Si la solution choisie est de corriger les problèmes recensés, la version mise à jour doit être déployée dans l'environnement UAT et testée à nouveau par toutes les parties prenantes eTIR pendant une certaine période avant d'être validée. Les problèmes mineurs peuvent être ajoutés au backlog eTIR afin d'être corrigés dans une version ultérieure ;

e) **Déploiement dans l'environnement PRD** : si aucun problème majeur n'est signalé après une certaine période de test dans l'environnement UAT, il est possible de programmer le déploiement de la version dans l'environnement d'exploitation après en avoir informé de manière appropriée les parties prenantes eTIR. Une fois le déploiement effectué, le service d'assistance eTIR surveille activement les indicateurs pour vérifier que tout fonctionne correctement.

178. Si par la suite un problème est détecté dans l'environnement d'exploitation, trois cas peuvent se présenter :

a) **Il s'agit d'un problème bloquant** : les informaticiens reviennent à la version précédente de l'environnement PRD et en informent toutes les parties prenantes eTIR ;

b) **Il s'agit d'un problème majeur** : les informaticiens préparent rapidement un correctif, effectuent tous les tests nécessaires dans l'environnement SIT et déploient le correctif dans l'environnement PRD pour résoudre le problème. Toutes les parties prenantes eTIR sont informées en conséquence ;

c) **Il s'agit d'un problème mineur** : le problème est enregistré et ajouté au backlog eTIR afin d'être corrigé dans une version ultérieure.

F. Processus de maintenance

1. Introduction

179. La présente section décrit les processus relatifs à la maintenance et au support du système international eTIR qui ont été adoptés par les experts en informatique de la CEE afin d'assurer son bon fonctionnement, de traiter correctement les problèmes, de les anticiper et de les prévenir. Elle décrit également les démarches que doivent effectuer les parties prenantes eTIR pour signaler un problème et informe sur les activités internes mises en œuvre pour le résoudre.

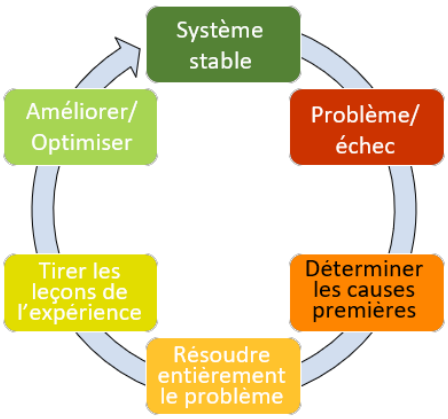
2. Amélioration continue

180. L'un des principes fondamentaux des pratiques DevOps consiste à adopter une approche d'amélioration continue. Cela signifie qu'un extrant quel qu'il soit (logiciel, processus, documentation, etc.) n'est jamais le produit définitif, car il peut toujours être amélioré. En particulier, si un problème (un défaut du système, une faille dans un processus,

ou une omission ou une imprécision dans la documentation) est soulevé, il doit toujours être considéré comme une occasion d'améliorer le produit. Ce principe est analogue à celui du cycle de Deming (méthode PDCA)[33].

181. En adoptant cette approche, les experts reconnaissent qu'il est essentiel de toujours saisir l'occasion de tirer des leçons des problèmes rencontrés afin de s'assurer que les mêmes problèmes ne se reproduiront pas (ou, au moins, que les mesures prises diminueront leur probabilité d'occurrence). Il est en particulier important de prendre le temps de déterminer la ou les causes premières d'un problème pour pouvoir les éliminer et améliorer ou optimiser les processus, si possible. Cette approche est également appliquée dans les processus de développement, mais elle est cruciale pour les processus de maintenance, dont les principaux objectifs sont de résoudre et de prévenir les problèmes. Les principales étapes du processus d'amélioration continue sont illustrées à la figure suivante. Elles sont également expliquées plus en détail dans les sections suivantes.

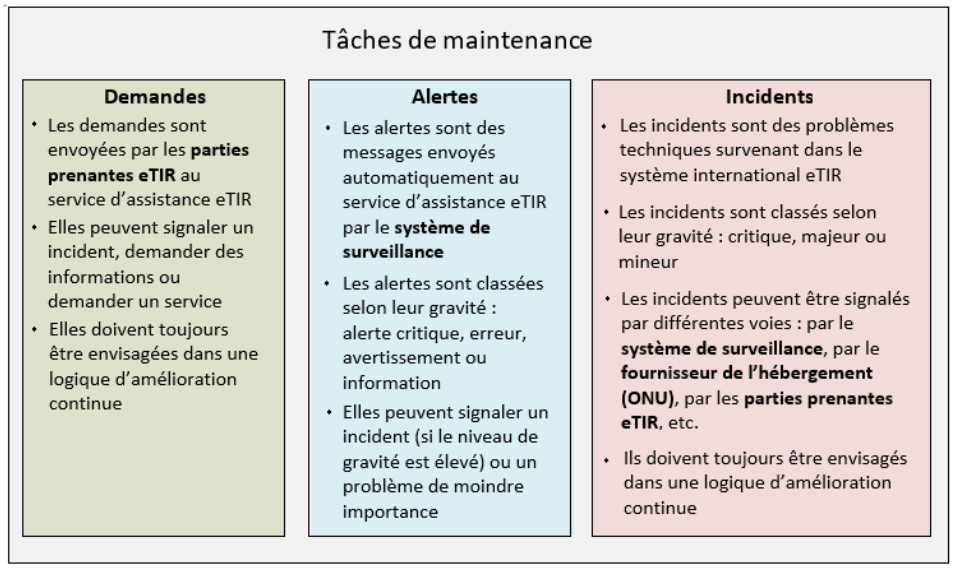
Figure XVII
Processus d'amélioration continue



3. Gestion des tâches de maintenance

182. Il existe trois types de tâches de maintenance, qui ont leurs propres caractéristiques et qui sont traités à l'aide de procédures spécifiques. Ces différents types sont présentés ci-après.

Figure XVIII
Types de tâches de maintenance



[33] Voir fr.wikipedia.org/wiki/Roue_de_Deming.

183. Les demandes sont présentées dans la section consacrée au service d'assistance eTIR. Les alertes sont présentées dans la section consacrée à la gestion de la surveillance. Les incidents sont présentés dans la section consacrée à la gestion des incidents.

4. Service d'assistance eTIR

184. Le service d'assistance eTIR est le point de contact unique auquel les parties prenantes eTIR doivent s'adresser pour toute demande liée au système eTIR. Elles peuvent pour ce faire envoyer un message à son adresse électronique (etir@un.org) ou utiliser le formulaire « Contactez-nous » du site Web eTIR[34]. Le service d'assistance eTIR est composé d'experts en informatique et d'experts techniques de la Convention TIR de la CEE.

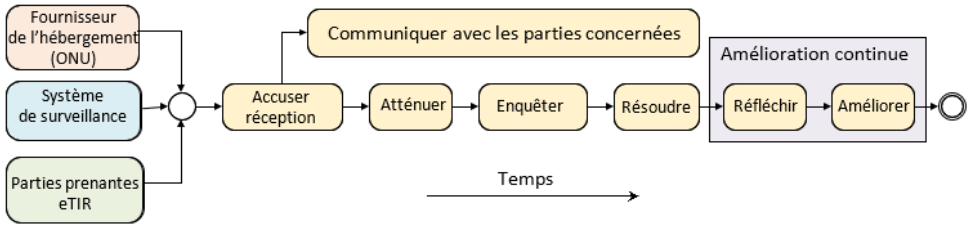
185. Les demandes reçues par le service d'assistance eTIR sont envoyées par un agent du service d'assistance (niveau 1) à l'expert compétent (niveau 2), selon la nature de la demande. Les demandes qui signalent un incident ou un problème technique sont traitées en priorité.

186. Dans le cadre des projets d'interconnexion, le service d'assistance eTIR aide les parties prenantes eTIR à connecter leurs systèmes d'information au système international eTIR. Ces projets sont plus étroitement associés aux processus de développement, et les parties prenantes eTIR définissent pendant leur phase de lancement les meilleurs moyens de communiquer avec le service d'assistance eTIR pour obtenir des informations et formuler des demandes. Compte tenu des maigres ressources dont il dispose, le service d'assistance eTIR se limite à fournir des informations et à guider les experts des parties prenantes eTIR dans leurs projets d'interconnexion. Ainsi, le service d'assistance eTIR ne peut pas effectuer directement des modifications dans les systèmes d'information des parties prenantes eTIR pour les connecter au système international eTIR.

5. Gestion des incidents

187. Les incidents sont généralement des problèmes techniques aux conséquences importantes, qui doivent être traités en priorité par le service d'assistance eTIR. Ils sont associés à un niveau de gravité (critique, majeur ou mineur) qui détermine le type de réponse à donner. L'ensemble du processus de gestion des incidents s'inspire de la méthode de gestion des services informatiques de l'Information Technology Infrastructure Library (ITIL). Ses étapes sont illustrées à la figure suivante et décrites ci-après.

Figure XIX
Processus de gestion des incidents



a) **Accuser réception** : après avoir été alertés, les informaticiens confirment qu'il s'agit d'un incident (et non d'un faux positif) et que celui-ci persiste (il n'a pas encore été résolu). Ils déterminent sa portée (les composants affectés), sa gravité et la liste des parties concernées. Toutes les actions sont ensuite enregistrées pour être analysées de manière plus approfondie à l'étape « Réfléchir » ;

b) **Communiquer avec les parties concernées** : il est essentiel de communiquer de manière transparente avec les parties concernées par l'incident afin de les informer du temps nécessaire à la résolution du problème, car cela peut les amener à appliquer des mesures spécifiques (par exemple, des procédures de secours). Les informaticiens décident du contenu et de la fréquence des communications jusqu'à ce que l'incident soit résolu (étape e)) ;

c) **Atténuer** : des mesures d'atténuation sont mises en œuvre si possible afin de

[34] Voir etir.org/contact-us

diminuer la gravité du problème ou de le résoudre temporairement ;

d) **Enquêter** : les informaticiens prennent le temps nécessaire pour enquêter de manière approfondie sur l'incident et en déterminer la ou les causes premières ;

e) **Résoudre :** une fois l'enquête terminée, la ou les causes premières sont traitées et des corrections sont apportées ; l'incident doit être considéré comme résolu pour qu'il soit possible de passer à l'étape suivante ;

f) **Réfléchir** : les experts rassemblent toutes les données concernant l'incident, établissent la liste des mesures déjà prises pour le résoudre et organisent une analyse rétrospective non culpabilisante. L'objectif est d'examiner en profondeur l'incident et de déterminer ce qui s'est passé, les raisons pour lesquelles l'incident s'est produit, la manière dont les informaticiens ont réagi, ainsi que ce qui peut être fait pour éviter que ce type d'incident ne se reproduise et pour améliorer les futures interventions, tout en assumant collectivement la responsabilité de l'incident. Un « rapport d'incident » est préparé au cours de cette réunion et des mesures de suivi sont prise et planifiées ;

g) **Améliorer :** les mesures de suivi arrêtées aux deux étapes précédentes sont progressivement sélectionnées dans le backlog eTIR en fonction de leur niveau de priorité, et mises en œuvre pour améliorer le logiciel, les processus, la documentation et les autres ressources informatiques, en vue de réduire la probabilité d'occurrence de l'incident.

188. À l'étape « Réfléchir », les experts préparent un rapport d'incident qui est ensuite enregistré dans le système de gestion des connaissances pour préserver la mémoire institutionnelle. Ce rapport contient les informations suivantes sur l'incident (y compris la date et l'heure le cas échéant) : sa gravité, sa description, les services affectés, qui l'a signalé et de quelle manière, les mesures prises pour l'atténuer puis le résoudre, les échanges d'informations, les résultats de l'enquête, la liste des causes premières, les enseignements tirés de l'analyse rétrospective non culpabilisante et la liste des mesures de suivi.

189. En mettant en œuvre ce processus, les experts cherchent à atteindre les objectifs suivants : la prévention d'incidents analogues (ou du moins la diminution de leur probabilité d'occurrence), l'amélioration du temps moyen de résolution des incidents, une réduction supplémentaire du temps d'indisponibilité du système international eTIR et une amélioration générale de l'expérience des parties prenantes du système eTIR.

6. Incidents gérés par le fournisseur de l'hébergement (ONU)

190. Comme le montre la figure XIX, des incidents peuvent être signalés au service d'assistance eTIR par l'entité de l'ONU qui héberge le système international eTIR. Un accord de prestation de service a été signé avec cette entité en vue d'assurer un support permanent du système. Les experts préparent les procédures d'exploitation normalisées destinées aux agents du fournisseur de l'hébergement (ONU), afin que ces derniers puissent répondre à des types d'incidents spécifiques.

191. Lorsqu'un incident se produit, les agents du fournisseur de l'hébergement (ONU) sont avertis par les alertes envoyées par le système de surveillance, et ils interviennent en mettant en œuvre les procédures d'exploitation normalisées. Si leur intervention permet de résoudre l'incident, ils en informent le service d'assistance eTIR afin qu'une enquête plus approfondie soit menée, en mentionnant que l'incident est clos. Si leur intervention ne résout pas l'incident, ils signalent le problème au service d'assistance eTIR, comme illustré à la figure XIX, en recourant à divers moyens et procédures de communication en fonction de la gravité de l'incident.

7. Gestion des sauvegardes et des restaurations

192. La gestion des sauvegardes et des restaurations désigne la stratégie et les procédures connexes mises en place pour garantir que les données eTIR sont fréquemment copiées et peuvent être rapidement restaurées en cas de perte de données. En effet, des pertes de données peuvent se produire au cours de différents types d'événements, notamment le

dysfonctionnement d'un serveur, l'incendie du centre informatique ou une cyber-attaque. Le fournisseur de l'hébergement (ONU) et la CEE sont conjointement responsables de l'élaboration des procédures d'exploitation normalisées, qui figurent dans l'accord de prestation de service.

193. Les données stockées dans tous les emplacements de stockage eTIR (la base de données eTIR, les journaux eTIR et les documents eTIR) sont sauvegardées deux fois par jour. Ces données sauvegardées sont stockées en toute sécurité dans au moins un autre lieu que le site principal, afin d'éviter leur destruction si ce site subit un sinistre. Ce lieu n'est pas accessible depuis le même réseau pour éviter que les données ne soient compromises en cas de cyber-attaque par logiciel rançonneur. Seules les sauvegardes les plus récentes et complètes sont conservées ; les anciennes sauvegardes sont effacées.

194. Il est prévu que la restauration de la dernière sauvegarde ne prenne pas plus de six heures en cas de perte de données. Des tests sont régulièrement effectués avec le fournisseur de l'hébergement (ONU) pour vérifier que cette exigence peut être respectée.

8. Gestion de la surveillance

195. La surveillance d'un système d'information implique la collecte d'informations générées par ce système et la capacité d'émettre des alertes lorsque certains événements se produisent, afin que des mesures (automatisées ou manuelles) puissent être prises pour y faire face. Cette surveillance permet de détecter de manière proactive tout problème susceptible de se transformer en défaillance et d'affecter la disponibilité du système. Le fait de pouvoir intervenir rapidement en cas d'alerte précoce permet généralement de réduire l'impact des défaillances et parfois même d'éviter ces dernières.

196. Le fournisseur de l'hébergement (ONU) dispose d'un système de surveillance qui est configuré en collaboration avec la CEE ; ce système permet de surveiller les ressources et le fonctionnement des serveurs virtuels, ainsi que la disponibilité et le fonctionnement des différents services du système international eTIR. Les indicateurs suivis par le système de surveillance sont notamment les suivants : utilisation de l'unité centrale, utilisation de la mémoire vive, pourcentage d'espace disque utilisé, processus, disponibilité des services, temps de réponse du système et utilisation des ressources par les applications.

197. Les alertes sont configurées pour se déclencher lorsque des seuils spécifiques sont dépassés. Elles sont associées à un niveau de gravité qui détermine le type de réponse à donner : alerte critique, erreur, avertissement ou information. Plusieurs types de réponses peuvent être mis en œuvre en fonction de la configuration des alertes : exécution d'un processus automatisé, ou envoi à une ou plusieurs personnes d'un message (courrier électronique, SMS ou appel téléphonique) les informant de la situation afin qu'elles puissent agir au plus vite. Les premières personnes averties sont généralement les agents du fournisseur de l'hébergement (ONU), afin qu'ils puissent prendre immédiatement des mesures en appliquant les procédures d'exploitation normalisées préparées à cet effet. Les alertes peuvent également être envoyées au service d'assistance eTIR, en fonction de l'urgence et de l'importance du problème. Une liste complète d'indicateurs, de seuils, d'alertes et de réponses connexes est établie conjointement par le fournisseur de l'hébergement (ONU) et la CEE, et figure dans l'accord de prestation de service.

198. Outre le suivi des paramètres des serveurs virtuels et des processus, le système de surveillance assure l'exploitation des données contenues dans les journaux eTIR. Ces informations (ou indicateurs) enregistrées par le système international eTIR fournissent des données précieuses qui peuvent être utilisées pour détecter tout problème potentiel imminent. Elles renseignent également sur les performances du système et fournissent aux experts des indications sur les tendances en la matière. Il est important de suivre ces données pour vérifier que les valeurs cibles fixées dans les spécifications techniques du système international eTIR sont respectées.

