

DIN EN ISO 19299

ICS 03.220.20; 35.240.60

Entwurf

Einsprüche bis 2020-01-15
Vorgesehen als Ersatz für
DIN CEN ISO/TS 19299
(DIN SPEC 74125):2016-02

**Elektronische Gebührenerhebung –
Sicherheitsgrundstruktur;
Englische Fassung prEN ISO 19299:2019**

Electronic fee collection –
Security framework;
English version prEN ISO 19299:2019

Perception de télépéage –
Cadre de sécurité;
Version anglaise prEN ISO 19299:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-11-15 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an naautomobil@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Automobiltechnik (NAAutomobil), 10004 Berlin, Postfach 8 04 62, Behrenstr. 35, 10117 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 168 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)

Nationales Vorwort

Dieses Dokument (prEN ISO 19299:2019) wurde vom Technischen Komitee ISO/TC 204 „Intelligent Transport Systems“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“, dessen Sekretariat von NEN (Niederlande) gehalten wird, erarbeitet.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 052-00-71 GA „Gemeinschaftsarbeitsausschuss NAAutomobil/DKE: Intelligente Verkehrssysteme“ des DIN-Normenausschusses Automobiltechnik (NAAutomobil).

Dieses Dokument ist derzeit zur parallelen Abstimmung vorgelegt.

Dieser Normenentwurf dient Entwicklern von Systemen zur elektronischen Gebührenerhebung (EFC) zur Prüfung sicherheitsrelevanter Funktionen und Anforderungen. Dabei werden Angriffsmodelle sowie dazugehörige Messmethoden festgelegt. Nutzer von EFC-Schemata, die die Sicherheitsgrundstruktur verwenden wollen, müssen dabei die folgenden Aspekte beachten:

- 1) Identifizierung der notwendigen Prozesse, des Systems sowie der Schnittstellen für die Sicherheitsgrundstruktur,
- 2) Ableitung der entsprechenden Sicherheitsanforderungen nach dieser Sicherheitsstrategie,
- 3) Beweisführung, dass die entsprechenden Systeme, Prozesse und Schnittstellen konform zu den gestellten Anforderungen dieser Norm sind.

Änderungen

Gegenüber DIN CEN ISO/TS 19299 (DIN SPEC 74125):2016-02 wurden folgende Änderungen vorgenommen:

- a) Überführung in eine Europäische Norm;
- b) Ergänzung neuer Anforderungen und Securitymaßnahmen zur Nutzung gemeinschaftlicher Bezahlmedien nach ISO/TS 21193;
- c) Datenschutzüberlegungen nach Anhang G wurden überarbeitet, um das neue Gesetz der Europäischen Union zum allgemeinen Datenschutz zu berücksichtigen (Direktive 2016/679/EC).

Nationaler Anhang NA (informativ)

Begriffe

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe in ISO/IEC 7498-1:1994, ISO/IEC 10746-2, ISO/IEC 10746-3, ISO/IEC 15414 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Haftung

(en: accountability)

Eigenschaft, die sicherstellt, dass die Aktion einer Einheit einmalig für die Einheit aufgezeichnet werden kann

[QUELLE: ISO/TR 17573-2:2019¹, 3.5]

3.2

Aktivist

(en: activist)

besonders aktiver, energischer Fürsprecher eines Falles, speziell eines politischen Falls

[QUELLE: ISO/TR 17573-2:2019, 3.6]

3.3

Bestand

(en: asset)

Etwas von Wert für einen Interessensvertreter

Anmerkung 1 zum Begriff: Ein Bestand kann materiell oder immateriell sein.

[QUELLE: ISO/DTR 17573-2:2019, 3.8, Anmerkung 1 wurde ergänzt]

3.4

Angriff

(en: attack)

Versuch, zu zerstören, bloßzustellen, abzuändern, deaktivieren, stehlen oder unautorisierten Zugriff oder nicht autorisierte Nutzung von Beständen (3.3) zu erlangen

[QUELLE: ISO/DTR 17573-2:2019, 3.10]

1 Unter Vorbereitung (Stufe zum Zeitpunkt der Beantragung der DIS-Umfrage: ISO/DTR:2019 angenommen. Der finale Text wird vorbereitet)

3.5

Authentizität

(en: authenticity)

Merkmal, dass vorgibt, eine Einheit zu sein

[QUELLE: ISO/DTR 17573-2:2019, 3.15]

3.6

Verfügbarkeit

(en: availability)

Merkmal der Zugänglichkeit und Nutzbarkeit nach einer Aufforderung einer autorisierten Einheit

[QUELLE: ISO/DTR 17573-2:2019, 3.17]

3.7

Back End

Teil eines Systems einer Abrechnungsstelle, welches die Schnittstelle zu mehreren Front Ends (3.17) bildet

[QUELLE: ISO/DTR 17573-2:2019, 3.19]

3.8

Zertifikat Aufhebungsliste

(en: certificate revocation list)

unterschiedene Liste, die eine Menge von Zertifikaten anzeigt, die nicht länger Gültigkeit beim Zertifikatsnutzer haben

[QUELLE: ISO/DTR 17573-2:2019, 3.25]

3.9

Zertifikatsbehörde

CA

(en: certification authority)

Instanz, der von einer oder mehreren Instanz(en) vertraut wird(werden), zur Erstellung und Zuordnung von Zertifikaten öffentlicher Schlüssel

[QUELLE: ISO 21188:2018, 3.21]

3.10

Kommunikationsanbieter

(en: communication provider)

Anbieter von Kommunikationsübertragungsdiensten

[QUELLE: ISO/DTR 17573-2:2019, 3.40]

3.11

Vertraulichkeit

(en: confidentiality)

Schutz vor Informationslecks zu nicht autorisierten Personen, Einheiten und/oder Prozessen

[QUELLE: ISO/DTR 17573-2:2019, 3.42]

3.12

Datenschutz

Informationsschutz

(en: data privacy, information privacy)

Rechte und Verpflichtungen von Personen und Organisationen bezüglich der Sammlung, Verwendung, Speicherung, Offenlegung und Entsorgung persönlicher Informationen

[QUELLE: ISO/TR 17573-2:2019, 3.54]

3.13

Datenschutzbeauftragter

(en: data protection commissioner, data privacy commissioner)

Person, die für die Durchführung und Überwachung der Konformität mit vorhandenen Datensicherungsgesetzen verantwortlich ist

[QUELLE: ISO/DTR 17573-2:2019, 3.55]

3.14

Dateninhaltsgenehmigung

(en: data subject's consent)

freiwillig bereitgestellte spezifische und sachkundige schriftliche Wunschangabe, bei der der Dateninhalt die Zustimmung zu personenbezogenen Daten (3.31) kennzeichnet, die verarbeitet werden

3.15

digitale Signatur

(en: digital signature)

ein oder mehrere Datenelement(e) als Ergebnis des Signaturprozesses

[QUELLE: ISO/DTR 17573-2:2019, 3.58]

3.16

Vollstreckung

(en: enforcement)

Maßnahmen oder Aktionen zur Einhaltung von Gesetzen, Regulierungen oder Regeln

Anmerkung 1 zum Begriff: In diesem Zusammenhang der Prozess der zwingenden Einhaltung eines Mautregimes (3.46).

[QUELLE: ISO/DTR 17573-2:2019, 3.70, Anmerkung 1 wurde ergänzt]

3.17

ausländische Bundesbehörde

(en: foreign state agency)

Behörde eines beliebigen Staates mit Ausnahme des Staates, unter dessen Jurisdiktion ein spezifisches Mautschema (3.48) betrieben wird

[QUELLE: ISO/DTR 17573-2:2019, 3.80]

3.18

Front End

Teil eines Mautsystems, bestehend aus eine OBE und wahrscheinlich einem optionalen Vertreter (Proxy), mit dem Mautinformationen und Nutzungsdaten zur Übermittlung an das Back-End (3.7) gesammelt werden

[QUELLE: ISO/DTR 17573-2:2019, 3.82]

3.19

Computereindringling

(en: hacker)

Person, die versucht oder erfolgreich nicht autorisierten Zugang zu einem geschützten Betriebsmittel zu erlangen

[QUELLE: ISO/DTR 17573-2:2019, 3.85]

3.20

Informationsgewinn

(en: information asset)

Wissen oder Daten, die für den Interessensvertreter einen Wert haben

[QUELLE: ISO/DTR 17573-2:2019, 3.91, modifiziert]

3.21

Informationssicherheit

(en: information security)

Bewahrung von Vertraulichkeit (3.11), Integrität (3.24), Verfügbarkeit (3.6), Authentizität (3.5), Haftung (3.1), Nachweisbarkeit (3.28) und Verlässlichkeit von Informationen

[QUELLE: ISO/DTR 17573-2:2019, 3.92]

3.22

Informationssicherheitsereignis

(en: information security event)

identifiziertes Auftreten eines System-, Dienst- oder Netzwerkzustandes, welcher eine mögliche Lücke des Sicherheitsinformationsgrundsatzes (3.21) (3.32) oder Regelungsfehler oder eine zuletzt unbekannte mögliche sicherheitsrelevante Situation anzeigt

[QUELLE: ISO/DTR 17573-2:2019, 3.93]

3.23

Informationssicherheitsvorfall

(en: information security incident)

ungewollte Informationssicherheitsereignisse (3.22), die mit signifikanter Wahrscheinlichkeit kompromittierende Geschäftsabläufe und Bedrohung der Informationssicherheit (3.21) zu Folge haben

[QUELLE: ISO/IEC 27000:2018, 3.31]

3.24

Integrität

(en: integrity)

Merkmal, dass Daten nicht in unautorisierter Art und Weise verändert oder zerstört wurden

[QUELLE: ISO/DTS 17574:2017, 3.9]

3.25

Interoperabilität

(en: interoperability)

Fähigkeit eines Systems, Informationen auszutauschen und die ausgetauschten Informationen gegenseitig zu verwenden

[QUELLE: ISO/DTR 17573-2:2019, 3.99]

3.26

Posten

(en: lot)

exakte Menge von Dingen, die zusammen geliefert werden

Anmerkung 1 zum Begriff: Ein Inspektionsposten kann aus mehreren Mengen oder Teilmengen bestehen.

[QUELLE: ISO 2859-1:1999, 3.1.13, modifiziert]

3.27

Botschaft Authentifizierungscode

MAC

(en: message authentication code)

Kette von Bits als Ergebnis einer MAC-Gleichung

Anmerkung 1 zum Begriff: Der MAC wird manchmal auch kryptografischer Prüfwert genannt (siehe als Beispiel ISO 7498-2)

[QUELLE: ISO 9797-1:2011, 3.9]

3.28

Nachweisbarkeit

(en: non-repudiation)

Fähigkeit zur Überprüfung des Auftretens eines geforderten Ereignisses oder einer Aktion und deren ursprünglichen Instanzen

[QUELLE: ISO/DTR 17573-2:2019, 3.118]

3.29

fahrzeuginterne Einrichtung

OBE

(en: on-board equipment)

alle notwendigen Einrichtungen im Fahrzeug zur Ausführung notwendiger EFC-Funktion und Kommunikationsdiensten

[QUELLE: ISO/DTR 17573-2:2019, 3.121]

3.30

Bezahlmedium

(en: payment medium)

Träger von Bezahlmitteln

BEISPIEL Papierticket, Chipkarten, Smartphones

[QUELLE: ISO/TS 121193², 3.14]

2 Unter Vorbereitung (Stufe zum Zeitpunkt der Beantragung der DIS-Umfrage: ISO/DTR:2019 angenommen. Der finale Text wird vorbereitet)

3.31

persönliche Daten

(en: personal data)

Informationen, bezogen auf eine identifizierte- oder identifizierbare natürliche Person

[QUELLE: ISO/DTR 17573-2:2019, 3.131]

3.32

Grundsatz

(en: policy)

allgemeine Absichten und Richtungen, die vom Management formal vorgegeben werden

[QUELLE: ISO/DTR 17573-2:2019, 3.136, modifiziert]

3.33

Auswertung persönlicher Daten

(en: processing of personal data)

