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.

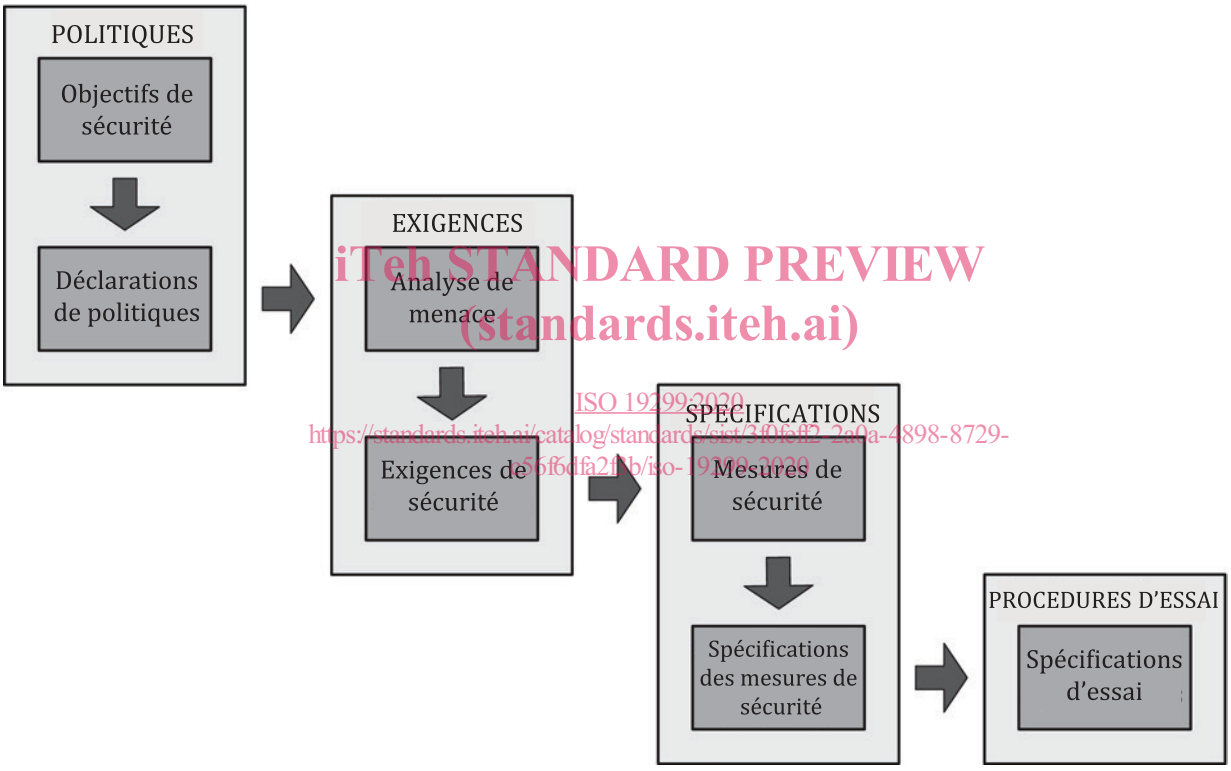

Figure 1 — Plan de développement des documents de sécurité

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.

h) Un modèle de confiance général (voir Article 5) est défini pour former la base de la mise en œuvre de procédures cryptographiques afin de garantir la confidentialité, l'intégrité et l'authenticité des données échangées. Dans ce contexte, le cadre de sécurité référence les normes internationales approuvées pour la mise en œuvre de procédures cryptographiques améliorées par des détails EFC spécifiques lorsque cela s'avère nécessaire.

Une partie prenante d'un plan EFC souhaitant utiliser ce cadre de sécurité devrait notamment:

— définir une politique de sécurité pour le plan EFC (pouvant impliquer plus d'une partie prenante dans un plan EFC interopérable). Quelques exemples de la politique de sécurité et de ses éléments sont fournis (à l'Annexe E et l'Annexe F) à titre d'aide à la conception d'un système sécurisé pour un cadre d'interopérabilité concret (y compris le service européen de télépéage [SET]);

— identifier les processus, systèmes et interfaces applicables, puis les associer au cadre de sécurité EFC;

— sélectionner les exigences de sécurité correspondantes en fonction de la politique de sécurité;

— mettre en œuvre les mesures de sécurité associées aux exigences sélectionnées;

— fournir une preuve de la conformité de ses systèmes, processus et interfaces aux exigences définies dans le présent document. La preuve peut être une autodéclaration, un audit interne ou externe, voire d'autres certifications.

