
**Perception de télépéage — Cadre de
sécurité**

Electronic fee collection — Security framework

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO 19299:2020](https://standards.itih.ai/catalog/standards/iso/3f0feff2-2a0a-4898-8729-c56f6dfa2f3b/iso-19299-2020)

<https://standards.itih.ai/catalog/standards/iso/3f0feff2-2a0a-4898-8729-c56f6dfa2f3b/iso-19299-2020>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 19299:2020

<https://standards.iteh.ai/catalog/standards/iso/3f0feff2-2a0a-4898-8729-c56f6dfa2f3b/iso-19299-2020>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2020

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos.....	v
Introduction.....	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	2
4 Termes abrégés	3
5 Modèle de confiance	5
5.1 Vue d'ensemble.....	5
5.2 Relations de confiance entre les parties prenantes.....	5
5.3 Modèle de confiance technique.....	6
5.3.1 Généralités.....	6
5.3.2 Modèle de confiance pour les relations entre le perceuteur de péage (TC) et le prestataire de services de péage (TSP).....	6
5.3.3 Modèle de confiance pour les relations entre le prestataire de services de péage (TSP) et l'utilisateur du service (SU).....	7
5.3.4 Modèle de confiance pour les relations du gestionnaire de l'interopérabilité (IM).....	8
5.4 Mise en œuvre.....	8
5.4.1 Instauration des relations de confiance.....	8
5.4.2 Renouvellement et révocation des relations de confiance.....	9
5.4.3 Émission et révocation des certificats de l'autorité de certification (CA) subordonnée et d'entité finale.....	9
5.4.4 Profil et format de certificat et de liste de révocation de certificats (CRL).....	10
5.4.5 Extensions de certificat.....	10
6 Exigences relatives à la sécurité	11
6.1 Généralités.....	11
6.2 Système de management de la sécurité de l'information (ISMS).....	12
6.3 Interfaces de communication.....	13
6.4 Stockage des données.....	13
6.5 Perceuteur de péage.....	14
6.6 Prestataire de services de péage.....	16
6.7 Gestionnaire de l'interopérabilité (IM).....	18
6.8 Limitation des exigences.....	19
7 Mesures de sécurité — Contre-mesures	19
7.1 Vue d'ensemble.....	19
7.2 Mesures de sécurité générales.....	19
7.3 Mesures de sécurité relatives aux interfaces de communication.....	20
7.3.1 Généralités.....	20
7.3.2 Interface DSRC-EFC.....	21
7.3.3 Interface CCC.....	22
7.3.4 Interface LAC.....	23
7.3.5 Interface entre le système frontal et le système dorsal du prestataire de services de péage (TSP).....	23
7.3.6 Interface entre le TC et le TSP.....	24
7.3.7 Interface ICC.....	25
7.4 Mesures de sécurité de bout en bout.....	26
7.5 Mesures de sécurité relatives au prestataire de services de péage (TSP).....	28
7.5.1 Mesures de sécurité relatives au système frontal.....	28
7.5.2 Mesures de sécurité relatives au système dorsal.....	28
7.6 Mesures de sécurité relatives au perceuteur de péage (TC).....	29
7.6.1 Mesures de sécurité relatives à l'équipement au sol (RSE).....	29
7.6.2 Mesures de sécurité relatives au système dorsal.....	30

7.6.3	Autres mesures de sécurité relatives au perceuteur de péage (TC).....	31
8	Spécifications de sécurité relatives à la mise en œuvre d'une interface interopérable.....	31
8.1	Généralités.....	31
8.1.1	Sujet.....	31
8.1.2	Signature et algorithmes de hachage.....	31
8.2	Spécifications de sécurité relatives à l'interface DSRC-EFC.....	31
8.2.1	Sujet.....	31
8.2.2	OBE.....	31
8.2.3	RSE.....	32
9	Gestion de clés.....	32
9.1	Vue d'ensemble.....	32
9.2	Clés asymétriques.....	32
9.2.1	Échange de clés entre les parties prenantes.....	32
9.2.2	Génération et certification de clés.....	32
9.2.3	Protection des clés.....	33
9.2.4	Application.....	33
9.3	Clés symétriques.....	33
9.3.1	Généralités.....	33
9.3.2	Échange de clés entre les parties prenantes.....	34
9.3.3	Cycle de vie des clés.....	34
9.3.4	Stockage et protection de clé.....	36
9.3.5	Clés de session.....	36
	Annexe A (normative) Profils de sécurité.....	37
	Annexe B (normative) Formulaire de déclaration de conformité de mise en œuvre (ICS).....	42
	Annexe C (informative) Objectifs des parties prenantes et exigences génériques.....	61
	Annexe D (informative) Analyse des menaces.....	66
	Annexe E (informative) Politiques de sécurité.....	132
	Annexe F (informative) Exemple de politique de sécurité d'un service européen de télépéage (SET).....	139
	Annexe G (informative) Recommandations relatives à une mise en œuvre axée sur la vie privée.....	141
	Bibliographie.....	143