Arbeit oder Menge von Arbeiten, die an persönlichen Daten (3.31) durchgeführt wird/werden in oder nicht in automatischer Art und Weise wie Sammlung, Aufnahme, Speicherung, Anpassung oder Veränderung, Rettung, Abfrage, Nutzung, Offenlegung während der Übertragung, Verteilung oder andere Art von Bereitstellung, Anordnung oder Kombination, Blockierung, Löschung oder Zerstörung

3.34

Straßenrand-Einrichtung

RSE

(en: roadside equipment)

Einrichtung entlang einer Fahrbahn, entweder installiert oder mobil

[QUELLE: ISO/DTR 17573-2:2019, 3.155]

3.35

Muster

(en: sample)

Satz von einem Gegenstand oder mehreren Gegenständen, der/die einem Posten (3.26) entnommen wurden mit der Absicht, Informationen dieses Postens (3.26) zu liefern

[QUELLE: ISO 2859-1:1999, 3.1.15]

3.36

Sicherheitsanwendungsmodul

SAM

(en: security policy)

physikalisches Modul, das in sicherer Art und Weise kryptografische Funktionen ausführt und Schlüssel speichert

[QUELLE: ISO/DTR 17573-2:2019, 3.159]

3.37

Sicherheitsgrundsatz

(en: security policy)

Menge an Regeln, die bestimmen, wie Sicherheitsbedrohungen bewältigt werden, oder welcher Grad an Sicherheitsniveau beibehalten werden soll

[QUELLE: ISO/DTR 17573-2:2019, 3.162]

3.38

Sicherheitsdienst

(en: security service)

Dienst, der von Kommunikationssystemen zur Verfügung gestellt wird, der adäquate Sicherheit des Systems oder des Datentransfers sicherstellt

[QUELLE: ISO/DTR 17573-2:2019, 3.163]

3.39

Dienstnutzer

SU

(en: service user)

generischer Begriff für einen Kunden eines Maut-Dienstansbieters (3.49), wobei einer als Mautverantwortlicher (3.43), ein Fahrzeugbesitzer, ein Flottenbetreiber, ein Fahrer, usw., abhängig vom Kontext, gemeint sein kann

3.40

Bedrohung

(en: threat)

potentielle Ursache eines ungewollten sicherheitsrelevanten Informationsvorfalls (3.23), welches zu Schäden an einem System oder für eine Organisation führen könnte

[QUELLE: ISO/DTR 17573-2:2019, 3.181, modifiziert]

3.41

Bedrohungsermittler

(en: threat agent)

Instanz, die die Absicht hat, nachteilig zu einem Bestand (3.3) zu handeln

[QUELLE: ISO/DTR 17573-2:2019, 3.182]

3.42

Bedrohungsanalyse

(en: threat analysis)

systematische Erkennung, Identifizierung und Auswertung von Bedrohungen (3.40)

[QUELLE: ISO/DTR 17573-2:2019, 3.183]

3.43

Maut

(en: toll)

Gebühr, Steuer oder Verpflichtung für die Fahrzeugbenutzung innerhalb eines Mautgebiets (3.46)

[QUELLE: ISO/DTR 17573-2:2019, 3.185, modifiziert]

3.44

Mauterheber

TC

(en: toll charger)

Instanz, die Maut (3.43) zur Nutzung eines Fahrzeuges in einem Mautgebiet (3.46) einzieht

[QUELLE: ISO/DTR 17573-2:2019, 3.186]

3.45

Mauterklärung

(en: toll declaration)

Aussage, um die Nutzung einer gegebenen Maut an einen Mauterheber (3.43) zu vereinbaren

[QUELLE: ISO/DTR 17573-2:2019, 3.191]

3.46

Mautgebiet

(en: toll domain)

Bereich oder Teil eines Straßennetzwerks, in dem ein bestimmtes Mautregime (3.47) angewendet wird

[QUELLE: ISO/DTR 17573-2:2019, 3.193]

3.47

Mautregim

(en: toll regime)

Menge von Regeln, inklusive von Gesetzesregelungen, welche die Sammlung von Maut (3.43) in einem Mautgebiet (3.46) regeln

[QUELLE: ISO/DTR 17573-2:2019, 3.195]

3.48

Mautschema

(en: toll scheme)

organisatorischer Blick auf ein Mautregime (3.47) inklusive der Akteure und deren Beziehungen

[QUELLE: ISO/DTR 17573-2:2019, 3.196]

3.49

Maut-Dienstanbieter

TSP

(en: toll service provider)

Instanzen, welche Mautdienste in einem- oder mehreren Mautgebiet(en) (3.46) anbietet

[QUELLE: ISO/DTR 17573-2:2019, 3.198]

3.50

zuverlässiger Drittanbieter

TTP

(en: trusted third party)

Sicherheitsdienststelle oder deren Behörde, welche zuverlässig im Sinne zu einigen sicherheitsrelevanten Aktivitäten ist

[QUELLE: ISO/IEC 10181-1:1996, 3.3.30, modifiziert]

3.51

Angreifbarkeit

(en: vulnerability)

Schwäche eines Bestandes (3.3) oder Steuerung, die von einem Computereindringling ausgenutzt werden kann

[QUELLE: ISO/DTR 17573-2:2019, 3.227]

Contents

Page

Foreword.....	vii
Introduction.....	viii
1 Scope	1
2 Normative references	2
3 Terms and definitions.....	4
4 Symbols and abbreviated terms.....	11
5 Trust model.....	12
5.1 Overview	12
5.2 Stakeholders trust relations.....	12
5.3 Technical trust model	13
5.3.1 General	13
5.3.2 Trust model for TC and TSP relations	13
5.3.3 Trust model for TSP and service user relations	15
5.3.4 Trust model for Interoperability Management relations	15
5.4 Implementation.....	15
5.4.1 Setup of trust relations.....	15
5.4.2 Trust relation renewal and revocation.....	16
5.4.3 Issuing and revocation of sub CA and end-entity certificates.....	16
5.4.4 Certificate and certificate revocation list profile and format.....	17
5.4.5 Certificate extensions.....	17
6 Security requirements	19
6.1 General	19
6.2 Information security management system	20
6.3 Communication interfaces	20
6.4 Data storage.....	21
6.5 Toll charger.....	21
6.6 Toll service provider	24
6.7 Interoperability Management.....	26
6.8 Limitation of requirements.....	26
7 Security measures — countermeasures.....	27
7.1 Overview	27
7.2 General security measures.....	27
7.3 Communication interfaces security measures.....	28
7.3.1 General	28
7.3.2 DSRC-EFC interface.....	29
7.3.3 CCC interface.....	30
7.3.4 LAC interface	31
7.3.5 Front End to TSP back end interface.....	32
7.3.6 TC to TSP interface	32
7.3.7 ICC interface.....	34
7.4 End-to-end security measures	35
7.5 Toll service provider security measures	36
7.5.1 Front end security measures.....	36

7.5.2	Back end security measures.....	37
7.6	Toll charger security measures	38
7.6.1	RSE security measures	38
7.6.2	Back end security measures.....	39
7.6.3	Other TC security measures	40
8	Security specifications for interoperable interface implementation	40
8.1	General.....	40
8.1.1	Subject.....	40
8.1.2	Signature and hash algorithms	40
8.2	Security specifications for DSRC-EFC	41
8.2.1	Subject.....	41
8.2.2	OBE	41
8.2.3	RSE.....	41
9	Key management.....	41
9.1	Overview	41
9.2	Asymmetric keys	42
9.2.1	Key exchange between stakeholders.....	42
9.2.2	Key generation and certification.....	42
9.2.3	Protection of keys	42
9.2.4	Application	42
9.3	Symmetric keys.....	43
9.3.1	General.....	43
9.3.2	Key exchange between stakeholders.....	43
9.3.3	Key lifecycle.....	44
9.3.4	Key storage and protection	45
9.3.5	Session keys	46
Annex A	(normative) Security profiles	47
A.1	General.....	47
A.2	Communication interface profiles	47
A.2.1	TC to TSP profiles	47
A.2.2	Communication provider profile.....	48
A.2.3	ICC interface profile.....	49
A.3	Data storage profiles.....	49
A.3.1	OBE data storages profile.....	49
A.3.2	ICC data storage profile.....	50
A.3.3	RSE data storage profile.....	50
A.3.4	Back end data storage profile	50
Annex B	(normative) Implementation conformance statement (ICS) proforma	51
B.1	Guidance for completing the ICS proforma.....	51
B.1.1	Purposes and structure.....	51
B.1.2	Abbreviations and conventions	51
B.2	Identification of the implementation.....	53
B.2.1	General.....	53
B.2.2	Date of the statement.....	53
B.2.3	Implementation Under Test (IUT) identification	53
B.2.4	System Under Test (SUT) identification	53
B.2.5	Supplier.....	53
B.2.6	Actor (if different from supplier)	54
B.2.7	ICS contact person.....	54
B.3	Identification of the standard.....	54
B.4	Global statement of conformance	55

B.5	Roles	55
B.6	Trust model.....	55
B.7	Profiles.....	58
B.8	Requirements.....	59
B.9	Security measures	62
B.10	Specifications for interoperable interfaces security	67
B.11	Specifications for key management.....	67
Annex C	(informative) Stakeholder objectives and generic requirements	69
C.1	General	69
C.2	Toll chargers.....	70
C.2.1	Toll chargers and their main interests	70
C.2.2	Security service requirements for a toll charger	70
C.3	Toll service providers	71
C.3.1	Toll service providers and their main interests.....	71
C.3.2	Security service requirements for a toll service provider.....	71
C.4	Service users.....	72
C.4.1	Service users and their main interests	72
C.4.2	Service user requirements.....	72
C.5	Interoperability management.....	72
C.5.1	Interoperability management and its main interests	72
C.5.2	Security service requirements for interoperability management	73
Annex D	(informative) Threat analysis.....	74
D.1	General	74
D.1.1	General approach	74
D.1.2	Naming conventions	74
D.1.3	Statement of completeness	75
D.2	Attack trees-based threat analysis.....	75
D.2.1	Overview	75
D.2.2	System model	75
D.2.3	Presentation of attack trees.....	77
D.2.4	Attacker class 1: Service user.....	78
D.2.5	Attacker class 2: Toll service provider	82
D.2.6	Attacker class 3: Toll charger.....	85
D.2.7	Attacker class 4: Hacker	88
D.2.8	Attacker class 5: Activist	92
D.2.9	Attacker class 6: Communication provider.....	93
D.2.10	Attacker class 7: Enterprise	95
D.2.11	Attacker class 8: Government	98
D.2.12	Attacker class 9: Foreign state agency	100
D.3	Asset based threat analysis.....	102
D.3.1	General	102
D.3.2	Threatened Assets.....	103
D.3.3	Compliance matrix	103
D.3.4	Presentation of threats.....	105
D.3.5	Generic threats	105
D.3.6	Asset 203: Billing details.....	107
D.3.7	Asset 204: OBE Charge Report	108
D.3.8	Asset 205: Customization information	109
D.3.9	Asset 206: Service user contract information	110
D.3.10	Asset 207: Exception list	110
D.3.11	Asset 208: Customer service.....	111

D.3.12 Asset 209: OBE.....	111
D.3.13 Asset 210: Service user privacy	113
D.3.14 Asset 211: RSE	114
D.3.15 Asset 212: EFC stakeholder image and reputation	115
D.3.16 Asset 213: TC and TSP central system	116
D.3.17 Asset 214: Road usage data	118
D.3.18 Asset 215: Trust objects.....	119
D.3.19 Asset 216: Service user identification	120
D.3.20 Asset 217: Toll context data	121
D.3.21 Asset 218: Payment means	122
D.3.22 Asset 219: Limited autonomy	123
D.3.23 Asset 220: EFC schema	123
D.3.24 Asset 221: Contractual conditions	124
D.3.25 Asset 222: Operational rules.....	125
D.3.26 Asset 223: Complaints	126
D.3.27 Asset 224: Certification	127
D.3.28 Asset 225: Quality assurance parameter reporting	128
D.3.29 Asset 226: Enforcement data	129
D.3.30 Asset 227: Invoice	130
D.3.31 Asset 228: ICC	130
Annex E (informative) Security policies	132
E.1 General.....	132
E.1.1 Overview of this Annex	132
E.1.2 Motivation for the need of security policies.....	132
E.2 Example EFC scheme security policy	132
E.2.1 Motivation for information security	132
E.2.2 Purpose of the security policy	133
E.2.3 Scope of the security policy	133
E.2.4 Policy statements	135
E.3 Development of operators' security policies	138
E.3.1 General.....	138
E.3.2 Interface requirements.....	138
E.3.3 Data storage requirements.....	138
Annex F (informative) Example for an EETS security policy	139
F.1 General.....	139
F.2 Basic laws and regulations	139
F.3 Organization of EETS Information Security.....	139
F.3.1 General.....	139
F.3.2 Steering committee	139
F.3.3 Trust model.....	139
Annex G (informative) Recommendations for privacy-focused implementation.....	141
G.1 General.....	141
G.2 Legal basis in the EU.....	141
G.2.1 European general data protection regulation (EU Directive 2016/679/EC)	141
G.2.2 European General Data Protection Directive (GDPR)	142
G.3 Service users' requirements	142
Annex H (informative) Proposal for end-entity certificates.....	143
Bibliography.....	144

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This edition cancels and replaces the first edition of ISO/TS 19299:2015, which has been technically revised.

