ISO 19299:2020 (E)

Electronic fee collection — Security framework

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Trust model

5.1 Overview
5.2 Stakeholders trust relations
5.3 Technical trust model
5.3.1 General
5.3.2 Trust model for TC and TSP relations
5.3.3 Trust model for TSP and service user relations
5.3.4 Trust model for interoperability management relations
5.4 Implementation
5.4.1 Setup of trust relations
5.4.2 Trust relation renewal and revocation
5.4.3 Issuing and revocation of sub CA and end-entity certificates
5.4.4 Certificate and certificate revocation list profile and format
5.4.5 Certificate extensions

6 Security requirements

6.1 General
6.2 Information security management system
6.3 Communication interfaces
6.4 Data storage
6.5 Toll charger
6.6 Toll service provider
6.7 Interoperability management
6.8 Limitation of requirements

7 Security measures — Countermeasures

7.1 Overview
7.2 General security measures
7.3 Communication interfaces security measures
7.3.1 General
7.3.2 DSRC-EFC interface
7.3.3 CCC interface
7.3.4 LAC interface
7.3.5 Front End to TSP back end interface
7.3.6 TC to TSP interface
7.3.7 ICC interface
7.4 End-to-end security measures
7.5 Toll service provider security measures
7.5.1 Front end security measures
7.5.2 Back end security measures
7.6 Toll charger security measures
7.6.1 RSE security measures

7.6.2 Back end security measures
7.6.3 Other TC security measures

8 Security specifications for interoperable interface implementation

8.1 General
8.1.1 Subject
8.1.2 Signature and hash algorithms
8.2 Security specifications for DSRC-EFC
8.2.1 Subject
8.2.2 OBE
8.2.3 RSE

9 Key management

9.1 Overview
9.2 Asymmetric keys
9.2.1 Key exchange between stakeholders
9.2.2 Key generation and certification
9.2.3 Protection of keys
9.2.4 Application
9.3 Symmetric keys
9.3.1 General
9.3.2 Key exchange between stakeholders
9.3.2.1 General
9.3.2.2 Key encryption algorithm
9.3.2.3 Padding algorithm
9.3.2.4 Key transfer
9.3.3 Key lifecycle
9.3.3.1 General
9.3.3.2 DSRC keys
9.3.3.3 MAC keys
9.3.4 Key storage and protection
9.3.4.1 Master keys
9.3.4.2 OBE keys
9.3.5 Session keys

Annex A (normative) Security profiles

A.1 General
A.2 Communication interface profiles
A.2.1 TC to TSP profiles
A.2.2 Communication provider profile
A.2.3 ICC interface profile
A.3 Data storage profiles
A.3.1 OBE data storages profile
A.3.2 ICC data storage profile
A.3.3 RSE data storage profile
A.3.4 Back end data storage profile

Annex B (informative) Implementation conformance statement (ICS) proforma

B.1 Guidance for completing the ICS proforma
B.1.1 Purposes and structure
B.1.2 Abbreviations and conventions
B.2 Identification of the implementation
B.2.1 General
B.2.2 Date of the statement
B.2.3 Implementation Under Test (IUT) identification
B.2.4 System Under Test (SUT) identification
B.2.5 Supplier
B.2.6 Actor (if different from supplier)
B.2.7 ICS contact person
B.3 Identification of the standard
B.4 Global statement of conformance
B.5 Roles
B.6 Trust model
B.7 Profiles

B.8 Requirements
B.9 Security measures
B.10 Specifications for interoperable interfaces security
B.11 Specifications for key management

Annex C (informative) Stakeholder objectives and generic requirements

C.1 General
C.2 Toll chargers
C.2.1 Toll chargers and their main interests
C.2.2 Security service requirements for a toll charger
C.3 Toll service providers
C.3.1 Toll service providers and their main interests
C.3.2 Security service requirements for a toll service provider
C.4 Service users
C.4.1 Service users and their main interests
C.4.2 Service user requirements
C.5 Interoperability management
C.5.1 Interoperability management and its main interests
C.5.2 Security service requirements for interoperability management

