PD CEN/TR 16968:2016

BSI Standards Publication

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

bsi.

National foreword

This Published Document is the UK implementation of CEN/TR 16968:2016.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 92597 9

ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2016.

Amendments issued since publication

Date	Text affected

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

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.

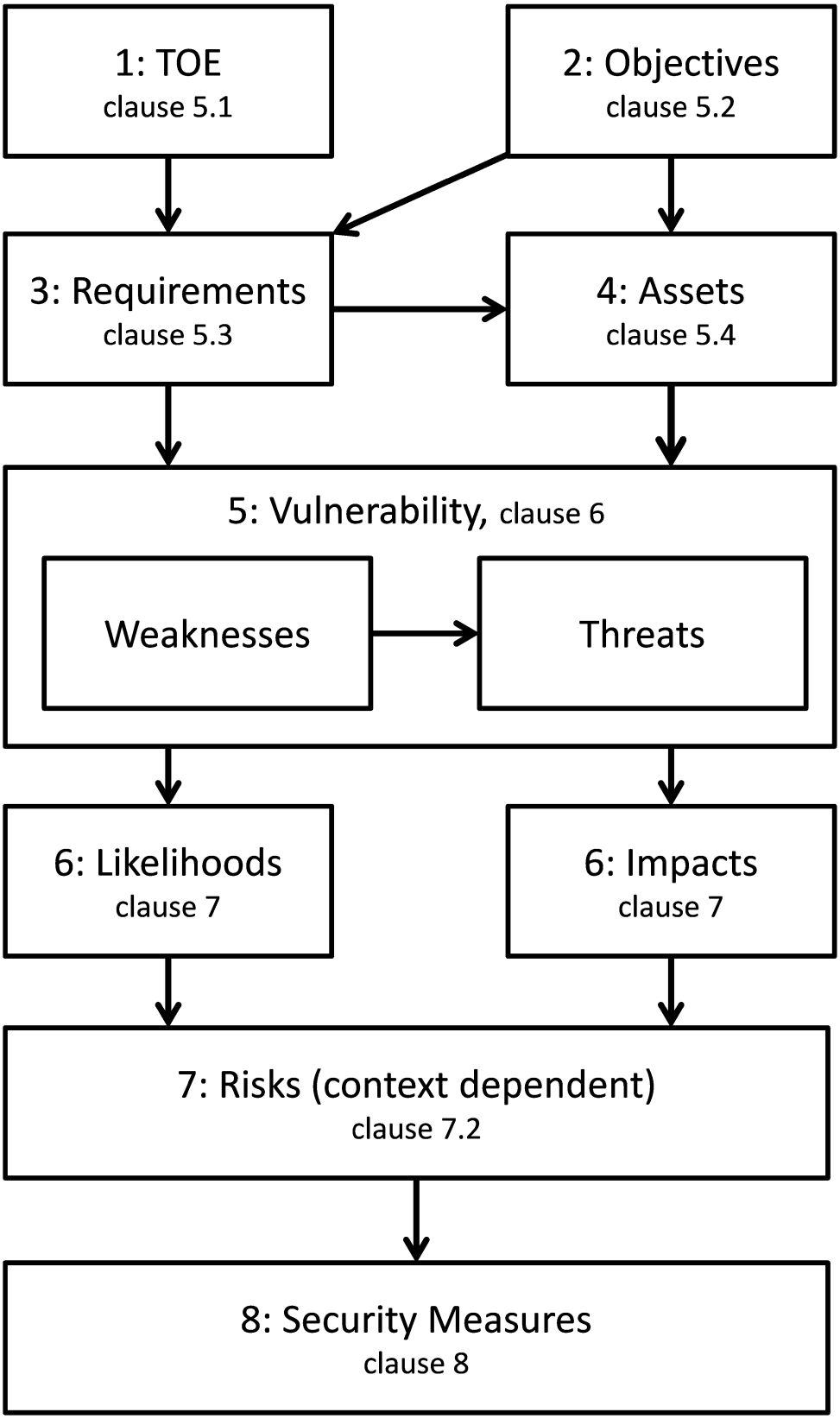

Figure 1 — Adapted TVRA methodology used in this report

5 Security Objectives and Functional Requirements

5.1 Target of evaluation

There are two potential Targets of Evaluation (TOE) for security analysis purposes:

— The OBU

— The RSE

Per definition, a TOE can only be attacked through its exposed interfaces and the presence of a threat agent is necessary to launch an attack. The scope of this analysis is the communication link over 5.8 GHz CEN DSRC, see Figure 2. Communication over the other interfaces identified in Figure 2 is out of scope for this TR.