The main changes compared to the previous edition are as follows:

- added requirements and security measures for the use of common payment media according to ISO/TS 21193;
- updated data protection considerations in Annex G, in order to take the European Union's new General Data Protection Regulation (i.e. Directive 2016/679/EC) into account.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Context of this document

The development process for a security concept and implementation to protect any existing electronic fee collection (EFC) system normally includes several steps as follows (see Figure 1):

- definition of the security objectives and policy statements in a security policy;
- threat analysis with risk assessment to define the security requirements;
- development of the security measures followed by the development of security test specifications.

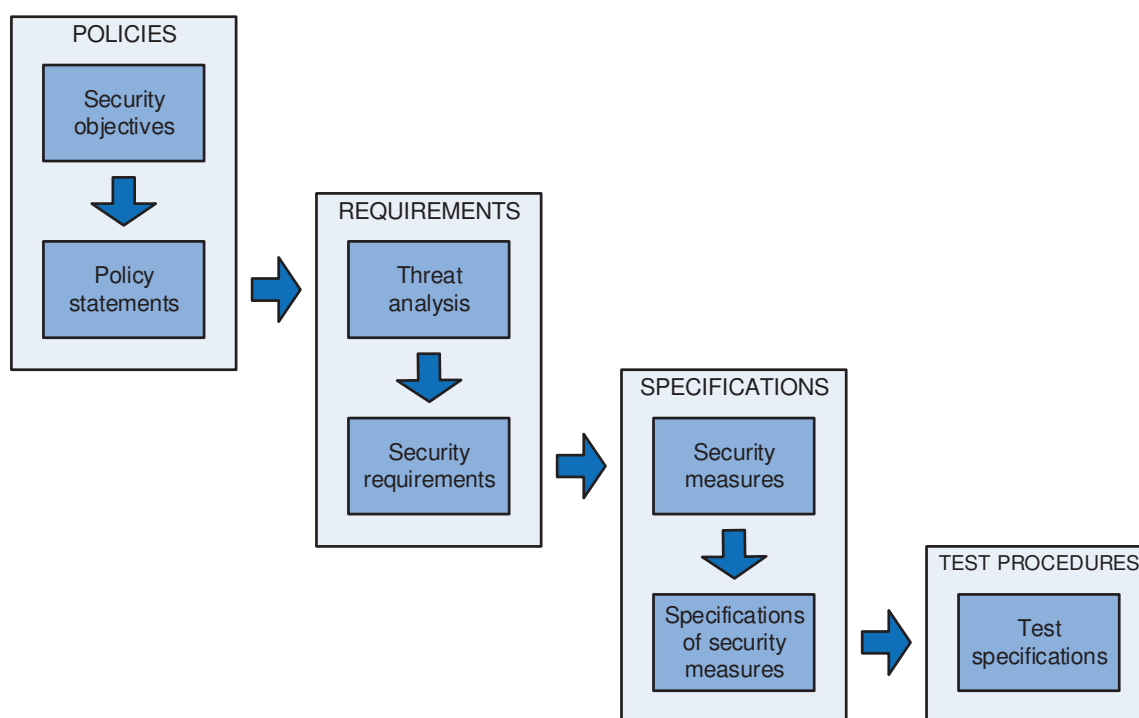


Figure 1 — Development path for the security documents

Each actor in an existing EFC system has to implement the defined security measures and supervise the effectiveness. Security measures which do not work properly need to be improved. The development of the EFC security framework follows this approach as closely as possible, with the following limitations:

- No security policy exists: The security policy can only be defined by the responsible stakeholders and it is limited by laws and regulations. Nonetheless, this document provides basic examples of possible security policies (in Annex E to Annex F).
- No risk assessment possible: Risk assessment compares the possible loss for the stakeholder and the required resources (e.g. equipment, knowledge, time, etc.) to perform an attack. In a real system, risk assessment is based on the evaluation of the costs and benefits of each countermeasure.
- No specific system design or configuration was deemed as universally applicable. Only the available EFC base standards were taken as references. Specific technical details of a particular system (e.g. servers, computer centres, and de-centralised elements like roadside equipment) need to be additionally taken into consideration when implementing security measures.

Selection of requirements and respective security measures for an existing EFC system is based on the security policy and the risk assessment of several stakeholders' systems. Due to the fact that there is no overall valid security policy, nor is there the possibility to provide a useful risk assessment, the EFC security framework provides a toolbox of requirements and security measures covering as many threats as possible without claiming to provide an exhaustive list.

Having stated that, in order to be compliant to this document, if a requirement is selected, the associated security measure(s) have to be implemented.

To understand the content of this document, the reader should be aware of the methodological assumptions used to develop it. Security of an (interoperable) EFC scheme depends on the correct implementation and operation of a number of processes, systems, and interfaces. Only a reliable end-to-end security ensures the accurate and trustworthy operation of interacting components of toll charging environments. Therefore, this security framework also covers systems or interfaces which are not EFC specific, like back office connections. The application independent security framework for such system parts and interfaces, the Information Security Management System (ISMS), is provided in the ISO 2700x family of standards.

The development process of this document is described briefly in the steps below:

- a) Definition of the stakeholder objectives and generic requirements as the basic motivation for the security requirements (Annex C). A possible security policy with a set of policy statements is provided in Annex E, and an example of a European electronic toll service (EETS) security policy is given in Annex F.
- b) Based on the EFC role model and further definitions from the EFC architecture standard (ISO 17573-1), the specification defines an abstract EFC system model as the basis for a threat analysis, definition of requirements, and security measures.
- c) The threats on the EFC system model and its assets are analysed by two different methods: an attack-based analysis and an asset-based analysis. The first approach considers several threat scenarios from the perspective of various attackers. The second approach looks in depth on threats against the various identified assets (tangible and intangible). This approach, although producing some redundancy, ensures completeness and coverage of a broad range of risks (see Annex D).
- d) The requirements specification (see Clause 6) is based on the threats identified in Annex D. Each requirement is at least motivated by one threat and each threat is covered by at least one requirement.
- e) The definition of security measures (see Clause 7) provides a high-level description of recommended possible methods to cover the developed requirements.
- f) The security specifications for interoperable interface implementation (Clause 8) provide detailed definitions, e.g. for message authenticators. These specifications represent an add-on for security to the corresponding relevant interface standards.
- g) Basic key management requirements that support the implementation of the interoperable interfaces are described in Clause 9. The toll charging environment uses cryptographic elements (keys, certificates, certificate revocation lists, etc.) to support security services like confidentiality, integrity, authenticity, and non-repudiation. This section of the specification covers the (initial) setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.

- h) A general trust model (see Clause 5) is defined to form the basis for the implementation of cryptographic procedures to ensure confidentiality, integrity, and authenticity of exchanged data. In this context, the security framework references approved international standards for the implementation of cryptographic procedures enhanced by EFC specific details where needed.

A stakeholder of an EFC scheme who wants to use this security framework needs to do the following:

- define a security policy for the EFC scheme (may involve more than one stakeholder in an interoperable EFC scheme). Some examples for a security policy and its elements are provided (in Annex E and Annex F) as an aid to build up a secure system for a concrete interoperability framework (including the European electronic toll service).
- identify the relevant processes, systems and interfaces, and match them to the EFC security framework;
- select the corresponding security requirements according to the security policy;
- implement the security measures associated to the selected requirements;
- provide evidence of compliance of its systems, processes, and interfaces with the requirements set forth in this document. Evidence can be provided by a self-declaration, an internal or external audit, or other certifications.

EFC role model

This document complies with the role model defined in ISO 17573-1. According to this role model, the toll charger (TC) is the provider of the tolled infrastructure or transport service and hence, the recipient of the road usage fees. The TC is the actor associated with the toll charging role (see Figure 2).

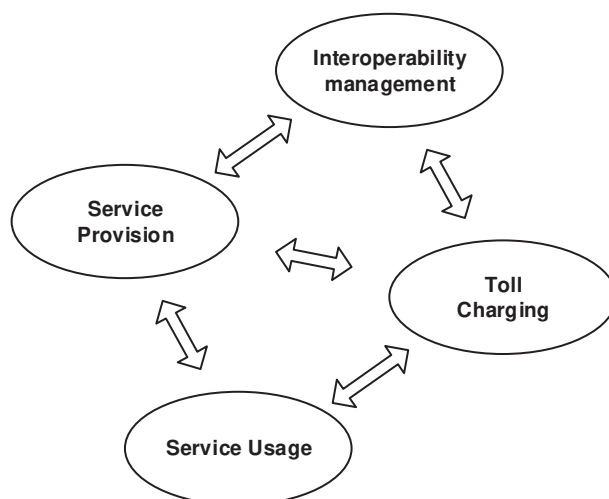


Figure 2 — The role model underlying this document

Toll service providers (TSP) issue on-board equipment (OBE) to the users of the tolled infrastructure or transport service. The OBE will be used for collecting data, enabling the TC to send a claim to the TSP for the use of the infrastructure or transport service by their service users (SU). In autonomous systems, each TSP delivers toll declarations to the TC who operates the autonomous system. In dedicated short-range communication (DSRC)-based systems, the TC receives the main toll declarations from its own RSE which communicates with the TSP's OBEs. Interoperability management (IM) in Figure 2 comprises all specifications and activities that in common, define and maintain a set of rules that govern the overall toll charging environment.

The trust model defined in this document is based on the role model summarized above and it is also the technical base for the protection of the data communication between the entities of the role model. Besides this communication security, trust in the secure implementation and management of the back end and other equipment for the EFC framework is required. A TC or TSP compliant to this document needs to be able to give evidence of security management as required. Such evidence is the basis of trust relations between the involved entities.

Figure 3 below illustrates the abstract EFC system model used to analyse the threats, define the security requirements and associated security measures for this document. This document assumes an OBE that is dedicated to EFC purposes only and does not consider value added services based on EFC OBE, nor more generic OBE platforms (also called in-vehicle ITS Stations) which could be used to host the EFC application. The OBE may either be connected to a central account or use a payment medium such as integrated circuit cards (ICC) or mobile payment for on-board-account EFC system. Any financial transactions are out of scope of this document.

