SPÉCIFICATION TECHNIQUE

ISO/TS 19299

Première édition
2015-10-01

Perception de télépéage — Cadre de sécurité

Electronic fee collection — Security framework

Numéro de référence
ISO/TS 19299:2015(F)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 appelée 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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires.

L'ISO/TS 19299 a été élaborée par le comité européen de normalisation (CEN), en collaboration avec le comité technique CEN/TC 204, *Systèmes intelligents de transport*, conformément à l'accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette première édition de l'ISO/TS 19299 annule et remplace la CEN/TS 16439:2013.

Introduction

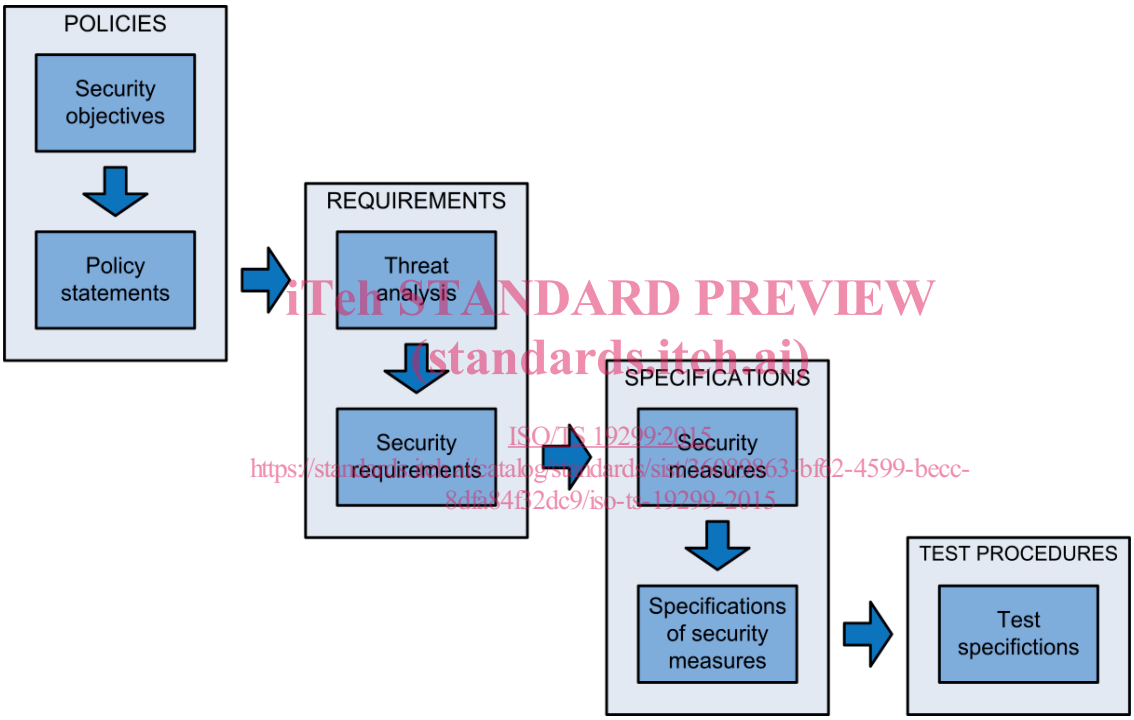
Note explicative

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:

— 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.



Anglais	Français
POLICIES	POLITIQUES
Security objectives	Objectifs de sécurité
Policy statements	Déclarations de politique
REQUIREMENTS	EXIGENCES
Threat analysis	Analyse des menaces
Security requirements	Exigences de sécurité
SPECIFICATIONS	SPECIFICATIONS
Security measures	Mesures de sécurité
Specifications of security measures	Spécifications de mesures de sécurité
TEST PROCEDURES	PROCEDURES D'ESSAI
Test specifications	Spécifications d'essai

Figure 1 — Plan de développement des documents de sécurité

Pour la deuxième étape, chaque acteur d'un système EFC existant doit mettre en œuvre les mesures de sécurité définies et superviser leur efficacité. Les mesures de sécurité ne fonctionnant pas ou fonctionnant de manière incorrecte doivent être améliorées. Le développement du cadre de sécurité EFC s'attache à suivre cette approche autant que possible. La méthodologie utilisée doit tenir compte des limitations suivantes:

— Il n'existe aucune politique de sécurité: la politique de sécurité peut seulement être définie par les parties prenantes responsables, et son rayon d'action est uniquement limité par la réglementation et les lois applicables. Néanmoins, la présente Spécification technique propose quelques exemples simples des politiques de sécurité possibles (de l'Annexe E à l'Annexe F).

