Nations Unies ECE/TRANS/WP.30/GE.1/2021/32/Rev.1

Conseil économique et social

Distr. générale
2 juillet 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

Troisième session
Genève, 13-15 septembre 2021
Point 4 d) de l'ordre du jour provisoire
Version 4.3 de la documentation sur les concepts, les fonctions et les techniques eTIR :
Spécifications techniques du système eTIR

Glossaire technique, analyse des capacités requises, codes d'erreur, fichiers XSD et listes de codes du système eTIR et mesures d'atténuation des risques

Révision

Note du secrétariat

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/WP30/2019/9 et Corr.1), sous réserve de l'accord du Comité exécutif de la Commission économique pour l'Europe (CEE). Le Comité exécutif, à sa réunion informelle à distance du 20 mai 2020, a approuvé la création du WP.30/GE.1 jusqu'en 2022, sur la base du mandat figurant dans les documents ECE/TRANS/WP.20/2019/9 et Corr.1, comme indiqué dans le document ECE/TRANS/294 (ECE/EX/2020/L.2, par. 5 b[3])).

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

[2] Mandat du Groupe nouvellement créé, approuvé par le Comité des transports intérieurs et le Comité exécutif de la CEE : www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09f.pdf%20et%20www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANSWP30-2019-09c1f.pdf et rectificatif : www.unece.org/fileadmin/DAM/trans/bcf/wp30/.

[3] Décision du Comité exécutif, ECE/EX/2020/L.2, par. 5 b), https://unece.org/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/Item_4_ECE_EX_2020_L.2_Mandates_fr.pdf.

2. Le mandat du Groupe dispose que celui-ci doit concentrer ses travaux sur l'élaboration d'une nouvelle version des spécifications 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 de la procédure eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications fonctionnelles de la procédure eTIR ; b) d'établir une nouvelle version des spécifications fonctionnelles de la procédure eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications conceptuelles de la procédure eTIR ; c) d'élaborer des amendements aux spécifications conceptuelles de la procédure eTIR, à la demande du Groupe de travail des problèmes douaniers intéressant les transports (WP.30).

3. On trouvera dans le présent document le glossaire technique, l'analyse des besoins du système international eTIR en matière de capacités et d'extensibilité, la liste des codes d'erreur et les listes de codes du système eTIR, ainsi qu'une analyse relative aux fichiers XSD et XML et une liste des menaces visant la sécurité de l'information et des mesures d'atténuation correspondantes. Tous ces éléments seront intégrés dans les spécifications techniques du système eTIR.

II. Le système international eTIR

A. Glossaire technique

4. On trouvera dans la présente section, sous forme de tableau, les définitions de tous les termes techniques qui sont utilisés dans les spécifications techniques eTIR.

Tableau 1
Glossaire technique

Terme	*Définition*
Accord de prestation de services	Un accord de prestation de services est un accord passé entre un prestataire de services et un client. Les détails des services (qualité, disponibilité, responsabilités) sont convenus entre les deux parties.
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).
Authentification multifactorielle	L'authentification multifactorielle est une méthode d'authentification électronique qui exige des utilisateurs souhaitant accéder à un site Web ou une application qu'ils confirment leur identité en présentant au moins deux éléments (facteurs) selon les critères suivants : connaissance (un élément connu uniquement de l'utilisateur), possession (un élément détenu uniquement par l'utilisateur) et inhérence (un élément exclusif à l'identité de l'utilisateur).
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.

Terme	*Définition*
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[4].
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.
Conseil consultatif sur le changement	Un conseil consultatif sur le changement est chargé d'appuyer une équipe de gestion du changement en prodiguant des conseils sur les changements demandés, en contribuant à l'évaluation de ces changements et en aidant à établir les priorités à cet égard. Les membres du conseil consultatif doivent être sélectionnés avec soin, de sorte que les changements demandés soient dûment vérifiés et évalués sur les plans tant technique qu'opérationnel.
Contrôle d'accès en fonction du rôle	Le contrôle d'accès en fonction du rôle est un mécanisme de contrôle d'accès neutre sur le plan des politiques, qui repose sur les notions de rôles et de privilèges. Grâce aux composants de ce type de contrôle d'accès, tels que les relations rôles-permissions, utilisateurs-rôles et rôles-rôles, l'affectation d'utilisateurs est chose aisée. Le contrôle d'accès en fonction du rôle peut permettre de mieux gérer, dans les grandes entités, la sécurité de plusieurs centaines d'utilisateurs et de plusieurs milliers de permissions.
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.