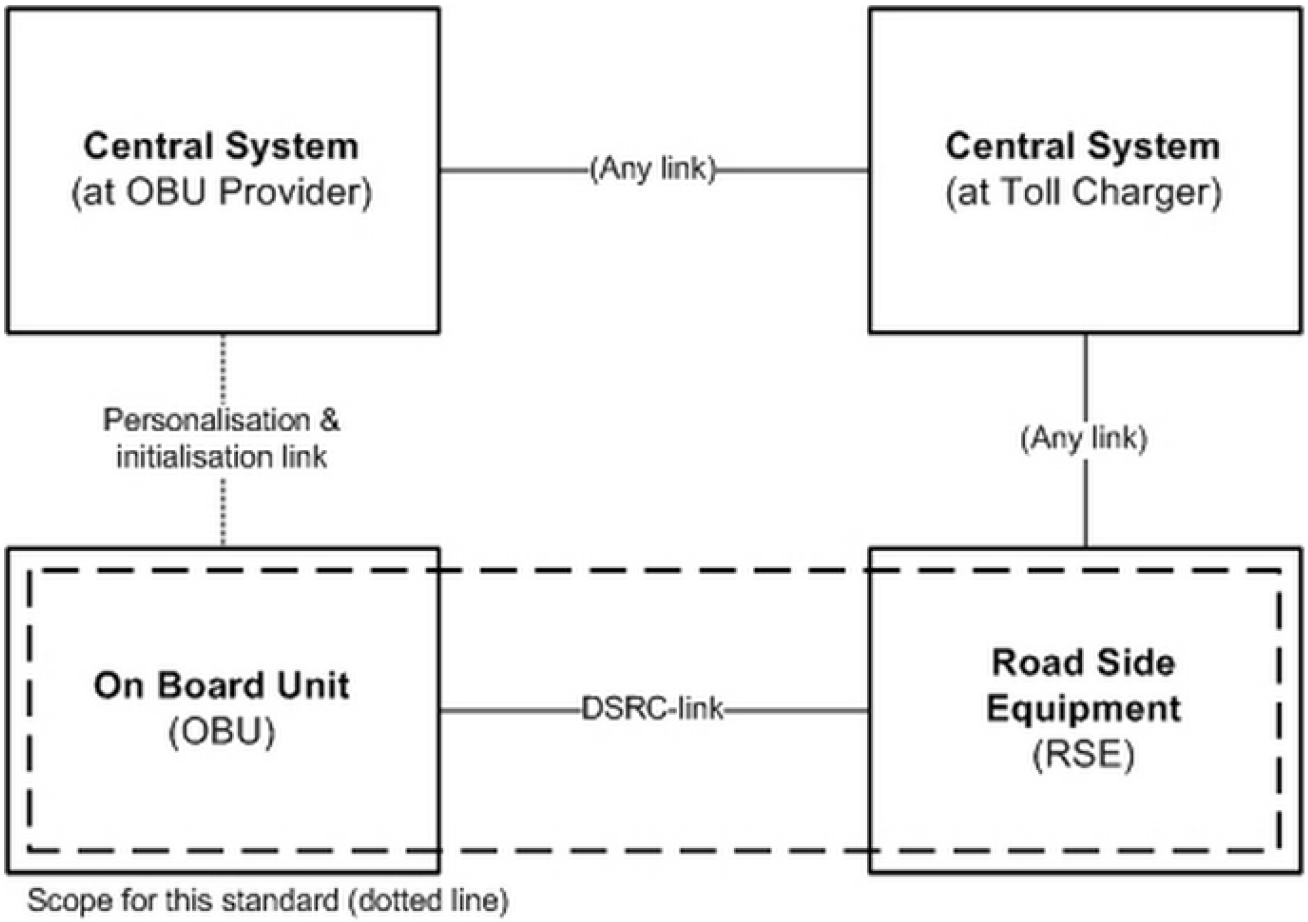

Figure 2 — TOE

NOTE Figure 2 is copied from Figure 1 in EN 15509.

The CEN DSRC link is the communication link between the RSE and OBU according to EN 15509:2014 (DSRC-EFC), EN ISO 12813:2015 (CCC), EN ISO 13141:2015 (LAC) and CEN/TS 16702-1:2014 (SM-CC).

For the sake of this Technical Report analysis it is assumed that a valid OBU is issued by and is in the domain of the Toll Service Provider (TSP) and likewise that the road side equipment (RSE) is in the domain of the Toll Charger (TC) managing a given toll domain. However, most of the analysis will hold true even in the case of a different assignement of responsibilities.

The analysis only applies to EN 15509 Security Level 1 with Access Credentials and Message authentication code. Security level 0 is not considered.

5.2 Security objectives

5.2.1 Introduction

In accordance with NIST Special Publication 800-33 the security objectives considered are: availability, integrity, confidentiality and accountability.

The fifth NIST security objective “assurance”, which is the basis for confidence that the security measures, both technical and operational, work as intended, is not considered here, as this TR does not cover implementation aspects.

NOTE Authentication, authorization and access control are security services that focus on preventing a security breach and are used to fulfil the objectives.

5.2.2 Confidentiality

The following security objectives relative to the confidentiality of stored and transmitted information are specified:

— Co1 Information relating to the identity of a Service User should not be revealed to any unauthorized 3rd party

— Co2 Information held within the OBU and RSE should be protected from unauthorized access.

— Co3 Information sent from an OBU to an authorized RSE should not reveal the vehicle's travel history to any party not authorized to receive the information.

— Co4 Data exchange guarantees data confidentiality

5.2.3 Availability

The following security objective relative to the availability of services is specified:

— Av1 Access to and the operation of DSRC-EFC/CCC/LAC/SM-CC services should not be prevented by malicious activity performed on the TOE.

5.2.4 Accountability

The following security objective relative to the accountability of services is specified:

— Ac1 The data exchanged should provide authentication and non-repudiation for the respective service.

5.2.5 Data integrity

The following security objectives relative to the integrity of data in the TOE:

— In1 Information stored within an OBU or RSE should be protected from unauthorized modification and deletion.

— In2 Information sent to or from an OBU or RSE should be protected against unauthorized or malicious modification or manipulation during transmission.

5.3 Functional security requirements

5.3.1 Introduction

The following clauses present a number of functional security requirements that covers the security objectives listed in 5.2.

As far as possible this has been done by selecting appropriate requirements from CEN ISO/TS 19299:2015. Those have been given identifiers according to the template RQ.TC/TSP.XX with the corresponding requirement description copied from CEN ISO/TS 19299:2015.

NOTE It was considered to only reference to the requirements in CEN ISO/TS 19299:2015, and not to repeat these in this Technical Report. However, this approach was discarded as it would significantly have hampered the readability of this Technical Report. As a consequence of the adopted approach, to reference the requirements identifiers and to cite the associated requirements, is that this Technical Report contains "shall" statements in 5.3.

For those objectives not fully covered by CEN ISO/TS 19299:2015 functional security requirements original to this technical report have been defined. They are given identifiers according to the template DSRC-SEC.RQ.TC/TSP.XX.

5.3.2 Confidentiality

Table 1 — Toll charger confidentiality requirements

Obj. Id.	Objective	Req. Id.	Requirement
Co3	Information sent from an OBU to an authorized RSE should not reveal the vehicle's travel history to any party not authorized to receive the information.	RQ.TC.01	DSRC-EFC, CCC, LAC and SM-CC applications shall either not request information about the vehicle's travel history or protect its confidentiality in transfer.
Co2	Information held within the OBU and RSE should be protected from unauthorized access.	RQ.TC.24	The RSE shall not allow unauthorized access to software and data.
		RQ.TC.90	The TCs systems shall be designed in a way that access to stored or processed data are only possible within the legal context of the respective country (e.g. lawful interception).

Table 2 — OBU confidentiality requirements

Obj. Id.	Objective	Req. Id.	Requirement
Co3	Information sent from an OBU to an authorized RSE should not reveal the vehicle's travel history to any party not authorized to receive the information.		DSRC-EFC, CCC, LAC and SM-CC applications shall either not provide information about the vehicle's travel history or protect its confidentiality in transfer.
Co2	Information held within the OBU and RSE should be protected from unauthorized access.	Derived from RQ.TC.22	The TSP shall implement RSE authentication measures for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.
			The OBU shall not allow unauthorized access to software and data.
		RQ.TSP.90	The TSP systems shall be designed in a way that access to stored or processed data is only possible within the legal context of the respective country (e.g. lawful interception).
Co1	Information relating to the identity of a Service User should not be revealed to any unauthorized 3rd party.		The OBU's VST shall not contain data identifying a Service User
			DSRC-EFC, CCC, LAC and SM-CC applications shall either not provide information identifying a Service User or protect its confidentiality in transfer.
Co4	Data exchange guarantees data confidentiality	RQ.IF.10	DSRC-EFC, CCC and SM-CC applications shall protect its confidentiality in transfer.