— Aucune évaluation des risques n'est possible: l'évaluation des risques compare la perte possible pour la partie prenante et les ressources nécessaires (par exemple équipement, connaissances, temps, etc.) à la réalisation d'une attaque. Il s'agit d'une évaluation comparative des coûts et bénéfices de chaque contre-mesure, ce qui n'est possible que dans le cas d'un système mis en œuvre.

— Pendant le développement de la présente Spécification technique, aucune conception ou configuration système spécifique n'a été envisagée à des fins d'applicabilité à l'échelle universelle. Seules les normes EFC de base disponibles et les commentaires reçus vis-à-vis de la CEN/TS 16439:2013 (l'édition précédente du cadre de sécurité EFC) ont été pris comme références. Outre le cadre de sécurité EFC présent, 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.

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. Etant donné qu'il n'existe pas de politique de sécurité générale valide et qu'aucune évaluation des risques ne peut être fournie, la cadre de sécurité EFC propose un ensemble d'exigences et de mesures de sécurité couvrant le plus de menaces possibles, sans prétendre à l'exhaustivité.

Cependant, il existe une condition de conformité à la présente Spécification technique: si une exigence est sélectionnée, la ou les mesures de sécurité associées doivent être mises en œuvre.

Pour comprendre le contenu de la présente Spécification technique, 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 de bout en bout fiable garantit le fonctionnement précis et fiable des composants d'interaction des environnements de perception du péage. 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). Le cadre de sécurité indépendant de l'application pour ces parties et interfaces, le système de management de la sécurité de l'information (ISMS, *Information Security Management System*), est fourni dans la collection de normes ISO 2700x.

Le processus d'élaboration de la présente Spécification technique 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), 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 du point de vue des agresseurs. La seconde approche étudie de manière approfondie les menaces à l'égard des différents actifs identifiés (entités corporelles et incorporelles). Cette approche, même si elle introduit une certaine redondance, garantit l'exhaustivité et la couverture d'une gamme plus vaste 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, par exemple 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 péage utilise des éléments cryptographiques (clés, certificats, liste de révocation de certificats, etc.) pour prendre en charge les services de sécurité tels que la confidentialité, l'intégrité, l'authenticité et la non-répudiation. Le présent paragraphe de la spécification 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, etc.

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 doit 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 à l'Annexe F) à titre d'aide à l'utilisation de la présente Spécification technique pour concevoir 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;

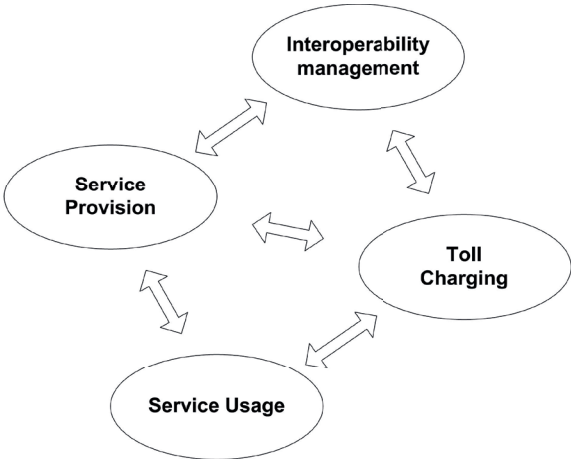
— sélectionner les exigences de sécurité correspondantes en fonction de la politique de sécurité;

— 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 la présente Spécification technique. La preuve peut être une autodéclaration, un audit interne ou externe, voire d'autres certifications.

Modèle de rôle EFC

La présente Spécification technique satisfait au modèle de rôle défini dans l'ISO 17573. Selon ce modèle de rôle, le percepteur de péage (TC, *Toll Charger*) est le fournisseur de l'infrastructure de péage ou du service de transport et ainsi le destinataire des redevances du réseau routier. Le TC est l'acteur associé au rôle Perception du péage (voir Figure 2).