Modèle de rôle EFC

Le présent document satisfait au modèle de rôle défini dans l'ISO 17573-1. Selon ce modèle de rôle, le percepteur de péage (TC, Toll Charger) gère l'infrastructure de péage ou du service de transport et est le destinataire des redevances du réseau routier. Le TC est l'acteur associé au rôle Perception du télépéage (voir Figure 2).

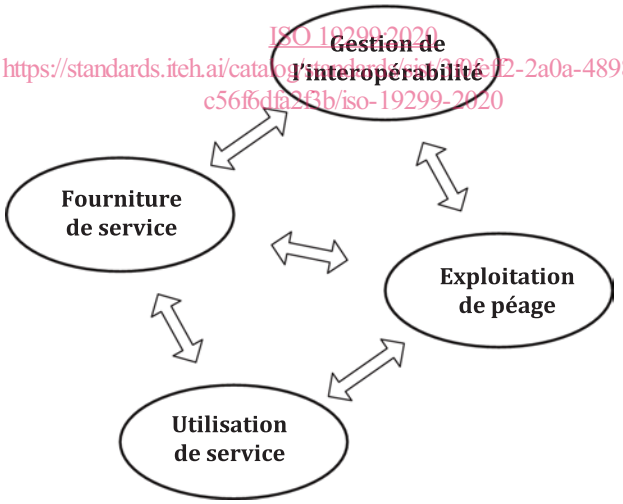

Figure 2 — Modèle de rôle sous-tendant le présent document

Les prestataires de services de péage (TSPs, Toll Service Providers) agissent en tant qu'intermédiaire entre les TC et les usagers de la route, en fournissant à ces derniers des relations contractuelles et des dispositifs (généralement des équipements embarqués (OBE, On-Board Equipment) pour interfacer le service d'infrastructure ou de transport à péage. L'OBE sera utilisé pour la collecte des données, ce qui permet au TC d'envoyer une demande au TSP en ce qui concerne l'utilisation de l'infrastructure ou du service de transport par leurs utilisateurs de services (SU, Service User). Dans les systèmes autonomes, chaque TSP fournit les déclarations de péage au TC qui exploite le système autonome. Dans les systèmes de communications dédiées à courte portée (DSRC, Dedicated Short-Range Communication), le TC reçoit les déclarations de péage principales de son propre équipement au sol (RSE, Road-Side Equipment) qui communique avec les OBE du TSP. Le rôle de gestionnaire de l'interopérabilité (IM, Interoperability

Management) représentée à la Figure 2 inclut toutes les spécifications et activités qui définissent et maintiennent un ensemble de règles gouvernant l'environnement global de perception du télépéage.

Le modèle de confiance défini dans le présent document est basé sur le modèle de rôle résumé ci-dessus et constitue également la base technique pour la protection de la communication des données entre les entités du modèle de rôle. Outre la sécurité des communications, la mise en œuvre et la gestion sécurisées du système dorsal et des autres équipements de l'infrastructure EFC sont essentiels. Un percepteur de péage (TC) ou un prestataire de services de péage (TSP) en conformité avec le présent document devrait être capable de fournir une preuve du management de la sécurité exigée. Une telle preuve constitue la base de relations de confiance entre les entités impliquées.

La Figure 3 ci-après représente le modèle de système EFC abstrait utilisé pour l'analyse des menaces, et décrit les exigences de sécurité et des mesures de sécurité associées pour le présent document. Ce document suppose qu'un OBE qui est dédié exclusivement à des fins EFC et ne s'intéresse pas aux services à valeur ajoutée basés sur un OBE EFC, et ne considère pas non plus que les plateformes OBE plus génériques (également appelées « stations STI embarquées ») pourraient être utilisées pour héberger l'application EFC. L'OBE peut soit être connecté à un compte central, soit utiliser un moyen de paiement tel qu'une carte à puce intégrée (ICC, Integrated Chip Card) ou un paiement mobile pour un système EFC à compte embarqué. Les transactions financières n'entrent pas dans le domaine d'application du présent document.

