

DIN CEN/TS 16702-1:2015-02 (E)

Electronic fee collection - Secure monitoring for autonomous toll systems - Part 1: Compliance checking; English version CEN/TS 16702-1:2014

Contents

Page

Foreword	5
0 Introduction	6
0.1 Overview	6
0.2 Processes	6
0.3 Options	8
0.4 Privacy aspects	11
1 Scope	12
1.1 General scope	12
1.2 Relation to CEN/TS 16439	12
1.3 Relation to other standards	14
2 Normative references	14
3 Terms and definitions	15
4 Abbreviations	17
5 Processes	18
5.1 Introduction and overview	18
5.2 Processes needed for different types of Secure Monitoring	19
5.3 Itinerary Freezing	21
5.3.1 Introduction	21
5.3.2 Generate Itinerary	21
5.3.3 Real-time freezing	23
5.3.4 Freezing per declaration	24
5.4 Checking of Itinerary Freezing	25
5.4.1 Introduction	25
5.4.2 Observing a vehicle	25
5.4.3 Retrieving Proof of Itinerary Freezing (PIF)	26
5.4.4 Checking PIF against Observation	27
5.5 Checking of Toll Declaration	27
5.5.1 Introduction	27
5.5.2 Retrieve Itinerary Data	27
5.5.3 Check Itinerary Consistency	28
5.5.4 Checking Toll Declaration against Itinerary	28
5.6 Claiming incorrectness	29
5.7 Providing EFC Context Data	29
5.8 Key Management	29
5.8.1 Introduction	29
5.8.2 Requirements	29
6 Transactions	30
6.1 Introduction	30
6.2 Description of Itinerary Data	32
6.2.1 Introduction	32
6.2.2 Itinerary Batch	34
6.2.3 Itinerary Record Data Elements	35
6.3 Retrieving PIF in real-time (DSRC Transaction)	37
6.3.1 Introduction	37

6.3.2	Transactional Model	38
6.3.3	Syntax and Semantics	38
6.3.4	Security	40
6.4	Toll Declaration	40
6.4.1	Introduction	40
6.4.2	Transactional Model	40
6.4.3	Syntax and semantics	41
6.4.4	Itinerary Sequence	42
6.4.5	Security	44
6.5	Back End Data Checking	44
6.5.1	Introduction	44
6.5.2	Transactional model	45
6.5.3	Checks of the Itinerary	46
6.5.4	Syntax and semantics	47
6.5.5	Security	50
6.6	Claiming incorrectness	50
6.6.1	Introduction	50
6.6.2	Transactional model	51
6.6.3	Syntax and semantics	52
6.6.4	Security	52
6.7	Providing EFC Context Data	53
6.7.1	Introduction	53
6.7.2	Transactional Model	53
6.7.3	Syntax and semantics	53
6.7.4	Security	55
7	Security	55
7.1	Security functions and elements	55
7.1.1	Hash functions	55
7.1.2	MAC	55
7.1.3	Digital signatures	55
7.1.4	Public Keys, Certificates and CRL	55
7.2	Key Management	56
7.2.1	Key Exchange between Stakeholders	56
7.2.2	Key generation and certification	56
7.3	Trusted Recorder and SM_CC Verification SAM characteristics	57
7.3.1	Introduction	57
7.3.2	Trusted Recorder	57
7.3.3	SM_CC Verification SAM	58
Annex A (normative) Data type specification		59
Annex B (normative) Protocol Implementation Conformance Statement		67
B.1	Guidance for completing the PICS proforma	67
B.1.1	Purposes and structure	67
B.1.2	Abbreviations and conventions	67
B.1.3	Instructions for completing the PICS proforma	69
B.2	Identification of the implementation	69
B.2.1	General	69
B.2.2	Date of the statement	69
B.2.3	Implementation Under Test (IUT) identification	69
B.2.4	System Under Test (SUT) identification	69
B.2.5	Product supplier	70
B.2.6	Applicant (if different from product supplier)	70
B.2.7	PICS contact person	70
B.3	Identification of the protocol	71
B.4	Global statement of conformance	71
B.5	Roles	71
B.6	Types of Secure Monitoring	71
B.7	Capabilities and conditions	72
B.8	Processes	73

Annex C (informative) Example transactions	74
Annex D (informative) Addressed threats (in CEN/TS 16439)	78
D.1 Introduction	78
D.2 Threats where Secure Monitoring can provide Security Measures	78
D.3 Related Requirements	80
D.4 Related Security Measures	81
Annex E (informative) Essentials of the SM_CC concept	84
E.1 Introduction	84
E.2 The SM_CC concept - FAQs	84
E.3 SM_CC options	86
E.3.1 SM_CC_1	86
E.3.2 SM_CC_2	90
E.3.3 SM_CC_3a	93
E.3.4 SM_CC_3b	95
E.4 Managing multiple toll domains	96
E.4.1 Overlapping toll domains	96
E.4.2 The 'catch-all' toll domain counter	98
Annex F (informative) Use of this Technical Specification for the EETS	99
F.1 General	99
F.2 Overall relationship between European standardization and the EETS	99
F.3 European standardization work supporting the EETS	99
F.4 Correspondence between this technical specification and the EETS	100
Bibliography	101