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

Terme	*Définition*
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 appelle l'entropie logicielle. La réécriture du code peut permettre de réduire progressivement l'entropie logicielle.
Environnement de développement intégré	Les environnements de développement intégrés sont des applications qui offrent aux programmeurs des ressources complètes pour la conception de logiciels. Généralement, ils comprennent au moins un éditeur de code source, des outils d'automatisation de la production des versions et un débogueur.
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.
Intégration continue	L'intégration continue consiste à intégrer automatiquement dans un projet de logiciel donné les modifications apportées au code par plusieurs personnes. Il s'agit de l'une des principales pratiques optimales de l'approche DevOps, qui permet aux développeurs de fréquemment verser les modifications du code dans un répertoire central où les différentes versions peuvent ensuite être produites et mises à l'essai. Des outils automatisés sont utilisés pour apprécier la validité du nouveau code avant son intégration.
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.

Terme	*Définition*
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.
Logiciel libre	Les logiciels libres sont des programmes dont la licence permet aux personnes qui s'en servent d'utiliser, d'étudier, de modifier et de distribuer le logiciel et son code source à quiconque et à toutes fins. Ces logiciels, qui peuvent être développés de manière publique et collaborative, constituent un exemple saillant de collaboration libre.
Logiciel malveillant	Les logiciels malveillants sont des programmes conçus expressément dans le but de détériorer un ordinateur, un serveur, un client ou un réseau. Il existe de nombreux types de logiciels malveillants, notamment les virus et les vers informatiques, les chevaux de Troie, les logiciels rançonneurs, les logiciels espions, les logiciels publicitaires, les roguewares (faux logiciels de sécurité), les wipers (logiciels effaçant les données d'un disque dur) et les scarewares (faux logiciels simulant des alertes de sécurité).
Procédure d'exploitation normalisée	Une procédure d'exploitation normalisée consiste en une série d'instructions étape par étape établies par une entité au bénéfice du personnel affecté aux tâches courantes. Les procédures de ce type visent à garantir l'efficacité des opérations, la qualité des prestations et l'homogénéité du fonctionnement, tout en réduisant les erreurs de communication et les risques de non-respect de la réglementation de l'entité.
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.

Terme	*Définition*
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.
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 (due à 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.

Terme	*Définition*
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 fonction de hachage cryptographique 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.

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

1. Introduction

5. La présente section 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.

6. 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

7. 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 2
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.

Année	*Nombre de carnets TIR vendus*	*Nombre de garanties électroniques vendues*	*Augmentation annuelle du nombre de garanties électroniques vendues*
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 %

8. 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.

9. 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.

10. 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 3
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
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

11. En 2020, l'IRU a déclaré les ventes suivantes[5] : 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.

12. 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.

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

13. 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 4
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

14. 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 5
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 6
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

15. 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 7
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

16. 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.

17. 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).

18. 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 8
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

19. 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 9
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

20. 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 10
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

21. 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.

22. 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.

C. Codes d'erreur

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

24. 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 11
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	Champ manquant	Un champ obligatoire manque dans le message.
102	Domaine non valide pour la valeur	Une valeur ne fait pas partie d'une liste définie de valeurs acceptables.
103	Format de date non conforme	Un champ contenant une valeur de date ne peut pas être correctement converti.
104	Valeur non entière	Un champ numérique contient une valeur qui n'est pas numérique.
105	Longueur de la valeur du champ dépassée	Un champ de type Chaîne contient une valeur constituée d'un trop grand nombre de caractères.
106	Modèle non valide	Un champ de type Chaîne ne correspond pas au modèle défini pour ce champ dans la définition du schéma XML du message.
107	Champ non valide	Le champ spécifié ne correspond pas à l'ordre défini dans la définition du schéma XML du message.
108	Attribut XML manquant	Un attribut manque dans la balise XML spécifiée (par exemple l'attribut formatCode pour tous les champs de date).
109	Attribut XML non valide	Une valeur d'un attribut n'est pas valide dans la balise XML spécifiée (par exemple l'attribut formatCode pour tous les champs de date).
151	Échec de la condition C001	La condition C001 n'est pas satisfaite.
152	Échec de la condition C002	La condition C002 n'est pas satisfaite.
153	Échec de la condition C003	La condition C003 n'est pas satisfaite.
154	Échec de la condition C004	La condition C004 n'est pas satisfaite.
155	Échec de la condition C005	La condition C005 n'est pas satisfaite.
156	Échec de la condition C006	La condition C006 n'est pas satisfaite.
157	Échec de la condition C007	La condition C007 n'est pas satisfaite.
158	Échec de la condition C008	La condition C008 n'est pas satisfaite.
159	Échec de la condition C009	La condition C009 n'est pas satisfaite.
160	Échec de la condition C010	La condition C010 n'est pas satisfaite.
181	Échec de la règle R001	La règle R001 n'est pas satisfaite.
182	Échec de la règle R002	La règle R002 n'est pas satisfaite.