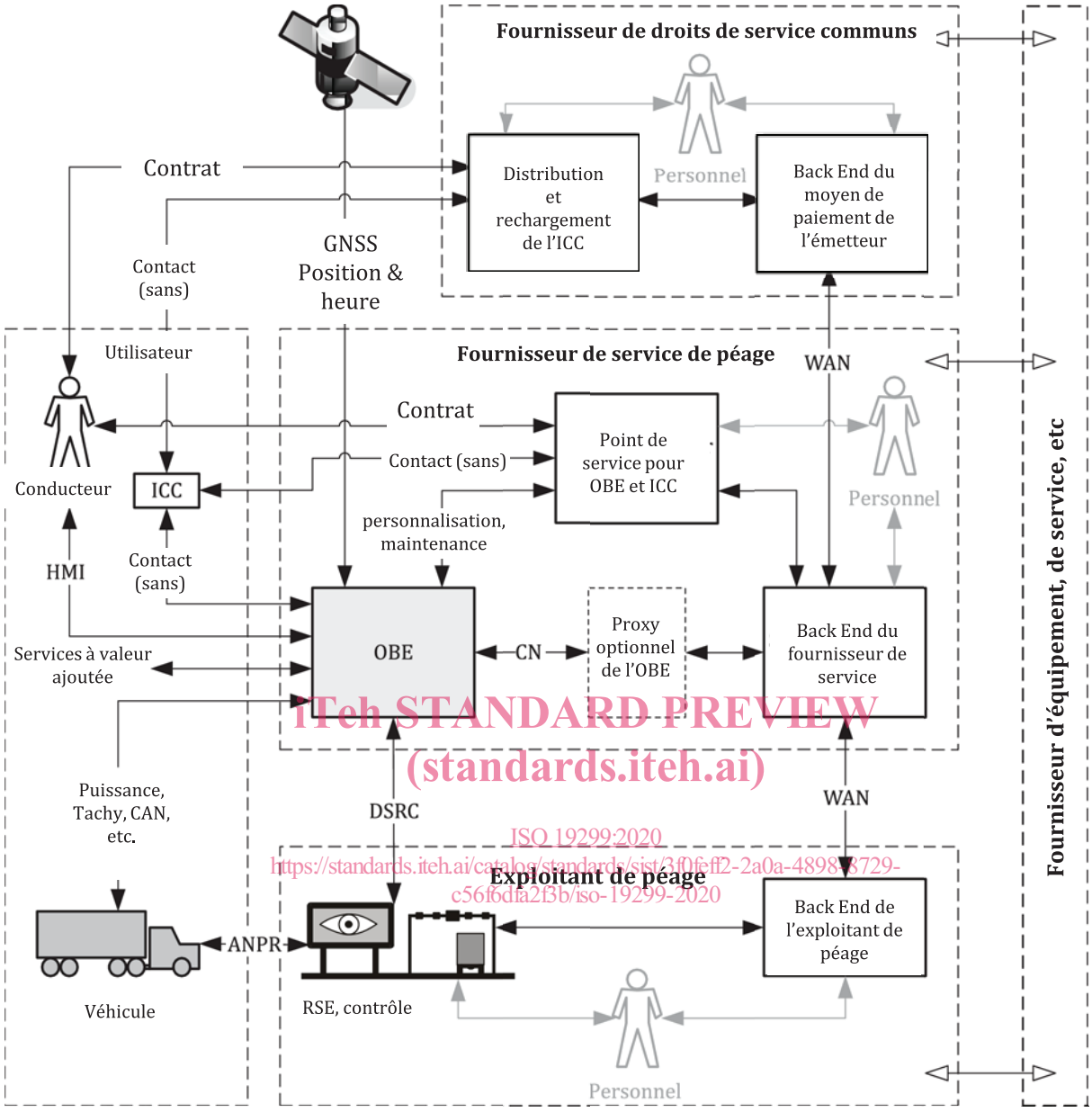

Figure 3 — Modèle de système EFC du cadre de sécurité EFC

Relation avec les autres normes de sécurité

Plusieurs normes génériques et spécifiques et Rapports techniques traitent déjà des problèmes de sécurité relatifs aux technologies de l'information. Le présent document fait usage de normes existantes et élargit leur usage aux applications EFC. Ce cadre référence et adapte les techniques et méthodologies de sécurité découlant de normes pertinentes.