Annex D (informative) Threat analysis

D.1 General
D.1.1 General approach
D.1.2 Naming conventions
D.1.3 Statement of completeness
D.2 Attack trees-based threat analysis
D.2.1 Overview
D.2.2 System model
D.2.3 Presentation of attack trees
D.2.4 Attacker class 1: Service user
D.2.4.1 General
D.2.4.2 Goal 101: Avoiding payment of toll
D.2.4.2.1 Sub goal: Manipulating the system to not register road usage
D.2.4.2.2 Sub goal: Manipulating the system to register the wrong road usage
D.2.4.2.3 Sub goal: Faking toll parameters
D.2.4.2.4 Sub goal: Manipulating the system to lose road usage data
D.2.4.3 Goal 102: Undermining the system
D.2.4.4 Goal 103: Protecting the service user's privacy
D.2.5 Attacker class 2: Toll service provider
D.2.5.1 General
D.2.5.2 Goal 104: Increase revenue from service user/overcharge service user
D.2.5.3 Goal 105: Profiling of service user(s)
D.2.5.4 Goal 106: Reselling of data about service user(s)
D.2.5.5 Goal 107: Reduction of payments to toll charger
D.2.5.6 Goal 108: Use of cheaper (substandard) equipment
D.2.5.7 Goal 109: Neglect maintenance of equipment
D.2.5.8 Goal 110: Delaying payment to TC
D.2.6 Attacker class 3: Toll charger
D.2.6.1 General
D.2.6.2 Goal 111: Increase revenue
D.2.6.3 Goal 106: Reselling of data about service users
D.2.6.4 Goal 112: Neglect maintenance of equipment
D.2.6.5 Goal 113: Poor management of toll context data
D.2.6.6 Goal 114: Delaying payment of TSP remuneration
D.2.7 Attacker class 4: Hacker
D.2.7.1 General
D.2.7.2 Goal 115: Demonstrate system vulnerability
D.2.7.3 Goal 116: Obtain respect amongst their peers
D.2.7.4 Goal 117: Improve understanding of the system or to research its operation
D.2.7.5 Goal 118: Provide fake OBE or ICC
D.2.8 Attacker class 5: Activist
D.2.8.1 General
D.2.8.2 Goal 119: Societal destabilization
D.2.8.3 Goal 120: Raise in profile of the activists' cause

D.2.8.4 Goal 121: Direct furthering of activists' cause
D.2.8.5 Goal 122: Reduction in credibility of the system
D.2.9 Attacker class 6: Communication provider
D.2.9.1 General
D.2.9.2 Goal 123: Increase network utilization
D.2.9.3 Goal 124: Decrease network utilization
D.2.9.4 Goal 125: Collecting travel behaviour
D.2.10 Attacker class 7: Enterprise
D.2.10.1 General
D.2.10.2 Goal 126: Movement tracking
D.2.10.3 Goal 127: Creation and distribution of cloned equipment
D.2.10.4 Goal 128: Disable/compromise system encryption
D.2.10.5 Goal 129: Steal equipment
D.2.10.6 Goal 130: Extortion
D.2.11 Attacker class 8: Government
D.2.11.1 General
D.2.11.2 Goal 131: In theatre commercial advantage
D.2.11.3 Goal 132: Political targeting of individuals and organizations
D.2.11.4 Goal 133: Tracking of individuals by interception of data communication
D.2.11.5 Goal 134: Tracking of individuals by direct access to data through power of authority
D.2.12 Attacker class 9: Foreign state agency
D.2.12.1 General
D.2.12.2 Goal 119: Societal destabilization
D.2.12.3 Goal 135: Movement tracking
D.2.12.4 Goal 136: Extortion
D.2.12.5 Goal 137: International prestige
D.3 Asset-based threat analysis
D.3.1 General
D.3.2 Threatened assets
D.3.3 Compliance matrix
D.3.4 Presentation of threats
D.3.5 Generic threats
D.3.5.1 Asset 201: Information assets
D.3.5.2 Asset 202: Infrastructure assets
D.3.6 Asset 203: Billing details
D.3.7 Asset 204: OBE charge report
D.3.8 Asset 205: Customization information
D.3.9 Asset 206: Service user contract information
D.3.10 Asset 207: Exception list
D.3.11 Asset 208: Customer service
D.3.12 Asset 209: OBE
D.3.13 Asset 210: Service user privacy
D.3.14 Asset 211: RSE
D.3.15 Asset 212: EFC stakeholder image and reputation
D.3.16 Asset 213: TC and TSP central system
D.3.17 Asset 214: Road usage data
D.3.18 Asset 215: Trust objects
D.3.19 Asset 216: Service user identification
D.3.20 Asset 217: Toll context data
D.3.21 Asset 218: Payment means
D.3.22 Asset 219: Limited autonomy
D.3.23 Asset 220: EFC schema
D.3.24 Asset 221: Contractual conditions
D.3.25 Asset 222: Operational rules
D.3.26 Asset 223: Complaints
D.3.27 Asset 224: Certification
D.3.28 Asset 225: Quality assurance parameter reporting
D.3.29 Asset 226: Enforcement data
D.3.30 Asset 227: Invoice
D.3.31 Asset 228: ICC

Annex E (informative) Security policies

E.1 General
E.1.1 Overview of this Annex

E.1.2 Motivation for the need of security policies
E.2 Example EFC scheme security policy
E.2.1 Motivation for information security
E.2.2 Purpose of the security policy
E.2.3 Scope of the security policy
E.2.4 Policy statements
E.2.4.1 General
E.2.4.2 General policy statements
E.2.4.3 Organization of information security
E.2.4.4 Asset management
E.2.4.5 Violations and sanctions
E.2.4.6 Review and evaluation
E.2.4.7 Audits
E.3 Development of operators' security policies
E.3.1 General
E.3.2 Interface requirements
E.3.3 Data storage requirements

Annex F (informative) Example for an EETS security policy

F.1 General
F.2 Basic laws and regulations
F.3 Organization of EETS information security
F.3.1 General
F.3.2 Steering committee
F.3.3 Trust model

Annex G (informative) Recommendations for privacy-focused implementation

G.1 General
G.2 Legal basis in the EU
G.2.1 European general data protection regulation (EU Directive 2016/679/EC)
G.2.2 European General Data Protection Directive (GDPR)
G.3 Service users' requirements

Page count: 129