199. Il convient par ailleurs de tenir compte d'un inconvénient généralement associé à la surveillance. La configuration initiale des seuils et des alertes peut entraîner des faux positifs (fausses alarmes) ou, au contraire, des faux négatifs (non-détection de problèmes). Le recours à l'amélioration continue est donc particulièrement utile, et la configuration du système de surveillance doit être régulièrement revue pour être optimisée.

9. Gestion des correctifs

200. Un correctif est un ensemble de modifications apportées à un logiciel afin de le mettre à jour, de le corriger ou de l'améliorer. Il s'agit notamment de remédier aux failles de sécurité et autres défauts. Dans le présent document, la gestion des correctifs désigne la stratégie et les procédures connexes mises en place pour garantir que des modifications sont régulièrement apportées à tous les composants logiciels, y compris les systèmes d'exploitation des serveurs sous-jacents, afin de remédier à tout problème récemment découvert.

201. Il est particulièrement important de remédier aux failles de sécurité mises en évidence par la communauté de la cybersécurité dans les versions existantes de tous les logiciels. L'apport régulier de correctifs provenant de sources autorisées et vérifiées est l'un des moyens les plus efficaces de protéger le système international eTIR contre les cyberattaques (voir la partie consacrée à la sécurité du système eTIR).

202. Des procédures d'exploitation normalisées sont préparées et mises en œuvre régulièrement (tous les trois mois au minimum) pour apporter les correctifs disponibles aux composants logiciels suivants : infrastructures, bibliothèques (par exemple, la machine virtuelle Java) et systèmes d'exploitation sous-jacents, et systèmes de gestion des bases de données. Ces schémas réguliers n'empêchent pas d'appliquer des correctifs importants si nécessaire, la plupart du temps pour des raisons de sécurité. Les composants logiciels sont corrigés par le fournisseur de l'hébergement (ONU) et par la CEE, en fonction des responsabilités précisées dans l'accord de prestation de service.

10. Gestion des mises à niveau

203. Une mise à niveau consiste à remplacer un matériel, un logiciel ou un micrologiciel par une version plus récente ou plus performante, afin de mettre le système à jour ou d'améliorer ses fonctionnalités. Dans le présent document, la gestion des mises à niveau désigne la stratégie et les procédures connexes mises en place pour garantir que la question de la dette technique est régulièrement abordée et que celle-ci n'augmentera pas avec le temps (voir les exigences relatives à la maintenabilité du système international eTIR). La gestion des mises à niveau diffère de la gestion des correctifs, car les mises à niveau sont de nouvelles versions des logiciels, qu'il convient de tester soigneusement avant de les installer, afin de détecter et de résoudre les problèmes potentiels.

204. Le remplacement du matériel et des micrologiciels associés relève de la responsabilité du fournisseur de l'hébergement (ONU). En ce qui concerne les logiciels, les responsabilités sont partagées entre le fournisseur de l'hébergement (ONU), qui doit planifier et effectuer les mises à niveau de tous les composants logiciels qui relèvent de sa compétence (par exemple, la batterie de serveurs virtuels et les systèmes d'exploitation des serveurs virtuels), et la CEE, qui doit planifier et effectuer les mises à niveau de tous les composants logiciels du système international eTIR.

205. Les dernières versions des langages, infrastructures et bibliothèques de programmation utilisés pour développer le système international eTIR sont passées en revue au moins une fois par trimestre. Les experts procèdent ensuite régulièrement à l'étude documentée des avantages et inconvénients de la migration d'un composant logiciel vers l'une de ses nouvelles versions. Les critères suivants sont pris en compte pour décider à quel moment il convient de procéder à une telle migration : date de la fin du support de la version actuellement utilisée, maturité de la nouvelle version telle qu'évaluée par la communauté informatique, avantages potentiels en matière de sécurité, et fonctionnalités supplémentaires.

206. Lorsque la décision de faire migrer un composant logiciel vers une nouvelle version est prise, un projet interne est lancé et les tâches qui lui sont associées sont ajoutées dans le backlog eTIR ; une priorité est également attribuée à ces tâches, afin de permettre leur prise en compte dans l'approche habituelle de développement par itération. Les objectifs de ce type de projet sont les suivants : tester de manière exhaustive la nouvelle version du composant logiciel afin de détecter tout problème pouvant survenir dans le cadre du système international eTIR ; corriger tout problème majeur constaté ; tirer éventuellement parti des nouvelles fonctionnalités apportées par la mise à niveau pour améliorer le système international eTIR ; et procéder à des tests et des validations supplémentaires dans

l'environnement UAT avant de déployer une nouvelle version du système international eTIR dans l'environnement PRD.

IV. Sécurité du système eTIR

207. Le présent chapitre décrit tous les aspects du système eTIR ayant trait à la sécurité informatique. Il y est en particulier question des objectifs et des exigences, ainsi que des mesures et des contrôles mis en place à cet égard. La sécurité étant, en raison de l'importance qu'elle revêt pour les systèmes informatiques d'aujourd'hui, considérée comme un axe fondamental de la conception du système international eTIR, la CEE entend prendre correctement en compte cette question. L'objectif est de préciser de façon exhaustive tous les aspects fondamentaux de la sécurité informatique. Ces éléments devront ensuite être régulièrement examinés et actualisés par le TIB.

208. La sécurité informatique ne concerne pas seulement les logiciels, mais tous les domaines qui peuvent jouer un rôle dans la sécurité d'un système. C'est pourquoi il sera ici question des domaines suivants : la sécurité et la gestion des risques ; la sécurité des biens ; l'architecture et l'ingénierie de la sécurité ; la sécurité des communications et des réseaux ; la gestion des identités et des accès ; l'évaluation et la mise à l'épreuve de la sécurité ; les activités liées à la sécurité ; la sécurité du développement des logiciels.

209. Comme il a été dit au chapitre précédent, qui porte sur les aspects techniques du système international eTIR, le niveau de détail des sections suivantes dépend des éléments décrits et toutes les informations ne peuvent être divulguées pour des raisons de sécurité.

A. Objectifs et principes de la sécurité

1. Classification de l'information et politiques de sécurité

210. Il importe, en préambule à toute discussion relative à la sécurité informatique, de déterminer la sensibilité des informations gérées par les systèmes informatiques. Aux Nations Unies, ces aspects sont régis par la circulaire du Secrétaire général intitulée « Informations sensibles ou confidentielles : classification et maniement »[35]. Les données échangées entre les acteurs du système eTIR ou entre les utilisateurs de la banque de données internationale TIR (ITDB) sont classées dans la catégorie « Confidentiel », telle que définie dans la section 2 de la circulaire.

211. Il est question du niveau de confidentialité, ou il y est fait référence, dans d'autres documents des Nations Unies précisant les règles, les directives et les bonnes pratiques applicables. Ainsi, plusieurs circulaires du Bureau de l'informatique et des communications (OICT) portant sur la sécurité informatique décrivent les contrôles de sécurité qui doivent être effectués pour un niveau donné[36]. Les mesures et les contrôles de sécurité définis dans les spécifications techniques eTIR sont à cet égard aussi stricts que l'exigent les circulaires portant sur la gestion des informations confidentielles.

2. Les objectifs de la sécurité

212. La sécurité informatique consiste à atteindre les trois objectifs fondamentaux suivants[37] :

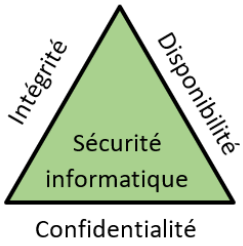
- **L'intégrité** : l'information conserve sa véracité et n'est modifiée intentionnellement que par des sujets autorisés ;
- **La disponibilité** : les sujets autorisés bénéficient d'un accès rapide et permanent aux informations ;
- **La confidentialité** : les informations ne sont pas divulguées à des sujets non

[35] Voir le document ST/SGB/2007/6.
[36] On trouvera une liste de ces circulaires à l'adresse iseek.un.org/nyc/department/policies.
[37] On trouvera la définition complète de ces trois termes dans le glossaire technique.

autorisés.

213. Ces trois objectifs fondamentaux, tels que représentés dans la figure ci-après, sont les principales composantes de la sécurité informatique. Ils impliquent l'observation de certaines règles lors du développement des systèmes informatiques.

Figure XX
Les objectifs fondamentaux de la sécurité informatique

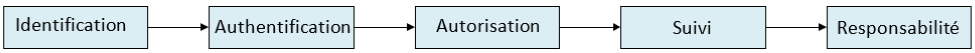


214. Dans le cas du système eTIR, l'atteinte de ces trois objectifs impose des règles strictes. En effet, les données traitées relevant de la catégorie « Confidentiel », leur confidentialité doit être garantie par des contrôles de sécurité appropriés. Étant donné le grand nombre d'acteurs impliqués dans un transport international de marchandises effectué selon la procédure eTIR, le système doit toujours être disponible pour ses utilisateurs. Enfin, il convient de préserver l'intégrité des données transférées entre les différents acteurs pour créer la confiance et pour assurer la non-répudiation.

3. Faire en sorte que les acteurs assument la responsabilité de leurs actions et assurer la non-répudiation

215. Après avoir présenté les notions d'intégrité, de disponibilité et de confidentialité, il est également important de préciser le mode d'identification d'un sujet[38] dans un système et de déterminer de quelle manière on fait en sorte que les acteurs assument la responsabilité de leurs actions et comment est assurée la non-répudiation. On peut résumer cela à une série de cinq étapes, qui est schématisée dans la figure ci-après et présentée dans la suite du document.

Figure XXI
De l'identification au respect du principe de responsabilité



a) **L'identification**, première étape de la procédure permettant l'application du principe de responsabilité, permet à un sujet de décliner son identité. Un sujet doit s'identifier pour être authentifié par un système. Pour s'identifier, il peut par exemple saisir son nom d'utilisateur ou positionner un doigt à proximité d'un dispositif de lecture. Le fait que chaque sujet doive posséder une identité unique est un principe fondamental de l'authentification ;

b) **L'authentification** consiste à vérifier ou à mettre à l'essai la validité d'une identité déclarée. Pour être authentifié, un sujet doit fournir des informations supplémentaires correspondant à l'identité qu'il revendique, par exemple un mot de passe ou un certificat numérique. L'authentification consiste à vérifier l'identité du sujet en comparant un ou plusieurs éléments à ceux enregistrés dans la base de données des identités valides (par exemple les comptes utilisateurs) ;

c) **L'autorisation** est le processus qui consiste à accorder l'accès à une ressource ou à un objet, une fois son identité authentifiée. Dans la plupart des cas, le système évalue une matrice de contrôle d'accès qui compare le sujet, l'objet et l'activité prévue.

[38] On entend ici par « sujet » une personne ou un système informatique qui tente d'accéder à un système informatique.

L'autorisation n'est accordée au sujet que si l'action en question est permise ;

d) **Le suivi** permet de connaître et d'enregistrer l'activité d'un sujet afin de pouvoir le tenir responsable de ses actes lorsqu'il est authentifié par un système. Le dispositif de suivi permet également au système de détecter toute activité non autorisée ou anormale ;

e) **La responsabilité** est le principe en vertu duquel les sujets doivent assumer les conséquences de leurs actions. Pour que les sujets puissent être efficacement tenus responsables de leurs actions, il faut être en mesure de prouver leur identité et de suivre leur activité. La responsabilité est avérée lorsqu'on établit un lien entre une personne et les activités d'une identité en ligne au moyen des fonctions de sécurité et des mécanismes de suivi, d'authentification et d'identification.

216. **La non-répudiation** est un objectif de sécurité dérivé important reposant sur le principe selon lequel le sujet à l'origine d'une activité ou d'un événement ne peut pas contester le fait d'être à l'origine de ladite activité. En vertu de ce principe, un sujet ne peut pas prétendre qu'il n'a pas envoyé un message, accompli une action ou été à l'origine d'un événement. Cet objectif est important parce que les informations stockées dans le système international eTIR peuvent être demandées par les Parties contractantes en cas de réclamation[39]. Lorsque sont atteints les objectifs relatifs à la responsabilité des sujets et à l'intégrité des données stockées dans le système international eTIR, l'objectif de non-répudiation est également atteint.

4. Principes relatifs à la sécurité

217. Comme dans le cas des principes directeurs arrêtés pour le développement du système international eTIR, la CEE a fait siens et adopté des principes reconnus et largement appliqués par la communauté des experts en sécurité informatique.

218. Le premier de ces principes est celui de la **diligence raisonnable**. Dans le contexte de la sécurité informatique, cela signifie l'obligation de prendre les précautions qui s'imposent pour protéger les biens d'une organisation de manière continue. Le respect de ce principe exige un niveau élevé d'anticipation et l'instauration d'une culture de la sécurité. La mise en œuvre des principes et des procédures de sécurité dont il est question dans cette partie, ainsi que la réalisation d'audits et d'examens périodiques de la sécurité, garantissent aux acteurs du système eTIR que la CEE prend les mesures qui s'imposent pour respecter son obligation de diligence.

219. Le deuxième principe est celui du **moindre privilège**, en vertu duquel un élément d'une couche d'abstraction donnée d'un environnement informatique (qu'il s'agisse d'un processus, d'un utilisateur ou d'un programme, selon le sujet) ne peut accéder qu'aux informations et ressources correspondant à ses besoins légitimes[40]. Ce principe s'applique également aux fonctionnaires de la CEE chargés d'élaborer et de faire fonctionner le système international eTIR : les autorisations et les accès ne leur sont accordés que de manière sélective pour leur permettre de faire leur travail et un système de contrôle passe régulièrement en revue la liste des autorisations et supprime ces dernières lorsqu'elles ne sont plus nécessaires. À cela s'ajoute le fait que toutes les personnes (fonctionnaires, consultants, stagiaires, etc.) cessant de travailler pour la CEE se voient retirer les accès dont elles disposaient. Enfin, des contrôles d'accès physiques et techniques sont également mis en place pour que seules les personnes autorisées aient accès aux informations et aux systèmes leur permettant de faire leur travail.

220. Le troisième principe est celui de la **défense en profondeur**, qui consiste à prévoir des contrôles de sécurité (défenses) à plusieurs niveaux du système informatique. L'idée est de maintenir un niveau de sécurité adéquat dans l'éventualité d'une défaillance d'un contrôle de sécurité ou de l'exploitation d'une vulnérabilité, en ce qui concerne par exemple la sécurité du personnel, des procédures et des aspects techniques ou la sécurité physique[41]. Il est fait

[39] Conformément au paragraphe 3 de l'article 12 de l'annexe 11 de la Convention TIR.

[40] Voir : en.wikipedia.org/wiki/Principle_of_least_privilege.

[41] Voir : en.wikipedia.org/wiki/Defense_in_depth_(computing).

usage de ce principe à plusieurs reprises. Ainsi, dans le système international eTIR il existe plusieurs niveaux de validation pour la saisie des données (reçues dans les messages eTIR), l'objectif étant de vérifier leur qualité et leur conformité aux spécifications eTIR.

221. Le quatrième principe est celui de la **partition des tâches**, en vertu duquel une tâche ne peut être effectuée par une seule personne. Pour les activités sensibles, la partition, qui consiste à confier l'exécution d'une même tâche à plus d'une personne, est une mesure de contrôle interne destinée à empêcher les fraudes et les erreurs[42]. Ce principe est utilisé par les développeurs du système international eTIR, par exemple lorsqu'un informaticien examine des lignes de code entrées et validées précédemment par un collègue. Il permet de repérer les omissions et les erreurs éventuelles, qui pourront être immédiatement corrigées par l'auteur du code.

B. Exigences relatives à la sécurité

1. Exigences techniques mentionnées précédemment

222. Comme expliqué au chapitre précédent, la sécurité informatique porte sur un large éventail d'exigences non fonctionnelles (techniques) applicables à un système informatique, car beaucoup jouent un rôle en ce qui concerne un ou plusieurs des trois objectifs principaux que sont l'intégrité, la disponibilité et la confidentialité. En particulier, il est à noter que les exigences suivantes, dont il a déjà été question ailleurs, jouent un rôle en dans la sécurité informatique du système eTIR :

- En ce qui concerne la **disponibilité**, qui est l'un des trois principaux objectifs en matière de sécurité et donc l'un des plus importants, les informaticiens doivent accorder une attention particulière aux exigences suivantes : AV.1, AV.2, AV.3 et AV.4 ;

- La **sauvegarde**, avec ses deux exigences (BK.1 et BK.2), est une composante de l'objectif de disponibilité, puisqu'il s'agit de rétablir l'accès des sujets autorisés aux informations en cas de perte de données ;

- La première exigence relative à la **capacité**, CP.1, contribue également à la réalisation de l'objectif de disponibilité, puisqu'elle consiste à faire en sorte que le système international eTIR puisse traiter à tout moment les messages envoyés par les différents acteurs. Il en va de même pour les autres exigences (CP.2, CP.3 et CP.4), quoique dans une moindre mesure ;

- Toutes les exigences relatives à la **gestion de la configuration** (CM.1, CM.2, CM.3, CM.4 et CM.5) ont une incidence sur les trois objectifs (disponibilité, intégrité et confidentialité) dans la mesure où elles ont trait à des aspects importants du développement et de la gestion du système international eTIR ;

- Les exigences relatives à la **conservation des données** (RE.1 et RE.2) ont un lien avec certains aspects précis de l'objectif de disponibilité puisqu'elles permettent de savoir combien de temps les données échangées dans le système eTIR doivent être conservées et comment y accéder ;

- Les exigences en matière de **reprise après sinistre** (DR.1 et DR.2) sont aussi manifestement liées à l'objectif de disponibilité. En effet, elles concernent la remise en marche du système international eTIR en cas de sinistre ;

- Les exigences en matière de **tolérance aux pannes** (FT.1, FT.2, FT.3 et FT.4) qui portent sur certains aspects techniques précis liés aux solutions de secours du système international eTIR, jouent également un rôle en ce qui concerne l'objectif de disponibilité ;

[42] Voir : en.wikipedia.org/wiki/Separation_of_duties.

