DIN CEN/TS 16702-2:2015-05 (E)

Electronic fee collection - Secure monitoring for autonomous toll systems - Part 2: Trusted recorder; English version CEN/TS 16702-2:2015

Contents

Page

Foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 8

4 Symbols and abbreviations 11

5 SAM concept and scenarios 12
5.1 General 12
5.2 The concepts of TR and Verification SAM 13
5.3 Scenarios for a Trusted Recorder 14
5.3.1 General 14
5.3.2 Real-Time Freezing without using a Trusted Time Source 14
5.3.3 Real-Time Freezing using a Trusted Time Source 15
5.4 Scenarios for a Verification SAM 15
5.4.1 General 15
5.4.2 MAC verification 16
5.5 General Scenarios 16
5.5.1 General 16
5.5.2 Assigning a Toll Domain Counter 17
5.5.3 Obtaining SAM Information 17

6 Functional requirements 18
6.1 General 18
6.1.1 SAM options 18
6.1.2 Presentation of requirements 19
6.2 Basic requirements 19
6.3 Key management 20
6.4 Cryptographic functions 20
6.5 Real-time freezing 21
6.6 Verification SAM 21
6.7 Toll Domain Counter 22
6.8 Trusted time source 23
6.9 Security protection level 24

7 Interface requirements 24
7.1 General 24
7.2 Calculate MAC for real-time freezing 24
7.2.1 General 24
7.2.2 Calculation of MAC 25
7.2.3 Coding of request 25
7.2.4 Coding of response 26
7.3 Calculate digital signature for real-time freezing 26
7.3.1 General 26
7.3.2 Calculation of digital signature 26
7.3.3 Coding of request 27
7.3.4 Coding of response 27

7.4 Get device information **28**
7.4.1 General **28**
7.4.2 Coding of request **28**
7.4.3 Coding of response **28**
7.5 Get toll domain counter information **28**
7.5.1 General **28**
7.5.2 Coding of request **29**
7.5.3 Coding of response **29**
7.6 Get key information **29**
7.6.1 General **29**
7.6.2 Coding of request **30**
7.6.3 Coding of response **30**
7.7 Error handling **31**

Annex A (normative) **Data type specification** **32**
A.1 General **32**
A.2 Data specifications **32**

Annex B (normative) **Implementation Conformance Statement (ICS) proforma** **33**
B.1 Guidance for completing the ICS proforma **33**
B.1.1 Purposes and structure **33**
B.1.2 Abbreviations and conventions **33**
B.1.3 Instructions for completing the ICS proforma **34**
B.2 ICS proforma for Trusted Recorder **35**
B.2.1 Identification implementation **35**
B.2.2 Identification of the standard **35**
B.2.3 Global statement of conformance **35**
B.2.4 ICS proforma tables for TR **36**
B.3 ICS proforma for Verification SAM **39**
B.3.1 Identification implementation **39**
B.3.2 Identification of the standard **39**
B.3.3 Global statement of conformance **39**
B.3.4 ICS proforma tables for Verification SAM **40**

Annex C (informative) **Trusted time source implementation issues** **43**
C.1 General **43**
C.2 Possible implementations of a TTS **43**
C.2.1 TTS based on a real time clock **43**
C.2.2 TTS with the need for external calibration **43**
C.3 TTS power supply **44**

Annex D (informative) **Use of this Technical Specification for the EETS** **45**
D.1 General **45**
D.2 Overall relationship between European standardization and the EETS **45**
D.3 European standardization work supporting the EETS **45**
D.4 Correspondence between this Technical Specification and the EETS **46**

Bibliography **47**