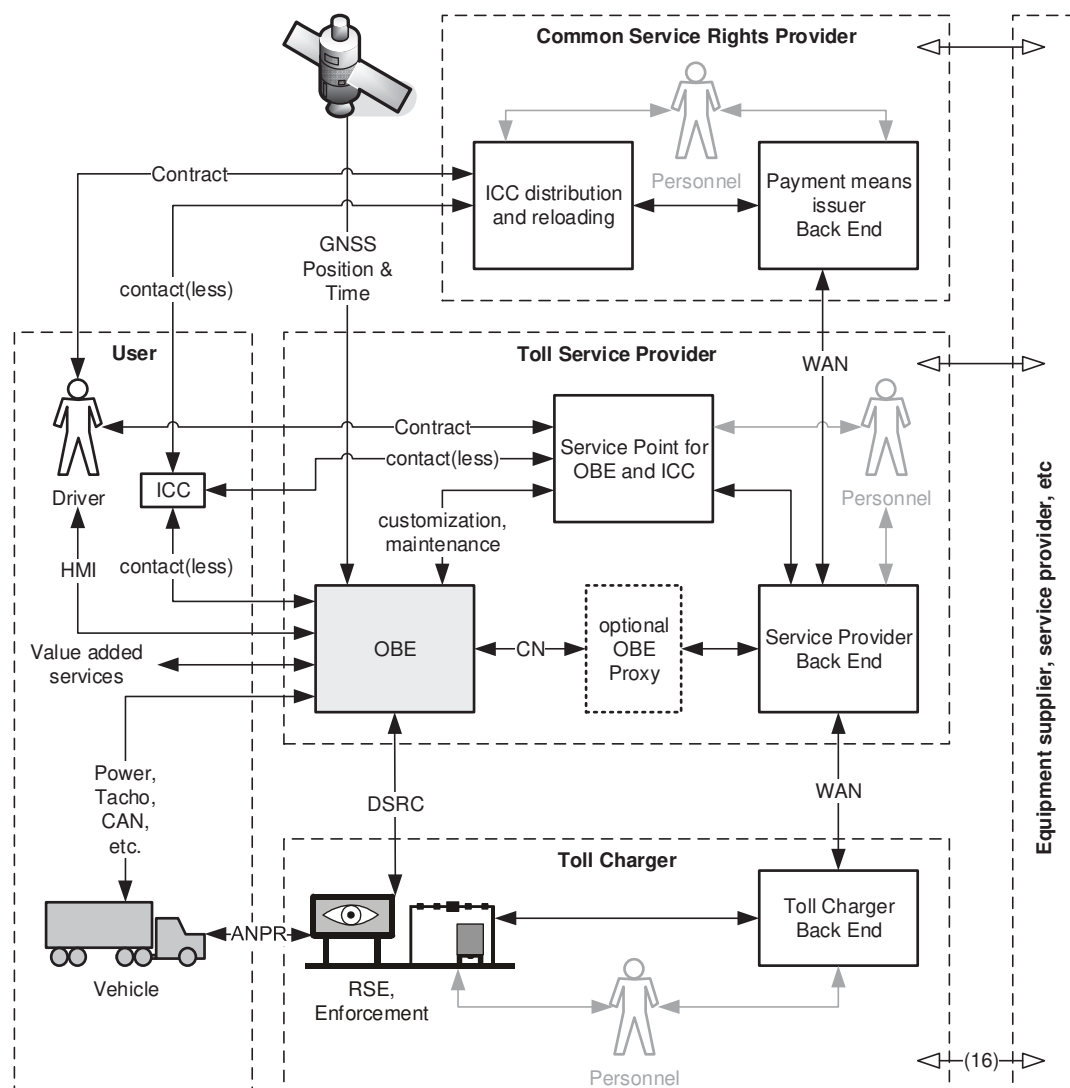


Figure 3 — EFC system model of the EFC Security framework

Relation to other security standards

Several generic and specific standards and technical reports concerning security issues for information technology already exist. This document uses these existing standards and expands their usability for

EFC applications. This framework references and adapts security techniques and methodologies from these standards.

Figure 4 shows the context of the EFC security framework to the most relevant security standards that gave input to this document. Standards that are directly used and referenced are highlighted in black.

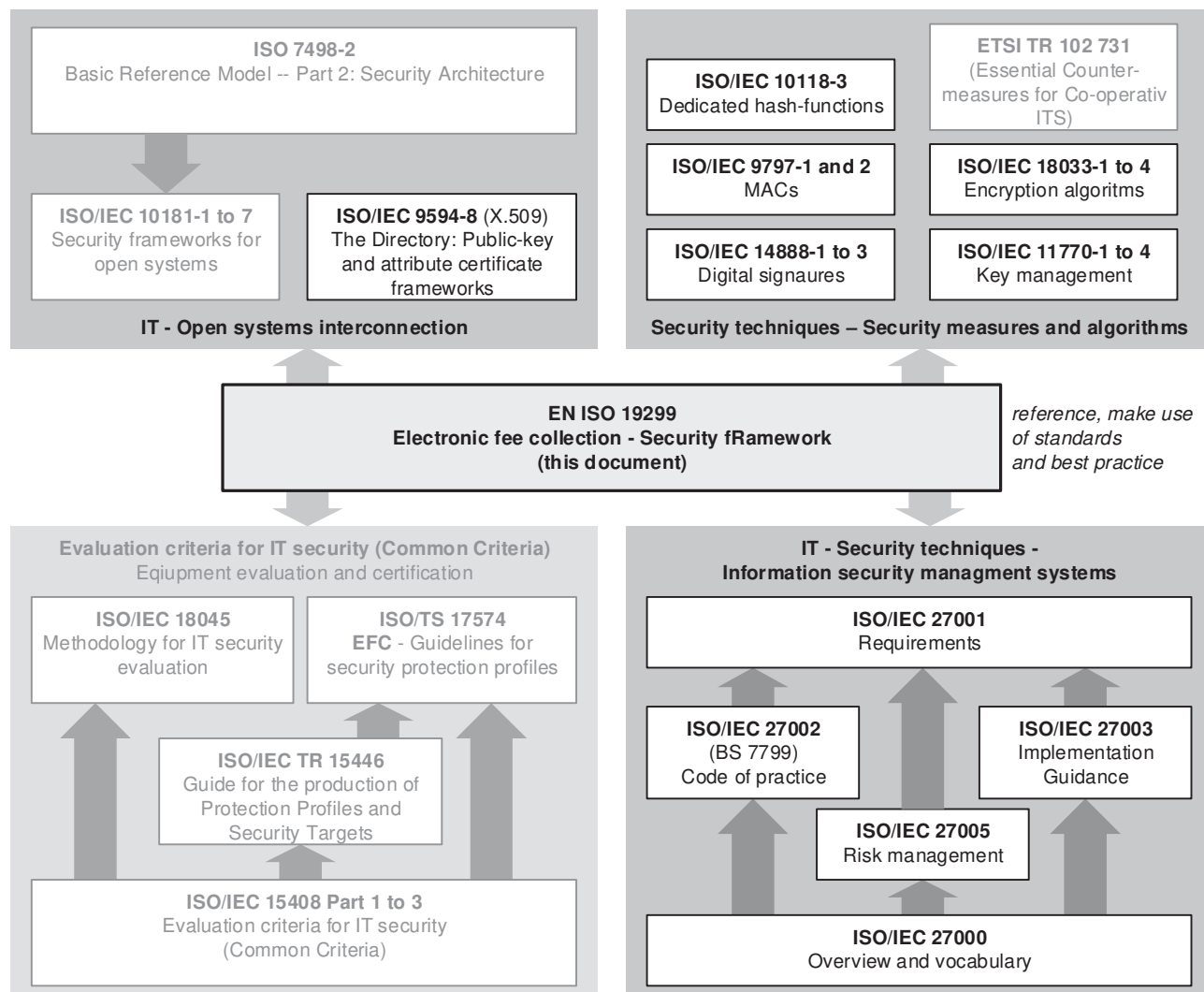


Figure 4 — Relevant security standards in the context of the EFC — Security framework

Standards shown in Figure 4 are grouped in the following categories, where arrows inside each group indicate which standard provides input to other standards:

- **Security techniques — Security measures and algorithms:** This group is a collection of essential security measures and recommended cryptographic algorithms including the guidelines for accurate use.
- **IT — Open system interconnection:** This group provides mechanisms for the secure communications between open systems. These standards address some of the security requirements in the areas of authentication and other security services through the provision of a set of frameworks.

- **Evaluation criteria for IT security (common criteria):** This group defines methodologies and processes for the security evaluation and certification for most categories of products used in the EFC environment.
- **IT — Security techniques — Information security management system:** This group defines requirements and guidelines for the implementation of security management systems for all types of organizations. The standards in this group are suited for security solutions of back end and other fixed or installed equipment of EFC systems, including their software.

An ISO/IEC 27001 certification of a TC or TSP organization may be used to demonstrate compliance to this document, provided that the scope and the Statements of Applicability (SoA) include the EFC business processes specified in ISO 17573-1 and that security requirements and their associated security measures provided by this document are applied, e.g. by using them as part of the so-called catalogues containing the security measures and control objectives. Figure 5 below illustrates how this approach works in two parallel paths. The first step of both paths is analysing the business processes, which is then followed by a threat analysis. A common risk analysis combines the generic and the EFC related analysis and results in the respective security measures and controls.

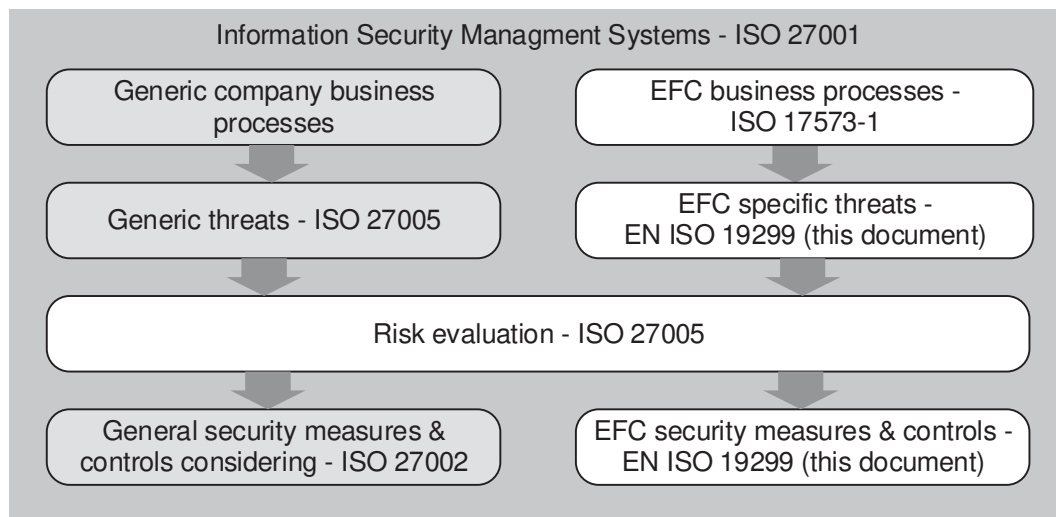


Figure 5 — Scope in relation to the Information Security Management System

In addition, the EFC security framework makes use of existing threat analysis methods and uses existing threat analysis with relation to EFC or ITS, such as ETSI/TR 102 893.

Electronic fee collection — Security framework

1 Scope

The overall scope of this document is the definition of an information security framework for all organizational and technical entities of an EFC scheme and for the related interfaces, based on the system architecture defined in ISO 17573-1. The security framework describes a set of requirements and associated security measures.

The scope of this document comprises the following:

- definition of a trust model (Clause 5): basic assumptions and principles for establishing trust between the stakeholders.
- security requirements (Clause 6): security requirements to support actual EFC system implementations;
- security measures — countermeasures (Clause 7);
- security specifications for interface implementation (Clause 8): security add-on to EFC standards, as shown in Figure 6;
- key management (Clause 9): initial setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.;
- security profiles (Annex A);
- implementation conformance statement (Annex B): checklist to be used by an equipment supplier, a system implementation, or an actor of a role declaring his conformity to this document;
- general information security objectives of the stakeholders (Annex C) which provide a basic motivation for the security requirements;
- threat analysis (Annex D) on the EFC system model and its assets using two different complementary methods, an attack-based analysis, and an asset-based analysis;
- security policy examples (Annex E and Annex F);
- recommendations for privacy-focused implementation (Annex G);
- proposal for end-entity certificates (Annex H).