- Les deux premières exigences relatives à la **maintenabilité**, qui concernent la dette technique (MT.1 et MT.2), font partie des mesures préventives mises en place pour éviter les problèmes de sécurité informatique dans le système international eTIR ;

- Comme pour la CP.1, les deux exigences relatives à la **performance** PE.2 et PE.3 relèvent aussi de l'objectif de disponibilité, puisqu'il s'agit de faire en sorte que l'échange de messages entre le système international eTIR et une autre partie prenante eTIR soit toujours effectué dans un délai raisonnable. Les deux dernières exigences relatives à la **performance** (PE.4 et PE.5) font également partie des mesures préventives visant à éviter un éventuel problème du système international eTIR susceptible de compromettre sa disponibilité ;

- La plupart des exigences relatives à la **fiabilité** (RL.1, RL.2, RL.3, RL.5 et RL.7) sont également des mécanismes mis en place pour éviter dans la mesure du possible que le système international eTIR connaisse des problèmes susceptibles de compromettre sa disponibilité.

223. Il est évident que la sécurité informatique est un sujet transversal et omniprésent qui ne peut être traités de manière fragmentaire et qu'il est nécessaire, si l'on veut que cette dimension soit prise en compte à toutes les étapes du cycle de développement des logiciels, d'adopter une démarche homogène. Les exigences non fonctionnelles (et pas nécessairement techniques) dont il est question ci-après sont propres à la sécurité informatique. Elles sont généralement applicables à tous les composants du système eTIR, à savoir le système international eTIR, les systèmes informatiques de toutes les autres Parties prenantes au système eTIR (y compris ceux mis à la disposition des titulaires pour soumettre des renseignements anticipés) et les connexions réseau entre tous ces systèmes. Il est toutefois important de noter que plusieurs de ces exigences peuvent ne s'appliquer qu'à un sous-ensemble desdites composantes.

224. Dans les sections suivantes, on entend par « compte utilisateur » un compte ouvrant à une personne ou à un système informatique l'accès à un système informatique donné (qui utilise et gère ces comptes).

2. Suivi

225. Le tableau ci-après porte sur les exigences liées à l'étape du suivi représentée dans la figure XXI. Bien que cette exigence s'applique principalement au système international eTIR, il est recommandé de l'appliquer également aux autres systèmes informatiques du système eTIR.

Tableau 20
Exigences relatives au suivi

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AU.1	Toutes les informations envoyées au et reçues par le système international eTIR sont liées à un compte utilisateur et peuvent être vérifiées.	La totalité des messages transmis vers ou reçus par le système eTIR sont entièrement enregistrés, y compris la signature numérique. Ces journaux, qui sont conservés et gérés en toute sécurité dans l'espace de stockage des journaux eTIR, peuvent ensuite être réclamés par les autorités douanières en cas de réclamation.

3. Authentification

226. Le tableau ci-après énumère les exigences liées à l'étape de l'authentification représentée dans la figure XXI. Seule la première (AE.1) s'applique à l'authentification des acteurs eTIR dans le système international eTIR. Les autres exigences s'appliquent aux autres systèmes informatiques en lien avec le système eTIR.

Tableau 21
Exigences relatives à l'authentification

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AE.1	Choisir pour le système international eTIR un mécanisme d'authentification rigoureux afin d'empêcher tout accès non autorisé.	Les acteurs du système eTIR qui souhaitent accéder aux services Web du système international eTIR doivent s'authentifier à l'aide d'un certificat numérique. La clé privée de ce certificat doit être stockée en toute sécurité par chaque acteur du système eTIR.
AE.2	Activer le verrouillage de la session après une période d'inactivité pour protéger l'accès aux comptes utilisateurs.	Pour les comptes utilisateurs attribués à des personnes uniquement : sur les interfaces mises à la disposition des utilisateurs pour accéder à un système informatique (que ce soit sur une page Web ou sur une application mobile), une période d'inactivité de quinze minutes doit entraîner l'interruption de la session.
AE.3	Gérer les mots de passe de manière sécurisée pour éviter tout accès non autorisé.	Les mots de passe doivent être stockés en toute sécurité dans des bases de données utilisant des fonctions de hachage cryptographiques modernes. Les mots de passe doivent être conformes aux meilleures pratiques en la matière, notamment en ce qui concerne leur longueur minimale et leur complexité.
AE.4	Recommander l'authentification multifactorielle pour l'accès au système afin de protéger les comptes utilisateurs.	S'il y a lieu, les comptes utilisateur attribués à des personnes doivent être dotés d'un système d'authentification multifactorielle, qui peut par exemple reposer sur les deux éléments suivants : « quelque chose que l'utilisateur connaît » (un mot de passe) et « quelque chose que l'utilisateur possède » (une carte de sécurité ou un téléphone mobile).

4. Autorisation

227. Le tableau suivant énumère les exigences liées à l'étape de l'autorisation représentée dans la figure XXI, pour les systèmes informatiques associés au système eTIR.

Tableau 22
Exigences relatives à l'autorisation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AO.1	N'accorde que l'accès ou les droits strictement nécessaires, de façon à empêcher tout accès non autorisé.	On n'attribuera à un compte utilisateur que l'accès ou les autorisations qui lui sont strictement nécessaires pour obtenir les informations qu'il est habilité à obtenir et pour effectuer les actions qu'il est habilité à accomplir.
AO.2	Utiliser le contrôle d'accès en fonction des rôles pour améliorer la gestion des comptes utilisateur.	S'il y a lieu, les comptes utilisateur doivent se voir accorder des accès et des autorisations en fonction des rôles ou des groupes. Il s'agit d'une façon pérenne de gérer les listes de contrôle d'accès. En effet, l'examen et la mise à jour de l'ensemble des accès et des autorisations est plus facile et présente moins de risques d'erreur lorsqu'ils portent sur tous les membres d'un groupe que sur chaque compte utilisateur.
AO.3	Retirer aux employés l'accès au système à la fin de leur contrat pour empêcher toute intervention non autorisée.	Lorsque le contrat d'un employé se termine, il convient de prévoir des procédures assurant la suppression de ses accès et autorisations à un compte utilisateur. Le compte utilisateur en question doit ensuite être désactivé.
AO.4	Passer en revue les comptes utilisateur au moins une fois par an afin d'éviter le cumul des autorisations d'accès.	Il convient de mettre en place une procédure prévoyant l'examen de tous les comptes utilisateur au moins une fois par an afin de vérifier et de valider que les accès et les autorisations attribués sont justifiés.

5. Sensibilisation et formation

228. Il a déjà été démontré à plusieurs reprises que l'homme est le maillon le plus faible de la chaîne de la sécurité informatique. Il est donc essentiel de sensibiliser et de former le personnel qui doit utiliser les systèmes informatiques en lien avec le système eTIR à la sécurité informatique et aux meilleures pratiques et menaces courantes en la matière. Les humains étant la cible d'attaques spécifiques comme le hameçonnage, le harponnage et le piratage psychologique, il est important d'insister sur ces aspects. Il est donc recommandé à toutes les Parties prenantes au système eTIR de mettre en place de telles mesures.

229. Le tableau suivant énumère les exigences liées aux processus mis en place pour sensibiliser et former l'ensemble du personnel concerné.

Tableau 23
Exigences en matière de sensibilisation et de formation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AW.1	Sensibiliser l'ensemble du personnel concerné en lui dispensant des formations sur les fondamentaux de la sécurité informatique.	Il convient de proposer au personnel utilisant les systèmes informatiques liés au système eTIR des formations sur les fondamentaux de la sécurité informatique (portant sur les meilleures pratiques et les menaces courantes). Des procédures doivent être mises en place pour faire en sorte que tout le personnel utilisant les systèmes informatiques liés au système eTIR ait suivi ces formations.
AW.2	Tenir des registres de participation aux formations obligatoires.	Ces registres doivent être tenus et gérés de telle façon qu'il soit possible de vérifier que la totalité du personnel utilisant les systèmes informatiques liés au système eTIR a bénéficié d'une formation sur les fondamentaux de la sécurité informatique. L'idéal serait que ces formations soient dispensées périodiquement (tous les trois ans, par exemple).

6. Confidentialité

230. Les informations échangées avec le système eTIR et stockées dans celui-ci sont confidentielles. Il convient par conséquent de mettre en place des mesures de contrôle pour faire en sorte que les données soient à l'abri de tout accès non autorisé lorsqu'elles sont échangées avec le système international eTIR (données échangées) et lorsqu'elles y sont stockées (données stockées). On trouvera dans le tableau ci-dessous la liste des exigences relatives à la confidentialité dans le système international eTIR.

Tableau 24
Exigences relatives à la confidentialité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
CO.1	Les informations transférées entre les systèmes informatiques du système eTIR restent confidentielles.	Tous les messages échangés entre les systèmes informatiques du système eTIR sont cryptés à l'aide de protocoles et de mécanismes de cryptage considérés comme sécurisés par la communauté des professionnels de la sécurité informatique[43]. Ces protocoles et mécanismes doivent être mentionnés dans les spécifications techniques eTIR et leur liste doit être régulièrement examinée pour que ceux qui ne sont plus considérés comme sûrs soient retirés et remplacés par des dispositifs plus sécurisés.
CO.2	L'accès aux informations stockées dans le système international eTIR est restreint.	L'accès aux informations enregistrées dans les trois espaces de stockage du système international eTIR (base de données eTIR, documents eTIR et journaux eTIR) est limité aux seuls comptes utilisateur autorisés. Ces espaces

[43] Cette « communauté » comprend les organismes nationaux spécialisées dans la sécurité informatique qui publient régulièrement sur le sujet, ainsi que les experts et les chercheurs en informatique spécialisés dans ce domaine.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
		de stockage sont situés dans un environnement sécurisé protégé par des contrôles de sécurité physiques et logiciels.

7. Identification

231. Le tableau qui suit énumère les exigences liées à l'étape de l'identification représentée dans la figure XXI, pour les systèmes informatiques associés au système eTIR.

Tableau 25
Exigence relative à l'identification

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
ID.1	L'identification d'une personne ou d'un système informatique bénéficiant d'un compte utilisateur est unique, ce qui permet de tenir le détenteur du compte responsable de ses actions.	Un compte utilisateur doit être attribué et lié à une seule personne et non à un groupe d'utilisateurs (s'il s'agit de personnes) ou à un système d'information unique (dans le cas des systèmes). Un même système informatique doit avoir une identité différente dans chaque environnement utilisé (développement, tests d'acceptation et production).

8. Intégrité

232. L'intégrité des informations échangées et stockées dans le système international eTIR doit être préservée. Il est donc nécessaire de mettre en place des contrôles pour empêcher toute modification des données, quelle que soit l'origine de cette modification (erreur lors du transfert des données, erreur humaine, mauvaise configuration ou cyberattaque). On trouvera dans le tableau ci-dessous la liste des exigences relatives à la confidentialité dans le système international eTIR.

Tableau 26
Exigences relatives à l'intégrité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
IN.1	L'intégrité des informations transférées entre les systèmes informatiques du système international eTIR est assurée.	Tous les messages envoyés vers ou reçus par le système international eTIR sont signés numériquement par l'expéditeur. Le destinataire valide la signature électronique du message à sa réception et la rejette si elle n'est pas valide.
IN.2	L'intégrité des informations stockées dans le système eTIR est assurée.	La totalité des messages envoyés vers ou reçus par le système eTIR est intégralement enregistrée, y compris la signature numérique. Ces journaux sont ensuite conservés et gérés en toute sécurité dans l'espace de stockage des journaux eTIR, dont l'accès est restreint.

9. Sécurité des nœuds

233. Le terme nœud désigne, selon la définition figurant dans la section consacrée à l'architecture, tout dispositif, physique ou virtuel, qui héberge les programmes ou les informations composant le système international eTIR ou interagit avec eux. Il peut s'agir de serveurs virtuels hébergeant les différents composants logiciels du système international eTIR ou de dispositifs faisant partie de l'infrastructure du réseau, comme les pare-feu, les routeurs, les proxies, les proxies inverses, ou de dispositifs affectés à la sécurité informatique tels que les systèmes de détection ou de prévention des intrusions. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la sécurité des nœuds dans le système international eTIR.

Tableau 27
Exigences relatives à la sécurité des nœuds

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NS.1	Configurer les serveurs virtuels, les conteneurs ou les pods de manière sécurisée pour empêcher tout accès non autorisé.	On s'assurera que toutes les recommandations relatives à la sécurité de l'information formulées par les fournisseurs du système d'exploitation sont appliquées. Les moyens d'identification électronique des comptes de service de ces serveurs sont conservés en toute sécurité dans un système de gestion des mots de passe et ne sont accessibles qu'au personnel autorisé. S'il y a lieu, on activera le pare-feu logiciel et on mettra en œuvre les principes du blocage par défaut et du moindre privilège.
NS.2	Configurer les périphériques de l'infrastructure réseau de manière sécurisée pour empêcher tout accès non autorisé.	Appliquer les principes du blocage par défaut et du moindre privilège sur les périphériques réseau tels que les pare-feu. S'assurer que toutes les recommandations des fournisseurs sont appliquées. Disposer d'une documentation fiable sur les interconnexions de réseaux et la configuration des dispositifs. Ces actions sont effectuées par l'entité hôte.
NS.3	Isoler les réseaux dignes de confiance contenant des données sensibles des réseaux non dignes de confiance pour empêcher tout accès non autorisé.	Appliquer les meilleures pratiques en matière de conception de l'infrastructure de réseau en répartissant les serveurs dans différentes zones de sécurité, en fonction de leur rôle et de la sensibilité des informations qui y sont stockées. Mettre en place une liste blanche d'adresses IP, de telle façon que l'accès au système international eTIR soit interdit par défaut, sauf aux serveurs externes figurant sur une liste précise (parties prenantes eTIR). Ces actions sont effectuées par l'entité hôte.
NS.4	Observer ce qui se passe sur les nœuds pour détecter d'éventuels problèmes de sécurité.	Activer la journalisation pour les nœuds qui la prennent en charge et diriger les données vers le système de surveillance. Restreindre l'accès aux journaux aux seuls employés autorisés. Protéger les données des journaux contre les modifications non autorisées et les problèmes de fonctionnement. Configurer des alertes automatiques fondées sur des règles, y compris pour les échecs de journalisation.

10. Non-répudiation

234. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la non-répudiation dans le système international eTIR.

Tableau 28
Exigences relatives à la non-répudiation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NR.1	Les Parties prenantes au système eTIR sont responsables des messages qu'elles envoient au système international eTIR.	Lorsqu'elles envoient des messages au système international eTIR, les Parties prenantes au système eTIR doivent les signer électroniquement de façon à être identifiées et authentifiées avec certitude. En outre, la condition AU.1 doit être remplie.
NR.2	L'intégrité du message envoyé par les parties prenantes eTIR au système international eTIR est assurée.	Il doit être satisfait aux exigences IN.1 et IN.2.
NR.3	Le système international eTIR peut continuer à valider les messages stockés dans les journaux	Les certificats numériques devant être renouvelés périodiquement, un système de gestion des clés doit être mis en place pour conserver les anciens certificats numériques de toutes les Parties prenantes au système

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
	eTIR jusqu'à la fin de la période de conservation des données.	eTIR, de façon à pouvoir continuer à authentifier et à vérifier l'intégrité des messages échangés dans le passé et conservés dans les journaux eTIR.

11. Sécurité physique

235. Cette section regroupe les principales exigences relatives à la sécurité physique des locaux, des bâtiments et des infrastructures de l'Organisation des Nations Unies (ONU) hébergeant le système international eTIR, et les mesures connexes mises en place. Le tableau ci-après énumère les exigences relatives à la sécurité physique des bâtiments et des infrastructures accueillant le système international eTIR.