Code	*Nom*	*Description*
188	Échec de la règle R008	La règle R008 n'est pas satisfaite.
190	Échec de la règle R010	La règle R010 n'est pas satisfaite.
200	État non valide	L'état d'un objet interne n'est pas valide et aucun détail supplémentaire n'est disponible pour 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 garantie ou 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 disponible pour 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.
307	Déclaration non trouvée	La déclaration n'a pas été trouvée dans la base de données.
308	Informations sur le transfert du message non trouvées	Le système international eTIR n'a pas trouvé de destinataire à qui transférer le message.
320	Non-correspondance titulaire/garantie	La valeur d'identification du titulaire et la valeur de référence de la garantie ne correspondent pas à ce qui est enregistré dans la base de données.

Code	*Nom*	*Description*
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 chaîne de garantie/garantie	La valeur du code de la chaîne de garantie et la valeur de référence de la garantie ne correspondent pas à ce qui est enregistré dans la base de données.
332	Non-correspondance type de 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.
333	Référence à la déclaration non trouvée	La valeur FunctionalReferenceID ne correspond pas à ce qui est enregistré dans la base de données.
334	Déclaration déjà annulée	La déclaration n'a pas pu être modifiée parce qu'elle a déjà été annulée.
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.
500	Erreur de traitement de la déclaration en douane	Le message n'a pas été accepté par les douanes et on ne dispose d'aucune autre information sur cette erreur.
501	Renseignements anticipés TIR non acceptés	Les douanes n'ont pas accepté les renseignements anticipés TIR
502	Renseignements anticipés rectifiés non acceptés	Les douanes n'ont pas accepté les renseignements anticipés rectifiés

25. 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[6].

Tableau 12
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
107	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

[6] 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*
108	X			X	X	X	X				X				X	X	X
109	X			X	X	X	X				X				X	X	X
120	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
151				X				X							X	X	
152				X											X	X	
153				X				X							X	X	
154				X				X							X	X	
155				X				X							X	X	
156																	
157															X		X
158				X													
159																X	
160								X								X	
181				X				X							X	X	
182				X				X							X	X	
188				X				X							X	X	
190									X							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										
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

Code d'erreur	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
303	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
304				X	X	X	X								X		
305				X	X	X	X								X		
306					X	X	X										
307				X													
308															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					
333																X	X
334																X	X
400	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
500															X	X	X
501															X		
502																X	

26. 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 13
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 leur envoyant le contenu du message communiqué, l'horodatage et la marche à suivre pour reproduire ce problème afin de le régler.**
101	Champ 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	Domaine non valide pour la valeur	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 de codes correspondante.
103	Format de date non conforme	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 au modèle et que la valeur de l'attribut formatCode est correcte.