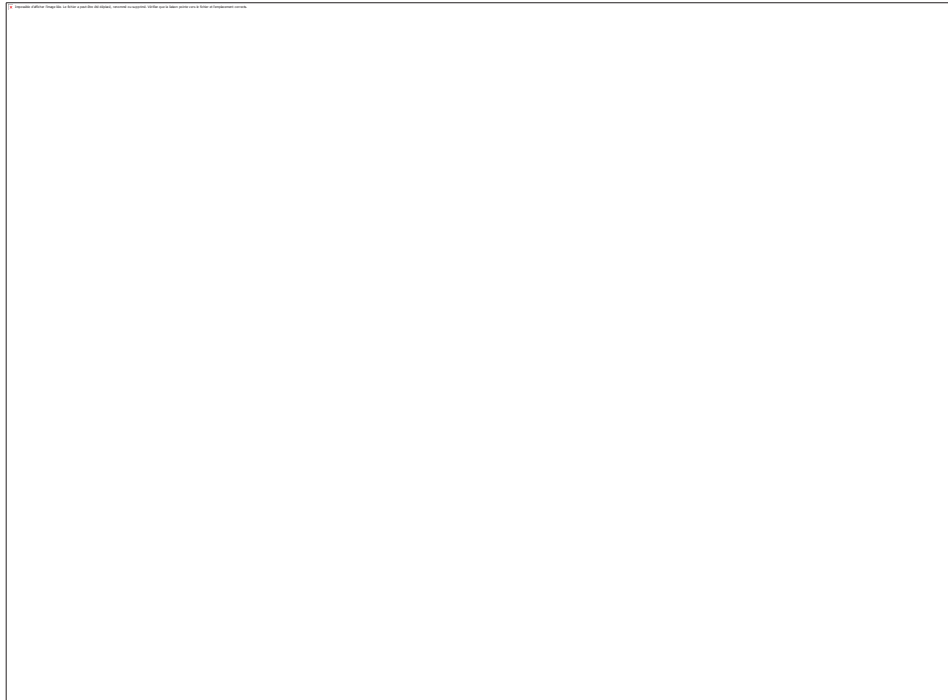


Figure 6 — Scope of EFC security framework for secure communication

The following are outside the scope of this document:

- a complete risk assessment for an EFC system;
- security issues rising from an EFC application running on an ITS station;

NOTE Security issues associated with an EFC application running on an ITS station are covered in CEN/TR 16690.

- entities and interfaces of the interoperability management role;
- the technical trust relation between TSP and service user;
- concrete implementation specifications for implementation of security for specific EFC services (e.g. European Electronic Toll Service (EETS));
- detailed specifications required for privacy-friendly EFC implementations;
- any financial transactions between the payment service provider and the payment medium (e.g. ICC) issued by it.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 2859-1:1999, *Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection*

- ISO/FDIS 12813:¹, *Electronic fee collection — Compliance check communication for autonomous systems*
- ISO 12855:2015, *Electronic fee collection — Information exchange between service provision and toll charging*
- ISO 13141:2015, *Electronic fee collection — Localization augmentation communication for autonomous systems*
- ISO 14906:2018, *Electronic fee collection — Application interface definition for dedicated short-range communication*
- EN 15509:2014, *Electronic fee collection — Interoperability application profile for DSRC*
- CEN/TS 16702-1:², *Electronic fee collection — Secure monitoring for autonomous toll systems — Part 1: Compliance checking*
- ISO 17575-1:2016, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging*
- ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*
- ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*
- ISO/IEC 9594-8:2017, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*
- ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
- ISO/IEC 11770-1:2010, *Information technology — Security techniques — Key management — Part 1: Framework*
- ISO/IEC 11770-3:2015, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*
- ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*
- ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*
- ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*
- ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

¹ Under preparation. (Stage at the time of launching of the DIS ballot: ISO/FDIS:2019.)

² Under preparation. (Stage at the time of launching of the DIS ballot: FprCEN/TS:2019)

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

IETF Request for Comments (RFC) 4301:2005-12, *Security Architecture for the Internet Protocol*

IETF Request for Comments (RFC) 4347:2006-04, *Datagram Transport Layer Security*

IETF Request for Comments (RFC) 4648:2006-10, *The Base16, Base32, and Base64 Data Encodings*

IETF Request for Comments (RFC) 5035:2007-08, *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*

IETF Request for Comments (RFC) 5246:2008-08, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF Request for Comments (RFC) 5280:2008-05, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

IETF Request for Comments (RFC) 5746:2010-02, *Transport Layer Security (TLS) Renegotiation Indication Extension*

Federal Information Processing Standards (FIPS) PUB 140-2, December 2002, *Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1

accountability

property that ensures that the actions of an entity may be traced uniquely to the entity

[SOURCE: ISO/TR 17573-2:2019³, 3.5]

3.2

activist

especially active, vigorous advocate of a cause, especially a political cause

[SOURCE: ISO/DTR 17573-2:2019, 3.6]

³ Under preparation. (Stage at the time of launching of the DIS ballot: ISO/DTR:2019 approved. The final text is being prepared)

3.3

asset

anything that has value to a stakeholder

Note 1 to entry: An asset may be tangible or intangible.

[SOURCE: ISO/DTR 17573-2:2019, 3.8, Note 1 added]

3.4

attack

attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset (3.3)

[SOURCE: ISO/DTR 17573-2:2019, 3.10]

3.5

authenticity

property that an entity is what it claims to be

[SOURCE: ISO/DTR 17573-2:2019, 3.15]

3.6

availability

property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/DTR 17573-2:2019, 3.17]

3.7

back end

part of the back office system interfacing to one or more front ends (3.18)

[SOURCE: ISO/DTR 17573-2:2019, 3.19]

3.8

certificate revocation list

signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

[SOURCE: ISO/DTR 17573-2:2019, 3.25]

3.9

certification authority

CA

entity trusted by one or more entities to assign and revoke public key certificates

[SOURCE: ISO 21188:2018, 3.21]

3.10

communication provider

provider of information transmission services

[SOURCE: ISO/DTR 17573-2:2019, 3.40]

3.11

confidentiality

prevention of information leakage to non-authenticated individuals, parties, and/or processes

[SOURCE: ISO/DTR 17573-2:2019, 3.42]

3.12

data privacy

information privacy

rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/DTR 17573-2:2019, 3.54]

3.13

data protection commissioner

data privacy commissioner

person responsible for the enforcement and monitoring of compliance with the applicable data protection legislation

[SOURCE: ISO/DTR 17573-2:2019, 3.55]

3.14

data subject's consent

any freely given specific and informed written indication of his wishes by which the data subject signifies his agreement to personal data (3.31) relating to him being processed

3.15

digital signature

one or more data elements resulting from the digital signature process

[SOURCE: ISO/DTR 17573-2:2019, 3.58]

3.16

enforcement

measures or actions performed to achieve compliance with laws, regulations, or rules

Note 1 to entry: In this context, the process of compelling observance of a toll regime (3.47).

[SOURCE: ISO/DTR 17573-2:2019, 3.70, added Note 1]

3.17

foreign state agency

agency of any state except the state under whose jurisdiction a particular toll scheme (3.48) is operated

[SOURCE: ISO/DTR 17573-2:2019, 3.80]

3.18

front end

part of a tolling system consisting of OBE and possibly, a proxy where road tolling information and usage data are collected and processed for delivery to the back end (3.7)

[SOURCE: ISO/DTR 17573-2:2019, 3.82]

3.19

hacker

person who attempts or succeeds to gain unauthorized access to protected resources

[SOURCE: ISO/DTR 17573-2:2019, 3.85]

3.20

information asset

knowledge or data that has value to the stakeholder

[SOURCE: ISO/DTR 17573-2:20129, 3.91, modified]

3.21

information security

preservation of confidentiality (3.11), integrity (3.24), availability (3.6), authenticity (3.5), accountability (3.1), non-repudiation (3.28), and reliability of information

[SOURCE: ISO/DTR 17573-2:2019, 3.92]

3.22

information security event

identified occurrence of a system, service or network state indicating a possible breach of information security (3.21) policy (3.32) or failure of controls, or a previously unknown situation that may be security relevant

[SOURCE: ISO/ DTR 17573-2:2019, 3.93]

3.23

information security incident

single or a series of unwanted or unexpected information security events (3.22) that have a significant probability of compromising business operations and threatening information security (3.21)

[SOURCE: ISO/IEC 27000:2018, 3.31]

3.24

integrity

property that data have not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 17574:2017, 3.9]

3.25

interoperability

ability of systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/DTR 17573-2:2019, 3.99]

3.26

lot

definite amount of items, delivered together

Note 1 to entry: An inspection lot may consist of several batches or parts of batches.

[SOURCE: ISO 2859-1: 1999, 3.1.13, modified]

3.27

message authentication code

MAC

string of bits which is the output of a MAC algorithm

Note 1 to entry: A MAC is sometimes called a cryptographic check value (see, for example, ISO 7498-2).

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

3.28

non-repudiation

ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: ISO/DTR 17573-2:2019, 3.118]

3.29

on-board equipment

OBE

all required equipment on-board a vehicle for performing required EFC functions and communication services

[SOURCE: ISO 17573-2:2019, 3.121]

3.30

payment medium

carrier of payment means

EXAMPLE paper ticket, IC-card, smart phone

[SOURCE: ISO/TS 21193⁴, 3.14]

3.31

personal data

information relating to an identified or identifiable natural person

[SOURCE: ISO 17573-2:2019, 3.131]

3.32

policy

overall intentions and directions of an organization, as formally expressed by its management

[SOURCE: ISO/DTR 17573-2:2019, 3.136, modified]

3.33

processing of personal data

operation or set of operations which is performed upon personal data (3.31), whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval,

⁴ Under preparation. (Stage at the time of launching of the DIS ballot: ISO/DTS:2019)

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction

3.34

roadside equipment

RSE

equipment located along the road either fixed or mobile

[SOURCE: ISO/DTR 17573-2:2019, 3.155]

3.35

sample

set of one or more items taken from a lot (3.26) and intended to provide information on the lot (3.26)

[SOURCE: ISO 2859-1: 1999, 3.1.15]

3.36

secure application module

SAM

physical module that securely executes cryptographic functions and stores keys

[SOURCE: ISO/DTR 17573-2:2019, 3.159]

3.37

security policy

set of rules that regulate how to handle security threats or define the appropriate security level

[SOURCE: ISO/DTR 17573-2:2019, 3.162]

3.38

security service

service provided by communicating systems which ensures adequate security of the systems or of data transfers

[SOURCE: ISO/DTR 17573-2:2019, 3.163]

3.39

service user

SU

generic term used for the customer of a toll service provider (3.49), one liable for toll (3.43), the owner of the vehicle, a fleet operator, a driver, etc. depending on the context

3.40

threat

potential cause of an unwanted information security incident (3.23), which may result in harm to a system or organization

[SOURCE: ISO/DTR 17573-2:2019, 3.181, modified]

3.41

threat agent

entity that has the intention to act adversely on an asset (3.3)

[SOURCE: ISO/DTR 17573-2:2019, 3.182]

3.42

threat analysis

systematic detection, identification, and evaluation of threats (3.40)

[SOURCE: ISO/DTR 17573-2:2019, 3.183]

3.43

toll

charge, tax, or duty levied for the use of a vehicle in a toll domain (3.46)

[SOURCE: ISO/DTR 17573-2:2019, 3.185, modified]

3.44

toll charger

TC

entity which levies toll (3.43) for the use of vehicles in a toll domain (3.46)

[SOURCE: ISO/DTR 17573-2:2019, 3.186]

3.45

toll declaration

statement to declare the usage of a given toll service to a toll charger (3.44)

[SOURCE: ISO/DTR 17573-2:2019, 3.191]

3.46

toll domain

area or a part of a road network where a certain toll regime (3.47) is applied

[SOURCE: ISO/DTR 17573-2:2019, 3.193]

3.47

toll regime

set of rules, including enforcement rules, governing the collection of toll (3.43) in a toll domain (3.46)

[SOURCE: ISO/DTR 17573-2:2019, 3.195]

3.48

toll scheme

organizational view of a toll regime (3.47) including the actors and their relationships

[SOURCE: ISO/DTR 17573-2:2019, 3.196]

3.49

toll service provider

TSP

entity providing toll services in one or more toll domains (3.46)

[SOURCE: ISO/DTR 17573-2:2019, 3.198]

3.50

trusted third party

TTP

security authority or its agent trusted by other entities with respect to security-related activities

[SOURCE: ISO/IEC 10181-1:1996, 3.3.30 modified]

3.51

vulnerability

weakness of an asset (3.3) or control that can be exploited by an attacker

[SOURCE: ISO/DTR 17573-2:2019, 3.227]