Tableau 29
Exigences relatives à la sécurité physique

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
PS.1	Le centre informatique hébergeant le système international eTIR doit être à l'abri de toute perquisition, réquisition ou confiscation, le but étant de protéger les informations qui y sont stockées.	Le système international eTIR est hébergé dans un centre informatique situé dans les locaux de l'ONU et il n'est géré que par des employés de l'Organisation. Il est donc protégé par les dispositions de la Convention sur les privilèges et immunités des Nations Unies.
PS.2	Le centre informatique hébergeant le système international eTIR doit être suffisamment protégé contre les intrusions et les catastrophes.	Les locaux de l'ONU sont entièrement cernés par une clôture, gardés 24 heures sur 24 et 7 jours sur 7 par des agents de sécurité et protégés par un système de vidéosurveillance. Seules les personnes agréées porteuses d'un badge électronique y sont admises. Le centre informatique n'est accessible qu'aux membres d'une petite équipe d'informaticiens accrédités. Il est équipé de systèmes de détection et d'extinction des incendies performants.

12. Codage sécurisé et sécurité logicielle

236. Le codage sécurisé est l'art de développer des logiciels de façon à éviter qu'ils ne soient accidentellement porteurs de failles de sécurité. Les erreurs et les failles logiques sont à l'origine de la plupart des vulnérabilités logicielles couramment exploitées. On trouvera dans le tableau ci-dessous la liste des exigences relatives au codage sécurisé et à la sécurité des applications dans le système international eTIR.

Tableau 30
Exigences relatives au codage sécurisé et à la sécurité des applications

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
SC.1	Définir les exigences en matière de sécurité dès les premières étapes du cycle de développement des logiciels[44] afin de diminuer leur coût et le nombre de problèmes de sécurité.	Prendre en compte tous les aspects liés à la sécurité pour chaque fonctionnalité lors de sa conception et de son ajout à la liste des tâches à effectuer pour le développement du système eTIR. Valider systématiquement les données en entrée avant de les traiter. Concevoir et intégrer des tests de validation axés sur la sécurité (« scénarios criminels »). Effectuer un traitement correct des erreurs afin de toujours laisser le système dans un état stable. Veiller à ce que tous les problèmes de sécurité soient dûment consignés et se voient attribuer le degré de gravité adéquat. Examiner régulièrement le code source pour en éliminer les classes et fonctions inutiles et remanier certaines parties du code.

[44] Voir en.wikipedia.org/wiki/Systems_development_life_cycle.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
SC.2	Distinguer les différentes étapes du cycle de développement des logiciels pour éviter de mélanger différentes versions.	Utiliser différents environnements avec des contrôles et des procédures de sécurité appropriés pour les étapes « Développement », « Intégration et test des systèmes », « Tests d'acceptation » et « Production ».

13. Gestion de la vulnérabilité

237. La gestion de la vulnérabilité consiste à repérer, classer, hiérarchiser, corriger et atténuer les vulnérabilités des logiciels. La gestion de la vulnérabilité fait partie intégrante de la sécurité informatique et de la sécurité des réseaux. Elle comprend l'évaluation des vulnérabilités. On trouvera dans le tableau ci-après la liste des exigences relatives à la gestion de la vulnérabilité dans le système international eTIR.

Tableau 31
Exigences relatives à la gestion de la vulnérabilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
VU.1	Veiller à ce que les vulnérabilités connues soient corrigées afin d'empêcher d'éventuels problèmes de sécurité.	Mettre à jour et corriger les nœuds, y compris les systèmes d'exploitation et les logiciels médiateurs, de façon régulière. Faire des mises à jour régulières en installant les dernières versions stables des sections des logiciels dépendant de tierces parties. Migrer régulièrement vers les dernières versions des composants des systèmes externes (ITDB, système de courrier et système de non-répudiation).
VU.2	Effectuer des évaluations et des tests de vulnérabilité pour éviter les éventuels problèmes de sécurité.	Analyser régulièrement les nœuds, les systèmes et leurs composants pour y détecter des vulnérabilités connues. Effectuer des examens de sécurité du code (par exemple des tests d'intrusion) pour valider les nouvelles versions du système international eTIR.
VU.3	Veiller à ce que les incidents soient correctement gérés afin d'éviter les problèmes de sécurité éventuels.	Les alertes émises par le système de surveillance doivent être analysées en fonction de leur gravité et selon les procédures appropriées. La gestion de chaque incident est étudiée, ce qui permet d'apprendre, d'améliorer et d'effectuer des actions de suivi permettant d'éviter d'autres problèmes similaires.

C. Sécurité du système international eTIR

1. Introduction

238. Le présent chapitre vient compléter les parties précédentes des spécifications techniques. Il a pour objectif d'expliquer aux Parties contractantes à la Convention TIR et aux Parties prenantes au système eTIR divers aspects de la sécurité du système international eTIR. On y montre comment la CEE s'emploie à satisfaire à plusieurs des exigences relatives à la sécurité dont il a été question précédemment. Cette volonté de transparence présente également l'intérêt de permettre à toutes les Parties prenantes au système eTIR de faire des propositions d'amélioration, l'objectif étant de disposer à long terme d'un système eTIR plus sûr.

2. Sensibilisation à la sécurité informatique

239. Il est important de considérer la sécurité informatique comme une chaîne dont le niveau de solidité serait celui de son maillon le plus faible. Étant donné que des êtres humains font partie de cette chaîne, quel que soit le nombre de dispositifs de sécurité ou de barrières logicielles présentes, la sécurité de l'ensemble du système sera menacée si l'élément humain

ne dispose pas des connaissances et de l'expérience nécessaires pour comprendre les menaces courantes et savoir comment y faire face.

240. La sensibilisation à la sécurité informatique repose essentiellement sur la prise de conscience des risques que fait planer l'évolution rapide des méthodes de cyberattaque qui ciblent le comportement humain. À l'heure où la menace progresse et où la valeur des informations augmente, les cybercriminels étendent leurs capacités et leurs domaines d'action, développent de nouvelles méthodes et techniques d'attaque et agissent pour des motifs plus variés. Ils ciblent de plus en plus (et exploitent avec succès) le comportement humain individuel pour s'introduire dans les réseaux d'entreprise et les systèmes d'infrastructures critiques. Les personnes visées peuvent ne pas être conscientes de la sensibilité des informations et des menaces et faire l'économie des contrôles et processus de sécurité traditionnels, rendant ainsi leur organisation vulnérable.

241. Pour que les mesures prises dans ce domaine soient efficaces, il importe que tous les employés de la CEE soient sensibilisés à la sécurité informatique, et pas seulement les informaticiens du système international eTIR. En effet, à titre d'exemple, tout employé ouvrant un document infecté par un logiciel malveillant (qui serait par exemple joint à un courriel) est susceptible d'ouvrir une porte dérobée permettant à un cybercriminel de compromettre la sécurité informatique de son organisation. C'est pourquoi le Bureau de l'informatique et des communications a mis sur pied en 2015 un ensemble de trois formations de sensibilisation à la sécurité informatique (niveaux « élémentaire », « avancé » et « complémentaire »). La formation élémentaire est obligatoire pour tous les employés de l'ONU. Elle vise à les sensibiliser et à les familiariser aux mesures à prendre en cas de menace potentielle.

3. Les aspects juridiques

242. La Convention sur les privilèges et immunités des Nations Unies[45], adoptée par l'Assemblée générale des Nations Unies le 13 février 1946 à New York, comporte de nombreuses dispositions relatives au statut de l'Organisation, de ses biens et de ses fonctionnaires, en ce qui concerne les privilèges et immunités qui doivent leur être accordés par les États Membres. L'article 2 de cette convention dispose en particulier que les locaux de l'ONU sont inviolables : Ses biens et avoirs, où qu'ils se trouvent et quel que soit leur détenteur, sont exempts de perquisition, réquisition, confiscation, expropriation ou de toute autre forme de contrainte.

243. Cela signifie en pratique que seuls les agents de sécurité du Département de la sûreté et de la sécurité de l'ONU s'occupent de la sûreté et de la sécurité des biens et des avoirs situés dans les locaux de l'ONU. La police et les autres forces de sécurité du pays hôte ne peuvent pas entrer dans les locaux de l'ONU sans y avoir été autorisées par ces agents de sécurité. Par conséquent, tant que le système international eTIR est hébergé dans un centre informatique situé dans les locaux de l'ONU, il est protégé par les privilèges et immunités décrits ci-dessus.

4. La sécurité physique

244. On entend par mesures de sécurité physique les dispositions prises pour interdire tout accès non autorisé aux installations, aux équipements et aux ressources et pour protéger le personnel et les biens contre tous dommages ou préjudices (tels que les actes d'espionnage, le vol ou les attaques terroristes). La sécurité physique implique le recours à plusieurs strates de systèmes interdépendantes qui peuvent inclure la vidéosurveillance, les agents de sécurité, les barrières de protection, les serrures, le contrôle d'accès, la détection des intrusions dans le périmètre, les dispositifs de dissuasion, la protection contre l'incendie ou tout autre système conçu pour protéger les personnes et les biens. Dans les organismes du système des Nations Unies, cet aspect de la sécurité est assuré par le Département de la sûreté et de la sécurité, qui fournit des services professionnels permettant à l'ONU de mener à bien son action dans le monde entier. Pour des raisons évidentes de sécurité, il ne sera question, dans ce chapitre, que des aspects généraux de la sécurité physique.

[45] Voir treaties.un.org/doc/treaties/1946/12/19461214%2010-17%20pm/ch_iii_1p.pdf.

245. Les locaux de l'ONU sont entourés d'un périmètre de protection fermé (murs, clôtures, bornes de sécurité, etc.) qui empêche toute personne ou tout véhicule non autorisé d'y pénétrer. Les locaux sont surveillés par des agents de sécurité 24 heures sur 24, d'un bout à l'autre de l'année. Ils sont équipés d'un système de vidéosurveillance contrôlé en permanence par les agents de sécurité, dont les images sont enregistrées en prévision d'éventuelles enquêtes. Seules les personnes autorisées porteuses d'un badge électronique délivré par le Département de la sûreté et de la sécurité y sont admises. Le centre informatique n'est accessible qu'aux membres d'une petite équipe d'informaticiens accrédités et l'emplacement du centre informatique dans les locaux n'est pas connu du public.

246. En outre, des systèmes de détection et d'extinction des incendies équipent l'ensemble des locaux, et en particulier le centre informatique, et des exercices de sécurité sont effectués plusieurs fois par an.

5. L'entité hôte

247. En ce qui concerne l'entité hôte, c'est à dire l'ONU, plusieurs aspects liés à la sécurité ont déjà été décrits dans les parties précédentes des spécifications techniques eTIR :

- La présentation détaillée de l'architecture du système international eTIR montre comment le recours à une infrastructure fondée sur une batterie de serveurs virtuels et à un équilibreur de charge peut jouer un rôle dans la conception d'un système exempt de tout point de défaillance isolé ;

- Dans les prescriptions techniques, le rôle important de l'entité hôte est décrit de façon détaillée au chapitre des exigences relatives à la disponibilité, à la sauvegarde et, surtout, à la tolérance aux pannes, où sont présentées plusieurs caractéristiques du centre informatique ;

- En ce qui concerne la maintenance, l'entité hôte joue également un rôle important dans des domaines tels que la gestion des incidents, la sauvegarde et la restauration, la surveillance et la gestion des correctifs et des mises à niveau.

248. L'entité hôte est également responsable de la sécurité générale de son centre informatique, de ses réseaux et de son infrastructure (ainsi qu'il est mentionné plus haut au chapitre des exigences relatives à la sécurité des nœuds). L'idéal serait en outre que l'entité d'hôte, pour démontrer sa maturité et son implication en matière de sécurité informatique, soit détentrice d'un certification reconnue, par exemple selon la norme ISO/IEC 27001:2013.

249. Enfin, étant donné que l'entité hôte est obligée de procéder régulièrement à des modifications sur ses réseaux, son infrastructure et ses nœuds (matériel des réseaux, du système de sécurité ou des serveurs), un processus de gestion des modifications bien défini doit être mis en place pour tester, hiérarchiser, autoriser et mettre en œuvre ces modifications de façon contrôlée et efficace. L'entité hôte doit communiquer avec ses clients de façon appropriée et opportune à propos de ces modifications, et lorsqu'une période d'indisponibilité paraît inévitable il doit en être question à l'avance pour que la recherche de solutions de substitution soit possible ou pour que les parties prenantes eTIR concernées en soient au moins informées. L'idéal serait que la CEE puisse exprimer son point de vue lors de l'autorisation et de la planification des modifications ayant une incidence sur le système international eTIR ou sur l'ITDB, éventuellement en siégeant au Conseil consultatif sur le changement de l'entité hôte.

6. La sécurité logicielle

250. L'un des objectifs de l'approche DevOps (ou DevSecOps) est de penser à la sécurité informatique dès les premières étapes du processus de développement, au lieu de n'en tenir compte qu'à la fin, c'est à dire lorsque il est plus coûteux d'apporter des modifications aux logiciels. Pour atteindre cet objectif, la CEE a adopté les règles suivantes :

- **Prise en compte des exigences relatives à la sécurité en tant que fonctions** : la sécurité et le respect des obligations en la matière ne sont pas des aspects distincts traités à la fin du développement du logiciel ; ils sont au contraire pris en compte

pendant le développement et intégrés à la liste des tâches au même titre que les autres fonctions ;

- **Système de validation** : toutes les données en entrée contenues dans les messages eTIR sont validées à plusieurs niveaux, l'objectif étant de vérifier leur exactitude, leur conformité aux spécifications et leur pertinence. Ce système prévoit entre autres une couche de validation pour chaque message de demande, une couche de validation utilisant le fichier XSD correspondant et des contraintes d'intégrité dans la base de données eTIR. En outre, on effectue des tests de validation automatisés avec des données en entrée non conformes, des valeurs nulles ou vides, des valeurs trop longues et certains scénarios criminels[46] ;

- **Traitement des erreurs** : les erreurs survenant pendant le fonctionnement du système international eTIR doivent être traitées comme il se doit pour que le système soit toujours en bon état de fonctionnement. Toutes les erreurs doivent être enregistrées en vue d'une étude plus approfondie. Elles doivent faire l'objet de tests, si possible automatisés, dont le but sera de vérifier que le mécanisme de traitement des erreurs se comporte comme prévu ;

- **Analyse de la vulnérabilité** : on utilise un outil d'analyse statique de code pour vérifier régulièrement le code source afin de détecter les mauvaises pratiques susceptibles de créer des failles de sécurité. En outre, comme de nombreuses bibliothèques sont utilisées de nos jours dans les logiciels, on utilise un outil de vérification pour vérifier la vulnérabilité des versions desdites bibliothèques en consultant une base de données des vulnérabilités connues, afin de repérer les mises à niveau importantes à effectuer pour corriger ces problèmes ;

- **Protéger les outils de développement** : il est important d'assurer la sécurité des outils et des connaissances internes qu'utilisent ou produisent les informaticiens. Tout d'abord, le système de contrôle de version, qui conserve le code source du système international eTIR et de tous les utilitaires connexes. Ensuite, la documentation interne conservée dans le système de gestion des connaissances et dans le système de suivi des problèmes. Enfin, le pipeline d'intégration continue et tous les outils connexes nécessaires aux différents processus de développement, y compris la documentation destinée aux Parties prenantes au système eTIR (comme les guides techniques) ;

- **Télémétrie** : enregistrement du comportement du système international eTIR. Les informaticiens doivent concevoir et mettre en oeuvre ce système de telle façon qu'il génère et enregistre des données qui pourront ensuite être analysées dans l'optique, entre autres, d'éviter les incidents (de sécurité). Ces données doivent fournir des informations sur les éléments suivants : succès ou échec de la validation des messages eTIR, utilisation de signatures numériques non valides, erreurs détectées par le système, efficacité du traitement des messages, etc. Toutes les données générées et enregistrées dans les journaux eTIR sont ensuite exploitées et peuvent être visualisées sous forme de graphiques, pour étudier les variations et, si besoin est, déclencher des alertes, sur la base de modèles spécifiques pouvant signaler une cyberattaque éventuelle ;

- **Veille technologique permanente** : les informaticiens doivent suivre régulièrement des formations pour se tenir au courant de l'évolution des technologies et des techniques de sécurisation des logiciels, notamment en étudiant les derniers produits d'entités telles que l'OWASP[47].

[46] On entend par « scénario criminel » une stratégie qui pourrait être utilisée par des cybercriminels pour violer la sécurité du système international eTIR.

[47] L'Open Web Application Security Project® (OWASP) est une fondation à but non lucratif qui s'efforce d'améliorer la sécurité des logiciels. Voir owasp.org.

7. Évaluations de la sécurité

251. Une évaluation de la sécurité informatique est une étude visant à localiser les vulnérabilités et les risques en matière de sécurité informatique. Elle peut être réalisée en interne par la CEE, par des experts en sécurité informatique de l'ONU, ou encore par des sociétés spécialisées externes mandatées par la CEE. L'objectif d'une évaluation de la sécurité est de faire en sorte que les contrôles de sécurité nécessaires soient intégrés à la conception et à la mise en œuvre du système international eTIR. Une évaluation de la sécurité correctement réalisée doit déboucher sur le signalement des éventuelles failles en matière de sécurité et sur des propositions relatives à la manière d'y remédier. Les résultats des évaluations de la sécurité sont confidentiels.