5.3.3 Availability

Table 3 — Toll charger availability requirements

Obj. Id.	Objective	Req. Id.	Requirement
Av1	Access to and the operation of DSRC-EFC/CCC/LAC/SM-CC services should not be prevented by malicious activity performed on the TOE.	RQ.TC.08	The TC shall check the model and make of OBE during a vehicle check (enabled by RQ.TSP.58) to identify the use of OBE versions not certified by the TC.
		RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality within an agreed time frame.
		RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part within an agreed time frame.
		RQ.TC.23	The TC shall detect RSE malfunction or underperformance and correct it within an agreed time frame.
		RQ.TC.24	The RSE shall not allow unauthorized access to software and data.
		RQ.TC.96	The TC shall be responsible for the availability of his RSE interfaces to an OBE according to agreed service levels.

Table 4 — Toll service provider availability requirements

Obj. Id.	Objective	Req. Id.	Requirement
Av1	Access to and the operation of DSRC-EFC/CCC/LAC/SM-CC services should not be prevented by malicious activity performed on the TOE.	RQ.TSP.09	The TSP shall notify the service user if the OBE or ICC is not working correctly.
		RQ.TSP.05	The OBE shall prevent or detect illegal modification of parameters through its external interfaces.

5.3.4 Accountability

Table 5 — Toll charger accountability requirements

Obj. Id.	Objective	Req. Id.	Requirement
Ac1	The following security objective relative to the accountability of services is specified: The data exchanged should provide authentication and non-repudiation for the respective service	RQ.TC.01	The TC shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations either acquired directly through the TCs RSE or through a TSP (enabled by RQ.TSP.51 for autonomous systems).
		RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the OBE.
		RQ.TC.32	The TC shall make sure that the enforcement case data is court proof.
		RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific OBE (enabled by RQ.TSP.62).

Table 6 — Toll service provider accountability requirements

Obj. Id.	Objective	Req. Id.	Requirement
Ac1	The following security objective relative to the accountability of services is specified: The data exchanged should provide authentication and non-repudiation for the respective service	RQ.TC.01	The TC shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations either acquired directly through the TCs RSE or through a TSP (enabled by RQ.TSP.51 for autonomous systems).
		RQ.TSP.04	The TSP shall determine if toll declarations are based on data originating from a legitimate OBE or ICC.
		RQ.TSP.08	The TSP shall detect duplicate or false OBE or ICC identities and block such OBE or ICC identities by placing them on the exception list.
		RQ.TSP.19	The TSP shall notify the TC about stolen or cloned OBE or ICC.
		RQ.TSP.21	The TSP shall detect cloned OBE or ICC and block them by placing them on the exception list.
		RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of correct and complete toll declarations sent either directly from the OBE to the TCs RSE (in a DSRC system) or through a back office data exchange (required to enable RQ.TC.01 for autonomous systems).
		RQ.TSP.53	The TSP shall enable the TC to perform spot checks through CCC (required to enable RQ.TC.02 for autonomous systems).
		RQ.TSP.55	The TSP shall enable the TC to determine if toll declarations are based on data originating from a legitimate Front End (required to enable RQ.TC.05 for autonomous systems) or OBE (in a DSRC system).

5.3.5 Data integrity

Table 7 — Toll charger integrity requirements

Obj. Id.	Objective	Req. Id.	Requirement
In1	Information stored within an OBU or RSE should be protected from unauthorized modification and deletion.	RQ.TC.24	The RSE shall not allow unauthorized access to software and data.
In2	Information sent to or from an OBU or RSE should be protected against unauthorized or malicious modification or manipulation during transmission.		The TC shall implement OBU Data Integrity verification for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.
			The TC shall implement application data integrity verification as defined in SM-CC
			The TC shall provide application data integrity measures as defined in LAC (LACData MAC1 and MAC2)
			The TC shall provide application data integrity measures for EFC-DSRC (ReceiptData Authenticator)
			The TC shall implement application data integrity verification for EFC-DSRC (ReceiptData Authenticator)
		RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the OBE.
		RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate OBE or TSP Back End (enabled by RQ.TSP.55).

Table 8 — Toll service provider integrity requirements

Obj. Id.	Objective	Req. Id.	Requirement
In1	Information stored within an OBU or RSE should be protected from unauthorized modification and deletion.		The TSP shall provide OBU authentication measures for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.
			The TSP shall not allow unauthorized access to software and data.
In2	Information sent to or from an OBU or RSE should be protected against unauthorized or malicious modification or manipulation during transmission.		The TSP shall provide OBU data integrity measures for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.
			The TSP shall provide application data integrity measures as defined in SM-CC
			The TSP shall implement application data integrity verification as defined in LAC
		RQ.IF.11	Data exchange shall guarantee data integrity.
		RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.
		RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.
		RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.

5.4 Inventory of assets

5.4.1 Functional Assets

The functional assets in the OBU and RSE that concern the TOE can be classified as follows:

— The implementation of the communication protocol stack, incl. the parameters defining its behaviour;

— The DSRC-EFC/CCC/LAC/SM-CC application

The functional assets from the security point of view for OBU and RSE are:

— The OBU key derivation algorithm for authentication and AC key

— The MAC generation algorithms based on DEA

— The AC calculation algorithm based on DEA

5.4.2 Data Assets

5.4.2.1 OBU

The data assets in the OBU are discussed in CEN/TR 16152:2011, Clause 5.2. The assets that concern the TOE can be classified as follows:

— Communication initialization data provided in the VST

— Application data that can be transferred to or from the OBU over the DSRC interface as DSRC attributes

— Cryptographic key material for DSRC Security, i.e. OBU DEA authentication, non-repudiation and access control keys. These assets are described in EN 15509:2014, Clauses 6.1.5.2, 6.1.5.3 and Table A.4. Notice that the OBU only carries diversified keys.

— Parameters for DSRC behaviour

5.4.2.2 RSE

The data assets in the RSE that concern the TOE can be classified as follows:

— Application data communicated (written) over the DSRC interface as part of DSRC attributes

— Cryptographic key material for DSRC Security, i.e. RSE authentication and access control master keys. These assets are described in EN 15509:2014, Clauses 6.1.5.2, 6.1.5.3 and Table A.4. Notice that the RSE carries master keys, but only derived keys are used for the authentication and access control procedures.

— Parameters for DSRC behaviour

6 Threat analysis

Within a TOE, vulnerability is considered to be a combination of an identified system weakness with one or more threats that are able to exploit that weakness. The weaknesses have been identified by analysis of requirements and assets.

