NORME INTERNATIONALE

ISO 19299

Première édition
2020-08

Perception de télépéage — Cadre de sécurité

Electronic fee collection — Security framework

Numéro de référence
ISO 19299:2020(F)

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

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.

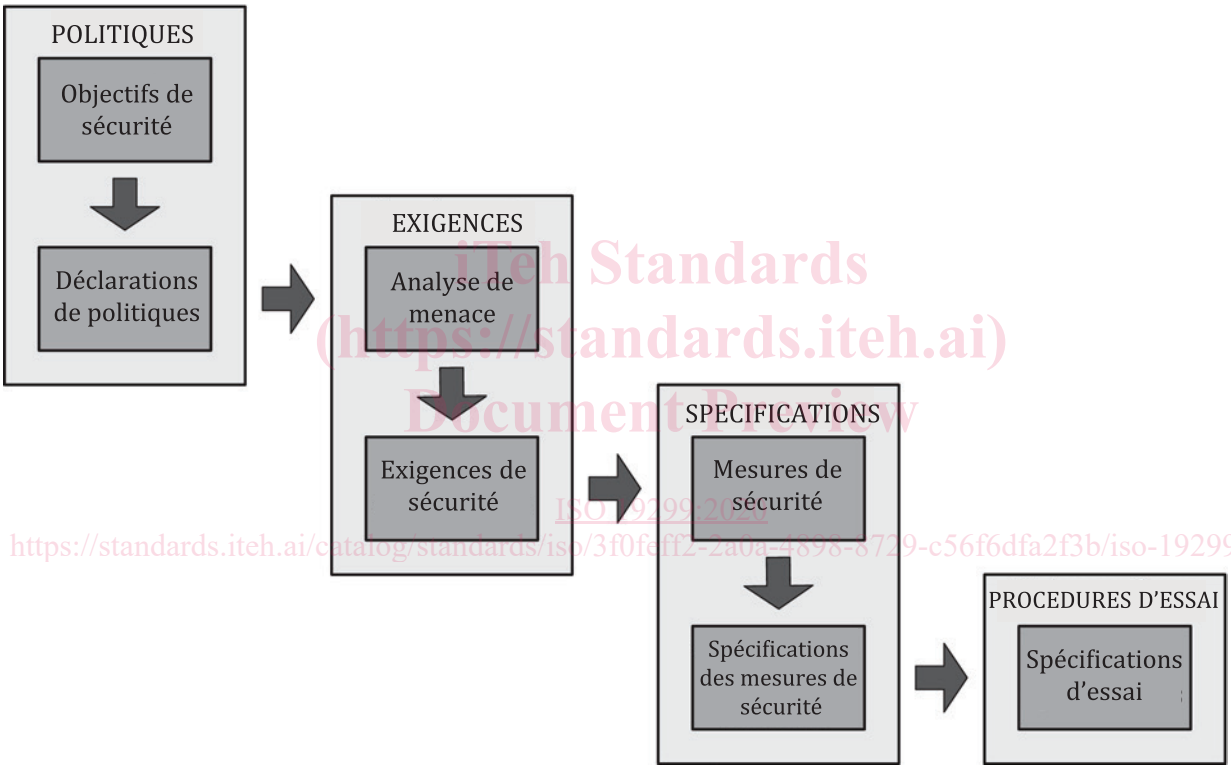

Figure 1 — Plan de développement des documents de sécurité

Chaque acteur d'un système EFC existant mets 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.