Code	*Nom*	*Mesures recommandées*
104	Valeur non entière	Vérifiez les paramètres qui doivent être exprimés par des nombres entiers. Pour chacun, assurez-vous que la valeur est bien un nombre entier.
105	Longueur de la valeur du champ dépassée	Vérifiez la longueur de la valeur du paramètre. Assurez-vous que la longueur de chaque 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 aux exigences définies pour cet attribut dans la définition du schéma XML du message.
107	Champ non valide	Vérifiez l'élément spécifié ; il se peut qu'il ne corresponde pas à l'ordre défini dans la définition du schéma XML du message.
108	Attribut XML manquant	Vérifiez que toutes les balises XML contiennent l'attribut requis ; en particulier, toutes les dates doivent contenir l'attribut formatCode pour préciser dans quel format la date est envoyée.
109	Attribut XML non valide	Vérifiez que toutes les valeurs des attributs des balises XML correspondent à la liste de codes spécifiée, en particulier la valeur de l'attribut formatCode pour les dates, qui peut seulement être « 102 » ou « 208 ».
120	Version des spécifications eTIR non valide	Vérifiez que votre système d'information, ainsi que la valeur des champs de métadonnées des messages, sont conformes à la dernière version du système international eTIR et des spécifications eTIR.
151	Échec de la condition C001	Vérifiez les paramètres imposés par la condition C001 et assurez-vous que leurs valeurs 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 leurs valeurs sont conformes au pseudo-code de la condition.
153	Échec de la condition C003	Vérifiez les paramètres imposés par la condition C003 et assurez-vous que leurs valeurs 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 leurs valeurs 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 leurs valeurs sont conformes au pseudo-code de la condition.
156	Échec de la condition C006	Vérifiez les paramètres imposés par la condition C006 et assurez-vous que leurs valeurs sont conformes au pseudo-code de la condition.
157	Échec de la condition C007	Vérifiez les paramètres imposés par la condition C007 et assurez-vous que leurs valeurs 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 leurs valeurs sont conformes au pseudo-code de la condition.
159	Échec de la condition C009	Vérifiez les paramètres imposés par la condition C009 et assurez-vous que leurs valeurs sont conformes au pseudo-code de la condition.
160	Échec de la condition C010	Vérifiez les paramètres imposés par la condition C010 et assurez-vous que leurs valeurs sont conformes au pseudo-code de la condition.
181	Échec de la règle R001	Vérifiez les paramètres imposés par la règle R001 et assurez-vous que leurs valeurs respectent les conditions fixées par la règle.
182	Échec de la règle R002	Vérifiez les paramètres imposés par la règle R002 et assurez-vous que leurs valeurs respectent les conditions fixées par la règle.

Code	*Nom*	*Mesures recommandées*
188	Échec de la règle R008	Vérifiez les paramètres imposés par la règle R008 et assurez-vous que leurs valeurs respectent les conditions fixées par la règle.
190	Échec de la règle R010	Vérifiez les paramètres imposés par la règle R010 et assurez-vous que leurs valeurs 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 est conforme 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 la garantie.
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 la garantie.
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'informations sur 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 sur la 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-vous que 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 envoyé et 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-vous que 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'opération déjà enregistré	Vérifiez l'identifiant du message et assurez-vous qu'il n'entre pas en conflit avec un autre identifiant d'opération.
215	Séquence de l'opération déjà enregistrée	Vérifiez le numéro de séquence de la dernière opération pour ce transport et incrémentez-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 encore été reçue. Assurez-vous que ce message est envoyé selon l'ordre prévu et vérifiez les valeurs définies dans ses paramètres.
299	Message doublonné	Vérifiez le message déjà envoyé à ce point de terminaison, car ce message a déjà été reçu par le système international eTIR.
300	Opération non valide	Vérifiez le contenu du message, car il a généré une erreur technique d'origine inconnue dans le système international eTIR.

Code	*Nom*	*Mesures recommandées*
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 non trouvée	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.
303	Type de garantie non trouvé	Vérifiez la valeur du type de garantie dans le message et assurez-vous qu'elle se trouve 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 non trouvé	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 la liste 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 la liste des codes de type de contrôle (CL25).
307	Déclaration non trouvée	Vérifiez la valeur de l'identifiant de référence de déclaration dans le message et assurez-vous qu'elle correspond à la valeur reçue dans les messages précédents.
308	Informations sur le transfert du message non trouvées	Vérifiez que les renseignements anticipés soumis sont corrects. Si l'erreur subsiste, 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.
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 du carnet et son statut en utilisant le message d'information eTIR « I3 − Obtenir des informations sur le titulaire », 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 le cas, vérifiez le statut du titulaire du carnet en utilisant le message d'information eTIR « I3 − Obtenir des informations sur le titulaire », les services Web ITDB ou l'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 du carnet en utilisant le message d'information eTIR « I3 − Obtenir des informations sur le titulaire », les services Web ITDB ou l'application Web ITDB.
333	Référence à la déclaration non trouvée	Vérifiez la valeur de l'identifiant de référence du message contenant les renseignements anticipés que vous souhaitez annuler. Si le précédent message a été envoyé directement au système douanier national, il ne peut pas être annulé au moyen du mécanisme de transfert du système international eTIR.
334	Déclaration déjà annulée	Vérifiez la valeur de l'identifiant de référence de renseignements anticipés que vous souhaitez annuler. Il se peut que cet identifiant ait déjà été annulé.
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 chaîne de 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.