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 204, *Systèmes de transport intelligents*, en collaboration avec le comité technique CEN/TC 278, *Systèmes de transport intelligents*, du Comité européen de normalisation (CEN) conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette première édition annule et remplace la première édition de l'ISO/TS 19299:2015 qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

- exigences et mesures de sécurité ajoutées pour l'utilisation de moyens de paiement communs selon l'ISO/TS 21193;
- mise à jour des considérations relatives à la protection des données en [Annexe G](#), afin de prendre en compte le nouveau règlement général sur la protection des données (Directive 2016/679/CE) de l'Union européenne.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Contexte du présent document

Le processus de développement d'un concept de sécurité et de sa mise en œuvre visant à protéger un système existant de perception du télépéage (EFC, Electronic Fee Collection) inclut normalement plusieurs étapes, notamment (voir [Figure 1](#)):

- la définition des objectifs de sécurité ainsi que des déclarations de politique dans le cadre d'une politique de sécurité;
- une analyse des menaces, associée à une évaluation des risques afin de définir les exigences de sécurité;
- le développement des mesures de sécurité suivies par le développement des spécifications d'essai de sécurité.

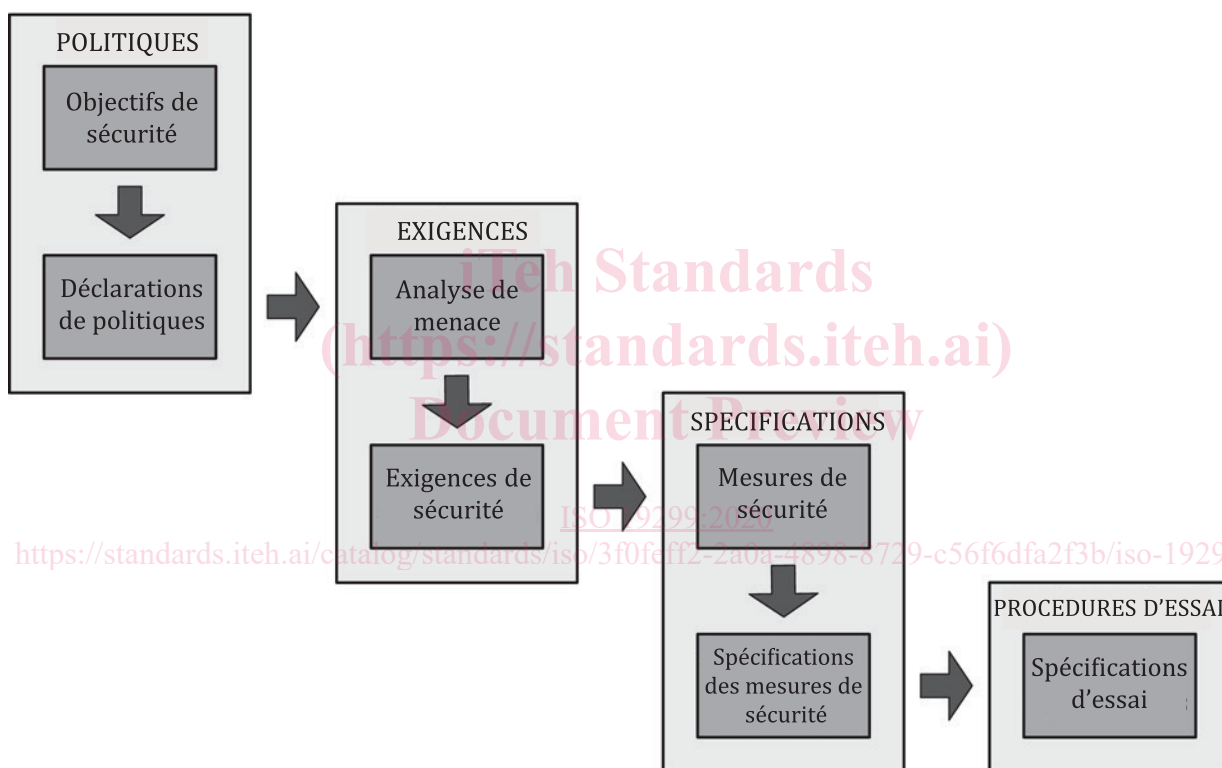


Figure 1 — Plan de développement des documents de sécurité

Chaque acteur d'un système EFC existant met en œuvre les mesures de sécurité définies et supervise leur efficacité. Lorsqu'une mesure de sécurité ne fonctionne pas correctement, un processus d'amélioration est lancé. Le développement du cadre de sécurité EFC s'attache à suivre cette approche avec les limitations suivantes:

- Il n'existe aucune politique standard de sécurité et elle ne peut pas non plus être définie: la politique de sécurité peut seulement être définie par les parties prenantes responsables, et son rayon d'action est limité par la réglementation et les lois applicables. Néanmoins, le présent document propose quelques exemples simples des politiques de sécurité possibles (de l'[Annexe E](#) à l'[Annexe F](#)).
- Aucune évaluation standard des risques n'est possible: l'évaluation des risques compare la perte possible pour la partie prenante avec les ressources nécessaires (par exemple équipement, connaissances, temps) à la réalisation d'une attaque. Dans un système réel, l'évaluation des risques repose sur l'évaluation des coûts et des avantages de chaque contre-mesure.

- Aucune conception ou configuration de système spécifique n'a été jugée universellement applicable. Seules les normes EFC de base disponibles ont été prises comme références. Les détails techniques spécifiques d'un système particulier (par exemple serveurs, centres informatiques et éléments décentralisés comme les équipements au sol) doivent être pris en considération lors de la mise en œuvre des mesures de sécurité.

La sélection des exigences et des mesures de sécurité respectives pour un système EFC existant dépend de la politique de sécurité et de l'évaluation des risques des systèmes des différentes parties prenantes. Étant donné qu'il n'existe pas de politique de sécurité générale valide et qu'aucune évaluation des risques ne peut être fournie, le cadre de sécurité EFC propose un ensemble complet (mais non exhaustif) d'exigences et de mesures de sécurité.

Pour comprendre le contenu du présent document, il convient que le lecteur ait connaissance des hypothèses méthodologiques utilisées pour son élaboration. La sécurité d'un plan EFC (interopérable) dépend de la réussite de la mise en œuvre et du bon fonctionnement de plusieurs processus, systèmes et interfaces. Seule une sécurité fiable de bout en bout garantit le fonctionnement précis et fiable des composants d'interaction des environnements de perception du télépéage. C'est pourquoi ce cadre de sécurité couvre également les systèmes ou interfaces qui ne sont pas spécifiques au concept EFC, notamment les connexions de back-office. Un cadre de sécurité indépendant de l'application pour ces parties et interfaces, un système de management de la sécurité de l'information (ISMS, Information Security Management System), peut être trouvé, par exemple, dans la série de normes ISO/IEC 27000.

Le processus d'élaboration du présent document est décrit de manière succincte ci-après:

- a) Définition des objectifs des parties prenantes et des exigences génériques qui constituent le principal motif des exigences de sécurité (voir [Annexe C](#)). Une politique de sécurité possible supportée par un ensemble de déclarations de politique est fournie à l'Annexe E, et un exemple de politique de sécurité SET (Service Européen de Télépéage) est donné à l'Annexe F.
- b) En fonction du modèle de rôle EFC et des définitions supplémentaires de la norme d'architecture EFC (ISO 17573-1), la spécification définit un modèle de système EFC abstrait comme base pour une analyse des menaces, la définition des exigences et les mesures de sécurité.
- c) Les menaces inhérentes au modèle de système EFC et à ses actifs sont analysées par deux méthodes distinctes: une analyse basée sur les attaques et une analyse basée sur les actifs. La première approche envisage plusieurs scénarios de menace du point de vue des agresseurs. La seconde approche étudie de manière approfondie les menaces à l'égard des différents actifs identifiés (corporels et incorporels). Cette approche, même si elle introduit une certaine redondance, garantit l'exhaustivité et la couverture d'un vaste éventail de risques (voir [Annexe D](#)).
- d) La spécification des exigences (voir [Article 6](#)) est basée sur les menaces identifiées à l'[Annexe D](#). Chaque exigence est au minimum motivée par une menace et au moins une exigence couvre chaque menace.
- e) La définition des mesures de sécurité (voir [Article 7](#)) propose une description générale des méthodes recommandées possibles pour couvrir les exigences élaborées.
- f) Les spécifications de sécurité relatives à la mise en œuvre d'une interface interopérable (voir [Article 8](#)) fournissent des définitions détaillées, tel que pour les authentificateurs de messages. Ces spécifications offrent une extension de sécurité aux normes d'interface applicables correspondantes.
- g) Les exigences fondamentales de gestion de clés prenant en charge la mise en œuvre des interfaces interopérables sont décrites à l'[Article 9](#). L'environnement de perception du télépéage utilise des éléments cryptographiques (par exemple clés, certificats, liste de révocation de certificats) pour prendre en charge les services de sécurité tels que la confidentialité, l'intégrité, l'authenticité et la non-répudiation. Le présent paragraphe du document couvre l'instauration (initiale) de l'échange de clés entre les parties prenantes et plusieurs procédures opérationnelles telles que le renouvellement de clés, la révocation de certificats.