A threat agent may exploit a weakness and recover keys in some of the threats. Notice that one successful attack only relates to one DSRC application and one EfcContextMark at a time. It is assumed that different applications co-existing inside one OBU are fully isolated from each other.

The consequences refer to functional security requirements (5.3) that are potentially violated by this threat.

The analysis does not fully analyze what entity that will lose income, it may be the Toll Charger or the Toll Service Provider or other entities.

The analysis is done on EN 15509 security level 1. In EFC system using security level 0 (without the use of access control), some threats do not apply.

Table 9 — Vulnerabilities, weaknesses and threats

Weaknesses in standards' system design	**Threat**		**Consequence**
DEA key(s) is subject to brute force attack.	T1: Access Credentials key can be obtained from an RSE by obtaining an AC response and executing a brute force attack	Attacker in possession of an OBU communication simulator	Confidentiality and integrity: Attributes on all OBUs with the same AC_CR-KeyReference can be read out and written according to access conditions in standards.
	T2: Proof of concept published: The authentication key can be obtained from an OBU by obtaining several MAC responses and executing a brute force attack.	Attacker with access to outcome of T1and possession of a RSE communication simulator	Accountability: Authentication keys can be obtained from valid OBUs.
	T3: Single OBUs can be cloned[1)].	Attacker with access to outcome of T2 and can build OBU hardware	Accountability: Toll is levied on incorrect service user
	T4: OBUs can be faked[2)].	Attacker with access to outcome of T2 and can build OBU hardware	Accountability and Integrity.
	T5: Authentication of OBU data can be repudiated on the basis that DES is not secure.	Service Provider not willing to pay. User repudiating the tolls	Accountability: OBU cannot be used for payment effectively. Toll Charger loses income.
	T6: Application data can be modified after the transaction took place	Toll Charger willing to obtain more payment from service provider /user	Integrity: A higher fee is proposed / debited to the user. Users loose trust in the system
Initialization phase is not secured	T7: Data in the VST is not secure.	Service Provider using not certified OBUs	Accountability: model and make of OBU is not authentic.

1) Cloning refers to copying the entire set of attributes and related cryptographic key material from a valid OBU. The resulting OBU will be indistinguishable from the original OBU.

2) Faking refers to copying some information from the original OBU, and changing some.

Weaknesses in standards' system design	**Threat**		**Consequence**
DSRC Communication is in plaintext	T8: DSRC Communication can be eavesdropped.	Attacker with DSRC-sniffer within DSRC communication range	Confidentiality: User can be tracked at the RSE and private information be exploited by unauthorized parties
Application data are not protected against integrity attacks	T9: Correctness of application data are repudiated.	Service Provider not willing to pay User repudiating the tolls	Integrity: OBU cannot be used for payment effectively. Toll Charger loses income.
Master key is subject to brute force attack	T10: Master keys may be obtained from RSE after successful T1 and T2 attacks.	Attacker with access to outcome of T1 and T2	Accountability, integrity and confidentiality.

7 Qualitative risk analysis

7.1 Introduction

7.1.1 General

This risk analysis provides an indicative analysis of the risk associated to the use of the TOE in generic contexts. This analysis is by no means representative of real risk in a real context.

In order to determine which countermeasures are needed for a specific system, the system owner/operator should perform a risk analysis of his system in the real context, specifically for the TOE or as part of a more general risk management process.

The qualitative risk analysis examines all identified threats and assigns a likelihood and impact value to them. The risk is defined as the product of the likelihood and the impact value. In order to take differing contexts into account both likelihood and impact can have multiple values resulting in multiple risk values, each one valid for a specific context (or combination of contexts).

This analysis scheme is adopted from ETSI/TS 102 165-1.

7.1.2 Likelihood of a threat

The likelihood of a threat occurring may be estimated with values from 0 to 3 as explained in Table 10.

Table 10 — Occurrence likelihood

Value	**Likelihood of occurrence**	**Explanation**
0	Extremely unlikely	According to up-to-date knowledge, a possible attacker needs to solve very strong technical difficulties to state the threat.
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.

At least the following factors should be taken into account when analyzing the likelihood of a threat being executed:

a) Time needed

b) Expertise needed

c) Knowledge of the TOE

d) Opportunity (for example physical access)

e) Equipment needed

f) The motivation of the attacker

   1) monetary profit

   2) unauthorized vehicle tracking

   3) discrediting the tolling system

   4) hacking/vandalism

   5) etc

7.1.3 Impact of a threat

Table 11 identifies the three levels of resulting impact in Step 4 of the TVRA process.

Table 11 — Resulting impact

Value	Impact	Explanation
1	Low	The concerned party is not harmed very strongly; the possible damage is low AND the attack is carried out in a single instance
2	Medium	The impact is between high and low
3	High	A basis of business is threatened and severe damage might occur in this context OR The threat addresses the interests of providers/subscribers and cannot be neglected AND is carried out in more than one single instance of attack.

At least the following factors should be taken into account when analyzing the impact of an executed threat:

— Monetary loss

— Damage to reputation

— Legal consequences

— Commercial consequences (loss of contract, exclusion from tenders)

— Monetary gain for the attacker

7.1.4 Classification of Risk

The product of occurrence likelihood and impact value as defined in 7.1 gives the risk which serves as a measurement for the risk that the concerned asset is compromised. The result is classified into three categories as shown in Table 12.

Table 12 — Risk classification

Value	Risk	Explanation
0, 1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be business critical. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
NOTE Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.		

7.2 Risk determination

7.2.1 Definition of high and low risk context

The likelihood of a threat as well as the impact on a system are properties that are context dependent. The risk analysis in this Technical Report has been carried out to reflect the worst and best case scenarios, and therefore the analysis has been split into high and low risk context. A context can cover both current and future scenarios with different threat agents.

The risk analysis for a real context should represent a situation that is typical for a specific system operated by one Toll Charger. Such a context will be somewhere in between the low and high risk context identified in this Technical Report. Assessments for a specific system should take into account all aspects of the specific system implementation such as system design, operational procedures, enforcement, attributes use, legislation, etc.

When evaluating if a context should be considered low or high risk, the following characteristics could be considered:

— History of observations of faked OBUs.

— History of observations of cloned OBUs.

— Existing security mechanisms, such as transaction counter, issuers authentication, ensure that suspicious OBUs are put on exception list relatively fast.

— Additional systems are used to verify the vehicle, such as identification of vehicle characteristics and license plates at the toll plaza. They are verified to attributes in the OBU and/or information stored in the back office.

— Efficient enforcement procedures and high penalties make use of non-compliant OBUs unattractive.