Code	*Nom*	*Mesures recommandées*
332	Non-correspondance type de 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.**
500	Erreur de traitement de la déclaration en douane	Contactez les autorités douanières compétentes pour demander des informations complémentaires sur le refus des renseignements anticipés.
501	Renseignements anticipés TIR non acceptés	Vérifiez le contenu des renseignements anticipés TIR puisque certaines informations n'ont pas été acceptées par les autorités douanières. Si vous ne parvenez pas à trouver le motif du refus, contactez les autorités douanières pour demander des informations complémentaires sur le refus des renseignements anticipés TIR.
502	Renseignements anticipés rectifiés non acceptés	Vérifiez le contenu des renseignements anticipés rectifiés puisque certaines informations n'ont pas été acceptées par les autorités douanières. Si vous ne parvenez pas à trouver le motif du refus, contactez les autorités douanières pour demander des informations complémentaires sur le refus des renseignements anticipés rectifiés.

D. Fichiers XML et XSD

1. Messages eTIR sous la forme de fichiers XML

27. Les acteurs du système eTIR échangent des messages eTIR dans le format XML, conformément aux lignes directrices de l'Organisation mondiale des douanes (OMD) sur les schémas XML. Dans la mesure où les messages peuvent contenir des caractères issus de plus d'un jeu de caractères ISO-8859, l'utilisation de la norme Unicode est obligatoire ; l'encodage adopté est donc UTF-8.

28. Les classes tout comme les attributs des messages eTIR sont mis en correspondance avec des éléments XML. Par souci de conformité, les balises XML utilisées à cet effet proviennent du modèle de données de l'OMD ; elles suivent en outre la nomenclature PascalCase[7], à l'exception des abréviations, qui contiennent des majuscules (par exemple : AuthorName, RegistrationNationalityCode, ID, MIMECode).

2. Fichiers de définition du schéma XML (XSD)

29. La structure des messages eTIR est définie au moyen de fichiers de définition du schéma XML (XSD). Les dernières versions des fichiers XSD se trouvent sur le site Web du système eTIR à l'adresse suivante : https://www.etir.org/xsd-files.

30. Les fichiers XSD peuvent servir à :

- Générer des classes automatiquement, afin de mettre en œuvre facilement le point d'extrémité des services Web pour communiquer avec les systèmes d'information qui utilisent les messages eTIR. Par exemple, sous Java, on peut utiliser la bibliothèque JAXB ;
- Exécuter automatiquement une validation partielle des messages eTIR entrants pour vérifier leur structure et le format des valeurs[8]. Par exemple, sous Java, on peut utiliser la bibliothèque javax.xml.validation.Validator.

[7] Voir techterms.com/definition/pascalcase.

[8] Aucune des règles ou conditions n'étant validée en utilisant les fichiers XSD, il convient de prévoir une couche de validation pour traiter ces aspects.

31. On trouvera ci-après une brève description de tous les types de fichiers XSD :

- **Jeux de données XSD (eTIR_DataSets.xsd)** : Ils doivent contenir la définition des types XSD complexes et des types XSD simples utilisés comme types de données pour les éléments XML qui correspondent aux classes et aux attributs dans les fichiers XSD propres aux messages. Les types XSD complexes et les types XSD simples qui sont utilisés de façon répétée dans les messages doivent être regroupés sous une définition commune dans ce fichier. En procédant ainsi, on évite la répétition du code source au moment de la génération des classes ;
- **Fichiers XSD propres aux messages (eTIR_xxx.xsd)** : Ils doivent définir uniquement la structure de chaque message. Les types simples et les types complexes qui se trouvent dans différents messages sont définis dans le jeu de données XSD ;
- **Fichiers XSD de définition des listes de codes (eTIR_CodeLists.xsd)** : Ils doivent contenir la définition des listes de codes utilisées dans les attributs des messages eTIR comme types simples, et donnent la liste des valeurs applicables pour chaque liste de codes ;
- **Fichiers de métadonnées XSD (eTIR_Metadata.xsd)** : Ils doivent définir l'ensemble des classes et des attributs de métadonnées qui figurent au début de tous les messages eTIR.