4 Symbols and abbreviated terms

AC_CR	Access Credentials (ISO 14906)
ADU	Application Data Unit
CA	Certification Authority (ISO 21188)
CCC	Compliance Check Communication (ISO 12813)
CN	Cellular Network
CRL	Certificate Revocation List
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (ISO 14906)
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection (ISO 17573-1)
GNSS	Global Navigation and Satellite System (ISO 17573-1)
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over Secure socket layer
HW	Hardware
ICC	Integrated Chip Card (IC card)
ICS	Implementation Conformance Statement (ISO/TS 14907-2)
IETF	Internet Engineering Task Force
IM	Interoperability Management
IPsec	Internet Protocol Security
ISMS	Information Security management system (ISO/IEC 27000)
LAC	Localization Augmentation Communication (ISO 13141)
MAC	Message Authentication Code
MAC_TC	DSRC Message Authentication Code for toll charger
MAC_TSP	DSRC Message Authentication Code for toll service provider
OBE	On-Board Equipment (ISO 14906)

OID	Object Identifier
PAN	Personal Account Number
PER	Packed Encoding Rules (ISO/IEC 8825-2)
PKI	Public Key Infrastructure
RQ	Requirement
RSA	Rivest, Shamir and Adleman
NOTE	RSA is an algorithm for public-key cryptography also referred to as asymmetrical cryptographic technique.
RSE	Roadside Equipment (ISO 14906)
SAM	Secure application module
SHA-1	Secure hash algorithm (ISO/IEC 10118-3)
SM	Security Measure (countermeasure)
SU	Service User
SW	Software
TC	Toll Charger (ISO 17573-1)
TLS	Transport Layer Security
TSP	Toll Service Provider
TTP	Trusted Third Party
VPN	Virtual Private Network
XER	XML Encoding Rules (ISO/IEC 8825-4)

5 Trust model

5.1 Overview

The trust model provides the basic trust and functionality for the implementation of authenticated and secured communication channels between TSP and TC.

The trust model has two different levels, the contractual framework between the stakeholders (TC, TSP, and SU) and the technical trust model between the IT infrastructure of the TC and TSP.

The trust model assumes that no initial technical trust relation between any of the stakeholders exists or is provided by a predefined third party.

5.2 Stakeholders trust relations

Three kinds of bidirectional contract-based peer-to-peer trust relations are present in the underlying EFC role model:

- between toll charger and toll service provider;
- between toll service provider and service user;
- between toll charger or toll service provider and interoperability management.

There is no direct trust relation between toll charger and service user, as illustrated in Figure 7. The obligation of the service user is to pay for the transport service (e.g. road use) according to laws and regulations of the respective toll domain by using the OBE issued by the TSP.

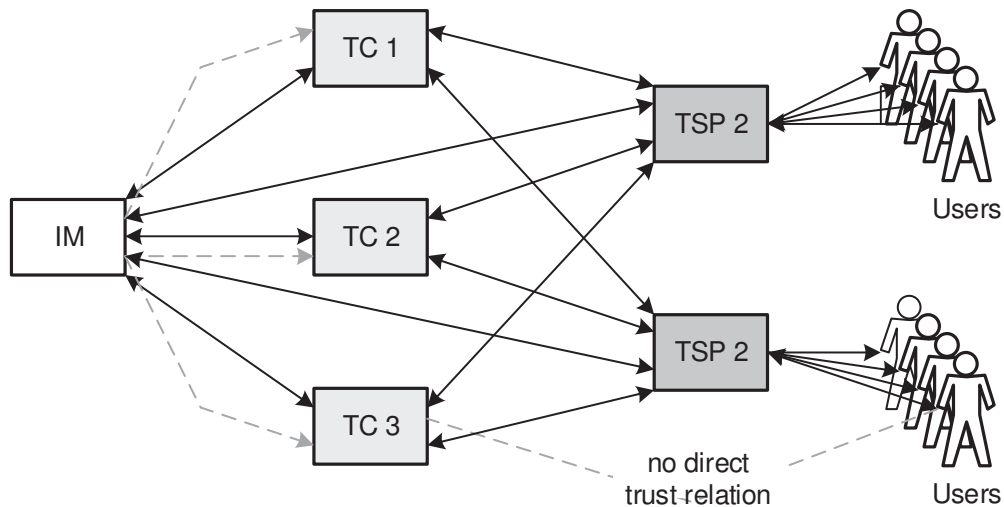


Figure 7 — Stakeholder trust relations

The interoperability management can be a single organization or a set of several entities performing different tasks. Issuing rules, regulations, and general user information by the interoperability management (IM) is performed by means of a trusted relation which is outside of the scope of this document (dotted arrows in Figure 7). Trust relations between IM and TC or TSP are among others used for certification of organization or equipment and TTP functions in case this is performed by the IM.

One supported model is an agreement between TC and TSP to use a Trusted Third Party (TTP) (e.g. for issuing public-key root certificates). Such relation can include the IM relations to TC and TSP. The TTP may either be performed as a part of the IM, or external TTP(s) may be used to issue the root certificates. This document does not require a mandatory TTP in a hierarchical trust model, but supports the use of it.

Another supported model is based on an agreement between TC and TSP (direct trust), which is performed by exchanging self-signed root certificates. Such a peer-to-peer trust relation can also include the IM relations to TC and TSP. This document does not require a mandatory peer-to-peer trust model but supports the use of it.

The technical trust relation of any chosen trust model between TSP and service user (SU) as well as the indirect trust relation between TC and SU are outside the scope of this document.

5.3 Technical trust model

5.3.1 General

The technical trust model defines the trust relations between the different stakeholders.

5.3.2 Trust model for TC and TSP relations

The technical trust model uses the ISO/IEC 9594-8, (X.509) version 3 public-key and attribute certificate frameworks for establishing secure communication channels. These secure communication channels

ensure confidentiality, integrity, authenticity, and non-repudiation (only with proof of origin) of the messages exchanged between TC and TSP.

The use of ISO/IEC 9594-8, i.e. using the possibility to import and use in parallel different (self-signed) root certificates in the trust model, enables the support of both a peer-to-peer approach and a hierarchical approach using a trusted third party. In addition, it also allows a mixed approach with peer-to-peer relations between TC and TSP on the one hand, and a TTP certification authority (CA) approach on the other hand.

Figure 8 illustrates an example of a trust model approach which is supported by this document.

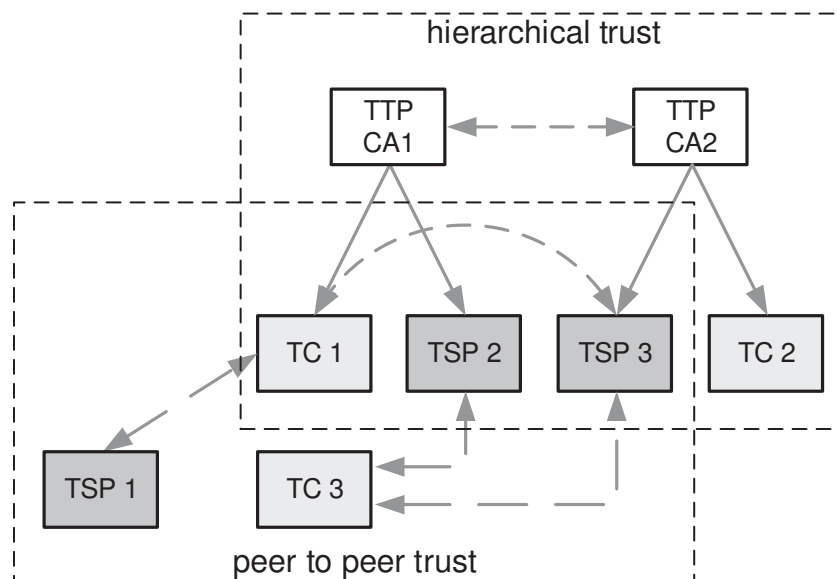


Figure 8 — Example of a mixed trust model environment

Figure 8 indicates the possibility of a trust model allowing an entity to participate in a mixed environment that uses both approaches. The dotted box marked as “hierarchical trust” shows the trusted third parties in their roles as certification authorities (CA1 and CA2), issuing certificates for each entity based on its self-signed root certificate imported by the entities. It is also possible that the TTP CAs directly issue certificates for the technical entities communicating with each other. In this case, no root certificate would exist and securing all interfaces would be established by bilaterally accepting self-signed certificates.

A trust relation can also be established across different TTP CAs as indicated by the dotted connections TC1 trusts TTP CA1 and TSP3 trusts TTP CA2. TTP CA1 also trusts TTP CA2 and vice versa. Therefore, there is also a trust relation between TC1 and TSP3.

The dotted box marked as “peer-to-peer trust” shows entities generating self-signed root certificates. Entities in the overlapping part of the boxes (i.e. TC1, TSP2, and TSP3) import both the certificates issued by the TTP CAs and the connected peer-to-peer trust partner (i.e. TC3, TSP1) self-signed root certificates.

The use of the ISO/IEC 9594-8 framework and certificates also enables hierarchical CA structures with a root CA and subordinate level CAs. To limit implementation complexity and to support interoperability, the set of allowed certification levels shall be limited as indicated in 5.4.3.

The used type and structure of the model for the trust relation between the involved stakeholders is a decision of their contractual framework and depends on their technical requirements, as well as on the

legal framework. The IM in an interoperable EFC system shall develop and maintain a suitable trust model. An example for EETS can be found in Annex F.

5.3.3 Trust model for TSP and service user relations

A standardized trust relation mechanism for the trust between TSP and service user is not required for interoperability. The solution for a trusted and secured communication between TSP and service user is a decision taken by the TSP based on the legal requirements for the contract between TSP and service user.

According to ISO 17573-1, the operation of the OBE and the provision of toll declarations in a secure way is part of the toll service provider role. Requirements for achieving end-to-end security from the OBE to the interface to the TCs systems is therefore considered to be an internal interface of the TSP. If security requirements from clause **Erreur ! Source du renvoi introuvable.** for end-to-end security are imposed by the security policy, the associated security measures from clause 7 need to be implemented.

5.3.4 Trust model for Interoperability Management relations

The interoperability management may issue rules, regulations, and standards for the EFC system via commonly recognized channels. Communication between IM and TC or TSP (e.g. for certification of organizations or equipment) can be done with methods such as physical mail and face to face meetings. No technical trust model is required for either of these communications.

For all cases where electronic data exchange channels are required, the same technical trust model as defined in 5.3.2 shall be used.

5.4 Implementation

5.4.1 Setup of trust relations

After TC and TSP have agreed on the trust relation to be used and have signed a contract, they shall setup the technical trust relation.

The initial step for the setup of the trust relation is the import of a root certificate. This can be either the CA root certificate of an agreed TTP acting as a root CA or a (self-signed) root certificate of the TC or TSP respectively, as explained in 5.3.2.

If using a TTP, the retrieval of the CA root certificate shall be done according to mechanism 3 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent. Several procedures might be used such as the following:

- downloading the certificate from a recognized and secure website;
- retrieving it per courier, if supported by the TTP;
- receiving it through signed e-mail, etc.

In the case of a peer-to-peer trust model, the exchange of the CA root certificates between TC and TSP shall be done using a secure communication channel which ensures the authenticity of the issuer and sender (proof of origin). Exchange of the root certificates shall be done with one of the following two public key transport mechanisms:

- Mechanism 1: This mechanism shall fulfil the requirements and implement the measures of mechanism 1 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by a physical meeting when both stakeholders (representatives of the TC and TSP, respectively) exchange valid identification tokens (e.g. passport) and documents proving the relationship with their organization.

ISO/IEC 11770-3 public key transport mechanism 1 may be implemented as a part of the contract signing process to guarantee the certificate and public key authenticity.

- Mechanism 2: This mechanism shall fulfil the requirements and implement the measures of mechanism 2 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by sending the root certificate through signed e-mail (using another certificate, e.g. issued by a TTP) and then checking the fingerprint through telephone or sending the certificate through courier which authenticates the sender.

If ISO/IEC 11770-3 public key transport mechanism 2 is used, the key token verification shall be done using fingerprint of the root certificate based on the algorithms defined in ISO 12855:2015.