— The user incentive to avoid payments compared to the risk of non-compliant behaviour being detected.

— Public acceptance of the toll system (e.g. hacker attacks motivated by political views).

— Considering organization complexity (e.g. roaming agreements) and number of users.

— Availability of tools to compromise the system (e.g. DSRC equipment).

7.2.2 Threat T1: Access Credentials keys can be obtained

7.2.2.1 Description

Access Credentials keys can be obtained from RSE by obtaining an AC response and a consequent brute force attack. The attacker may be in possession of an DSRC OBU communication simulator. This is not available commercially and may need to be purpose-build by the attacker.

7.2.2.2 Low Risk Context

Likelihood: Unlikely, because an attacker needs technical means not available as COTS

Impact: Low, the attack is only mounted on one OBU/user, and no significant data can be obtained

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.2.3 High Risk Context

Likelihood: Likely, knowledge about 5.8 GHz radio design are widespread and within the capability of electronics engineering students. The software complexity is low. Manufacturing capacity is available if threat agent is willing to invest. Threat agent has monetary profit motive, organized criminals.

Impact: Medium, DSRC attributes may be set to arbitrary values; privacy related information may be read out. TC/TSP may be accountable for privacy leaks.

Risk: Critical, the system is discredited and this may lead to threat “DES Authentication is not trusted”. Monetary loss for the EFC_DRSC service.

7.2.3 Threat T2: Authentication keys can be obtained

7.2.3.1 Description

Authentication keys can be obtained from an OBU by obtaining a few MAC responses and executing a brute force attack. The threat agent needs to be in possession of a RSE communication device. Because of GET_STAMPED semantics an attacker can pre-compute information and then be able to recover the MAC key in a few seconds. Master keys cannot be recovered in this way. Attackers may get direct monetary gain by altering entry data attributes in a closed toll system.

7.2.3.2 Low Risk Context

Likelihood: Possible, because RSE communication devices can be obtained commercially, knowledge about DES encryption is available.

Impact: Low, the attack is only mounted on one OBU/user by a hacker without monetary profit motive.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.3.3 High Risk Context

Likelihood: Possible, because RSE communication devices can be obtained commercially, knowledge about DES encryption is available. Threat agent has monetary profit motive, organized criminals.

Impact: Medium, the attack is only mounted on one OBU/user, but the case is communicated through the media and the system is discredited.

Risk: Major, the system is discredited and this may increase the likelihood for the High Risk Context scenarios for threats T3, T4, T6, T9, and T10.

7.2.4 Threat T3: OBU can be cloned

7.2.4.1 Description

Threat based on a successful outcome of threat T2, and with the knowledge and means to build a functional OBU. The complete attribute set and security keys are copied from a legitimate OBU.

7.2.4.2 Low Risk Context

Likelihood: Possible, because an attacker needs technical means not available as COTS to design and build an OBU which is difficult to manufacture. However, a hobbyist may be able to create a prototype for experimental use.

Impact: Low, the attack is only mounted on one OBU/user, and after a complaint by the user, the OBU is blocked and a new one is issued; the unduly debited fee is paid back to the user; a new OBU is issued to the user.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service, little money lost. The system is discredited.

7.2.4.3 High Risk Context

Likelihood: Likely, knowledge about 5.8 GHz radio design are widespread and within the capability of electronics engineering students. The software complexity is low. Manufacturing capacity is available if threat agent is willing to invest. Threat agent has monetary profit motive, organized criminals.

Impact: High, the attack can be constructed such that Toll Charger will not detect it, by using harvested keys and attributes only once. Toll Charger may need to pay back fees to many users, and may need to issue many new OBUs. The toll system may be discredited.

Risk: Critical, the system is severely discredited and this may lead to threat “DES Authentication is not trusted”.

7.2.5 Threat T4: OBU can be faked

7.2.5.1 Description

Threat based on a successful outcome of threat T2, and with the knowledge and means to build a functional OBU. Security keys and PAN are copied from a legitimate OBU and the attribute set is partially copied and partially filled with faked information.

This threat is very relevant for CCC transactions in an autonomous EFC system, in particular a context where CCC is not stored and processed in a central system due to privacy concerns.

7.2.5.2 Low Risk Context

Likelihood: Possible, because an attacker needs technical means not available as COTS to design and build an OBU which is difficult to manufacture. However, a hobbyist may be able to create a prototype for experimental use.

Impact: Low, the attack is only mounted on one OBU/user, and after a complaint by the user, the OBU is blocked and a new one is issued; the unduly debited fee is paid back to the user; a new OBU is issued to the user. Manual data consistency checks will reveal that illegal attributes was present.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service, little money lost

7.2.5.3 High Risk Context

Likelihood: Likely, knowledge about 5.8 GHz radio design are widespread and within the capability of electronics engineering students. The software complexity is low. Manufacturing capacity is available if threat agent is willing to invest. Threat agent has monetary profit motive, organized criminals.

Impact [DSRC EFC]: Low, the attack is only mounted on one OBU/user, and after a complaint by the user, the OBU is blocked and a new one is issued; the unduly debited fee is paid back to the user; a new OBU is issued to the user. Automatic online of off-line data consistency checks will reveal that illegal attributes was present.

Impact [autonomous EFC]: High, fake OBUs are mounted in several vehicles (with correct vehicle LPN). The OBE is able to make a compliant CCC transaction. The enforcement system will not be able to detect this fraudulent behaviour without real-time access to a central system which may be impossible due to operational and privacy constraints.

Risk: Critical, no effect on the EFC_DRSC/LAC/SM-CC service, little money lost. Investment in online consistency checks may be required to detect the issue. In an autonomous EFC system, there is significant impact on the effectiveness of the CCC service with subsequent money loss. Privacy policies may prohibit some consistency checks.

7.2.6 Threat T5: Authentication of OBU data can be repudiated

7.2.6.1 Description

Authentication of OBU data can be repudiated on the basis that DES is not secure. The use of DES is discouraged by standard bodies and industry driven organizations. The future use of DES is forbidden in some legislation.

7.2.6.2 Low Risk Context

Likelihood: Possible, even if information about DES is available in the internet, it is difficult to effectively claim this, and to reach out to media and legislators.

Impact: Low, TC and TSP may counterclaims that the attack is only mounted by some hacker communities, or some security authorities, and the intensity is low because the data and its authentication are considered court proof by the respective authorities.

Risk: Minor, no effect on existing EFC_DRSC/CCC/LAC/SM-CC services and systems.

7.2.6.3 High Risk Context

Likelihood: Likely, because anybody can claim this and be heard by media and legislators, information about DES is available in the internet. More legislation may explicitly deny the use of DES in the future.