32. Les conventions de dénomination suivantes doivent être respectées dans les fichiers XSD :

- **Cardinalité** : La cardinalité des champs doit être définie au moyen des attributs XML « minOccurs » et « maxOccurs », comme indiqué ci-dessous, en gardant à l'esprit que leur valeur par défaut est 1 :
  - **Répétitions de classes** : Ce critère doit être défini dans les fichiers XSD au moyen de l'attribut XML « maxOccurs » ;
  - **Caractère facultatif** : Les attributs ou classes facultatifs doivent être définis dans les fichiers XSD en fixant à zéro l'attribut XML « minOccurs » de l'élément correspondant. Lorsque cet attribut XML n'est pas utilisé, l'attribut ou la classe est obligatoire ;
- **Espaces de noms** : Chaque fichier XSD doit « importer » les espaces de noms requis, puis réutiliser les composants nécessaires en indiquant son origine (à savoir l'espace de noms) comme préfixe ;
- **Espace de noms cible** : Chaque fichier XSD est associé à un espace de noms cible distinct suivant la nomenclature « etir:xxx:vw.y », où « xxx » est le code du message eTIR, du jeu de données, des listes de codes ou des métadonnées, et « vw.y » la version des spécifications eTIR (par exemple, v4.3) ;
- **Version** : Chaque fichier XSD doit disposer d'un numéro de version suivant la nomenclature « w.y.z », où « w.y » est la version des spécifications eTIR (par exemple, v4.3) et « .z » la version du fichier XSD (par exemple, 4.3.6). Ce numéro permet de versionner correctement les versions suivantes du fichier XSD dans une même version des spécifications eTIR ;
- **Types et formats** : Les types et formats des attributs sont définis dans les types XSD simples au moyen de restrictions[9], lesquelles peuvent, par la suite, permettre à des mécanismes automatisés de valider les messages entrants en consultant le fichier XSD correspondant.

3. Attributs XML utilisés dans les attributs eTIR

33. Les attributs de types de données de base suivants n'apparaissent que dans les rapports détaillés sur les messages eTIR prévus dans les spécifications fonctionnelles eTIR ; ils

[9] Voir www.w3schools.com/xml/schema_facets.asp.

figurent dans les fichiers XSD sous la forme d'attributs XML qui caractérisent les attributs eTIR :

- **Type date/heure** : Tous les éléments XML d'horodatage doivent obligatoirement comprendre l'attribut XML « formatCode ». Les codes sont limités à 208 (CCYYMMDDHHMMSSZHHMM) et 102 (CCYYMMDD), selon l'élément XML ;
- **Type mesure** : Tous les éléments XML de mesure doivent obligatoirement comprendre l'attribut XML « unitCode ». Les codes sont repris de la liste de codes 21 (unités de mesure − Recommandation 20 de la CEE) et peuvent faire l'objet de restrictions selon l'élément XML ;
- **Type texte** : Tous les éléments XML de texte libre peuvent comprendre l'attribut XML « languageID ». Les codes sont repris de la liste de codes 20 (noms de langue − norme ISO 639-1) et, lorsque l'identifiant de la langue n'est pas utilisé, le texte est considéré comme de l'anglais.

E. Listes de codes

34. La présente section donne les détails techniques de toutes les listes de codes utilisées dans les spécifications eTIR (v4.3.0). On trouvera la liste complète des codes correspondant à toutes les listes de codes dans l'appendice qui y est consacrée, sur le site Web du système eTIR, à l'adresse suivante : https://etir.org/documentation/code-lists.