5.4.2 Trust relation renewal and revocation

The root certificate shall have a validity and key length recommended for the use during the planned contract duration between TC and TSP.

NOTE For recommended key length and validity periods, see, for example

- the ENISA recommendations from 2014 under <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>
- the NIST recommendations from 2016 under <https://www.keylength.com/en/4/> or
- the ECRYPT-CSA recommendations from 2018 under <https://www.keylength.com/en/3/>.

The trust relation shall automatically end when a root certificate is not replaced by the date of expiration.

Replacement of a root certificate shall be done as specified in 5.4.1. All issued end-entity certificates of this root certificate shall be renewed according to the process defined in 5.4.3.

A certificate issuer shall be able to revoke a root certificate before its expiration. Revocation of a root certificate shall be done by a procedure similar to the termination of the commercial contract between TC and TSP and results in a termination of the trust relation. The trust relation shall automatically end when a root certificate is revoked.

Information about revocation of a root certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8, signed with the private key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Further activities that are necessary to handle compromised root certificates are beyond the scope of this document.

5.4.3 Issuing and revocation of sub CA and end-entity certificates

The private key of the root certificate shall only be used for signing end-entity or sub CA certificates. The purpose and usage of the end-entity certificate (e.g. TC to TSP communication) shall be defined by using the extended key usage extension in the ISO/IEC 9594-8 certificate.

The implementation of the certificate verification process shall support a certificate chain starting from a root certificate and containing up to four certificate levels (i.e. Root > CA1 > CA2 > CA3 > End-Entity) signed by a sub CA or end-entity private key.

Each entity shall have at least three different end-entity certificates to be used for:

- secure communication channels,
- message signing, and
- message or key encryption purposes.

These end-entity certificates should have a validity period of less than two years.

Information about revocation of an end-entity certificate shall be distributed by issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8, signed by the private key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Exchange of certificates and CRLs is defined in Clause 9.

5.4.4 Certificate and certificate revocation list profile and format

The certificates issued according to ISO/IEC 9594-8 certificates version 3 and the CRL according to ISO/IEC 9594-8 version 2 shall be conformant to the profile defined in IETF RFC 5280 with the update specified in RFC 6818. An implementation compliant to the above documents shall at least support all possible critical certificate and CRL extensions as defined in IETF RFC 5280 profile with the update specified in RFC 6818.

All root, sub CA, and end-entity certificates shall be encoded according to the distinguished encoding rules (DER) as defined in ISO/IEC 8825-1 and thereafter, be Base64-encoded as defined in IETF RFC 4648 and enclosed by „---BEGIN CERTIFICATE---“ and „---END CERTIFICATE---“, i.e. as defined in the PEM (privacy enhanced mail) certificate format.

All CRL shall be DER encoded as defined in ISO/IEC 8825-1 and thereafter, be Base64-encoded (as defined in IETF RFC 4648) and enclosed by „---BEGIN X.509 CRL---“ and „---END X.509 CRL---“, i.e. as defined in the PEM CRL format.

All certificates and CRL shall have a fingerprint in hexadecimal format based on the algorithms defined in ISO 12855:2015.

5.4.5 Certificate extensions

Considering IETF RFC 5280:2008, 4.2 and clarifications in ISO/IEC 9594-8:2017, Clause 7, the processing of critical extensions is delicate and shall be clearly agreed between the stakeholders (TC and TSP) to avoid implementation problems when the involved PKI platform technologies do not support the processing of certificates with certain extensions marked as critical.

Each extension used in a certificate shall be designated as either critical or non-critical. A system shall reject a certificate if it encounters a critical certificate extension it does not recognize or a critical certificate extension that contains information it cannot process. A non-critical extension may be ignored if it is not recognized but shall be processed if it is recognized.

NOTE Any extension that is flagged non-critical can cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension and will ignore it.

A root certificate shall only use the certificate extensions listed below marked as critical:

- a) key usage;
- b) basic constraints.

An end-entity certificate shall use the certificate extensions listed below marked as critical:

- a) key usage: the values in Table 1 shall be used.
- b) Extended key usage with object identifier (OID) for the following:
 - TC to TSP interface certificate;
 - Front end to TSP back end interfaces certificate.

The following extensions may be present in root certificates as non-critical:

- a) CRL distribution points;
- b) authority information access.

The following extensions may be present in end-entity certificates as non-critical:

- a) basic constraints;
- b) CRL distribution points;
- c) authority information access.

Table 1 — Values for key usage

Value	Meaning
0	Digital signature
1	Content commitment
2	Key encipherment
3	Data encipherment
4	Key agreement
5	Key certificate signing
6	CRL signing
7	Encipher only
8	Decipher only

6 Security requirements

6.1 General

A security requirement is a functional or non-functional requirement that needs to be satisfied in order to protect against or mitigate the threats to an EFC system or to reduce its consequences.

Security requirements can be motivated by different sources. The following list presents some of the most relevant sources for EFC systems:

- generic information technology security requirements can be found in ISO Information Security Management System family of standards (e.g. in ISO/IEC 27001);
- security requirements for the protection of payment card data can be found in the Payment Card Industry Data Security Standard (PCI DSS),^[12] if applicable;
- system-specific security requirements based on a threat analysis of the EFC system as presented in this document in Annex D.

Mainly motivated by the threat analysis in Annex D, the following section specifies a basic set of information security requirements to protect the threatened assets in an EFC system.

The security policy for an EFC scheme or for an EFC operator's system may consider additional security requirements driven by the mentioned standards or other relevant sources.

NOTE A general and complete IT security guideline for an information security management system is provided in the ISO 2700x family of standards (see 1.2 and 6.2).

In order to be compliant with this document, an implementation shall fulfil all requirements selected in accordance with the applicable security policy. Any security measures from Clause 7 that are associated to the security requirements listed in this Clause shall be implemented when the relevant requirement is selected to be fulfilled.

If a requirement is not selected, implementation of the associated security measure. is not mandatory In addition to the security policy, there are also some security profiles defined in Annex A to ease the implementation of a common set of security requirements. If an entity states compliance with one or

more of the defined security profiles, all mentioned requirements are mandatory and the associated security measures shall be implemented.

Table 2 explains the notation of the requirements defined in this clause.

Table 2 — Notation of requirements

Table header	Meaning
No.	Unique number for every requirement to enable a later matching with the security measures.
Requirement	Definition of the requirement or recommendation.
DSRC	Marked with an X if this requirement is relevant for a DSRC system.
GNSS	Marked with an X if this requirement is relevant for an autonomous system.

Annex D provides a reference to the requirement(s) that is (are) driven by a given threat.

6.2 Information security management system

This document provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems, including their interoperable interfaces and specific assets. Those security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific.

TCs and TSPs shall analyse and evaluate the risks associated with those threats and should also identify and analyse more generic information and communication technology risks applicable to organizations operating EFC systems, by performing a comprehensive risk analysis according to ISO/IEC 27005.

In order to effectively ensure information security in a holistic approach, TCs and TSPs shall establish, implement, operate, monitor, review, maintain, and continuously improve an Information Security Management System (ISMS) according to ISO/IEC 27001. The ISMS shall consider the EFC business processes specified in ISO 17573-1 within its scope and consider, among others, the risks identified in this document. The security measures defined in this Technical Specification shall be used while defining and implementing the controls for minimizing the impact of the identified risks.

The ISMS should also consider the generic companies business processes as part of its scope (see Table 3).

Table 3 — ISMS requirements

No.	Requirement	DSRC	GNSS
RQ.ISMS.01	An Information Security Management System (ISMS) according to ISO/IEC 27001 shall be established, implemented, operated, maintained, and continuously improved.	X	X
RQ.ISMS.02	Non-EFC specific threats shall be covered by a security measure or security control defined by the ISO/IEC 27002 or equivalent standard.	X	X

6.3 Communication interfaces

Communication interfaces are some of the most threatened links in the security chain of the EFC system as shown in the threat analysis in Annex D. Protecting interfaces against all threats without a basic risk analysis results in unreasonably high implementation costs. Table 4 lists all requirements identified in the threat analysis.

Table 4 — General interface requirements

No.	Requirement	DSRC	GNSS
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	X	X
RQ.IF.10	Data exchange shall guarantee data confidentiality.	X	X
RQ.IF.11	Data exchange shall guarantee data integrity.	X	X
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	X	X
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	X	X
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.	X	X
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.	X	X
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	X	X
RQ.IF.31	Data exchange shall allow the detection of mass rejection of toll declarations (protection against interface errors).	X	X
RQ.IF.32	Data exchange shall allow the detection of mass rejection of billing details (protection against interface errors).	X	X

6.4 Data storage

Data storage shall fulfil the requirements in Table 5 independently of the state of data processing.

Table 5 — Data storage requirements

No.	Requirement	DSRC	GNSS
RQ.DS.01	Access to stored data shall only be granted after authorization.	X	X
RQ.DS.02	Access to stored data shall only be granted via defined interfaces and defined procedures.	X	X
RQ.DS.03	Stored data shall have an independent backup storage.	X	X
RQ.DS.04	The amount of sensitive EFC data stored on an ICC shall be minimized	X	X
RQ.DS.05	Data storage shall guarantee data integrity.	X	X
RQ.DS.06	Access to data storage shall guarantee data confidentiality.	X	X
RQ.DS.07	Data storage shall guarantee non-repudiation with proof of origin for applicable data.	X	X
RQ.DS.08	Data storage shall guarantee non-repudiation with proof of delivery for applicable data.	X	X

6.5 Toll charger

Table 6 lists the requirements for protection of the TCs assets.

Table 6 — Toll charger requirements (1 of 2)

No.	Requirement	DSRC	GNSS
RQ.TC.01	The TC shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations either acquired directly through the TCs RSE or through a TSP (enabled by RQ.TSP.51 for autonomous systems).	X	X
RQ.TC.02	In case the TC performs spot checks, he shall be able to determine the OBE working status (enabled by RQ.TSP.53 for autonomous systems).	X	X
RQ.TC.03	In case the TC performs spot checks, he shall be able to determine the ICC working status in the OBE.	X	X
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the OBE.	X	X
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate OBE or TSP back end (enabled by RQ.TSP.55).	X	X
RQ.TC.06	The TC shall make sure that any invoices generated in his name and on his behalf are conformant to the invoicing rules of his country (enabled by RQ.TSP.56).	X	X
RQ.TC.07	The TC shall ensure that the TSPs OBE is suitable for use in his toll domain.	X	X
RQ.TC.08	The TC shall check the model and make of OBE during a vehicle check (enabled by RQ.TSP.58) to identify the use of OBE versions not certified by the TC.	X	X
RQ.TC.10	The TC shall implement all necessary technical and organizational mechanisms for a correct implementation of a set of keys for OBE communication provided by the TSP.	X	X
RQ.TC.11	The TC shall implement all necessary technical and organizational mechanisms for a correct implementation of a set of keys for ICC communication provided by the ICC issuer.	X	X
RQ.TC.12	The TC shall make sure that his back end system can cope with a sudden change of the customization information of an OBE (e.g. change of license plate over the air).	X	X
RQ.TC.13	The TC shall verify the correctness of billing details received from the TSP. NOTE This requirement is not applicable where the billing details are provided by the TC (this is covered by RQ.TSP.12).	n.a.	X
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality within an agreed time frame.	X	X
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part within an agreed time frame.	X	X
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication based upon security level 1 as defined in EN 15509 or equivalent national standards/regulations.	X	X
RQ.TC.23	The TC shall detect RSE malfunction or underperformance and correct it within an agreed time frame.	X	X
RQ.TC.24	The TC shall not allow unauthorized access to RSE software and data.	X	X
RQ.TC.25	The TC shall guarantee confidentiality, integrity and non-repudiation with proof of origin of a set of keys for OBE communication during transfer to the RSE.	X	X

Table 6 — Toll charger requirements (2 of 2)