252. Les informaticiens doivent s'efforcer d'évaluer régulièrement la sécurité, et dans l'idéal d'automatiser certaines de ces évaluations pour qu'elles aient lieu fréquemment. Par exemple, le type d'évaluation de la sécurité baptisé « évaluation de la vulnérabilité », dont le but est d'analyser le code source et les composants logiciels utilisés pour élaborer et faire fonctionner le système international eTIR, doit être automatisé à l'aide d'outils spécifiques et exécuté régulièrement. Les vulnérabilités potentielles pourront ainsi être immédiatement détectées, et corrigées par l'application de correctifs et la mise à niveau des composants logiciels.

253. Chaque fois qu'une nouvelle version majeure du système international eTIR est développée, une évaluation plus approfondie de la sécurité doit être menée à bien, soit par des experts en sécurité informatique de l'ONU, soit par une société spécialisée externe mandatée par la CEE. Cette évaluation de la sécurité s'effectue le plus souvent sous la forme de « tests d'intrusion » dans lesquels les personnes chargées des essais jouent le rôle d'agresseurs et tentent de trouver et d'exploiter les failles de sécurité du système international eTIR. En fonction de différents facteurs, on déterminera si ce test essai doit être du type « boîte noire » (Black Box), « boîte grise » (Grey Box), ou « boîte blanche » (White Box). Ces types de test se distinguent par la quantité d'informations dont disposent les personnes chargées des essais. Dans la méthode « boîte noire », elles n'ont aucune connaissance préalable du système qui sera ciblé. Dans le cas d'une évaluation de type « boîte grise », le niveau d'accès au système et sa connaissance ne sont que partiels. Enfin, on parle d'évaluation de type « boîte blanche » lorsque les personnes chargées des essais ont un accès complet au code source, aux diagrammes de réseau et à d'autres informations pertinentes.

D. Security of exchanges with the eTIR international system[48]

1. Introduction

254. This section describes the security model and controls that should be followed by the different eTIR stakeholders while exchanging messages with the eTIR international system. The security model is designed to meet the requirements in terms of confidentiality, integrity and non-repudiation listed above. The technical details and versions of the algorithms and protocols mentioned should be regularly reviewed by TIB to ensure that the objectives and exigencies, in terms of security, are continuously covered.

2. Confidentiality

255. As the eTIR messages are exchanged between the eTIR stakeholders over the internet, these exchanges need to be encrypted to prevent any third party from being able to read the messages exchanged and, thus, get access to this confidential information. The HyperText Transfer Protocol Secure (HTTPS), used to access the eTIR international system endpoints, is an extension of the HyperText Transfer Protocol (HTTP) where communication is encrypted using Transport Layer Security (TLS), a cryptographic protocol designed to provide communications security over public networks like the internet. The bidirectional encryption of the exchanges using HTTPS/TLS between a client and server protects against

[48] Cette section et la suivante sont en Anglais afin de compléter la partie sur la Sécurité. Ces sections seront traduites dans le document informel 12.

eavesdropping and tampering of the communication. The version of TLS to be used should be either version 1.2 or 1.3[49].

256. As the encryption of the exchanges between the eTIR stakeholders uses the HTTPS/TLS protocols to ensure the confidentiality of the communication, there is no need to either set up Virtual Private Networks (VPN) or to perform a double encryption at the eTIR messages level using the techniques available using SOAP.

3. Integrity and non-repudiation

257. Messages exchanged with the eTIR international system must be authenticated and their integrity must be ensured to achieve non-repudiation. This is accomplished using the concept of electronic signatures. Definitions of electronic signatures vary depending on the applicable jurisdiction and a common denominator is therefore set in the context of the eTIR specifications. This common denominator states that electronic signatures should achieve the following requirements:

- The signatory can be uniquely identified and linked to the electronic signature;
- The signatory must have sole control of the private key that was used to create the electronic signature;
- The electronic signature must be capable of identifying if its accompanying data has been tampered with after the message was signed.

258. From a technical point of view, this is achieved using a digital certificate (also known as public key certificate) following the X.509 standard[50], version 3. Each eTIR stakeholder wishing to interconnect his or her information systems with the eTIR international system should be issued a X.509 certificate from a trusted Certificate Authority (CA)[51]. The X.509 certificate, which uniquely identifies the eTIR stakeholder is used to sign the eTIR messages. This way of implementing electronic signature not only ensures the identity of the sender but also guarantees that the message content has not been tampered during the transmission, thus ensuring integrity.

259. In order for the X.509 certificates to ensure a high level of security, they should be created using the following parameters:

- The validity period should be, maximally, one year;
- The public key algorithm should be RSA with a key length of 4096 bits;
- The signature algorithm should be one of the following: SHA-256 with RSA, SHA-384 with RSA or SHA-512 with RSA (recommended).
- The “Country (C)”, “State Name (ST)” and “Locality Name (L)” parameters should reflect where the eTIR stakeholder is located. Only the “State Name (ST)” parameter is optional;
- The “Email (E)” parameter should provide the email address of the IT service desk of the eTIR stakeholder;
- The “Common Name (CN)” and the “Organization Name (O)” parameters should hold the same value which is the full name of the eTIR stakeholder as an entity/organization.

260. As the X.509 certificates have a limited validity period, they will be regularly replaced with new ones and the exchange of new certificates should be properly planned between ECE and the other eTIR stakeholders to prevent any interruption of service. Also, since data exchanged and stored with the eTIR international system should be kept for ten years[52], ECE will keep all previous X.509 certificates of the eTIR stakeholders in a secure location to be

[49] Versions 1.0 and 1.1 of the TLS have been deprecated in 2020 as they are no longer considered as secure.

[50] See itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

[51] Also known as Trusted Third Parties.

[52] As per Article 12 of Annex 11 of the TIR Convention.

able to verify the electronic signature of old eTIR messages, in case ECE is requested by the competent authorities of contracting parties to provide all data related to a TIR transport.

4. Whitelisting

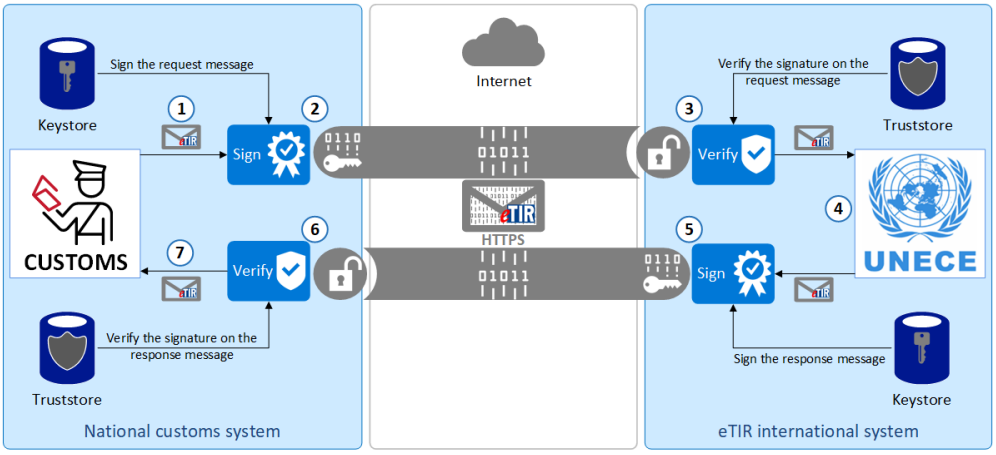
261. As the eTIR stakeholders who wish to communicate with the eTIR international system need to complete an interconnection project, ECE keeps an accurate and up-to-date list of these companies/entities/organizations. This approach allows to put an extremely effective security measure in place: whitelisting. The eTIR international system is configured not to be accessible by anyone from the internet, except by a restricted list of IP addresses which correspond to the main servers of the eTIR stakeholders which have completed their interconnection projects. This approach drastically reduces the potentiality of cyberattacks to the eTIR international system, including "denial of service" and trying to "spoof"[53] an eTIR stakeholder.

262. During the course of the interconnection project, ECE requests the IP addresses of the servers of the eTIR stakeholder which will connect with the eTIR international system, both on the UAT and PRD environments, and liaises with the United Nations hosting entity to configure the network appliances accordingly.

5. eTIR security model

263. The eTIR security model combines all security aspects mentioned above to provide a highly secured approach. The following figure illustrates how this security model works with an eTIR message being sent from a national customs systems to the eTIR international system using web services. The same approach applies when communicating in the same way with guarantee chains and holders.

Figure XXII
eTIR security model



264. In the example above, as a preliminary step, the X.509 certificate of the national customs system is installed in the eTIR international system truststore and the eTIR international system X.509 certificate is installed in the national customs system truststore. This mandatory initial step allows the validation of the digital signatures that are transferred as security tokens in all eTIR messages exchanged in the context of the eTIR procedure. The procedure below describes the steps numbered in the figure above and explains how a request message is sent by the national customs system to the eTIR international system, and how the related response is sent back:

(1) The national customs system generates a request message to be sent to the eTIR international system web service;

(2) The request message is signed with the private key of the national customs system X.509 certificate. It is then encrypted using HTTPS/TLS and sent over the internet.

[53] A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

The connection can be successfully established, as the national customs system is whitelisted by the network appliances of the eTIR international system;

(3) The eTIR international system receives the request message, decrypts it, verifies the signature of the message using the public key of the national customs system X.509 certificate to authenticate it and to confirm its integrity. The full message including its digital signature is then securely stored in the eTIR logs;

(4) The eTIR international system processes the request message and generates a response message in return;

(5) The response message is signed with the private key of the eTIR international system X.509 certificate and securely stored in the eTIR logs. It is then encrypted using HTTPS/TLS and sent over the internet;

(6) The national customs system receives the response message, decrypts it, and verifies the signature of the message using the public key of the eTIR international system X.509 certificate to authenticate it and to confirm its integrity;

(7) The national customs system finally processes the response message.

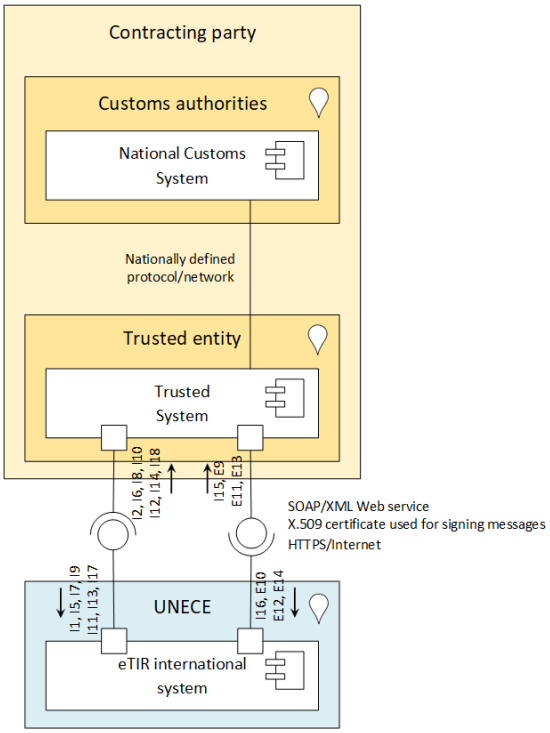
265. The completion of this whole process illustrates the implementation of the various security measures described in the sections above to achieve the requirements of confidentiality, integrity and non-repudiation.

6. Alternative security models

266. National legislations and regulations in contracting parties may prevent their customs authorities from interconnecting their national customs systems to the eTIR international system by following the specifications described above. In that case, an alternative security model should be designed and agreed between the IT experts of ECE and of the customs authorities. It should also be reviewed and approved by TIB. This alternative security model should meet the same security requirements in terms of confidentiality, integrity and non-repudiation, to be accepted.

267. A possible alternative security model is described below in case the customs authorities of a contracting party are required to use specific encryption algorithms or other technical aspects that would prevent them to initiate a direct connection with the eTIR international system. This security model is similar to the one described above, except that another entity under the contracting party government jurisdiction would play the role of a proxy between the eTIR international system and the national customs system. This entity should be trusted by the customs authorities and the technical details of the connection between this entity and the national customs system would be the sole decision of the contracting party and should be described in the eTIR technical specifications. The following figure shows the architecture of this alternative security model.

Figure XXIII
An alternative security model



268. This alternative security model still requires that the communication between the eTIR international system and the trusted system be done using HTTPS/TLS and signing the eTIR messages using X.509 certificates that would comply with the technical specifications described above. On the contracting party's end, the X.509 certificate signing messages sent by the customs authorities could belong to the customs authorities or to the trusted entity, at the decision of the customs authorities.

7. Common threats and mitigation measures

269. A table is provided in annex VI.D of the present document to summarize all security measures and controls that should be put in place for the eTIR international system, and to give an overview for the contracting parties to the TIR Convention on how these measures will mitigate the risks posed by common security threats.

E. Security of exchanges between other eTIR stakeholders

1. Introduction

270. The previous section describes the technical specifications of the exchanges between any eTIR stakeholders and the eTIR international system using web services. These eTIR stakeholders include customs authorities, guarantee chains and holders and all of them should have undergone an interconnection project. In addition to these types of exchanges, holders can also exchange information (advance TIR data and advance amendment data) directly with the customs authorities[54]. This section describes the technical specifications of this latter type of communication only.

2. Authentication of the holder

271. Each contracting party shall publish a list of all electronic means by which advance TIR data and advance amendment data can be submitted by the holder to the customs authorities[55]. The authentication mechanisms used by these electronic means should uniquely

[54] As per paragraph 2 of Article 6 of Annex 11 of the TIR Convention.
[55] As per paragraph 4 of Article 6 of Annex 11 of the TIR Convention.

identify the holder and should feature security measures and controls which provide sufficient assurance that the authentication mechanism is secure, in accordance with national laws[56]. In order to be specific and transparent about this important point, each contracting party shall publish the list of authentication mechanisms used by these electronic means[57]. Finally, it is also important to mention that the authentication of the holder performed in this context shall be recognized by the other contracting parties along the itinerary of the TIR transport following the eTIR procedure[58].

272. The authentication of the holder exchanging data directly with the customs authorities is, therefore, a matter of national concern and is not governed by the eTIR specifications. In order to assist and facilitate the decision of contracting parties about this important topic, the next sections provide guidelines and best practices of authentication mechanisms that do not rely on electronic signatures.

3. Multi-Factor Authentication (MFA)

273. MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two (or more) pieces of evidence (or factors) to an authentication mechanism. These two (or more) pieces should belong to at least two different classes among the three that exist:

- **Knowledge**: something only the user knows, like a password or a personal identification number (PIN) code;
- **Possession**: something only the user has, like a smartphone with a configured software-based authenticator, a smartcard or a security card (as used in ITDB);
- **Inherence**: something only the user is, like fingerprints, voice prints, retina patterns, iris patterns or face shapes.

274. It is recommended to use MFA in the authentication mechanism as it provides a high level of assurance that the user is indeed who he or she claims to be.

4. Password strength

275. Most of the web sites and web applications rely on passwords (either solely or as part of an MFA) to authenticate their users. It is important to understand and comply with the minimum requirements in terms of password length and complexity as effective attacks can crack passwords that would not be compliant in seconds. All passwords should conform to the following specifications:

- At least 12 characters long; more than 14 characters is better;
- Different from the default (initial) password;
- Not be the same as the username;
- Composed of, at least, three of the following character classes:
    - upper case letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - lower case letters: abcdefghijklmnopqrstuvwxyz
    - numbers: 0123456789
    - punctuation marks: !@#$%^&*()+=\`{}[]:";'< >?,./)
- Not be based on words found in dictionaries of any language or based on simple patterns such as “aaabbb”, “qwerty”, “zyxwvuts”, “123321”, etc.

276. In addition, users should be encouraged not to base their password on any personal information that is easily available to potential adversaries, such as names of family

[56] As per paragraph 1 of Article 7 of Annex 11 of the TIR Convention.
[57] As per paragraph 3 of Article 7 of Annex 11 of the TIR Convention.
[58] As per Article 8 of Annex 11 of the TIR Convention.

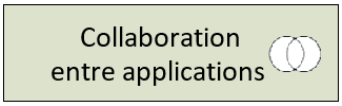
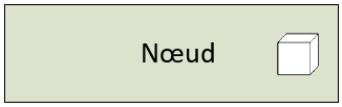
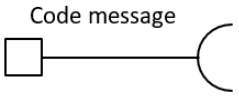
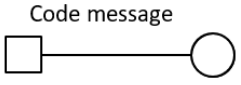
members, pets, friends, co-workers, birthdays, addresses, phone numbers, etc. And, finally, passwords should be regularly changed, at least once per year.

V. Annexes

A. Conventions de notation des diagrammes

277. La notation ArchiMate (Spécifications ArchiMate®, version 3.0.1 ; voir : pubs.opengroup.org/architecture/archimate3-doc/) est utilisée pour représenter les différents points de l'architecture du système dans les diagrammes du présent document. Seuls sont décrits dans le tableau ci-dessous les concepts ArchiMate qui sont utilisés dans ces diagrammes. On notera que les couleurs utilisées pour le fond des différents encadrés correspondent à différents acteurs ou systèmes, et non à des concepts ArchiMate particuliers.