Tableau 14
Liste des listes de codes

Liste de codes	*Nom*	*Type et référence, si externe*	*Numéro de version et date de publication*
CL01	Description taille et type équipement	EDIFACT-ONU 8155	D.21A, le 10/06/2021
CL02	Rôle partie	EDIFACT-ONU 3035	D.21A, le 10/06/2021
CL03	Identification type objet	EDIFACT-ONU 7143	D.21A, le 10/06/2021
CL04	Nom pays	ISO 3166-1 alpha-2	ISO 3166-1:2020
CL05	Description moyen transport	Recommandation 28 de la CEE	Révision 4.2 en 2018
CL06	Nom document	EDIFACT-ONU 1001	D.21A, le 10/06/2021
CL07	Description type emballage	Recommandation 21 de la CEE	Révision 11 en 2020
CL08	Type scellement	Interne	4.3.0, le 15/09/2021
CL09	Type réponse	Interne	4.3.0, le 15/09/2021
CL10	Supprimée	s.o.	s.o.
CL11	Supprimée	s.o.	s.o.
CL12	Type garantie	Interne	4.3.0, le 15/09/2021
CL13	Supprimée	s.o.	s.o.
CL14	Supprimée	s.o.	s.o.
CL15	Supprimée	s.o.	s.o.
CL16	Fonction message	EDIFACT-ONU 1225	D.21A, le 10/06/2021

Liste de codes	*Nom*	*Type et référence, si externe*	*Numéro de version et date de publication*
CL17	Type modification	Interne	4.3.0, le 15/09/2021
CL18	Supprimée	s.o.	s.o.
CL19	Supprimée	s.o.	s.o.
CL20	Nom langue	ISO 639-1	ISO 639-1:2002
CL21	Unité mesure	Recommandation 20 de la CEE	Révision 16 en 2020
CL22	État garantie	Interne	4.3.0, le 15/09/2021
CL23	État titulaire	Interne	4.3.0, le 15/09/2021
CL24	Résultat contrôle	Interne	4.3.0, le 15/09/2021
CL25	Type contrôle	Interne	4.3.0, le 15/09/2021
CL26	Type message	Interne	4.3.0, le 15/09/2021
CL27	Type achèvement	Interne	4.3.0, le 15/09/2021
CL28	Organisme contrôle	EDIFACT-ONU 0051	D.21A, le 10/06/2021
CL29	Nom spécifications	Interne	4.3.0, le 15/09/2021
CL30	Version spécifications	Interne	4.3.0, le 15/09/2021
CL31	Rôle bureau douane	Interne	4.3.0, le 15/09/2021
CL99	Erreur	Interne	4.3.0, le 15/09/2021

F. Menaces visant la sécurité de l’information et mesures d’atténuation

35. On trouvera dans le tableau suivant une liste des menaces courantes pour la sécurité de l’information qui concernent le système international eTIR, ainsi qu’une série de mesures et de contrôles de sécurité mis en place afin d’atténuer la probabilité que ces menaces se réalisent ainsi que leurs effets potentiels.

Tableau 15
Menaces visant la sécurité de l’information et mesures d’atténuation

Menace	*Description*	*Mesures d’atténuation*
Menace persistante avancée	Une menace persistante avancée est une entité, généralement un État-nation ou un groupe agissant à l’initiative d’un État, qui, opérant dans l’ombre, obtient un accès non autorisé à un réseau informatique tout en restant indétectée pendant une longue période. Récemment, le terme s’est également appliqué à des groupes se livrant à des intrusions ciblées de grande envergure en leur nom propre et dans un but précis.	Suivre toutes les mesures décrites dans la partie consacrée à la sécurité du système eTIR ; améliorer et renforcer continuellement les mesures et les contrôles de sécurité.