La Figure 4 illustre le contexte du cadre de sécurité EFC par rapport aux normes de sécurité les plus pertinentes qui ont servi à l'élaboration du présent document. Les normes qui sont utilisées et référencées directement sont en noir.

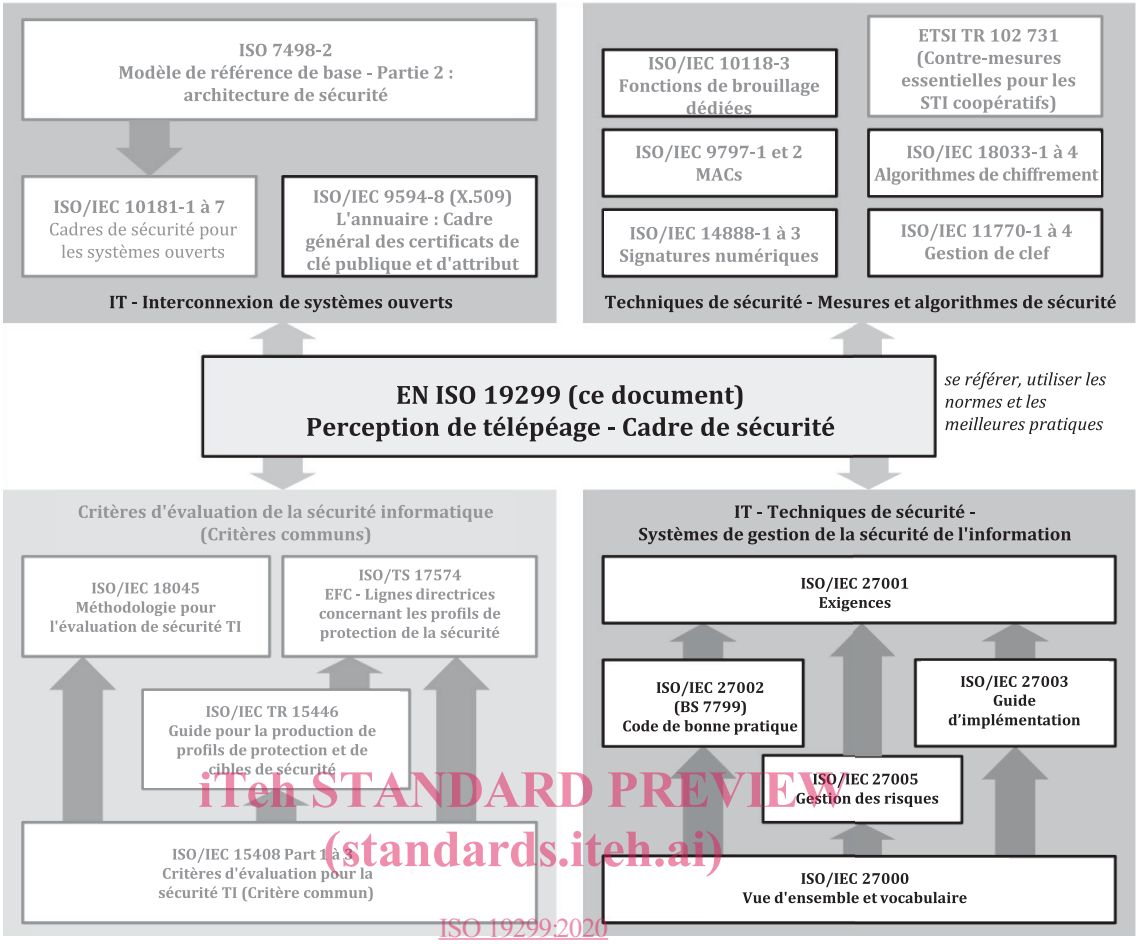

Figure 4 — Normes de sécurité pertinentes dans le contexte du cadre de sécurité EFC

Les normes illustrées à la Figure 4 sont regroupées dans les catégories suivantes, les flèches à l'intérieur de chaque groupe indiquant quelle norme sert à l'élaboration d'autres normes:

— **Techniques de sécurité – Mesures de sécurité et algorithmes**: mesures de sécurité essentielles et algorithmes cryptographiques recommandés, y compris les directives relatives à une utilisation précise.