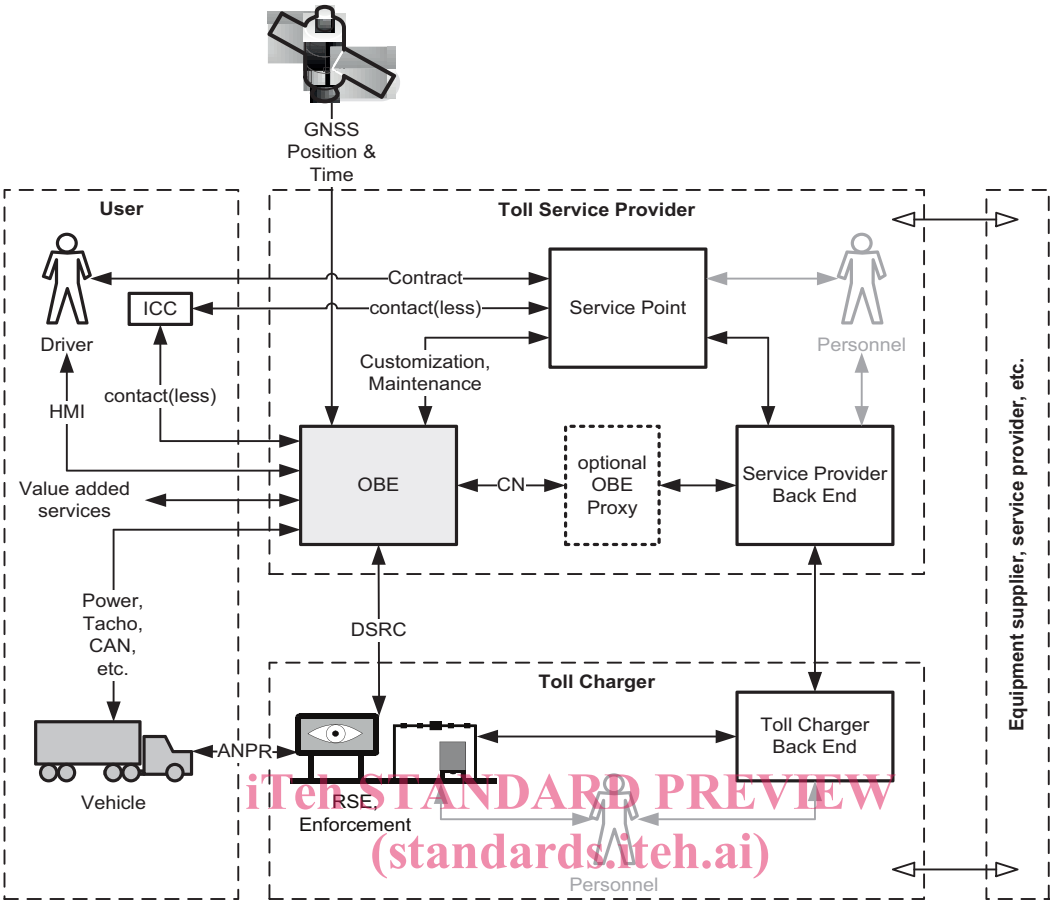
Anglais	Français
Interoperability management	Gestion de l'interopérabilité
Service provision	Fourniture du service
Toll charging	Perception du télépéage
Service usage	Utilisation du service

Figure 2 — Modèle de rôle sous-jacent de la présente Spécification technique

Les prestataires de services de péage (TSP, *Toll Service Provider*) fournissent un équipement embarqué (OBE, *On-Board Equipment*) aux utilisateurs du service d'infrastructure ou de transport à péage. Les TSP sont chargés de fournir l'OBE qui 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. Il se peut qu'un tel TC reçoive les déclarations de péage de plus d'un TSP. 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 l'OBE du TSP ainsi que les données de perception supplémentaires, si nécessaires, du TSP. La gestion de l'interopérabilité (IM, *Interoperability Management*) représentée à la Figure 2 inclut toutes les spécifications et activités qui permettent de définir et de maintenir un ensemble de règles gouvernant l'environnement global de perception du péage.

Le modèle de confiance défini dans la présente Spécification technique est basé sur le modèle de rôle 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 doivent être fiables. Un percepteur de péage (TC) ou un prestataire de services de péage (TSP) en conformité avec la présente Spécification technique doit être capable de fournir une preuve du management de la sécurité exigé. 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 la définition des exigences de sécurité et des mesures de sécurité associées pour la présente Spécification technique. La présente Spécification technique s'appuie sur la supposition d'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, ni aux plates-formes OBE plus génériques (également appelées «stations STI embarquées») 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 éventuelles transmises sur le moyen de paiement ne relèvent pas du domaine d'application de la présente Spécification technique.