Menace	*Description*	*Mesures d'atténuation*
Exécution de code arbitraire	L'exécution de code arbitraire représente la capacité qu'a un cybercriminel d'exécuter des commandes ou un code arbitraires sur un appareil cible ou dans un processus cible.	Éviter le téléchargement et l'exécution de logiciels malveillants dans le système international eTIR, en analysant les pièces jointes (aux messages eTIR) à l'aide de programmes antivirus.
Injection de code	Une attaque par injection de code consiste à exploiter un bogue informatique provoqué par le traitement de données non valides. L'injection est utilisée par un cybercriminel pour introduire (ou « injecter ») un code dans un programme informatique vulnérable et en modifier l'exécution.	Appliquer aux messages eTIR plusieurs couches de validation pour empêcher l'injection de données non valides ou de code non autorisé.
Déni de service	Une attaque par déni de service est une attaque électronique perpétrée en vue de rendre inaccessible un serveur ou une ressource en réseau en interrompant temporairement ou indéfiniment les services d'un hôte connecté à Internet.	L'utilisation de listes blanches d'adresses IP empêche toutes les sources (à l'exception des sources autorisées) d'accéder aux services en ligne du système international eTIR. De plus, en prévoyant des procédures de secours fonctionnelles, on réduit les effets potentiels d'une interruption du système.
Déni de service distribué	Une attaque par déni de service distribué est une attaque par déni de service provenant de nombreuses sources différentes.	Suivre les mêmes mesures que pour les attaques par déni de service.
Écoute de réseau	L'écoute de réseau est une attaque visant une couche réseau, qui vise à intercepter sur un réseau de petits paquets de données transmis par d'autres ordinateurs et à parcourir ces données à la recherche d'informations de tous types.	Utiliser la dernière version du protocole de chiffrement TLS (Transport Layer Security) pour éviter la divulgation non autorisée d'informations échangées lors de la transmission de messages eTIR, qui entraînerait une violation de confidentialité.
Réaffectation de privilèges	La réaffectation de privilèges consiste à exploiter un bogue ou une erreur de conception ou de configuration dans un système d'exploitation ou une application, afin d'obtenir un droit d'accèsà des ressources qui sont en principe inaccessibles aux applications et aux utilisateurs. En ajoutant ainsi, dans une application, des niveaux de privilège qui n'ont pas été prévus par les développeurs ou les administrateurs du système, on peut faire exécuter des actions non autorisées à l'application concernée.	Appliquer régulièrement aux systèmes d'exploitation, aux logiciels médiateurs et aux bibliothèques utilisés par le système international eTIR les correctifs disponibles. Réduire la surface d'attaque en désactivant les services non utilisés et en configurant correctement ceux qui le sont.
Logiciel rançonneur	Les logiciels rançonneurs sont des logiciels malveillants dont les utilisateurs se servent pour chiffrer les données d'une victime et lui offrir de les lui restituer contre rançon. Chiffrer les données essentielles d'un utilisateur ou d'une organisation permet de lui interdire l'accès à ses fichiers, bases de données ou applications. Le rétablissement de l'accès est conditionné au versement d'une rançon.	Installer le système international eTIR dans une zone de réseau séparée du réseau local (LAN). Effectuer régulièrement des copies de sauvegarde des emplacements de stockage afin de réduire les effets que pourrait avoir toute attaque réussie.
Ingénierie sociale	L'ingénierie sociale consiste à manipuler des gens pour leur faire exécuter certains actes ou divulguer des informations confidentielles.	Organiser des formations obligatoires sur la sécurité de l'information à l'intention de tous les membres du personnel de la CEE, et des formations avancées pour les experts en informatique et les membres du personnel qui ont la charge de systèmes sécurisés.

Menace	*Description*	*Mesures d'atténuation*
Bogue informatique	Un bogue informatique est une erreur, une imperfection ou un défaut dans un programme ou un système informatique qui entraîne un résultat inattendu ou un comportement imprévu.	Prendre des mesures préventives pendant le cycle de développement du logiciel pour garantir une qualité et une fiabilité élevées du système international eTIR (analyse statique de code, tests automatisés, chaîne d'intégration continue, etc.)
Accès non autorisé	S'entend du cas où une personne obtient, sans permission, un accès logique ou physique à un réseau, un système, une application, des données ou d'autres ressources.	Adopter une approche de la sécurité physique et logicielle et de la sécurité des réseaux qui soit fondée sur des couches multiples. Restreindre l'accès aux serveurs à un nombre limité de membres du personnel de la CEE.
Vulnérabilité	Une vulnérabilité est une faille qui peut être exploitée par une personne malveillante pour exécuter des actions non autorisées dans un système informatique.	Utiliser des outils de vérification pour évaluer périodiquement les vulnérabilités connues dans les composants logiciels du système international eTIR. Appliquer régulièrement aux systèmes d'exploitation, aux logiciels médiateurs et aux bibliothèques utilisés par le système international eTIR les correctifs disponibles afin d'éliminer ces vulnérabilités.
Attaque zero-day	Une attaque zero-day consiste à exploiter une faille qui est soit inconnue de tous sauf du cybercriminel, soit connue seulement d'un nombre de personnes restreint.	Supprimer ou désactiver les protocoles et les services non nécessaires, pour réduire la surface d'attaque, et configurer correctement les appareils du réseau (pare-feu, système de détection des intrusions, système de prévention des intrusions) afin de prévenir, de détecter et de bloquer les éventuelles attaques.