— **Technologies de l'information – Interconnexion de systèmes ouverts (OSI)**: fournit les mécanismes utilisés pour établir des communications sécurisées entre des systèmes ouverts. Ces normes décrivent quelques-unes des exigences de sécurité dans les domaines de l'authentification et d'autres services de sécurité en proposant un ensemble de cadres.

— **Critères d'évaluation de la sécurité informatique (critères communs)**: définit des méthodologies et des processus pour l'évaluation de la sécurité et la certification de la majorité des catégories de produits utilisés dans l'environnement EFC.

— **Technologies de l'information — Techniques de sécurité — Système de management de la sécurité de l'information (ISMS)**: définit les exigences et les directives relatives à la mise en œuvre des systèmes de management de la sécurité pour tous les types d'organisations. Les normes de ce groupe conviennent aux solutions de sécurité du système dorsal et des autres équipements fixes ou installés des systèmes EFC, y compris leurs logiciels.

Il est permis d'utiliser une certification ISO/IEC 27001 d'un percepteur de péage (TC) ou d'un prestataire de services de péage (TSP) pour prouver la conformité au présent document, sous réserve que le domaine d'application et les déclarations d'applicabilité (SoA, Statement of Applicability) incluent les processus métier EFC spécifiés dans l'ISO 17573-1 et que les exigences de sécurité et leurs

mesures de sécurité associées fournies par le présent document soient appliquées, par exemple en les utilisant dans ce que l'on appelle des catalogues, c'est-à-dire des ensembles contenant les mesures de sécurité et les objectifs de contrôle. La Figure 5 ci-après montre comment cette approche fonctionne dans deux méthodes parallèles. La première partie des deux méthodes consiste à réaliser une analyse des processus métiers, suivie d'une analyse des menaces. Une analyse des risques commune combine l'analyse générique et l'analyse spécifique au système EFC (ainsi que les résultats associés) dans les mesures et les contrôles de sécurité respectifs.

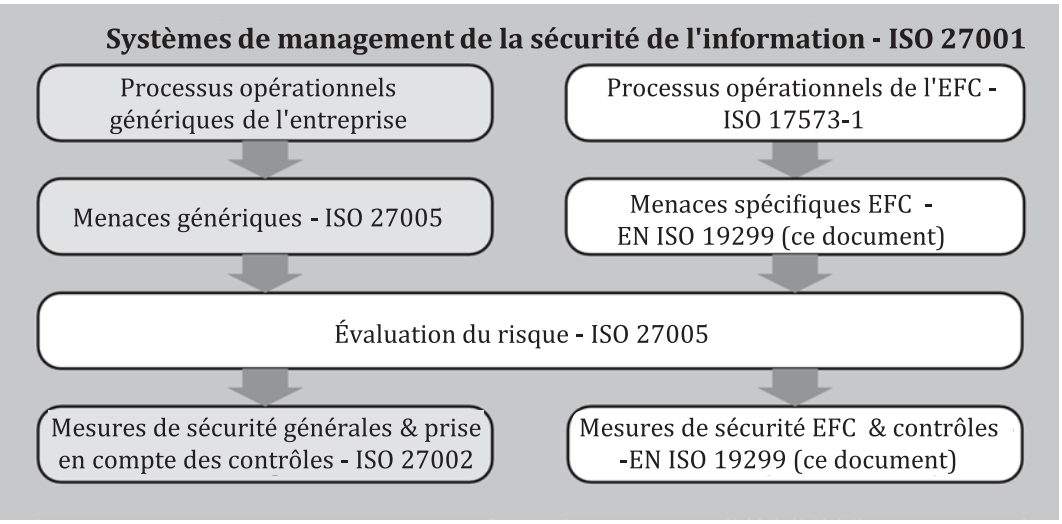

Figure 5 — Domaine d'application par rapport au système de management de la sécurité de l'information

En outre, le cadre de sécurité EFC utilise les méthodes existantes d'analyse des menaces ainsi que l'analyse des menaces existante en rapport avec l'EFC ou les STI, comme par exemple ETSI/TR 102 893.