Tableau 32
Conventions de notation ArchiMate des diagrammes

Concept	*Description*	*Symbole*
Lieu	Lieu où d'autres concepts sont situés.	
Composant d'application	Élément modulaire, déployable et remplaçable d'un système logiciel, qui est représentatif du comportement et des données dudit système et expose ces derniers à une série d'interfaces.	
Collaboration entre applications	Groupement de deux composants d'application ou plus, qui travaillent ensemble pour adopter un comportement logiciel collectif.	
Nœud	Ressource informatique ou physique qui héberge ou manipule d'autres ressources informatiques ou physiques, ou interagit avec elles.	
Réseau de communication	Ensemble de structures qui relie des systèmes informatiques ou d'autres dispositifs électroniques pour la transmission, le routage et la réception de données.	
Interface disponible	Point d'accès où les services d'application sont mis à la disposition d'un autre composant d'application. Les codes correspondant aux messages émis par cette interface peuvent être indiqués au-dessus du symbole.	
Interface requise	Obligation de réaliser la connexion avec les services d'application qui sont mis à la disposition d'un autre composant d'application. Les codes des messages renvoyés par l'intermédiaire de cette interface peuvent être indiqués au-dessus du symbole.	

B. Glossaire technique

278. On trouvera dans la présente annexe, sous forme de tableau, la définition de tous les termes techniques qui sont utilisés dans les spécifications techniques eTIR.

Tableau 33
Glossaire technique

Terme	*Définition*
Authentification	Processus consistant à vérifier ou à tester la validité d'une identité déclarée. Les sujets doivent fournir des informations supplémentaires qui correspondent à l'identité qu'ils revendiquent. Le système d'authentification le plus courant est l'utilisation d'un mot de passe (qui peut prendre des formes variables, comme le code secret (PIN) ou la phrase secrète). L'authentification consiste à vérifier l'identité du sujet en comparant un ou plusieurs éléments à ceux enregistrés dans la base de données des identités valides (c'est-à-dire les comptes utilisateurs).
Autorité de certification (AC)	Entité reconnue qui occupe une position de confiance : le certificat qu'elle émet lie l'identité d'une personne ou d'une entreprise à la paire de clefs publique et privée (cryptographie asymétrique) qui est utilisée pour sécuriser la plupart des transactions sur Internet. Par exemple, lorsqu'une entreprise ou une personne souhaite utiliser ces technologies, elle demande à une AC de lui délivrer un certificat. L'AC recueille des informations concernant la personne ou l'entreprise, qu'elle va vérifier avant de délivrer le certificat.
Batterie de serveurs virtuels	Environnement réseau qui utilise plusieurs serveurs d'applications et d'infrastructure fonctionnant sur deux serveurs physiques ou plus à l'aide d'un logiciel de virtualisation de serveurs. Cette architecture présente plusieurs avantages, notamment la consolidation et la redondance des serveurs ainsi que le basculement entre serveurs, et permet d'assurer une haute disponibilité et une utilisation optimisée des ressources.
Certificat numérique	En cryptographie, un certificat numérique (également appelé « certificat » dans le présent document) est un document électronique utilisé pour prouver la propriété d'une clef publique. Le certificat comprend des informations sur la clef et sur l'identité de son propriétaire (appelé « sujet ») ainsi que la signature numérique de l'entité qui a vérifié le contenu du certificat (appelée « autorité de certification »). Si la signature est valide et que le logiciel qui examine le certificat fait confiance à l'autorité qui l'a émis, il peut utiliser cette clef pour communiquer en toute sécurité avec le sujet du certificat.
Certificat X.509	Format courant pour les certificats numériques, largement utilisé sur Internet avec le protocole TLS. Un certificat X.509 spécifie un lien entre une clef publique et un ensemble d'attributs comprenant (au moins) les éléments suivants : nom du sujet, nom de l'autorité de certification, numéro de série et intervalle de validité. Il est défini dans le document RFC (Request for Comments) 5280[59].
Confidentialité	Principe appliqué en recourant à des mesures destinées à protéger le caractère secret des données, des objets ou des ressources. La protection de la confidentialité a pour but d'empêcher ou de réduire au minimum l'accès non autorisé aux données. Elle repose sur des mesures de sécurité qui visent à garantir que personne d'autre que le destinataire d'un message ne le reçoive ou ne puisse le lire. Il s'agit de donner aux utilisateurs autorisés un moyen d'accéder à des ressources et d'interagir avec elles, tout en empêchant activement les utilisateurs non autorisés de le faire.
Coût total de possession	Montant total que le propriétaire d'un système d'information a dû dépenser pendant le cycle de vie de ce dernier. Tous les coûts (directs et indirects) sont pris en compte.
Cryptographie asymétrique	Système cryptographique reposant sur l'utilisation de deux clefs : une clef publique, connue de tout le monde, et une clef privée (ou clef secrète), que seul le propriétaire de la paire de clefs connaît. À titre d'exemple, lorsqu'Alice veut envoyer un message sécurisé à Bob, elle utilise la clef publique de celui-ci pour chiffrer le message. Bob utilise ensuite sa clef privée pour le déchiffrer. L'algorithme RSA est un exemple d'algorithme de cryptographie asymétrique.
Défaut	La littérature informatique fait généralement une distinction entre les termes « bogue » et « défaut ». En effet, un « bogue » est le résultat d'une erreur de code et un « défaut » est une déviation par rapport aux exigences. Dans le présent document, seul le terme « défaut » est utilisé, et il recouvre les deux significations.
Définition du schéma XML (XSD)	Recommandation du W3C qui décrit la manière dont les éléments d'un document XML sont structurés et formatés.
Émetteur	Dans le présent document, système d'information de la partie prenante du système eTIR qui génère et envoie un message à une autre partie prenante.
Entropie logicielle	Selon la deuxième loi de la thermodynamique, le degré de désordre d'un système fermé ne peut pas diminuer, il ne peut que rester constant ou augmenter. Ce degré de désordre est mesuré par l'entropie. Certaines études montrent qu'il est possible que cette loi s'applique également aux systèmes logiciels : lorsqu'un système est modifié, son degré de désordre, ou entropie, tend à augmenter. C'est ce qu'on

[59] Voir tools.ietf.org/html/rfc5280.

Terme	*Définition*
	appelle l'entropie logicielle. La réécriture du code peut permettre de réduire progressivement l'entropie logicielle.
Environnements	Au cours de son cycle de vie, un logiciel est développé et maintenu dans plusieurs environnements qui ont des finalités différentes. Certains sont utilisés pour le développement, d'autres pour les tests et le dernier, l'environnement d'exploitation, est celui dans lequel le logiciel fonctionne une fois lancé et mis à la disposition des utilisateurs finals.
Équilibreur de charge	Composant logiciel qui répartit un ensemble de tâches sur un ensemble de ressources (nœuds de serveur), dans le but d'améliorer l'efficacité globale de leur traitement.
Erreur	Grave défaut de validation qui entraîne le rejet du message.
Git	Système de contrôle de version permettant de suivre les modifications de n'importe quel ensemble de fichiers, généralement utilisé pour coordonner le travail des programmeurs qui élaborent en collaboration le code source pendant le développement de logiciels. Il vise à optimiser les performances, protéger l'intégrité des données et prendre en charge des flux de travail distribués et non linéaires.
Infrastructure à clefs publiques (ICP)	Ensemble de rôles, de politiques, de matériel, de logiciels et de procédures nécessaires à la création, à la gestion, à la distribution, à l'utilisation, au stockage et à la révocation de certificats numériques et à la gestion de la cryptographie asymétrique.
Intégrité	Principe consistant à protéger la fiabilité et l'exactitude des données. La protection de l'intégrité empêche les altérations non autorisées des données. Il garantit que les données restent correctes, non modifiées et préservées. Convenablement assurée, la protection de l'intégrité permet d'apporter des modifications autorisées tout en protégeant les données des activités intentionnellement malveillantes (telles que les attaques de virus et les intrusions) ainsi que des erreurs commises par les utilisateurs autorisés (telles que les erreurs et les omissions).
Interface de programmation d'applications (API)	Interface logicielle utilisée pour accéder à une application ou à un service à partir d'un programme.
Java	Langage de programmation orienté objet, basé sur des classes, conçu pour avoir le moins de dépendances d'implémentation possible. Il s'agit d'un langage de programmation polyvalent destiné à permettre aux développeurs d'applications d'écrire leurs programmes une fois et de les faire tourner n'importe où, ce qui signifie que le code Java compilé peut être exécuté sur toutes les plateformes prenant en charge Java sans qu'il soit nécessaire de le recompiler.
Jeton	Parfois appelé jeton de sécurité. Objet contrôlant l'accès à un bien numérique. Traditionnellement, ce terme désigne un dispositif matériel d'authentification, c'est-à- dire un petit appareil utilisé pour générer un mot de passe à usage unique, que le propriétaire saisit dans un écran de connexion en plus d'un identifiant et d'un code secret. Dans le contexte des services Web, au vu du besoin croissant de dispositifs et de processus multiples d'authentification sur des réseaux ouverts, l'acception du terme « jeton » a été élargie pour englober également les dispositifs logiciels. Un jeton peut être un certificat X.509 qui associe par exemple une identité à une clef publique.
Jeton X.509	Représente la signature numérique générée à l'aide du certificat X.509 de l'expéditeur, qui sera utilisée pour authentifier l'entité qui envoie le message. Il fait donc partie du message, et se trouve dans l'en-tête de l'enveloppe SOAP.
Keystore	Base de données qui sert à stocker les certificats des systèmes d'information du propriétaire du keystore et qui peut inclure les certificats des parties de confiance (truststore), en vue de leur utilisation par un programme. Grâce à son fichier keystore, une entité peut s'authentifier auprès d'autres parties et authentifier d'autres parties.
Langage de description de services Web (WSDL)	Langage de description d'interface basé sur XML, utilisé pour décrire la fonctionnalité offerte par un service Web.
Non-répudiation	Principe qui garantit que le sujet d'une activité ou la personne qui a causé un événement ne peut pas nier que l'événement s'est produit. En vertu de ce principe, un sujet ne peut pas prétendre qu'il n'a pas envoyé un message, accompli une action ou été la cause d'un événement. Il est rendu possible par l'identification, l'authentification, l'autorisation, l'obligation de rendre compte et l'audit. La non-répudiation peut être appliquée à l'aide de certificats numériques, d'identifiants de session, de relevés des transactions et de nombreux autres dispositifs de contrôle des transactions et des accès.
OASIS	Organization for the Advancement of Structured Information Standards. Consortium international à but non lucratif dont l'objectif est de promouvoir l'adoption de normes indépendantes des produits.
Point unique de défaillance	Élément d'un système dont la défaillance provoque une panne du système. Ces éléments sont indésirables dans tout système devant assurer une haute disponibilité ou fiabilité des services, qu'il s'agisse d'une entreprise, d'une application logicielle ou d'un autre système industriel.

Terme	*Définition*
Récepteur	Dans le présent document, système d'information de la partie prenante du système eTIR qui reçoit un message eTIR envoyé par une autre partie prenante et le traite.
RSA	Algorithme inventé en 1977 par Ronald L. Rivest, Adi Shamir et Leonard Adleman. Il s'agit d'un algorithme asymétrique qui repose sur l'utilisation de deux clefs différentes liées par une relation mathématique. La clef publique et les clefs privées sont générées à l'aide de l'algorithme RSA et peuvent être utilisées pour chiffrer des informations ou pour signer.
Sécurité des services Web (WS-Security)	Spécification décrivant les améliorations apportées au protocole SOAP version 1.1 pour renforcer la protection (l'intégrité) et la confidentialité des messages. Ces améliorations passent par des fonctionnalités permettant de sécuriser les messages SOAP grâce à une signature numérique XML, d'assurer la confidentialité à l'aide du chiffrement XML et de propager les moyens d'identification électronique grâce aux jetons de sécurité (par exemple, le jeton X.509).
Serveurs Web frontaux	Serveurs Web qui reçoivent les messages de demande des points de terminaison du service Web du système international eTIR (ou qui envoient des messages de demande aux points de terminaison du service Web d'autres parties prenantes du système eTIR).
Service Web	Service ou fonction virtuels exposés sur un réseau (privé ou Internet) permettant la communication de système à système à l'aide de messages respectant un format strictement défini. Type de communication également appelé « communication de machine à machine ».
Signature numérique	Code numérique (chaîne de caractères) qui peut être joint à un message transmis par voie électronique, dans deux buts distincts : 1) garantir au destinataire que le message provient réellement de l'expéditeur déclaré, en appliquant le principe de non-répudiation(c'est-à-dire que l'expéditeur ne peut pas prétendre ultérieurement que le message était falsifié) ; 2) garantir au destinataire que le message n'a pas été altéré pendant son transit de l'expéditeur au destinataire (c'est-à-dire que son intégrité a été préservée). La signature numérique protège à la fois contre la modification malveillante (une tierce partie altère délibérément le sens du message) et contre la modification involontaire (dueà des failles dans le processus de communication, comme des interférences électriques).
Signature XML	Spécification établie conjointement par le World Wide Web Consortium (W3C) et le Groupe d'étude Signature numérique sur l'ingénierie Internet (IETF). La signature XML fournit des services de protection de l'intégrité et d'authentification du message ou du signataire pour des données de tous types, que ce soit dans le fichier XML comprenant la signature ou ailleurs.
SOAP	Simple Object Access Protocol. Protocole de messagerie défini pour l'échange d'informations dans le cadre de l'exécution de services Web. Il s'agit d'un protocole basé sur XML qui se compose de trois parties : • Une enveloppe, qui définit la structure du message (en-tête et corps) et la façon dont il doit être traité ; • Un ensemble de règles de codage permettant de décrire les instances des types de données liées à l'application ; Une convention pour la représentation des appels de procédure et des réponses.
Truststore	Fichier keystore qui contient les certificats d'autres parties avec lesquelles on prévoit de communiquer ou d'autorités de certification auxquelles on fait confiance pour identifier d'autres parties.
Valeur de hachage	Également appelée « hash » ou « résumé de message ». Valeur générée à partir d'un texte, sensiblement plus réduite que celui-ci. Elle est générée par une formule conçue de telle sorte qu'il est extrêmement improbable qu'un autre texte produise la même valeur de hachage.
XML	Langage de balisage extensible. Langage définissant un ensemble de règles pour le codage des documents sous une forme lisible à la fois par les personnes et par les machines. Il est utilisé dans le cadre du protocole SOAP pour encoder les messages envoyés par les services Web.

C. Analyse des besoins du système international eTIR en matière de capacités et d'extensibilité

1. Introduction

279. La présente annexe analyse, en s'appuyant sur les données existantes (février 2021) et sur l'expérience acquise pendant le développement du système international eTIR, les exigences relatives aux capacités de traitement des messages (débit de messages) et de stockage des données (volume de données) que doit satisfaire le système international eTIR.

280. Le système international eTIR n'étant pas encore en service, cette analyse ne repose pas sur des données en conditions réelles et adopte donc une approche prudente en

envisageant toujours les scénarios les plus défavorables et en fournissant des estimations fondées sur les maxima plutôt que sur les moyennes. Lorsque le système international eTIR sera opérationnel, la CEE réexaminera cette analyse afin d'améliorer les prévisions relatives aux capacités requises pour les années à venir et de les relier au nombre de garanties électroniques vendues.

2. Analyse du nombre de messages

281. Le tableau suivant présente une vue d'ensemble des données statistiques des années écoulées, combinée aux estimations des ventes de carnets TIR et de garanties électroniques pour les cinq prochaines années, en s'appuyant sur les données statistiques les plus récentes des ventes de carnets TIR et sur le nombre de garanties électroniques émises dans le cadre des projets pilotes eTIR.

