

E DIN EN ISO 19299:2019-12 (E)

Erscheinungsdatum: 2019-11-15

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

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