Le présent document inclut:

— la définition d'un modèle de confiance (voir Article 5): principes et hypothèses de base pour l'établissement de relations de confiance entre les parties prenantes;

— les exigences de sécurité (voir Article 6): exigences de sécurité relatives à la prise en charge des mises en œuvre du système EFC actuel;

— les mesures de sécurité — contre-mesures (voir Article 7);

— les spécifications de sécurité relatives à la mise en œuvre d'une interface (voir Article 8): extension de sécurité aux normes EFC, comme illustré à la Figure 6;

— la gestion de clés (voir Article 9): 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;

— les profils de sécurité (voir Annexe A);

— la déclaration de conformité de la mise en œuvre (voir Annexe B): liste de contrôle devant être utilisée par un fournisseur d'équipement, un chargé de mise en œuvre d'un système ou un acteur d'un rôle pour déclarer leur conformité au présent document;

— les objectifs généraux de sécurité de l'information des parties prenantes (voir Annexe C) qui constituent le principal motif des exigences de sécurité;

— l'analyse des menaces (voir Annexe D) inhérentes au modèle de système EFC et à ses actifs en utilisant deux méthodes complémentaires distinctes, une analyse basée sur les attaques et une analyse basée sur les actifs;

— des exemples de politiques de sécurité (voir Annexe E et Annexe F);

— des recommandations pour une mise en œuvre axée sur la confidentialité (voir Annexe G).

