DIN CEN/TR 16968:2018-12 (E)

Electronic Fee Collection - Assessment of security measures for applications using Dedicated Short-Range Communication; English version CEN/TR 16968:2016

Contents

Page

European foreword ... 4

Introduction ... 5

1 Scope ... 6

2 Terms and definitions ... 6

3 Abbreviations ... 9

4 Method ... 10

5 Security Objectives and Functional Requirements ... 13
5.1 Target of evaluation ... 13
5.2 Security objectives ... 14
5.2.1 Introduction ... 14
5.2.2 Confidentiality ... 14
5.2.3 Availability ... 14
5.2.4 Accountability ... 14
5.2.5 Data integrity ... 14
5.3 Functional security requirements ... 15
5.3.1 Introduction ... 15
5.3.2 Confidentiality ... 15
5.3.3 Availability ... 17
5.3.4 Accountability ... 18
5.3.5 Data integrity ... 20
5.4 Inventory of assets ... 21
5.4.1 Functional Assets ... 21
5.4.2 Data Assets ... 22

6 Threat analysis ... 22

7 Qualitative risk analysis ... 24
7.1 Introduction ... 24
7.1.1 General ... 24
7.1.2 Likelihood of a threat ... 24
7.1.3 Impact of a threat ... 25
7.1.4 Classification of Risk ... 26
7.2 Risk determination ... 26
7.2.1 Definition of high and low risk context ... 26
7.2.2 Threat T1: Access Credentials keys can be obtained ... 27
7.2.3 Threat T2: Authentication keys can be obtained ... 27
7.2.4 Threat T3: OBU can be cloned ... 28
7.2.5 Threat T4: OBU can be faked ... 28
7.2.6 Threat T5: Authentication of OBU data can be repudiated ... 29
7.2.7 Threat T6: Application data can be modified after the transaction ... 29
7.2.8 Threat T7: Data in the VST is not secure ... 30
7.2.9 Threat T8: DSRC Communication can be eavesdropped ... 30
7.2.10 Threat T9: Correctness of application data are repudiated ... 31
7.2.11 Threat T10: Master keys may be obtained from RSE ... 31
7.3 Summary ... 31

8 Proposals for new security measures 32
8.1 Introduction 32
8.2 Security measures to counter risks related to key recovery 32
8.3 Recommended countermeasures 34
8.4 Qualitative cost benefit analysis 35

9 Impact of proposed countermeasures 35
9.1 Current situation and level of fraud in existing EFC systems using CEN DSRC link 35
9.2 EETS legislation 36
9.3 Analysis of effects on existing EFC systems 36
9.3.1 Affected roles 36
9.3.2 The CEN DSRC equipment Manufacturers 36
9.3.3 The Toll Service Providers 37
9.3.4 The Toll Chargers 37

10 Recommendations 38
10.1 Add security levels and procedures to EN ISO 14906 38
10.2 Recommendation for other EFC standards 39
10.3 New standards 39

Annex A (informative) Current status of the DEA cryptographic algorithm 40
A.1 Overview 40
A.2 ISO/IEC 9797-1 (MAC Algorithm 1) 40
A.3 FIPS 46 (DEA Specification – DES) 40
A.4 ENISA recommendations 41

Annex B (informative) Security considerations regarding DSRC in EFC Standards 42
B.1 Security vulnerabilities in EN 15509 and EN ISO 14906 42
B.2 Security vulnerabilities in EN ISO 12813 (CCC) 42
B.3 Security vulnerabilities in EN ISO 13141 (LAC) 43
B.4 Security vulnerabilities in CEN/TS 16702-1 (SM-CC) 43

Bibliography 44