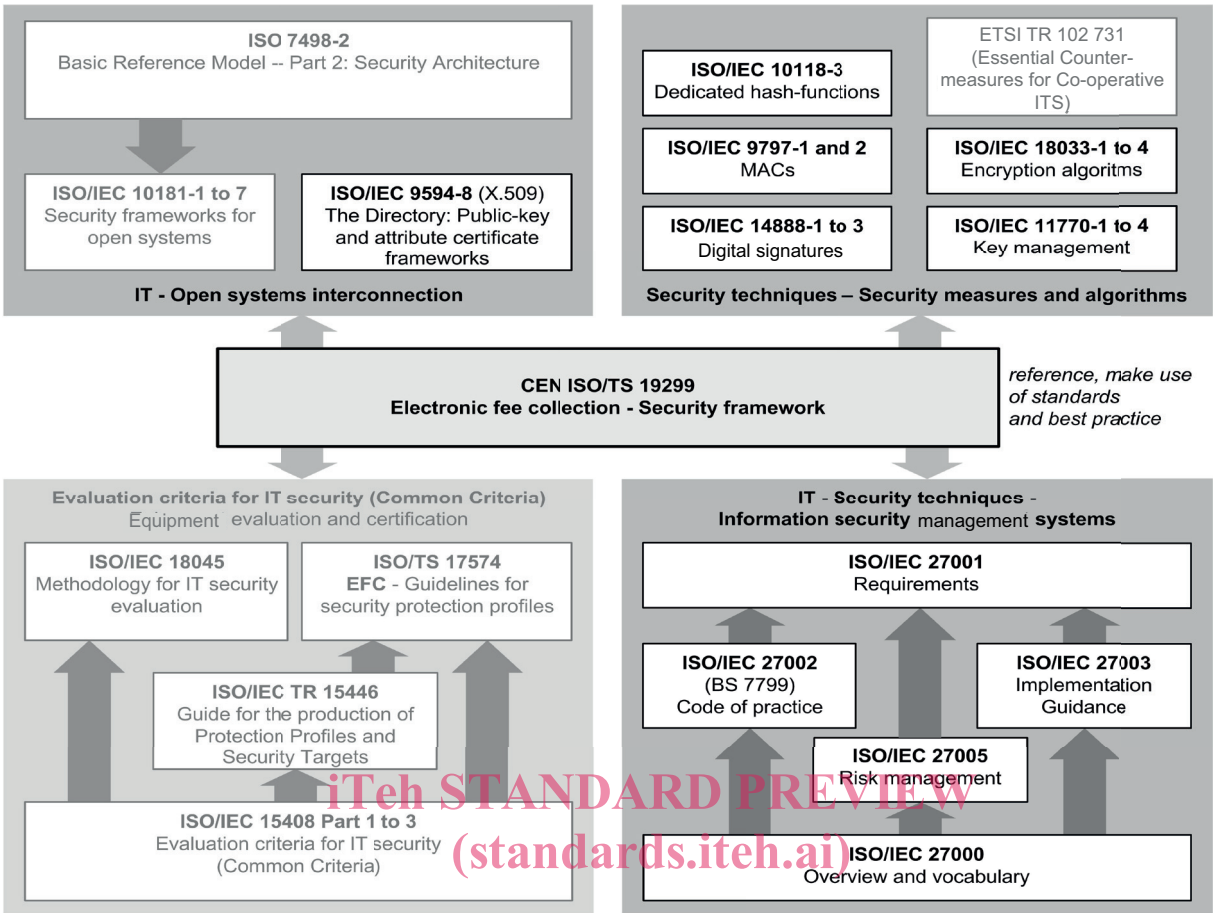
Anglais	Français
GNSS position & time	Position et heure GNSS
User	Usager
Driver	Conducteur
HMI	IHM
Contact(less)	(sans) contact
Value added services	Services à valeur ajoutée
Power, tacho, CAN, etc.	Alimentation électrique, tachygraphe, bus CAN, etc.
Vehicle	Véhicule
Toll service provider	Prestataire de services de péage
Service point	Point de service
Contract	Contrat
Contact(less)	(sans) contact
Customization, maintenance	Personnalisation, maintenance
Optional OBE proxy	Proxy OBE facultatif
Service provider back end	Système dorsal du prestataire de services
Toll charger	Percepteur de péage
RSE, enforcement	RSE, contrôle sanction
Toll charger back end	Système dorsal du percepteur de péage
Equipment supplier, service provider, etc.	Fournisseur d'équipements, fournisseur de services, etc.

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. La présente Spécification technique utilise ces normes existantes et élargit leur usage aux applications EFC. Le cadre référence et adapte les techniques et méthodologies de sécurité découlant de ces normes.

