DIN CEN/TS 16702-1:2020-04 (E)

Electronic fee collection - Secure monitoring for auto nomous toll systems - Part 1: Compliance checking; English version CEN/TS 16702- 1:2020

Contents

Page

European foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 9

4 Abbreviations 12

5 Processes 13
5.1 Overview 13
5.2 Profiles 15
5.3 Itinerary Freezing 20
5.3.1 Introduction 20
5.3.2 Generate Itinerary 21
5.3.3 Real-time freezing 22
5.3.4 Freezing per declaration 23
5.4 Checking of Itinerary Freezing 23
5.4.1 Introduction 23
5.4.2 Observing a vehicle 24
5.4.3 Retrieving Proof of Itinerary Freezing (PIF) 24
5.4.4 Checking PIF against Observation 25
5.5 Checking of Toll Declaration 26
5.5.1 Introduction 26
5.5.2 Retrieve Itinerary Data 26
5.5.3 Check Itinerary Consistency 26
5.5.4 Checking Toll Declaration against Itinerary 27
5.6 Inconsistency report 27
5.7 Providing EFC Context Data 27
5.8 Key Management 28
5.8.1 Introduction 28
5.8.2 Requirements 28

6 Transactions 29
6.1 Introduction 29
6.2 Description of Itinerary Data 31
6.2.1 Introduction 31
6.2.2 Itinerary Leaf 32
6.2.3 Itinerary Record Data Elements 33
6.3 Retrieving PIF in real-time (DSRC Transaction) 35
6.3.1 Transactional Model 35
6.3.2 Syntax and Semantics 36
6.3.3 Security 38
6.4 Toll Declaration 38
6.4.1 Transactional Model 38
6.4.2 Syntax and semantics 39

6.4.3 Itinerary Trunk 39
6.4.4 Security 41
6.5 Back end data checking 41
6.5.1 Introduction 41
6.5.2 Transactional model 41
6.5.3 Checks of the Itinerary 43
6.5.4 Syntax and semantics 44
6.5.5 Security 44
6.6 Inconsistency Report 44
6.6.1 Transactional model 44
6.6.2 Syntax and semantics 45
6.6.3 Security 46
6.7 Providing EFC Context Data 46
6.7.1 Transactional model 46
6.7.2 Syntax and semantics 47
6.7.3 Security 47

7 Security 47
7.1 Security functions and elements 47
7.1.1 Hash functions 47
7.1.2 MAC 47
7.1.3 Digital signatures 48
7.1.4 Public Keys, Certificates and CRL 48
7.2 Key Management 48
7.2.1 Key Exchange between Stakeholders 48
7.2.2 Key generation and certification 49
7.3 Trusted Recorder and SM_CC Verification SAM characteristics 49
7.3.1 Introduction 49
7.3.2 Trusted Recorder 50
7.3.3 SM_CC Verification SAM 51

Annex A (normative) Data type specification 52

Annex B (normative) Protocol Implementation Conformance Statement Proforma 53

Annex C (informative) Example transactions 62

Annex D (informative) Relationships to other standards 69

Annex E (informative) Essentials of the SM_CC concept 71

Annex F (informative) Use of this document for the EETS 85

Bibliography 87