

DIN CEN/TS 16702-2:2020-04 (E)

Electronic fee collection - Secure monitoring for autonomous toll systems - Part 2: Trusted recorder; English version CEN/ TS 16702-2:2020

| Contents | Page |
|---|-------------|
| European foreword..... | 4 |
| Introduction | 5 |
| 1 Scope..... | 7 |
| 2 Normative references | 7 |
| 3 Terms and definitions | 8 |
| 4 Symbols and abbreviations | 12 |
| 5 SAM concept and scenarios | 13 |
| 5.1 General..... | 13 |
| 5.2 The concepts of TR and verification SAM | 13 |
| 5.3 Scenarios for a trusted recorder..... | 15 |
| 5.3.1 General..... | 15 |
| 5.3.2 Real-Time Freezing without using a Trusted Time Source..... | 15 |
| 5.3.3 Real-Time Freezing using a Trusted Time Source | 16 |
| 5.4 Scenarios for a verification SAM | 16 |
| 5.4.1 General..... | 16 |
| 5.4.2 MAC verification | 16 |
| 5.5 General Scenarios | 17 |
| 5.5.1 General..... | 17 |
| 5.5.2 Assigning a Toll Domain Counter | 17 |
| 5.5.3 Obtaining SAM Information..... | 18 |
| 6 Functional requirements..... | 19 |
| 6.1 General..... | 19 |
| 6.1.1 SAM options..... | 19 |
| 6.1.2 Presentation of requirements | 20 |
| 6.2 Basic requirements | 20 |
| 6.3 Key management..... | 21 |
| 6.4 Cryptographic functions | 21 |
| 6.5 Real-time freezing..... | 22 |
| 6.6 Verification SAM | 23 |
| 6.7 Toll Domain Counter | 23 |
| 6.8 Trusted time source | 24 |
| 6.9 Security protection level | 25 |
| 7 Interface requirements..... | 26 |
| 7.1 General..... | 26 |
| 7.2 Calculate MAC for real-time freezing | 26 |
| 7.2.1 General..... | 26 |
| 7.2.2 Calculation of MAC | 27 |
| 7.2.3 Coding of request | 27 |
| 7.2.4 Coding of response..... | 28 |
| 7.3 Calculate digital signature for real-time freezing | 28 |
| 7.3.1 General..... | 28 |

| | | |
|--|--|----|
| 7.3.2 | Calculation of digital signature..... | 29 |
| 7.3.3 | Coding of request..... | 29 |
| 7.3.4 | Coding of response..... | 29 |
| 7.4 | Get device information | 30 |
| 7.4.1 | General | 30 |
| 7.4.2 | Coding of request..... | 30 |
| 7.4.3 | Coding of response..... | 31 |
| 7.5 | Get toll domain counter information..... | 31 |
| 7.5.1 | General | 31 |
| 7.5.2 | Coding of request..... | 31 |
| 7.5.3 | Coding of response..... | 32 |
| 7.6 | Get key information | 32 |
| 7.6.1 | General | 32 |
| 7.6.2 | Coding of request..... | 33 |
| 7.6.3 | Coding of response..... | 33 |
| 7.7 | Error handling | 34 |
| Annex A (normative) Data type specification..... | | 35 |
| Annex B (normative) Implementation Conformance Statement (ICS) proforma..... | | 36 |
| Annex C (informative) Trusted Time Source implementation issues..... | | 49 |
| Annex D (informative) Use of this document for the EETS | | 51 |
| Bibliography | | 53 |