SLOVENSKI STANDARD
SIST-TP CEN/TR 16968:2016

01-september-2016

Elektronsko pobiranje pristojbin - Ocena varnostnih ukrepov za aplikacije z uporabo posebne komunikacije kratkega dosega

Electronic Fee Collection - Assessment of security measures for applications using Dedicated Short-Range Communication

Elektronische Gebührenerhebung - Beurteilung von Sicherheitsmaßnehmen für Anwendungen mit dedizierter Nahbereichskommunikation

Perception de télépéage - Évaluation des mesures de sécurité pour les applications utilisant les communications dédiées à courte portée

Ta slovenski standard je istoveten z: **CEN/TR 16968:2016**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST-TP CEN/TR 16968:2016 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16968

May 2016

ICS 35.240.60

English Version

Electronic Fee Collection - Assessment of security measures for applications using Dedicated Short-Range Communication

Elektronische Gebührenerhebung - Beurteilung von Sicherheitsmaßnahmen für Anwendungen mit dedizierter Nahbereichskommunikation

This Technical Report was approved by CEN on 11 April 2016. It has been drawn up by the Technical Committee CEN/TC 278.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16968:2016 E

Contents

Page

European foreword

This document (CEN/TR 16968:2016) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

Introduction

Security for dedicated short-range communication (DSRC) applications in the context of electronic fee collection (EFC) has a long history in standardization. Currently the area is covered by several standards and technical specifications, successively developed over time:

— EN ISO 14906 (Electronic fee collection - Application interface definition for dedicated short-range communication) provides a toolbox of functions and security measures which can be used for DSRC application.

— CEN ISO/TS 19299 (Electronic fee collection - Security framework) analyzes the threats to an EFC system as a whole, and not specifically for the DSRC technology.

— EN ISO 12813 (Electronic fee collection - Compliance check communication for autonomous systems) and EN ISO 13141 (Electronic fee collection - Localisation augmentation communication for autonomous systems) mirrors the best-practice security measures of EN 15509.

— CEN/TS 16702-1 (Electronic fee collection - Secure monitoring for autonomous toll systems - Part 1: Compliance checking) provides an EFC enforcement concept, partially dependent on a DSRC application.

— EN 15509 (Electronic fee collection - Interoperability application profile for DSRC) defines an interoperable application profile which comprises a selection of such measures with a definition of security algorithms associated to it. It is based on the experience of many EU projects related to DSRC-EFC.

As the security domain has evolved, it is now necessary to analyze again the threats, vulnerabilities and risks of using the CEN DSRC technology in all DSRC-based applications related to EFC. Technological advances and proliferation of cryptographic tools and knowledge has made an attack on the security procedures of DSRC more likely.

This technical report (TR) identifies context dependent risks on the DSRC link and proposes security measures to counter them and the points out what new standard deliverables that are needed.

1 Scope

This Technical Report includes a threat analysis, based on CEN ISO/TS 19299 (EFC - Security Framework), of the CEN DSRC link as used in EFC applications according to the following Standards and Technical Specification

— EN 15509:2014,

— EN ISO 12813:2015,

— EN ISO 13141:2015,

— CEN/TS 16702-1:2014.

This Technical Report contains:

— a qualitative risk analysis in relation to the context (local tolling system, interoperable tolling environment, EETS);

— an assessment of the current recommended or defined security algorithms and measures to identify existing and possible future security leaks;

— an outline of potential security measures which might be added to those already defined for DSRC;

— an analysis of effects on existing EFC systems and interoperability clusters;

— a set of recommendations on how to revise the current standards, or proposal for new work items, with already made implementations taken into account.

The security analysis in this Technical Report applies only to Security level 1, with Access Credentials and Message authentication code, as defined in EN 15509:2014.

It is outside the scope of this Technical Report to examine Non DSRC (wired or wireless) interfaces to the OBE and RSE.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
access credentials
trusted attestation or secure module that establishes the claimed identity of an object or application

[SOURCE: EN 15509:2014, 3.1]

2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to that entity

[SOURCE: ISO 7498-2:1989, 3.3.3, modified]

2.3
asset
anything that has value to a stakeholder

[SOURCE: CEN ISO/TS 19299:2015, 3.3]

2.4
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: CEN ISO/TS 19299:2015, 3.4]

2.5
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

[SOURCE: EN ISO 17575-1:2016, 3.2]

2.6
authentication
security mechanism allowing verification of the provided identity

[SOURCE: EN 301 175]

2.7
authenticator
data, possibly encrypted, that is used for authentication

[SOURCE: EN 15509:2014, 3.3]