Impact: High, the threat has been demonstrated (thread T2 and T3), and the impact is high because the authentication is not considered court proof by the respective authorities

Risk: Critical, CEN DSRC cannot be used for the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.7 Threat T6: Application data can be modified after the transaction

7.2.7.1 Description

Threat based on a successful outcome of Threat T2, and attacker with access to toll charger internal systems.

7.2.7.2 Low Risk Context

Likelihood: Unlikely, because threat agent will not challenge his own integrity.

Impact: Low.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service

7.2.7.3 High Risk Context

Likelihood: Possible, because an attacker may use harvested MAC keys to modify transactions after the DSRC communication transaction was complete and overcharge the user to gain monetary profit.

Impact: Medium

Risk: Major, the system is discredited and this may lead to threat “DES Authentication is not trusted”

7.2.8 Threat T7: Data in the VST is not secure

7.2.8.1 Description

Data in the VST is not secure: integrity or accountability cannot be ensured. Specifically this affects the layer 7 data elements ObeConfiguration and ManufacturerId.

The data in the ApplicationContextMark is used for selection of the security keys for Level 1 security. Any breach of integrity would lead to wrong DSRC security calculations and can be detected.

TC may use this information to verify that only certified OBU's are used in a tolling system.

7.2.8.2 Low Risk Context

Likelihood: Unlikely, individuals have no gain from this.

Impact: Low, because it affect the availability of the service (which is monitored by enforcement) and the attack can only be mounted for one OBU at the time

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.8.3 High Risk Context

Likelihood: Possible, Service Provider may gain monetary profit from using uncertified OBU's.

Impact: Low, because it affect the availability of the service (which is monitored by enforcement) and the attack can only be mounted for one OBU at the time

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.9 Threat T8: DSRC Communication can be eavesdropped

7.2.9.1 Description

DSRC Communication is not encrypted and can be eavesdropped. Information relating to the identity of the Service User can be obtained and exploited by unauthorized parties.

7.2.9.2 Low Risk Context

Likelihood: Unlikely because technical means is not available as COTS.

Impact: Medium, the toll system may be discredited.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.9.3 High Risk Context

Likelihood: Unlikely, because an attacker needs technical means not available as COTS; there is no motivation for this attack, other than discrediting the system and to gain access private information.

Impact: Medium, the impact is low because it does not affect the business, and the attack can only be mounted on one RSE at the time, i.e. eavesdropping a limited number of OBUs at one location for a defined time. Vehicles can also easily be tracked using video equipment.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.10 Threat T9: Correctness of application data are repudiated

7.2.10.1 Description

Toll Charger willing to change application data to obtain more payment from service provider/user.

7.2.10.2 Low Risk Context

Likelihood: Unlikely, because threat agent will not challenge his own integrity.

Impact: Low.

Risk: Minor, no effect on the EFC_DRSC/CCC/LAC/SM-CC service.

7.2.10.3 High Risk Context

Likelihood: Possible, because Toll Charger has access to application data.

Impact: High, in combination with Threat 1 the impact is high.

Risk: Major, Integrity: A higher fee is proposed / debited to the user. Users loose trust in the system. Toll Charger is discredited.

7.2.11 Threat T10: Master keys may be obtained from RSE

7.2.11.1 Description

Master keys can be obtained after successful recovery of a large number of authentication and access control keys.

7.2.11.2 Low Risk Context

Likelihood: Unlikely, the algorithm for key derivation is considered secure and brute force attack is currently infeasible.

Impact: High.

Risk: Minor, because of the very unlikely scenario, the risk is minor for this specific threat, and thus not using the formula in 7.1.4.

7.2.11.3 High Risk Context

Likelihood: Extremely unlikely, the algorithm for key derivation is considered secure and brute force attack is currently infeasible.

Impact: High

Risk: Minor, because of the extremely unlikely scenario, the risk is minor for this specific threat.

7.3 Summary

Table 13 summarizes the qualitative risk analysis, contained in Clause 7.

Table 13 — Summary of qualitative risks

Threat	Low risk context			High risk context		
	Likelihood	**Impact**	**Risk**	**Likelihood**	**Impact**	**Risk**
T1 Access credentials key recovery	Unlikely	Low	Minor	Likely	High	**Critical**
T2 Authentication key recovery	Possible	Low	Minor	Possible	Medium	**Major**
T3 OBU can be cloned	Possible	Low	Minor	Possible	High	**Critical**
T4 OBU can be faked	Unlikely	Low	Minor	Likely	High	**Critical**
T5 Authentication of OBU data can be repudiated	Possible	Low	Minor	Likely	High	**Critical**
T6 Application data can be modified after the transaction	Unlikely	Low	Minor	Possible	Medium	**Major**
T7 Data in VST is not secure	Unlikely	Low	Minor	Possible	Medium	Minor
T8 DSRC communication data can be eavesdropped	Unlikely	Medium	Minor	Unlikely	Medium	Minor
T9 Correctness of application data are repudiated	Unlikely	Low	Minor	Possible	High	**Major**
T10 Master key can be obtained from RSE	Extremely unlikely	High	Minor	Unlikely	High	Minor

8 Proposals for new security measures

8.1 Introduction

This clause proposes counter measures for the threats that have risk classified as major or critical and are within the scope of EFC standards listed in clause 1.

For threats connected to the requirements of CEN ISO/TS 19299, the corresponding security measures are proposed to be used. For the threats connected to functional security requirements original to this Technical Report new security measures are proposed.

All major and critical risks identified in Table 13 have their root weakness in the cryptographic properties of the CR and MAC calculation procedures.

8.2 Security measures to counter risks related to key recovery

The table below lists applicable threats, each with a list of possible countermeasures.

Table 14 — Possible countermeasures to major and critical risks

Threat	Possible countermeasures
T1 Access credentials key recovery	AES, randomization of RndOBU and RndRSE, increasing the diversification space
T2 Authentication key recovery	AES, randomization of RndOBU and RndRSE, disallow empty attribute list, MAC enlargement, MAC randomization
T3 OBU can be cloned	AES, transaction-counter
T4 OBU can be faked	AES, transaction-counter
T5 Authentication of OBU data can be repudiated	AES
T6 Application data can be modified after the transaction	AES, encrypted attributes over the air
T9 Correctness of application data are repudiated	AES

AES countermeasure comprises replacing DEA algorithm with its 56-bit keys with AES-128 and 128 bit keys. The ASN.1 module is not altered. AES-128 was published as a FIPS standard in 2001 and there is no serious weakness found so far. For the 192 and 256 variant some minor weaknesses are identified. A brute force attack on AES-128 requires in the order of 10^{21} more processing steps than DEA. AES is recommended by *Algorithms, key size and parameters report* [11].