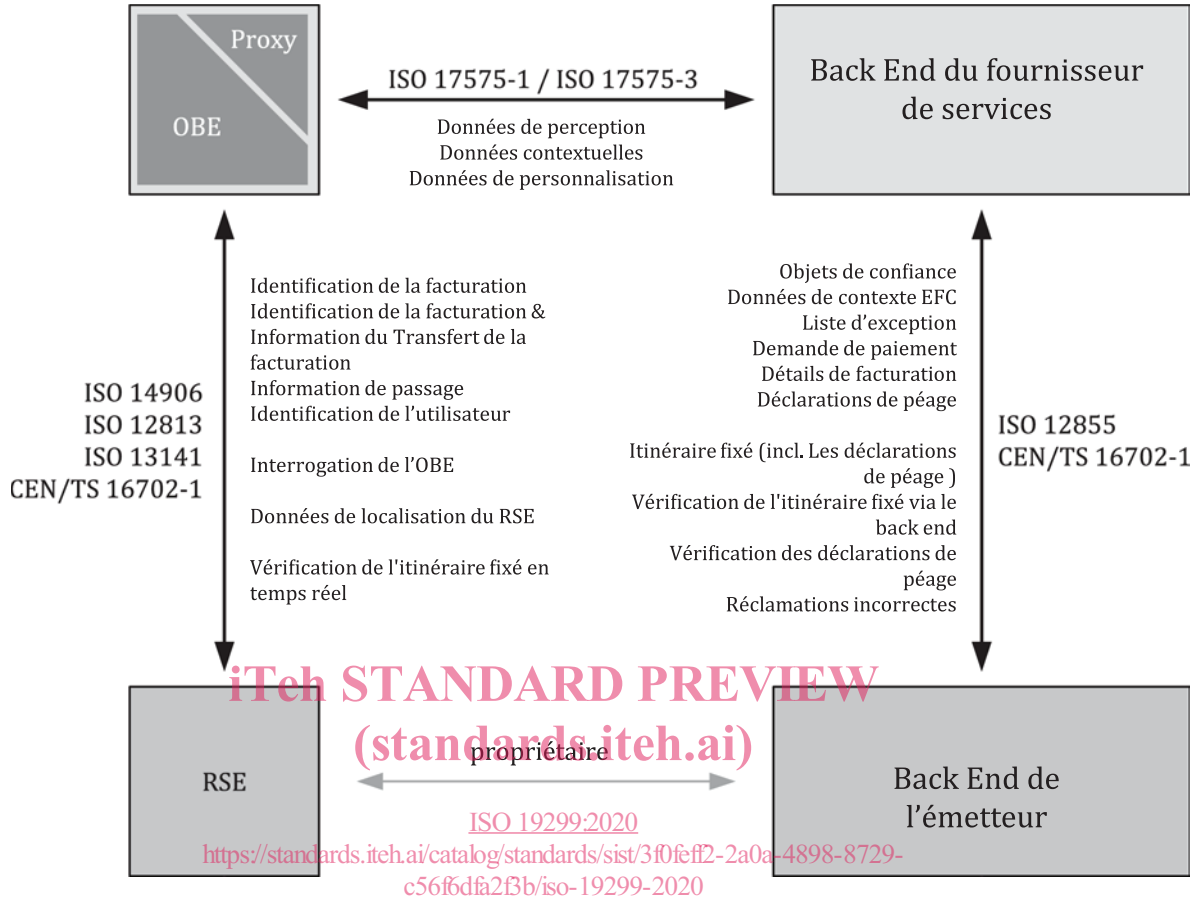

Figure 6 — Domaine d'application du cadre de sécurité EFC pour les communications sécurisées

Ce document n'englobe pas:

— une évaluation complète des risques d'un système EFC;

— les problèmes de sécurité découlant d'une application EFC s'exécutant sur une station STI;

NOTE Les problèmes de sécurité associés à une application EFC s'exécutant sur une station STI sont couverts dans la CEN/TR 16690.

— la relation de confiance technique entre le TSP et l'utilisateur du service;

— les spécifications pour la mise en œuvre de la sécurité des services EFC spécifiques tel que le Service Européen de Télépéage [SET];

— les spécifications détaillées nécessaires pour les mises en œuvre EFC respectueuses de la vie privée;

— les transactions financières éventuelles entre le prestataire de services de paiement et le moyen de paiement tel que l'ICC mis à disposition par ce dernier.

Perception de télépéage — Cadre de sécurité

1 Domaine d'application

Ce document définit un cadre de sécurité de l'information pour toutes les entités organisationnelles et techniques d'un système EFC et pour les interfaces correspondantes, sur la base de l'architecture système définie dans la norme ISO 17573-1. Le cadre de sécurité décrit un ensemble d'exigences de sécurité et de mesures de sécurité associées.

L'Annexe D contient une liste des menaces potentielles pour les systèmes EFC et une relation possible avec les exigences de sécurité définies. Ces menaces peuvent être utilisées pour une analyse des menaces afin d'identifier les exigences de sécurité pertinentes pour un système EFC.

Les mesures de sécurité pertinentes pour sécuriser les systèmes EFC peuvent ensuite être dérivées des exigences de sécurité identifiées.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 2859-1, *Règles d'échantillonnage pour les contrôles par attributs — Partie 1: Procédures d'échantillonnage pour les contrôles lot par lot, indexés d'après le niveau de qualité acceptable (NQA)*

ISO/IEC 7816-3, *Cartes d'identification — Cartes à circuit intégré — Partie 3: Cartes à contacts — Interface électrique et protocoles de transmission*

ISO/IEC 8825-1, *Technologies de l'information — Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER) — Partie 1 (disponible en anglais seulement)*

ISO/IEC 9594-8:2017, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire — Partie 8: Cadre général des certificats de clé publique et d'attribut*

ISO/IEC 9797-1:2011, *Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) — Partie 1: Mécanismes utilisant un chiffrement par blocs*

ISO/IEC 11770-1:2010, *Technologies de l'information — Techniques de sécurité — Gestion de clés — Partie 1: Cadre général*

ISO/IEC 11770-3:2015, *Technologies de l'information — Techniques de sécurité — Gestion de clés — Partie 3: Mécanismes utilisant des techniques asymétriques*

ISO 12813, *Perception de télépéage — Communication de contrôle de conformité pour systèmes autonomes*

ISO 12855, *Perception du télépéage — Échange d'informations entre la prestation de service et la perception du péage*

ISO 13141, *Perception de télépéage — Communications d'augmentation de localisations pour systèmes autonomes*

ISO 14906, *Perception du télépéage — Définition de l'interface d'application relative aux communications dédiées à courte portée*