La Figure 4 représente le contexte du cadre de sécurité EFC par rapport aux autres normes de sécurité. Il ne s'agit pas d'une description exhaustive, car seules les normes les plus pertinentes sont indiquées, c'est-à-dire les normes qui ont contribué le plus à la présente Spécification technique. Les normes qui sont utilisées et référencées directement sont en noir (les autres sont en gris). Les autres normes pouvant fournir d'autres informations de sécurité sont données à titre d'information et d'exhaustivité seulement, mais ne sont pas utilisées.



Anglais	Français
IT – Open systems interconnection	Technologies de l'information – Interconnexion de systèmes ouverts (OSI)
ISO 7498-2 Basic reference Model – Part 2: Security Architecture	ISO 7498-2 Modèle de référence de base – Partie 2: Architecture de sécurité
ISO/IEC 10171-1 to 7 Security frameworks for open systems	ISO/IEC 10171-1 à 7 Cadres de sécurité pour les systèmes ouverts
ISO/IEC 9594-8 (X.509) The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8 (X.509) The Directory: Public-key and attribute certificate frameworks
Security techniques – Security measures and algorithms	Techniques de sécurité – Mesures de sécurité et algorithmes
ISO/IEC 10118-3 Dedicated hash-functions	ISO/IEC 10118-3 Dedicated hash-functions
ISO/IEC 9797-1 and 2 MACs	ISO/IEC 9797-1 et 2 MACs
ISO/IEC 14888-1 to 3 Digital signatures	ISO/IEC 14888-1 à 3 Digital signatures
ETSI/TR 102 731 (Essential Counter-measures for Co-operative ITS)	ETSI/TR 102 731 (Essential Counter-measures for Co-operative ITS)
ISO/IEC 18033-1 to 4 Encryption algorithms	ISO/IEC 18033-1 à 4 Encryption algorithms

ISO/IEC 11770-1 to 4 Key management	ISO/IEC 11770-1 à 4 Key management
CEN ISO/TS 19299 Electronic fee collection – Security framework	CEN ISO/TS 19299 Perception de télépéage – Cadre de sécurité
Reference, make use of standards and best practice	Référencement et utilisation de normes et recommandations
Evaluation criteria for IT security (common criteria) Equipment evaluation and certification	Critères d'évaluation de la sécurité informatique (critères communs) Evaluation et certification de l'équipement
ISO/IEC 18045 Methodology for IT security evaluation	ISO/IEC 18045 Methodology for IT security evaluation
ISO/TS 17574 EFC – Guidelines for security protection profile	ISO/TS 17574 EFC – Guidelines for security protection profile
ISO/IEC/TR 15446 Guide for the production of protection profiles and security targets	ISO/IEC/TR 15446 Guide for the production of protection profiles and security targets
ISO/IEC 15408 Part 1 to 3 Evaluation criteria for IT security (common criteria)	ISO/IEC 15408-1 à 3 Evaluation criteria for IT security (common criteria)
IT – Security techniques – Information security management systems	Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information
ISO/IEC 27001 Requirements	ISO/IEC 27001 Exigences
ISO/IEC 27002 (BS 7799) Code of practice	ISO/IEC 27002 (BS 7799) Code de la bonne pratique
ISO/IEC 27003 Implementation Guidance	ISO/IEC 27003 Implementation Guidance
ISO/IEC 27005 Risk management	ISO/IEC 27005 Gestion des risques
ISO/IEC 27000 Overview and vocabulary	ISO/IEC 27000 Vue d'ensemble et vocabulaire

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

Chaque groupe de normes représenté à la Figure 4 assure les fonctionnalités suivantes:

— **Techniques de sécurité — Mesures de sécurité et algorithmes**: ce groupe de normes rassemble les mesures de sécurité essentielles et les algorithmes cryptographiques recommandés, incluant également les directives relatives à une utilisation précise.