2.8
confidentiality
prevention of information leakage to non-authenticated individuals, parties and/or processes

[SOURCE: CEN ISO/TS 19299:2015, 3.11]

2.9
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: CEN ISO/TS 19299:2015, 3.28]

2.10
hacker
person who attempts or succeeds to gain unauthorized access to protected resources

[SOURCE: CEN ISO/TS 19299:2015, 3.19]

2.11
key management
generation, distribution, storage, application and revocation of encryption keys

[SOURCE: CEN ISO/TS 17574:2009, 3.13 modified]

2.12
message authentication code
MAC
string of bits which is the output of a MAC algorithm

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

2.13
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: CEN ISO/TS 19299:2015, 3.27]

2.14
on-board equipment
OBE
all required equipment on-board a vehicle for performing required EFC functions and communication services

2.15
on-board unit
OBU
single electronic unit on-board a vehicle for performing specific EFC functions and for communication with external systems

Note 1 to entry: An OBU always includes, in this context, at least the support of the DSRC interface

2.16
reliability
ability of a device or a system to perform its intended function under given conditions of use for a specified period of time or number of cycles

[SOURCE: CEN ISO/TS 14907-1:2015, 3.17]

2.17
roadside equipment
RSE
equipment located along the road, either fixed or mobile

[SOURCE: CEN ISO/TS 14907-1:2015, 3.17]

2.18
security target
set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

[SOURCE: CEN ISO/TS 17574:2009, 3.25]

2.19
target of evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70]

2.20
threat
potential cause of an unwanted information security incident, which may result in harm

[SOURCE: CEN ISO/TS 19299:2015, 3.39]

2.21
threat agent
entity that has the intention to act adversely on an asset

[SOURCE: CEN ISO/TS 19299:2015, 3.40]

2.22
threat analysis
systematic detection, identification, and evaluation of threats

[SOURCE: CEN ISO/TS 19299:2015, 3.41]

2.23
toll charger
TC
entity which levies toll for the use of vehicles in a toll domain

[SOURCE: ISO 17573:2010, 3.16 modified]

2.24
toll service provider
TSP
entity providing toll services in one or more toll domains

[SOURCE: ISO 17573:2010, 3.23 modified]

2.25
transaction counter
data value in the on-board unit that is incremented by the roadside equipment at each transaction

[SOURCE: EN 15509:2014, 3.23]

2.26
vulnerability
weakness of an asset or control that can be exploited by an attacker

[SOURCE: CEN ISO/TS 19299:2015, 3.51]

3 Abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

AES	Advanced Encryption Standard
CCC	Compliance check communication (EN ISO 12813)
COTS	Commercial Off-the-Shelf
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (EN ISO 14906)
EETS	European Electronic Toll Service
IAP	Interoperable Application Profile
LAC	Localisation augmentation communication (EN ISO 13141)
MAC	Message authentication code
NIST	National Institute of Standards and Technology
OBE	On-board Equipment
OBU	On-board Unit
RSE	Roadside Equipment
SM-CC	Secure Monitoring Compliance Check (CEN/TS 16702–1:2014)
TOE	Target Of Evaluation
TVRA	Threat, Vulnerability and Risk Analysis
VST	Vehicle Service Table

4 Method

The method in this technical report is based on the method of ETSI/TS 102 165-1 which defines a 10 step method which in turn is based on ISO/IEC 15408 and is especially adapted to communication interfaces. This approach is also used in ETSI/TR 102 893. The 10 steps are listed below:

1) Identification of the Target of Evaluation (TOE) resulting in a high-level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the Threat, Vulnerability and Risk Analysis (TVRA). See 5.1.

2) Identification of the objectives resulting in a high-level statement of the security aims and issues to be resolved. See 5.2.

3) Identification of the functional security requirements, derived from the objectives from step 2. See 5.3.

4) Inventory of the assets as refinements of the high-level asset descriptions from step 1 and additional assets as a result of steps 2 and 3. See 5.4.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result. See Clause 6.

6) Quantifying the occurrence likelihood and impact of the threats. See 7.1.

7) Establishment of the risks. See 7.2.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk. See 8.2.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8. See Clause 9.

10) Specification of detailed requirements for the security services and capabilities from step 9. See Clause 10.

Steps 6-10 will be adapted to the generic case of DSRC communication addressed by this technical report. Furthermore, the analysis under step 5 and step 8 specifically takes CEN ISO/TS 19299 into account. The adapted methodology used in this report is illustrated in Figure 1.