DIN EN ISO 19299:2020-12 (E)

Electronic fee collection - Security framework (ISO 19299:2020); English version EN ISO 19299:2020

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Abbreviated terms **3**

5 Trust model **4**
5.1 Overview 4
5.2 Stakeholders trust relations 5
5.3 Technical trust model 6
5.3.1 General 6
5.3.2 Trust model for TC and TSP relations 6
5.3.3 Trust model for TSP and service user relations 7
5.3.4 Trust model for interoperability management relations 7
5.4 Implementation 7
5.4.1 Setup of trust relations 7
5.4.2 Trust relation renewal and revocation 8
5.4.3 Issuing and revocation of sub CA and end-entity certificates 8
5.4.4 Certificate and certificate revocation list profile and format 9
5.4.5 Certificate extensions 9

6 Security requirements **10**
6.1 General 10
6.2 Information security management system 11
6.3 Communication interfaces 12
6.4 Data storage 12
6.5 Toll charger 12
6.6 Toll service provider 14
6.7 Interoperability management 16
6.8 Limitation of requirements 17

7 Security measures — Countermeasures **17**
7.1 Overview 17
7.2 General security measures 18
7.3 Communication interfaces security measures 18
7.3.1 General 18
7.3.2 DSRC-EFC interface 19
7.3.3 CCC interface 20
7.3.4 LAC interface 21
7.3.5 Front End to TSP back end interface 21
7.3.6 TC to TSP interface 22
7.3.7 ICC interface 23
7.4 End-to-end security measures 24
7.5 Toll service provider security measures 25
7.5.1 Front end security measures 25
7.5.2 Back end security measures 26

7.6 Toll charger security measures 27
7.6.1 RSE security measures 27
7.6.2 Back end security measures 28
7.6.3 Other TC security measures 28

8 Security specifications for interoperable interface implementation 29
8.1 General 29
8.1.1 Subject 29
8.1.2 Signature and hash algorithms 29
8.2 Security specifications for DSRC-EFC 29
8.2.1 Subject 29
8.2.2 OBE 29
8.2.3 RSE 29

9 Key management 30
9.1 Overview 30
9.2 Asymmetric keys 30
9.2.1 Key exchange between stakeholders 30
9.2.2 Key generation and certification 30
9.2.3 Protection of keys 30
9.2.4 Application 31
9.3 Symmetric keys 31
9.3.1 General 31
9.3.2 Key exchange between stakeholders 31
9.3.3 Key lifecycle 32
9.3.4 Key storage and protection 33
9.3.5 Session keys 34

Annex A (normative) **Security profiles 35**

Annex B (informative) **Implementation conformance statement (ICS) proforma 39**

Annex C (informative) **Stakeholder objectives and generic requirements 57**

Annex D (informative) **Threat analysis 61**

Annex E (informative) **Security policies 118**

Annex F (informative) **Example for an EETS security policy 124**

Annex G (informative) **Recommendations for privacy-focused implementation 126**

Bibliography 128