

# DIN EN ISO 19299:2020-12 (E)

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

---

### Contents

Page

<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>2</b>
<b>4 Abbreviated terms</b> .....	<b>3</b>
<b>5 Trust model</b> .....	<b>4</b>
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
<b>6 Security requirements</b> .....	<b>10</b>
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
<b>7 Security measures — Countermeasures</b> .....	<b>17</b>
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
<b>8</b>	<b>Security specifications for interoperable interface implementation.....</b>	<b>29</b>
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
<b>9</b>	<b>Key management.....</b>	<b>30</b>
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
	<b>Annex A (normative) Security profiles.....</b>	<b>35</b>
	<b>Annex B (informative) Implementation conformance statement (ICS) proforma.....</b>	<b>39</b>
	<b>Annex C (informative) Stakeholder objectives and generic requirements.....</b>	<b>57</b>
	<b>Annex D (informative) Threat analysis.....</b>	<b>61</b>
	<b>Annex E (informative) Security policies.....</b>	<b>118</b>
	<b>Annex F (informative) Example for an EETS security policy.....</b>	<b>124</b>
	<b>Annex G (informative) Recommendations for privacy-focused implementation.....</b>	<b>126</b>
	<b>Bibliography.....</b>	<b>128</b>