No.	Requirement	DSRC	GNSS
RQ.TC.26	The TC shall guarantee confidentiality, integrity and non-repudiation with proof of origin of a set of keys for ICC communication during transfer to the RSE.	X	X
RQ.TC.30	The TC shall implement all necessary technical and organizational measures to avoid an enforcement case when a correct toll declaration was received.	X	X
RQ.TC.31	The TC shall make sure that the correct service user is charged for an enforcement case.	X	X
RQ.TC.32	The TC shall make sure that the enforcement case data are court proof.	X	X
RQ.TC.50	A data protection commissioner or delegate shall have the possibility to audit the system for compliance with data privacy regulations. NOTE Such audits shall be used to prove the data protection concept.	X	X
RQ.TC.51	The TC shall publish his procedures of collecting and processing personal data or register them with the responsible data protection authorities.	X	X
RQ.TC.70	The TC shall exhaustively test all features of an RSE update before it is implemented.	X	X
RQ.TC.71	The TC shall have a rollback scenario ready before an RSE update is implemented.	X	X
RQ.TC.90	The TCs systems shall be designed in a way that access to stored or processed data is only possible within the legal context of the respective country (e.g. lawful interception).	X	X
RQ.TC.91	The TC shall provide non-repudiation with proof of origin for distributed toll context data.	X	X
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific OBE (enabled by RQ.TSP.62).	X	X
RQ.TC.93	The TC shall only accept an OBE after detecting if the ICC in the OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific ICC.	X	X
RQ.TC.94	The TC shall only accept an exception list after verification of non-repudiation with proof of origin.	X	X
RQ.TC.95	The TC shall be responsible for the availability of his back office interfaces according to agreed service levels.	X	X
RQ.TC.96	The TC shall be responsible for the availability of his RSE interfaces to an OBE according to agreed service levels.	X	X
RQ.TC.97	The TC shall verify the provided non-repudiation with proof of delivery in the TSPs acknowledge for distributed toll context data.	X	X
RQ.TC.98	The TC shall implement all necessary technical and organizational measures to guarantee the distribution of correct toll context data to the TSP.	X	X
RQ.TC.99	The TC shall acknowledge a received exception list and provide non-repudiation with proof of delivery to the TSP.	X	X

6.6 Toll service provider

Table 7 lists the requirements for the protection of the TSPs assets.

Table 7 — Toll service provider requirements (1 of 3)

No.	Requirement	DSRC	GNSS
RQ.TSP.01	The TSP shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations.	n.a.	X
RQ.TSP.03	The TSP shall check the integrity and authenticity of the received road usage data sent from the OBE.	n.a.	X
RQ.TSP.04	The TSP shall determine if toll declarations are based on data originating from a legitimate OBE or ICC.	X	X
RQ.TSP.05	The OBE shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.06	The ICC shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.07	The OBE shall not allow the service user to modify fixed vehicle parameters.	X	X
RQ.TSP.08	The TSP shall detect duplicate or false OBE or ICC identities and block such OBE or ICC identities by placing them on the exception list.	X	X
RQ.TSP.09	The TSP shall notify the service user if the OBE or ICC is not working correctly.	X	X
RQ.TSP.10	The TSP shall determine if billing details are based on correct and complete road usage data.	n.a.	X
RQ.TSP.11	The TSP shall determine if factual road usage is represented by a corresponding set of billing details.	n.a.	X
RQ.TSP.12	The TSP shall verify the correctness of billing details received from the TC. NOTE This requirement is not applicable where the billing details are provided by the TSP (this is covered by RQ.TC.13).	X	n.a.
RQ.TSP.13	The TSP shall accept received toll context data only after verification of non-repudiation with proof of origin.	X	X
RQ.TSP.14	The TSP shall provide exception lists including non-repudiation with proof of origin to the TC.	X	X
RQ.TSP.15	The ICC shall not allow the service user to modify fixed account data.	X	X
RQ.TSP.16	The OBE shall detect signal input inconsistencies.	n.a.	X
RQ.TSP.17	The TSP shall acknowledge received toll context data and provide non-repudiation with proof of delivery to the TC.	X	X
RQ.TSP.18	The TSP shall verify the provided non-repudiation with proof of delivery in the TCs acknowledge for a distributed exception list.	X	X
RQ.TSP.19	The TSP shall notify the TC about stolen or cloned OBE or ICC.	X	X
RQ.TSP.20	The TSP shall accept reports of stolen OBE or ICC by service users.	X	X
RQ.TSP.21	The TSP shall detect cloned OBE or ICC and block them by placing them on the exception list.	X	X
RQ.TSP.40	The OBE shall not allow change of internal data through the user interface except the data allowed to be changed.	X	X

Table 7 — Toll service provider requirements (2 of 3)

No.	Requirement	DSRC	GNSS
RQ.TSP.41	The OBE shall only present intended data by the user interface.	X	X
RQ.TSP.42	The TSPs implementation of the front end and gathering and processing of data shall be in compliance with the privacy requirements of the toll domain.	X	X
RQ.TSP.43	The TSP shall store entry evidence data of a vehicle in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC in a closed toll regime.	X	X
RQ.TSP.44	The TSP shall verify the entry evidence data stored in the data group ReceiptEntryVehicle (see ISO/TS 21193) inside an ICC with the current vehicle information on an exit transaction in a closed toll regime.	X	X
RQ.TSP.50	The TSP shall ensure that only authenticated service users have access to systems that manage their personal data.	X	X
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of correct and complete toll declarations sent either directly from the OBE to the TCs RSE (in a DSRC system) or through a back office data exchange (required to enable RQ.TC.01 for autonomous systems).	X	X
RQ.TSP.53	The TSP shall enable the TC to perform spot checks through CCC (required to enable RQ.TC.02 for autonomous systems).	X	X
RQ.TSP.55	The TSP shall enable the TC to determine if toll declarations are based on data originating from a legitimate front end (required to enable RQ.TC.05 for autonomous systems) or OBE (in a DSRC system).	X	X
RQ.TSP.56	The TSP shall enable the TC to audit invoices to service users for tolls of his toll domain (required to enable RQ.TC.06).	X	X
RQ.TSP.57	The TSP shall enable the service user to check the correctness of an invoice.	X	X
RQ.TSP.58	The TSP shall enable the TC to check the model and make of OBE during a vehicle check (required to enable RQ.TC.08). NOTE The data in the relevant fields are set by the manufacturer during production. The responsibility of the TSP is to provide the TC with the different possible values for these fields to distinguish between the different OBE models and makes.	X	X
RQ.TSP.59	The TSP shall publish his procedures of collecting and processing personal data or register them with the responsible data protection authorities.	X	X
RQ.TSP.60	The TSP shall only use equipment that passed certification by the TC and delivers the agreed quality of service.	X	X
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).	X	X
RQ.TSP.70	The TSP shall extensively test all features of an OBE update before it is implemented (e.g. distributed over the air).	X	X
RQ.TSP.71	The TSP shall have a rollback scenario ready before an OBE update is implemented (e.g. distributed over the air).	X	X
RQ.TSP.80	The TSP shall implement all necessary technical and organizational quality control mechanisms for all OBE before they are distributed to the service users.	X	X

Table 7 — Toll service provider requirements (3 of 3)

No.	Requirement	DSRC	GNSS
RQ.TSP.81	The TSP shall implement all necessary technical and organizational quality control mechanism for the provision of a key set for OBE communication to the TC.	X	X
RQ.TSP.82	The TSP shall implement all necessary technical and organizational quality control mechanism for the maintenance or exchange of OBE with low performance.	X	X
RQ.TSP.89	The TSP shall take protective measures against repudiation of invoices and its underlying confirmation data by service users.	X	X
RQ.TSP.90	The TSPs systems should be designed in a way that access to stored or processed data is only possible within the legal context of the respective countries (lawful interception).	X	X
RQ.TSP.91	The data communication between front end (OBE) and back end (TSP) shall be protected against interception in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).	n.a.	X
RQ.TSP.92	Initialisation and customization of OBE shall be done in a secure way to guarantee data integrity and non-repudiation with proof of origin.	X	X
RQ.TSP.95	The TSP shall be responsible for the availability of his back office interfaces according to agreed service levels.	X	X
RQ.TSP.96	The TSP shall guarantee the availability of its POS network according to agreed service levels.	X	X
RQ.TSP.97	The TSP shall implement all necessary technical and organizational measures to guarantee that an update of the customization information is correct.	X	X

6.7 Interoperability Management

The main security requirement for an interoperability management is to ensure the trust of all stakeholders in the interoperability scheme (see Table 8).

Table 8 — Interoperability management requirements

No.	Requirement	DSRC	GNSS
RQ.IM.01	The interoperability management shall issue an EFC security policy. NOTE Examples explaining the content of such a security policy are given in Annex E and Annex F.	X	X
RQ.IM.02	The interoperability management shall have or define one or more auditing bodies supervising the security implementation of the TSP and TC involved in the interoperable EFC scheme.	X	X

6.8 Limitation of requirements

The requirements in Table 9 are included to document the limitation of security measures against some threats. This means that either no required security measure exists to protect against the threat, or the security measure is not feasible because it is much too expensive. The requirements in Table 9 are not further treated in this document.

Table 9 — Denial of service and hardware integrity threats

No.	Requirement	DSRC	GNSS
RQ.XX.01	Prevent denial of service attack. Prevent message transmission delay. This requirement covers attacks against a communication interface or against a whole service. A simple and/or cheap security measure does not exist due to the fact that long distance communication interfaces cannot be protected against all kinds of imaginable attacks.	X	X
RQ.XX.02	Prevent manipulating equipment; especially prevent OBE from hardware (HW) manipulation. Such a requirement can be fulfilled by developing a tamperproof OBE, which is not deemed viable from a cost efficiency perspective.	X	X

7 Security measures — countermeasures

7.1 Overview

A security measure describes actions to be taken by the addressed entity to satisfy one or more security requirements. The actual implementation of the action is up to the entity. A security measure describes one possible solution to satisfy one or more security requirements.

In order to be compliant with this document, an implementation shall fulfil all security measures that are associated to the security requirements in Clause 6 which are selected in accordance with the applicable security policy.

Table 10 explains the notation and relations of the security measures defined in this Clause.

Table 10 — Notation and relations of security measures

Table header	Meaning
No.	Unique number for every security measure
Security measure	Description of the security measure (countermeasure)
DSRC	Marked with an X if this security measure is relevant for a DSRC system
GNSS	Marked with an X if this security measure is relevant for an autonomous system
Fulfilled RQ	List of requirements that the security measure fulfils

NOTE For a detailed definition for the implementation of communication interface security measure, see Clause 8.

7.2 General security measures

This document provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems including their interoperable interfaces and specific assets. These security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific (see Table 11).

Table 11 — General security measures

No.	Security measure	DSRC	GNSS
		Fulfilled RQ	
SM.101	The TC and TSP shall publish their procedures of collecting and processing personal data or register the data processing application of the EFC system with the national data protection commissioner or authority for compliance with national data protection regulations if required by law.	X	X
		RQ.TC.50 RQ.TC.51 RQ.TSP.42 RQ.TSP.59 RQ.TSP.91	
SM.102	The TC and the TSP shall sign an agreement on the protection of personal data[HM1] to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the TSP are stated in regard to the data processing.	X	X
		RQ.TSP.42 RQ.TSP.91 RQ.TC.06 RQ.TSP.56 RQ.TSP.89	
SM.103	The contracting parties of communication providers shall sign an agreement on the protection of personal data to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the communication provider are stated in regard to the processing of personal data.	X	X
		RQ.TSP.42 RQ.TSP.91	
SM.104	The TC shall have the possibility to perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the agreement on the protection of personal data.	X	X
		RQ.TSP.42 RQ.TSP.91	
SM.105	The contracting parties of communication providers shall have the possibility to perform audit(s) of the communication providers systems and procedures to prove the adherence to the registered data processing application and the agreement on the protection of personal data.	X	X
		RQ.TSP.42 RQ.TSP.91	
SM.106	The TSP shall establish a quality control process for the maintenance or exchange of low performing OBE within an agreed time frame. This process may be initiated by the detection of a low performing OBE by the TSP or by a report of such an OBE by the TC.	X	X
		RQ.TSP.82	
SM.107	The TSP shall enable the TC to audit invoices generated in his name. The TC shall periodically audit invoices to service users for tolls of his toll domain.	X	X
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	

7.3 Communication interfaces security measures

7.3.1 General

Table 12 contains the security measures for the protection of data exchanged between entities using the different interfaces.