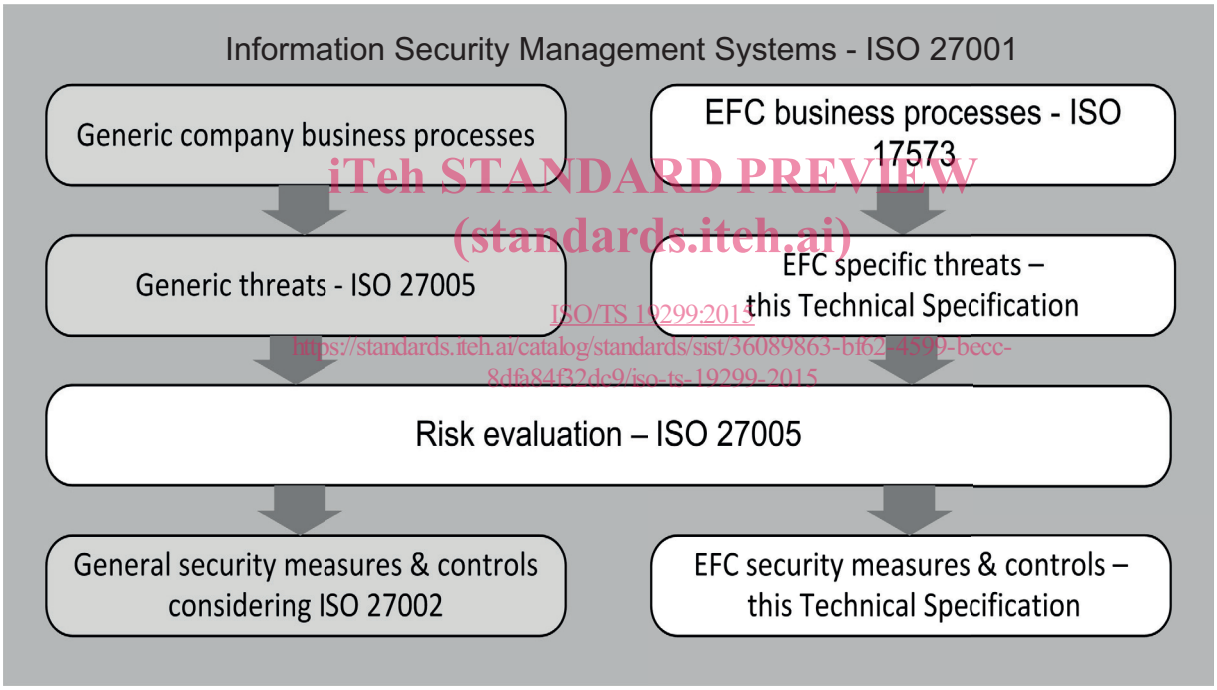
— **Technologies de l'information — Interconnexion de systèmes ouverts:** ce groupe de normes définit les mécanismes utilisés pour établir des communications sécurisées entre des systèmes ouverts. Les normes décrivent quelques-unes des exigences de sécurité dans les domaines de l'authentification et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

— **Critère d'évaluation de la sécurité informatique (critères communs):** ce groupe de normes 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. Les flèches à l'intérieur du groupe mettent en évidence la relation entre les normes dans le sens ascendant.

— **Technologies de l'information — Techniques de sécurité — Système de management de la sécurité de l'information (ISMS):** ce groupe de normes 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 conviennent parfaitement aux solutions de sécurité du système dorsal et des autres équipements fixes ou installés (y compris les logiciels des systèmes EFC).

Il est permis d'utiliser une certification ISO/IEC 27001 correspondante d'un percepteur de péage (TC) ou d'un prestataire de services de péage (TSP) pour prouver la conformité à la présente Spécification technique, 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 et que les exigences de sécurité sélectionnées et leurs mesures de sécurité associées fournies par la présente Spécification technique soient appliquées, par exemple en les utilisant dans les catalogues contenant les mesures de sécurité et les objectifs de contrôle. La Figure 5 ci-après montre comment cette approche fonctionne en parallèle. La première partie des deux méthodes consiste à analyser les processus métiers suivis 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.



Anglais	Français
Information security management systems – ISO 27001	Système de management de la sécurité de l'information – ISO 27001
Generic company business processes	Processus métier d'entreprises génériques
Generic threats – ISO 27005	Menaces génériques – ISO 27005
EFC business processes – ISO 15573	Processus métier EFC – ISO 15573
EFC specific threats – this Technical specification	Menaces spécifiques à l'EFC – la présente Spécification technique
Risk evaluation – ISO 27005	Evaluation des risques – ISO 27005
General security measures & controls considering ISO 27002	Mesures et contrôles de sécurité généraux selon l'ISO 27002

EFC security measures & controls – this Technical specification	Mesures et contrôles de sécurité EFC – la présente Spécification technique

Figure 5 — Domaine d'application relatif au système de management de la sécurité de l'information (ISMS)

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 [par exemple ETSI/TR 102 893 (systèmes de transport intelligents, sécurité, menace, vulnérabilité et analyse des risques)]