RndRSE (in GET_Stamped) countermeasure comprises redefining the current 32-bit nonce. Currently the RndRSE is designed to detect repeated transactions, and a sequence number is sufficient for this purpose. Stating that this nonce should be a random number will increase security. It will reduce the predictability of the messages. Furthermore its size should be increased from 32 bits to 64 bits. The later change would not impact the ASN.1 module because RndRSE is defined as OCTET STRING in the GetStampedRq type.

RndOBU/RndOBE (in VST for access credentials calculation) countermeasure comprises increasing the size from 32 bits to 64 bits. In EN ISO 14906 this value is part of an OCTET STRING in the ASN.1 module, it can be extended without changes to the ASN.1 module specification. In EN ISO 12813 and EN ISO 13141, it is defined as OCTET STRING (SIZE (4)), here a changes is required to accommodate the enlarged field.

MAC randomization countermeasure comprises adding random data in the data going from OBU to RSE. This would mitigate the plaintext attack and the use of rainbow tables. The current ASN.1 module does not have a data field for this purpose; it can be introduced by redefining the semantics of the existing authenticator field. MAC generation specification [ISO/IEC 9797-1:2011] and [11] recommend against calculating the MAC from identical messages multiple times. By introducing a random field into the message, there is no longer a one-to-one relationship between the MAC and the Attribute List from one OBU. Figure 3 show the input to the MAC calculation in grey and how the MAC and new RndOBU2 can be stored in the authenticator (OCTET STRING). Currently the MAC is calculated over the Attribute List and the Nonce and the padding. In the future, the new RndOBU2 will also be included in the calculation.

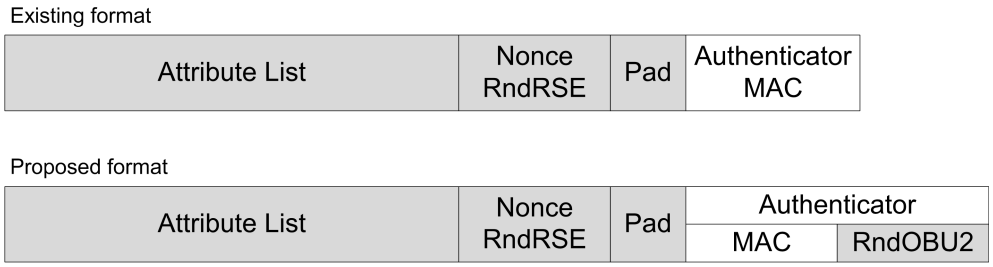

Figure 3 — Introduction of RndOBU2 in GetStampedRs

Increasing the diversification space of the access credential key countermeasure could mitigate Access Credential key recovery attacks. Currently 16-bits are allocated for access credentials diversification, this could be enlarged. This countermeasure will affect the ASN.1 module.

Disallow empty attribute list countermeasure would mitigate the rainbow table attack because it would imply that multiple encryption rounds would be necessary. This countermeasure would not have any impact on the ASN.1 module. It may also be possible, depending on RSE implementation details, be fully compatible with existing RSE.

MAC and AC enlargement countermeasure address MAC collisions. When the key length is increased from 56 to 128 bits, the MAC effectiveness is reduced [11], relatively and it is recommended to increase the MAC length from 32 bits to e.g. 64 bits. This would not affect the ASN.1 module because AC and MAC are defined as OCTET STRING.

Transaction counter countermeasure comprises more efficient use of the existing transaction counter mechanism. With real-time updates between all TSP and all RSE, vehicles with gaps in the transaction counter sequence could be identified by the RSE, in real time.

Encrypted attributes over the air countermeasure addresses privacy issues. The transaction list could be encrypted before transmission from OBE/RSE and decrypted after reception. A new encryption key derived from the MAC key could be used for this purpose. This countermeasure would not have any impact on the ASN.1 module.

Several of the countermeasures add new data fields or increase size of existing data fields. This may have a negative impact on DSRC system performance if the size increase is so large that messages needs to span several DSRC frames. This impact will be specific to individual system implementations because of the difference in attribute usage.

8.3 Recommended countermeasures

This technical report recommends to:

— replace DEA with AES (will reduce significantly all threats leading to major or critical risks that are related to key recovery threats). The root cause of the current threats is the weakness of the existing 56-bit DEA algorithm.

— increase the size of the cryptographic data field (RndOBE, RndRSE, AC and MAC) from 32 bits to 64 bits.

— use MAC randomization with a new random data field (RndOBU2) in each message that is to be authenticated with a MAC.

8.4 Qualitative cost benefit analysis

The proposed countermeasures will reduce the threats significantly and bring the DSRC cryptographic procedures and functions up to current standards. This will enhance the non-repudiation properties for the transactions.

A new DSRC system with the proposed countermeasures will have the similar capital and operational cost as existing systems.

Existing DSRC systems may be incrementally upgrading by introducing OBUs or OBE with improved security functions in new application. Old RSE will not interact with the new application but will continue to use old applications. Upgraded RSE will be able to select the improved DSRC OBU / OBE application based on EfcContextMark selection procedures.

9 Impact of proposed countermeasures

9.1 Current situation and level of fraud in existing EFC systems using CEN DSRC link

Presently in Europe, the CEN DSRC Toll systems encompass around 200 Toll Chargers, some playing the role of Toll Service Provider, 6 to 10 interoperable Toll Service Providers, and more than 25 million of OBU in circulation (mono technology DSRC, multi technologies including DSRC).

Regarding the security, the status is summarized hereafter.

a) All RSE are able to manage:

   1) the list of accepted “EFC ContextMark”, and of OBU model (Manufacturer/Equipment Class)

   2) the exception lists based on the PAN and to control the validity limit.

b) Some RSE are able to manage:

   1) limited number of security mechanisms,

   2) all security mechanisms, as specified in EN 15509 for level 0 (Transactions counters, Issuers and/or Operator Authenticators with GET Stamped) and level 1 (AC-CR),

   3) additional security mechanisms beyond EN 15509 security mechanisms, such as static Vehicle and/or contract Authenticators, dynamic “receiptDataAuthenticators” in ReceiptData Attribute.

The parameterization and personalization of OBUs, before delivery to customers for their vehicles, are secured via specific security mechanisms, only known by the Manufacturer and the Toll Service Provider, and using specific security personalization keys.

One of the operational challenges is for the TSP to monitor the transaction counters and to maintain and distribute updated exception lists to the Toll Chargers.

Depending on each operational context, there is or there is not, separation of role between Toll Chargers and Toll Service Providers.