Tableau 34
Données statistiques et prévisions des ventes de carnets TIR et de garanties électroniques

Année	*Nombre de carnets TIR vendus*	*Nombre de garanties électroniques vendues*	*Augmentation annuelle du nombre de garanties électroniques vendues*
2001	2 707 950	*s.o.*	*s.o.*
2002	3 095 200	*s.o.*	*s.o.*
2003	3 298 000	*s.o.*	*s.o.*
2004	3 211 050	*s.o.*	*s.o.*
2005	3 240 650	*s.o.*	*s.o.*
2006	3 599 850	*s.o.*	*s.o.*
2007	3 076 250	*s.o.*	*s.o.*
2008	3 253 800	*s.o.*	*s.o.*
2009	2 230 400	*s.o.*	*s.o.*
2010	2 822 200	*s.o.*	*s.o.*
2011	3 074 500	*s.o.*	*s.o.*
2012	3 158 300	*s.o.*	*s.o.*
2013	2 920 150	*s.o.*	*s.o.*
2014	1 945 050	*s.o.*	*s.o.*
2015	1 500 450	5 (projet pilote eTIR)	*s.o.*
2016	1 223 400	59 (projet pilote eTIR)	*s.o.*
2017	1 154 650	82 (projet pilote eTIR)	*s.o.*
2018	1 020 650	81 (projet pilote eTIR)	*s.o.*
2019	858 100	78 (projet pilote eTIR)	*s.o.*
2020	679 300	2 (projet pilote eTIR)	*s.o.*
2021	600 000 (estimation)	63 (projet pilote eTIR) ; 5 000 (estimation)	*s.o.*
2022	550 000 (estimation)	15 000 (estimation)	200 %
2023	500 000 (estimation)	60 000 (estimation)	300 %
2024	450 000 (estimation)	200 000 (estimation)	233 %
2025	400 000 (estimation)	400 000 (estimation)	100 %
2026	300 000 (estimation)	700 000 (estimation)	75 %

282. Les facteurs suivants ont été pris en compte dans le calcul des estimations des garanties électroniques vendues :

a) Le nombre de pays qui ont lancé des projets d'interconnexion entre leur système douanier national et le système international eTIR au cours de l'année 2020 ;

b) Le nombre de pays qui ont déjà exprimé le souhait d'être connectés au système eTIR et pour lesquels des projets devraient très probablement démarrer au cours de l'année 2021 ;

c) Le nombre de carnets TIR émis ces dernières années le long des corridors impliquant les parties contractantes qui ont lancé des projets d'interconnexion ou qui vont bientôt le faire ;

d) Les efforts entrepris ou l'intérêt exprimé par les organisations économiques régionales s'agissant de la validation de principe des projets d'interconnexion de leurs systèmes d'union douanière avec le système international eTIR, ainsi que les délais envisagés pour ces interconnexions ;

e) Les résultats de l'étude portant sur les raisons de la diminution du nombre de carnets TIR utilisés (ci-après « l'étude ») élaborée par la Commission de contrôle TIR (TIRExB) en 2020 et, en particulier, l'évolution des ventes de carnets TIR ;

f) Les efforts que la CEE et l'organisation internationale déploieront dans les années à venir afin d'attirer davantage de pays et de marchés (intermodaux, postaux) et d'étendre la Convention TIR à de nouvelles régions, comme le décrit l'étude ;

g) Aucune analyse de sensibilité ou autre méthode de prévision scientifique n'a été jusqu'à présent utilisée pour établir ces estimations.

283. Les estimations de l'augmentation annuelle des ventes de garanties électroniques montrent que, après les premières années suivant l'adoption du système, le pourcentage d'augmentation à long terme tend à devenir constant et pourrait le rester si le nombre de parties contractantes à la Convention TIR connectées au système international eTIR continue également à croître. Il est donc nécessaire de concevoir le système international eTIR de manière à ce qu'il puisse facilement absorber une augmentation annuelle régulière de 100 % des transports TIR appliquant la procédure eTIR.

284. Le nombre de messages envoyés et reçus par transport TIR dépend de plusieurs facteurs : le nombre d'opérations TIR, le nombre de messages de déclaration préalable (messages « Renseignements anticipés TIR », « Renseignements anticipés rectifiés » et « Annuler les renseignements anticipés ») envoyés par le titulaire, le nombre d'utilisations du mécanisme de demande, le nombre de fois où les scellements sont changés, la survenue ou non d'un incident ou d'un accident pendant le transport TIR, etc. Le tableau suivant présente plusieurs scénarios de transports TIR et indique, pour chacun d'eux, le nombre maximal de messages reçus et envoyés par le système international eTIR (si le titulaire envoie les messages de déclaration préalable via le système eTIR) ainsi que le nombre de messages de demande.

Tableau 35
Messages reçus et envoyés par le système international eTIR, par scénario

Nombre d'opérations TIR	*Messages reçus et envoyés pour les opérations TIR*	*Messages de déclaration préalable reçus et envoyés*	*Nombre total de messages par scénario*	*Nombre de messages de demande par scénario*
2	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 2, (E7/E8) x 9, (E5/E6) x 9, (I5/I6) x 2	E9/E10	64	21
3	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 3, (E7/E8) x 12, (E5/E6) x 12, (I5/I6) x 3	E9/E10	88	28
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E11/E12	110	36
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E13/E14, E9/E10, E11/E12, E13/E14, E11/E12	118	40

Nombre d'opérations TIR	*Messages reçus et envoyés pour les opérations TIR*	*Messages de déclaration préalable reçus et envoyés*	*Nombre total de messages par scénario*	*Nombre de messages de demande par scénario*
5	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 7, (I9/I10, I11/I12, I13/I14) x 5, (E7/E8) x 17, (E5/E6) x 17, (I5/I6) x 5	E9/E10, E11/E12, E11/E12	136	44
6	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 9, (I9/I10, I11/I12, I13/I14) x 6, (E7/E8) x 20, (E5/E6) x 20, (I5/I6) x 6	E9/E10, E11/E12, E11/E12	160	51
7	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 15, (I9/I10, I11/I12, I13/I14) x 7, (E7/E8) x 24, (E5/E6) x 24, (I5/I6) x 7	E9/E10, E11/E12, E11/E12, E11/E12	198	61
8	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 18, (I9/I10, I11/I12, I13/I14) x 8, (E7/E8) x 27, (E5/E6) x 27, (I5/I6) x 8	E9/E10, E11/E12, E11/E12, E11/E12	224	68
9	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 21, (I9/I10, I11/I12, I13/I14) x 9, (E7/E8) x 30, (E5/E6) x 30, (I5/I6) x 9	E9/E10, E11/E12, E11/E12, E11/E12	250	75
10	E1/E2, I1/I2, (I7/I8) x 4, (I15/I16) x 30, (I9/I10, I11/I12, I13/I14) x 10, (E7/E8) x 34, (E5/E6) x 34, (I5/I6) x 10	E9/E10, E11/E12, E11/E12, E11/E12, E11/E12	292	85

285. En 2020, l'IRU a déclaré les ventes suivantes[60] : 4 300 carnets TIR à 4 volets (0,6 %), 544 200 carnets TIR à 6 volets (80 %), 131 050 carnets TIR à 14 volets (19,3 %) et aucun carnet TIR à 20 volets. La plupart des transports TIR effectués cette année-là comportaient donc 3 opérations TIR (6 volets). En tenant compte du tableau précédent, et tout en restant prudent quant à la capacité du système international eTIR, on considérera que le nombre total moyen de messages échangés par transport TIR est de 120 et que le nombre moyen de messages de demande est de 40.

286. On supposera également que le nombre moyen de messages échangés par transport TIR augmentera de 5 % par an. Cette hypothèse est étayée par le fait que le nombre de parties contractantes connectées au système international eTIR augmentera au fil du temps, ce qui entraînera un accroissement de la longueur potentielle des transports TIR appliquant la procédure eTIR. Enfin, les nouvelles versions des spécifications eTIR pourraient également contribuer à cette augmentation.

287. Le tableau suivant donne des estimations du nombre de messages que le système international eTIR pourrait être amené à envoyer et à recevoir, et doit donc être en mesure de traiter, au cours des prochaines années.

Tableau 36
Estimation du nombre de messages à traiter par le système international eTIR

Année	*A. Estimation du nombre de garanties électroniques vendues*	*B. Estimation du nombre moyen de messages par transport TIR*	*C. Estimation du nombre moyen de messages par an, en millions (A x B)*	*D. Estimation du nombre moyen de messages de demande par transport TIR*	*E. Estimation du nombre moyen de messages de demande par an, en millions (A x D)*
2021	5 000	130	0,65	40	0,20
2022	15 000	137	2,06	42	0,63
2023	60 000	143	8,58	44	2,64
2024	200 000	150	30,00	46	9,20
2025	400 000	158	63,20	49	19,60
2026	700 000	166	116,20	51	35,70

[60] Voir document informel WP.30/AC.2 (2021) no 5.

288. On peut donc avancer l'hypothèse que le nombre maximal de messages que le système international eTIR devra transmettre se situe dans une fourchette comprise entre cinq et dix fois le nombre moyen de messages, ce qui permet d'établir les deux tableaux suivants : le premier pour le nombre maximal de messages reçus et envoyés par minute, et le second pour le nombre maximal de messages de demande reçus par minute.

Tableau 37
Estimation du nombre maximal de messages reçus et envoyés

Année	*A. Estimation du nombre moyen de messages par an, en millions*	*B. Estimation du nombre moyen de messages par minute (A / (365 x 24 x 60))*	*Estimation du nombre maximal de messages par minute (limite inférieure de la fourchette) (B x 5)*	*Estimation du nombre maximal de messages par minute (limite supérieure de la fourchette) (B x 10)*
2021	0,65	1,24	6,2	12,4
2022	2,06	3,92	20,0	39,2
2023	8,58	16,32	81,6	163,2
2024	30,00	57,23	286,2	572,3
2025	63,20	120,57	602,9	1 205,7
2026	116,20	221,69	1 108,5	2 216,9

Tableau 38
Estimation du nombre maximal de messages de demande reçus et envoyés

Année	*A. Estimation du nombre moyen de messages de demande par an, en millions*	*B. Estimation du nombre moyen de messages de demande par minute (A / (365 x 24 x 60))*	*Estimation du nombre maximal de messages de demande par minute (limite inférieure de la fourchette) (B x 5)*	*Estimation du nombre maximal de messages de demande par minute (limite supérieure de la fourchette) (B x 10)*
2021	0,20	0,38	1,9	3,8
2022	0,63	1,20	6,0	12,0
2023	2,64	5,02	25,1	50,2
2024	9,20	17,50	87,5	175,0
2025	19,60	37,29	186,5	372,9
2026	35,70	67,92	339,6	679,2

3. Analyse des exigences relatives au débit de messages

289. Le débit de messages que doit prendre en charge le système international eTIR est défini comme le nombre de messages de demande qu'il doit être capable de recevoir et de traiter par une unité de temps. Le nombre moyen et le nombre maximal (limite supérieure de la fourchette) de messages de demande par minute ont été déterminés à partir de l'analyse précédente.

Tableau 39
Estimation des débits moyen et maximal de messages à traiter

Année	*Estimation du nombre moyen de messages de demande par minute*	*Estimation du nombre maximal de messages de demande par minute*
2021	0,38	3,8
2022	1,20	12,0
2023	5,02	50,2
2024	17,50	175,0
2025	37,29	372,9
2026	67,92	679,2

4. Analyse des exigences relatives au volume de données

290. Il est important de tenir compte, en plus du débit de messages que devra prendre en charge le système international eTIR, de la taille de ces messages et du volume total de données que le système sera amené à échanger, traiter et enregistrer.

291. L'expérience acquise pendant le développement du système international eTIR a permis d'établir les points suivants : 70 % des messages font moins de 10 Ko ; 25 % font entre 11 Ko et 50 Ko ; et les 5 % restants font entre 51 Ko et 20 Mo (taille maximale autorisée). On considère que 5 % des messages comportent des documents supplémentaires (ce qui augmente considérablement leur taille).

292. On peut supposer par conséquent supposer que la taille moyenne des messages se calcule comme suit : (90 % x 5 Ko) + (9 % x 25 Ko) + (1 % x 5 Mo) = 57 Ko. Les résultats précédents permettent d'estimer le volume total maximal de données qui devront être traitées par le système international eTIR, et, plus particulièrement, le volume total maximal de données qu'il faudra stocker dans les journaux eTIR.

Tableau 40
Estimation du volume maximal de données à stocker dans les journaux eTIR

Année	*A. Estimation du nombre maximal de messages par minute (limite supérieure de la fourchette)*	*B. Estimation du volume maximal de données par minute, en Mo (A x 0,057)*	*C. Estimation du volume maximal de données par an, en To (B x 60 x 24 x 365)*
2021	12,4	0,7	0,371
2022	39,2	2,2	1,174
2023	163,2	9,3	4,889
2024	572,3	32,6	17,146
2025	1 205,7	68,7	36,121
2026	2 216,9	126,4	66,417

293. Seule une petite partie de ce volume est stockée dans la base de données eTIR. En effet, seuls les messages de demande sont traités et enregistrés dans cet emplacement de stockage. De plus, les documents supplémentaires n'étant pas stockés dans la base de données, les messages les plus gros (1 % du total) ne sont pas à prendre en compte, ce qui permet de calculer comme suit la taille moyenne des messages : (91 % x 5 Ko) + (9 % x 25 Ko) = 6,8 Ko. Enfin, seules les valeurs du corps du message sont stockées dans la base de données (contrairement à l'en-tête) ; elles représentent entre 3 % et 10 % de la taille du message, soit au maximum 0,68 Ko.

Tableau 41
Estimation du volume maximal de données à stocker dans la base de données eTIR

Année	*A. Estimation du nombre maximal de messages de demande par minute (limite supérieure de la fourchette)*	*B. Estimation du volume maximal de données par minute, en Mo (A x 0,68)*	*C. Estimation du volume maximal de données par an, en Go (B x 60 x 24 x 365)*
2021	3,8	2,6	1,36
2022	12,0	8,2	4,29
2023	50,2	34,1	17,94
2024	175,0	119,0	62,55
2025	372,9	253,6	133,28
2026	679,2	461,9	242,75

294. Les documents contenus dans les messages sont stockés séparément, dans le système de stockage des documents eTIR. Comme dans le cas de la base de données eTIR, ce stockage ne concerne que les messages de demande. Selon les hypothèses formulées précédemment, seuls les messages les plus gros contenant des documents sont à prendre en compte (1 % du

total) ; la taille moyenne des messages se calcule donc comme suit : 1 % x 5 Mo = 50 Ko. Il est ainsi possible d'estimer le volume total maximal de données qu'il faudra stocker dans les documents eTIR.

Tableau 42
Estimation du volume maximal de données à stocker dans les documents eTIR

Année	*A. Estimation du nombre maximal de messages de demande par minute (limite supérieure de la fourchette)*	*B. Estimation du volume maximal de données par minute, en Mo (A x 0,05)*	*C. Estimation du volume maximal de données par an, en To (B x 60 x 24 x 365)*
2021	3,8	0,2	0,100
2022	12,0	0,6	0,315
2023	50,2	2,5	1,319
2024	175,0	8,8	4,599
2025	372,9	18,6	9,800
2026	679,2	34,0	17,849

5. Conclusions

295. La fiabilité des estimations et des prévisions relatives aux capacités requises en manière de traitement des messages (débit de messages) et de stockage de données (volumes de données) dépend de la validité des différentes hypothèses sur lesquelles elles reposent. Le système international eTIR n'étant pas encore en service, cette analyse manque de données en conditions réelles. De ce fait, le système international eTIR devrait être conçu en tenant compte uniquement des besoins en matière de capacités et d'extensibilité déterminés pour les deux premières années, puisqu'il est très probable que plusieurs hypothèses seront remises en cause à la lumière des données obtenues en conditions réelles, ce qui modifiera totalement les calculs et les prévisions pour les années suivantes.

296. C'est pourquoi il est fortement conseillé de procéder de nouveau à cette analyse six mois après la mise en service du système international eTIR, afin de revoir les hypothèses, de refaire les calculs et d'améliorer la fiabilité des estimations et des prévisions relatives aux besoins du système en matière de capacités et d'extensibilité. Il conviendra par la suite de revoir cette analyse chaque année pour l'affiner de manière continue.

D. Codes d'erreur

297. La présente annexe contient des informations supplémentaires sur les codes d'erreur utilisés dans le cadre du système eTIR.

298. La liste des codes 99 (CL99) rassemble tous les codes d'erreur qui peuvent être utilisés dans un message de réponse pour indiquer les problèmes survenus pendant le traitement du message de demande correspondant. Cette liste de codes, présentée dans le tableau suivant, est propre au système eTIR et continuellement mise à jour par la CEE.

Tableau 43
Liste des codes d'erreur (CL99)

Code	*Nom*	*Description*
100	Message non valide	Le message n'est pas valide et aucun détail supplémentaire n'est disponible pour cette erreur.
101	Paramètre manquant	Un paramètre obligatoire manque dans le message.
102	Paramètre de valeur de domainenon valide	La valeur d'un paramètre ne fait pas partie d'une liste définie de valeurs acceptables.
103	Format de date non conforme	Un paramètre contenant une date ne peut pas être correctement converti.
104	Valeur non entière	Un champ numérique contient des données qui ne sont pas numériques.
105	Longueur du paramètre dépassée	Un champ de type Chaîne contient trop de caractères.

