ISO/TS 19299:2015-10 (E)

Electronic fee collection - Security framework

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 2

3 Termsanddefinitions 4

4 Symbols and abbreviated terms 9

5 Trust model 10
5.1 Overview 10
5.2 Stakeholders trust relations 10
5.3 Technical trust model 11
5.3.1 General 11
5.3.2 Trust model for TC and TSP relations 11
5.3.3 Trust model for TSP and service user relations 13
5.3.4 Trust model for Interoperability Management relations 13
5.4 Implementation 13
5.4.1 Setup of trust relations 13
5.4.2 Trust relation renewal and revocation 14
5.4.3 Issuing and revocation of sub CA and end-entity certificates 14
5.4.4 Certificate and certificate revocation list profile and format 15
5.4.5 Certificate extensions 15

6 Security requirements 17
6.1 General 17
6.2 Information security management system 18
6.3 Communication interfaces 18
6.4 Data storage 19
6.5 Toll charger 19
6.6 Toll service provider 21
6.7 Interoperability Management 23
6.8 Limitation of requirements 23

7 Security measures -- countermeasures 24
7.1 Overview 24
7.2 General security measures 24
7.3 Communication interfaces security measures 25
7.3.1 General 25
7.3.2 DSRC-EFC interface 26
7.3.3 CCC interface 27
7.3.4 LAC interface 28
7.3.5 Front End to TSP back end interface 28
7.3.6 TC to TSP interface 29
7.3.7 ICC interface 30
7.4 End-to-end security measures 30
7.5 Toll service provider security measures 32
7.5.1 Front end security measures 32
7.5.2 Back end security measures 33

7.6 Toll charger security measures 34
7.6.1 RSE security measures 34
7.6.2 Back end security measures 34
7.6.3 Other TC security measures 35

8 Securityspecificationsforinteroperableinterfaceimplementation 35
8.1 General 35
8.1.1 Subject 35

8.1.2 Signature and hash algorithms 35
8.2 Security specifications for DSRC-EFC 36
8.2.1 Subject 36
8.2.2 OBE 36
8.2.3 RSE 36

9 Key management 36
9.1 Overview 36
9.2 Asymmetric keys 36
9.2.1 Key exchange between stakeholders 36
9.2.2 Key generation and certification 37
9.2.3 Protection of keys 37
9.2.4 Application 37
9.3 Symmetric keys 38
9.3.1 General 38
9.3.2 Key exchange between stakeholders 38
9.3.3 Key lifecycle 39
9.3.4 Key storage and protection 40
9.3.5 Session keys 41

Annex A (normative)Securityprofiles 42

Annex B (normative) Implementation conformance statement (ICS) proforma 46

Annex C (informative) Stakeholder objectives and generic requirements 64

Annex D (informative) Threat analysis 68

Annex E (informative) Security policies 124

Annex F (informative) Example for an EETS security policy 131

Annex G (informative) Recommendations for privacy-focused implementation 133

Annex H (informative)Proposalforend-entitycertificates 135

Bibliography 136