Code	*Nom*	*Description*
106	Modèle non valide	Un champ de type Chaîne ne correspond pas au modèle défini dans la définition du schéma XML du message.
151	Échec de la condition C001	La condition C001 n'est pas remplie.
152	Échec de la condition C002	La condition C002 n'est pas remplie.
153	Échec de la condition C003	La condition C003 n'est pas remplie.
154	Échec de la condition C004	La condition C004 n'est pas remplie.
155	Échec de la condition C005	La condition C005 n'est pas remplie.
158	Échec de la condition C008	La condition C008 n'est pas remplie.
168	Échec de la règle R008	La règle R008 n'est pas respectée.
200	État non valide	L'état d'un objet interne n'est pas valide et aucun détail supplémentaire n'est disponiblepour cette erreur.
201	Garantie non acceptable	La garantie n'est pas dans un état permettant de l'accepter.
203	Garantie non annulable	La garantie n'est pas dans un état permettant de l'annuler.
204	Garantie déjà enregistrée	La garantie a déjà été enregistrée.
205	Garantie déjà annulée	La garantie est déjà annulée ou la demande d'annulation a déjà été envoyée.
210	Opération déjà lancée	L'opération est déjà lancée.
211	Opération déjà achevée	L'opération est déjà achevée.
212	Opération déjà apurée	L'opération est déjà apurée.
213	Opération non lancée	L'opération n'est pas encore lancée.
214	Identifiant de l'opération déjà enregistré	« Refuser le lancement » est une opération à part entière et doit être affecté d'un identifiant d'opération unique.
215	Séquence de l'opération déjà enregistrée	« Refuser le lancement » est une opération à part entière et doit être affecté d'un identifiant d'opération unique.
216	Refus du lancement non autorisé	Le « refus du lancement » ne peut pas être exécuté en raison de l'état actuel de la garantieou parce qu'il s'agit de la première opération pour ce transport.
220	Déclaration non reçue	L'opération ne peut pas être lancée parce que la déclaration n'a pas été reçue.
299	Message doublonné	Le même message a déjà été reçu de la même source.
300	Opération non valide	Une opération non valide a été effectuée, et aucun détail supplémentaire n'est disponiblepour cette erreur.
301	Garantie non trouvée	La garantie n'a pas été trouvée dans la base de données.
302	Chaîne de garantie non trouvée	La chaîne de garantie n'a pas été trouvée dans la base de données.
303	Type de garantie non trouvé	Le type de garantie n'a pas été trouvé dans la base de données.
304	Bureau de douane non trouvé	Ce code d'erreur n'est pas utilisé dans la version 4.3 des spécifications eTIR.
305	Pays non trouvé	Le pays n'a pas été trouvé dans la base de données.
306	Type de contrôle non trouvé	Le type de contrôle n'a pas été trouvé dans la base de données.
320	Non-correspondancetitulaire/garantie	Le paramètre d'identification du titulaire et le paramètre de référence de la garantie necorrespondent pas à ce qui est enregistré dans la base de données.
321	Titulaire non habilité	Le titulaire n'est pas habilité dans la banque de données internationale TIR (ITDB).
322	Titulaire non trouvé	Le titulaire ne figure pas dans l'ITDB.
330	Chaîne de garantie non habilitée	La chaîne de garantie n'est pas habilitée dans la base de données.
331	Non-correspondance chaînede garantie/garantie	Le paramètre du code de la chaîne de garantie et le paramètre de référence de la garantiene correspondent pas à ce qui est enregistré dans la base de données.
332	Non-correspondance typede garantie/garantie	Le paramètre de type de garantie et le paramètre de référence de la garantie ne correspondent pas à ce qui est enregistré dans la base de données.
400	Erreur interne eTIR	Une erreur interne s'est produite dans le système international eTIR et aucun détail supplémentaire n'est disponible pour cette erreur.

299. Il est impossible d'indiquer tous les codes d'erreur dans les messages de réponse ; le tableau suivant précise ceux qui peuvent l'être. Ces informations sont destinées à aider les

experts informatiques des parties prenantes eTIR à procéder aux vérifications requises lors de la réception de codes d'erreur spécifiques. La liste est fournie dans l'état où elle se trouvait au moment de l'établissement du présent document. La version la plus récente est consultable sur le site Web du système international eTIR[61].

Tableau 44
Liste des codes d'erreur utilisables en fonction du message de réponse

Code d'erreur	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
100	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
101	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
102	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
103	X			X	X	X	X				X				X		
104				X											X	X	X
105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
106	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
151				X											X		
152				X											X		
153				X											X		
154				X											X		
155				X											X		
158				X											X	X	
168				X													
200	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
201	X																
203												X					
204											X						
205												X					
210					X												
211						X											
212							X										
213						X	X										
214					X	X	X		X								
215					X	X	X		X								
216									X								
220					X												
299					X	X	X										

[61] Voir www.etir.org/error-codes-list.

Code d'erreur	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
300	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
301	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
302	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
303	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
304																	
305				X	X	X	X								X		
306					X	X	X										
320	X			X								X			X	X	X
321	X				X	X	X				X						
322	X	X	X		X	X	X				X		X				
330	X										X		X				
331	X											X					
332	X											X					
400	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

300. Pour finir, le tableau suivant rassemble, à l'attention des experts informatiques du système d'information, un ensemble de mesures qu'il est recommandé de mettre en œuvre lors de la réception d'un message de réponse comportant un ou plusieurs codes d'erreur.

Tableau 45
Mesures recommandées lors de la réception de codes d'erreur

Code	*Nom*	*Mesures recommandées*
100	Message non valide	Vérifiez le message lui-même et son format, car il n'est pas reconnu par le système international eTIR. **Contactez les services d'assistance eTIR en leurenvoyant le contenu du message communiqué, l'horodatage et la marche à suivre pour reproduire ce problème afin de le régler.**
101	Paramètre manquant	Vérifiez les paramètres du message, notamment ceux qui sont signalés comme étant obligatoires dans la description donnée dans le présent document, et assurez-vous que le message les contient tous.
102	Paramètre de valeur de domaine non valide	Vérifiez le paramètre codé, ses valeurs et les listes de codes correspondantes. Assurez-vous que chaque paramètre codé utilise l'une des valeurs de la liste decodes correspondante.
103	Format de date nonconforme	Vérifiez les paramètres de date et leur format. Assurez-vous que chaque format de date correspond au format prescrit, que la valeur est conforme au format ou aumodèle et que la valeur de l'attribut formatCode est correcte.
104	Valeur non entière	Vérifiez les paramètres qui doivent être exprimés par des nombres entiers. Pourchacun, assurez-vous que la valeur est bien un nombre entier.
105	Longueur du paramètre dépassée	Vérifiez la longueur de la valeur du paramètre. Assurez-vous que la longueur dechaque paramètre ne dépasse pas la longueur maximale définie dans la documentation (colonne Format).
106	Modèle non valide	Vérifiez le modèle de la valeur du paramètre, car il ne correspond pas auxexigences définies pour cet attribut dans la définition du schéma XML dumessage.
151	Échec de la condition C001	Vérifiez les paramètres imposés par la condition C001 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.
152	Échec de la condition C002	Vérifiez les paramètres imposés par la condition C002 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.

Code	*Nom*	*Mesures recommandées*
153	Échec de la condition C003	Vérifiez les paramètres imposés par la condition C003 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.
154	Échec de la condition C004	Vérifiez les paramètres imposés par la condition C004 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.
155	Échec de la condition C005	Vérifiez les paramètres imposés par la condition C005 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.
158	Échec de la condition C008	Vérifiez les paramètres imposés par la condition C008 et assurez-vous que leursvaleurs sont conformes au pseudo-code de la condition.
168	Échec de la règle R008	Vérifiez les paramètres imposés par la règle R008 et assurez-vous que leursvaleurs respectent les conditions fixées par la règle.
200	État non valide	Vérifiez l'état de l'objet visé (transport, garantie,…) et assurez-vous qu'il estconforme au service Web du système international eTIR demandé.
201	Garantie non acceptable	Vérifiez l'état de la garantie que vous avez essayé d'accepter et assurez-vous qu'elle est conforme au cheminement décrit dans le diagramme des états de lagarantie.
203	Garantie non annulable	Vérifiez l'état de la garantie que vous avez essayé d'annuler et assurez-vous qu'elle est conforme au cheminement décrit dans le diagramme des états de lagarantie.
204	Garantie déjà enregistrée	Vérifiez l'état de la garantie que vous avez essayé d'enregistrer, car elle semble qu'elle soit déjà enregistrée. Utilisez le service Web de demande d'informationssur la garantie pour vérifier qu'elle existe dans le système international eTIR.
205	Garantie déjà annulée	Vérifiez l'état de la garantie que vous avez essayé d'enregistrer, car elle semble qu'elle soit déjà annulée. Utilisez le service Web de demande d'informations surla garantie pour vérifier qu'elle existe dans le système international eTIR.
210	Opération déjà lancée	Ce message tente de lancer une opération TIR qui a déjà été lancée. Assurez-vousque ce message n'est pas un doublon d'un message précédemment envoyé et vérifiez les valeurs définies dans ses paramètres.
211	Opération déjà achevée	Ce message tente d'achever une opération TIR qui a déjà été achevée. Assurez-vous que ce message n'est pas un doublon d'un message précédemment envoyéet vérifiez les valeurs définies dans ses paramètres.
212	Opération déjà apurée	Ce message tente d'apurer une opération TIR qui a déjà été apurée. Assurez-vousque ce message n'est pas un doublon d'un message précédemment envoyé et vérifiez les valeurs définies dans ses paramètres.
213	Opération non lancée	Ce message tente d'exécuter une opération sur une opération TIR qui devrait avoir été lancée et qui ne l'a pas encore été. Assurez-vous que ce message est envoyé selon l'ordre prévu et vérifiez les valeurs définies dans ses paramètres.
214	Identifiant de l'opérationdéjà enregistré	Vérifiez l'identifiant du message et assurez-vous qu'il n'entre pas en conflit avecun autre identifiant d'opération.
215	Séquence de l'opérationdéjà enregistrée	Vérifiez le numéro de séquence de la dernière opération pour ce transport etincrémentez-le.
216	Refus du lancement non autorisé	Le « refus du lancement » ne peut pas être exécuté s'il s'agit de la première opération enregistrée ou si la garantie n'a pas été acceptée. Vérifiez également que la référence de garantie est correcte.
220	Déclaration non reçue	Ce message tente d'exécuter une opération alors que la déclaration n'a pas encoreété reçue. Assurez-vous que ce message est envoyé selon l'ordre prévu et vérifiezles valeurs définies dans ses paramètres.
299	Message doublonné	Vérifiez le message déjà envoyé à ce point de terminaison, car ce message a déjàété reçu par le système international eTIR.
300	Opération non valide	Vérifiez le contenu du message, car il a généré une erreur technique d'origineinconnue dans le système international eTIR.
301	Garantie non trouvée	Vérifiez la valeur de l'identifiant de référence de garantie dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.
302	Chaîne de garantie nontrouvée	Vérifiez la valeur de l'identifiant de la chaîne de garantie dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.

Code	*Nom*	*Mesures recommandées*
303	Type de garantie non trouvé	Vérifiez la valeur du type de garantie dans le message et assurez-vous qu'elle setrouve sur la liste des codes eTIR de type de garantie (CL12) et qu'elle correspond à la valeur reçue dans les messages précédents.
304	Bureau de douane nontrouvé	Ce code d'erreur n'est pas utilisé dans la version 4.3 des spécifications eTIR.
305	Pays non trouvé	Vérifiez la valeur du code de pays dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents et qu'elle figure sur laliste des codes (CL04) de noms de pays (ISO 3166-1-alpha-2).
306	Type de contrôle non trouvé	Vérifiez la valeur du type de contrôle dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents et qu'elle figure sur laliste des codes de type de contrôle (CL25).
320	Non-correspondance titulaire/garantie	Vérifiez le format et la valeur du titulaire du carnet TIR dans le message et assurez-vous que la valeur correspond à la valeur reçue dans les messages précédents. Si tel est le cas, vérifiez l'existence du titulaire et son statut en utilisant le message d'information eTIR « I3 − Obtenir des informations sur letitulaire », les services Web ITDB ou l'application Web ITDB.
321	Titulaire non habilité	Vérifiez la valeur du titulaire du carnet TIR dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents. Si tel est lecas, vérifiez le statut du titulaire en utilisant le message d'information eTIR « I3 − Obtenir des informations sur le titulaire », les services Web ITDB oul'application Web ITDB.
322	Titulaire non trouvé	Vérifiez la valeur du titulaire du carnet TIR dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents. Si tel est le cas, vérifiez l'identifiant du titulaire en utilisant le message d'information eTIR « I3 − Obtenir des informations sur le titulaire », les services Web ITDB oul'application Web ITDB.
330	Chaîne de garantie non habilitée	Vérifiez la valeur de l'identifiant de la chaîne de garantie dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.
331	Non-correspondance chaînede garantie/garantie	Vérifiez la valeur de l'identifiant de la chaîne de garantie dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.
332	Non-correspondance typede garantie/garantie	Vérifiez la valeur de l'identifiant du type de garantie dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.
400	Erreur interne eTIR	**Contactez les services d'assistance eTIR en leur envoyant le contenu du message communiqué, l'horodatage et la marche à suivre pour reproduire ce problème afin de le régler.**

Liste des tableaux

Tableau 1 Documents pertinents 5
Tableau 2 Définition de termes essentiels 5
Tableau 3 Sigles et abréviations 7
Tableau 4 Exigences qualitatives relatives à la disponibilité 21
Tableau 5 Exigences quantitatives relatives à la disponibilité 21
Tableau 6 Exigences relatives aux copies de sauvegarde 22
Tableau 7 Exigences relatives à la capacité et à l'extensibilité 23
Tableau 8 Exigences relatives à la gestion de la configuration 24
Tableau 9 Exigences relatives à la conservation des données 24
Tableau 10 Exigences relatives à la reprise après sinistre 25
Tableau 11 Exigences relatives à la tolérance de panne 26
Tableau 12 Exigences relatives à l'internationalisation et à la localisation 27
Tableau 13 Exigences relatives à l'interopérabilité 28
Tableau 14 Exigences relatives à la maintenabilité 29
Tableau 15 Exigences quantitatives relatives à la performance 30
Tableau 16 Exigences qualitatives relatives à la performance 30
Tableau 17 Exigences quantitatives relatives à la fiabilité 31
Tableau 18 Exigences qualitatives relatives à la fiabilité 32
Tableau 19 Exigence relative à la réutilisabilité 33
Tableau 20 Exigences relatives au suivi 54
Tableau 21 Exigences relatives à l'authentification 54
Tableau 22 Exigences relatives à l'autorisation 55
Tableau 23 Exigences en matière de sensibilisation et de formation 56
Tableau 24 Exigences relatives à la confidentialité 56
Tableau 25 Exigence relative à l'identification 57
Tableau 26 Exigences relatives à l'intégrité 57
Tableau 27 Exigences relatives à la sécurité des nœuds 58
Tableau 28 Exigences relatives à la non-répudiation 58
Tableau 29 Exigences relatives à la sécurité physique 59
Tableau 30 Exigences relatives au codage sécurisé et à la sécurité des applications 59
Tableau 31 Exigences relatives à la gestion de la vulnérabilité 60
Tableau 32 Conventions de notation ArchiMate des diagrammes 71
Tableau 33 Glossaire technique 71
Tableau 34 Données statistiques et prévisions des ventes de carnets TIR et de garanties électroniques 75
Tableau 35 Messages reçus et envoyés par le système international eTIR, par scénario 76
Tableau 36 Estimation du nombre de messages à traiter par le système international eTIR 77
Tableau 37 Estimation du nombre maximal de messages reçus et envoyés 78
Tableau 38 Estimation du nombre maximal de messages de demande reçus et envoyés 78
Tableau 39 Estimation des débits moyen et maximal de messages à traiter 78
Tableau 40 Estimation du volume maximal de données à stocker dans les journaux eTIR 79
Tableau 41 Estimation du volume maximal de données à stocker dans la base de données eTIR 79
Tableau 42 Estimation du volume maximal de données à stocker dans les documents eTIR 80
Tableau 43 Liste des codes d'erreur (CL99) 80
Tableau 44 Liste des codes d'erreur utilisables en fonction du message de réponse 82
Tableau 45 Mesures recommandées lors de la réception de codes d'erreur 83

Liste des figures

Figure I Architecture technique globale du système eTIR 11
Figure II Interactions entre les systèmes douaniers nationaux et les bureaux de douane 12
Figure III Interactions entre le système douanier national et le système international eTIR 13
Figure IV Interactions entre le système de l'union douanière et les systèmes douaniers nationaux 13
Figure V Interactions possibles entre le système du titulaire et le système douanier national 14
Figure VI Interactions entre le système du titulaire et le système d'une union douanière 14
Figure VII Interactions entre le système du titulaire et le système douanier national via le système international eTIR 15
Figure VIII Interactions entre la chaîne de garantie et le système international eTIR 16
Figure IX Interactions entre le système international eTIR et l'ITDB 16
Figure X Interfaces du système international eTIR 17
Figure XI Architecture logicielle du système international eTIR 18
Figure XII Architecture du système international eTIR 20
Figure XIII Développement par itération 34
Figure XIV Environnements du système international eTIR 39
Figure XV Cycle de vie des tâches 41
Figure XVI Processus de gestion des versions 43
Figure XVII Processus d'amélioration continue 45
Figure XVIII Types de tâches de maintenance 45
Figure XIX Processus de gestion des incidents 46
Figure XX Les objectifs fondamentaux de la sécurité informatique 51
Figure XXI De l'identification au respect du principe de responsabilité 51
Figure XXII eTIR security model 66
Figure XXIII An alternative security model 68