In this heterogeneous landscape, in operation since the end of the 90s, according to the available information, it has never been seen:

a) cloned OBU’s (duplication of database associated to a given element, including the security mechanisms if any,

b) unauthorized use of AC-CR (supposing a discovery of derived key(s) or Master Key(s) for cheating),

c) in case of separation of roles, repudiation of transaction by a Toll Service Provider:

   1) due to a non-conformant IssuerAuthenticator (or Vehicle/contract Authenticator) sent by a Toll Charger,

   2) due to a bad sequence of Transactions counter,

d) availability of OBUs, potentially used for making "cloned OBUs" (beyond the stolen OBUs)

The European CEN DSRC (EN 15509) tolling landscape can thus be characterized as a low risk context.

Due to the lack of operational experience, there is no possibility to make a judgement on the risk for autonomous EFC systems regarding fraud by compromising DEA (DES) encryption in the current CCC and LAC DSRC security mechanisms.

9.2 EETS legislation

The definition of the EETS is supported by European legislation:

— European Directive (2004/52/EC),

— European Commission Decision (2009/750/EC)

The Decision is making a reference to EN 15509, without providing information about which version of the standard is applicable at a given time and also do not impose any security profile (0 or 1).

"Guide for the application of Directive 2004/52/EC of The European Parliament and of the Council and of Commission Decision 2009/750/EC" [12] specifies as well, EN 15509 without any version reference.

Consequently, if and when a new profile should be added in the EN 15509, de facto, the RSE should be able to support the corresponding interoperable OBUs / OBE with AES, whatever the version used by a given Toll Service Provider, for parameterization and personalization of its OBUs / OBE.

9.3 Analysis of effects on existing EFC systems

9.3.1 Affected roles

The change of the existing security mechanisms will impact

— Manufacturers

— Toll Service Providers

— Toll Chargers.

They will need to invest to support the new defined algorithms, depending on their role, as detailed hereafter.

9.3.2 The CEN DSRC equipment Manufacturers

They will have to implement new algorithms taking into account updated database for storing and managing new security keys with a new format.

They will have:

— to certify any new OBU model (identified by a given EquipmentClass different from the former ones) with notified bodies and/or its own laboratories. Once the OBU / OBE model is "internally" certified, the certification processes will have to be managed for each Toll domain or cluster of Toll

Domains (like TIS, VIA-T, EASYGO, ...); the corresponding costs will be supported by the manufacturers.

— to certify any new RSE model (identified by a given Equipment type, different from the former ones) with notified bodies and/or own laboratories. The certification processes will have to be managed for each Toll domain or cluster of Toll Domains (like TIS, VIA-T, EasyGo, ...); the corresponding costs will be supported by the manufacturers.

9.3.3 The Toll Service Providers

If they decide to select a new OBU / OBE model, supporting updated security mechanisms (AC-CR and/or dynamic Authenticators), they will need to update their back office and the personalization stations to be able:

— to parameterize/personalize the OBUs / OBE (derived AC-CR keys and derived Authentication Keys)

— to check the authenticator transmitted by the Toll Chargers as computed in the OBUs /OBE with the use of AES.

— to manage the generation and the management of AC-CR keys toward the Toll Chargers. It could be assumed that the process to transfer the keys to the TC for AC-CR will be able to support the change without any major modifications at the exception of the update of few parameters.

The existing OBUs / OBE are not able to be updated to support AES. There are dozens of millions of OBU / OBE in circulation across the world at the present time. Therefore, for the existing EFC systems, migration could only be progressive and following the natural renewal of the OBUs / OBE. Only a major security break could accelerate the migration process. Moreover, for maintaining the interoperability across the around 200 TC in Europe, each OBU / OBE will have to support one element with the existing RSE (with 3DES), not supporting AES and new one element supporting AES, to be used by the "updated" RSE.

9.3.4 The Toll Chargers

For new OBU models to be "accepted" in a given Toll domain:

— They will need to update their RSE to be able to use AES instead of DES for managing the AC-CR Keys and, if any, the Operators Authentication Keys. Depending on the generation of RSE, this could imply a complete change of the existing RSE. For the most recent equipment, a software release could be sufficient to support AES. Some other software updates will be required to allow the existing systems of the TC to support the changes induced by the use of AES.

— They will have to support OBU / OBE interoperability certification processes for each Toll domain or cluster of Toll Domains (like TIS, VIA-T, EasyGo, ...).

As for the OBU renewal by the TSP, a migration phase should take place to enable the TC to support the use of AES. This migration phase will generate additional costs for the TC on top of the renewal of the equipment due to the coexistence for a given period of 2 kinds of equipment, e.g. maintenance costs.

As European DSRC toll system in operation can be considered as low risk cases (cf 9.1), the introduction of new security mechanisms as AES could be foreseen in medium - long term. On the other hand, for CCC authentication in autonomous EFC systems an earlier introduction would be preferable. The reason is that there is only a small number of autonomous EFC systems in operation and this would avoid implementations of "old" security measures for CCC authentication in new autonomous EFC systems.

For new systems, the choice of AES will not induce added cost compare to DES as this change will required to have a new generation of equipment.

For CCC (autonomous EFC) the Toll Charger should have mechanisms in place to detect faked OBU / OBE with old security, at least during the migration phase from DES to AES OBU / OBE authentication. The Toll Charger should oblige the TSP to provide information about the status of the migration of OBUs / OBE from DES to AES, for example via a white list including the security type of the OBU / OBE.

10 Recommendations

10.1 Add security levels and procedures to EN ISO 14906

This technical report recommends to define new security levels with stronger encryption using the AES algorithm. The most suitable document to define this is EN ISO 14906. Furthermore, a revised EN ISO 14906 should contain the detailed descriptions of security levels currently found in annexes of EN 15509.

Currently EN 15509 (2014) specifies one Interoperable Application Profile (EFC-DSRC-IAP 1) with two security levels as summarized in Table 15. In a future revision of EN 15509 the detailed security mechanisms currently described in annexes can be removed and replaced with references to EN ISO 14906.

Table 15 — EN 15509 EFC-DSRC-IAP-1 security levels

	EFC-DSRC-IAP 1	
	Level 0	Level 1
Authentication	DEA	DEA
Access Control	No	DEA

This technical report recommends adding new security mechanisms as summarized in Table 16.

Table 16 — Proposed new security mechanisms

	Access Control	Authentication
Encryption algorithms	AES	AES
RndOBU	increase size	n.a.
accessCredentials	increase size	n.a.
RndRSE	n.a.	random value increase size
RndOBU2	n.a.	new field
MAC	n.a.	increase size

The new security mechanisms should be based on the same procedures as the ones of the existing levels in EN 15509 where AES is used for security calculations in Chained Block Cipher mode according to ISO/IEC 9797-1:2011, MAC Algorithm 5 (CMAC), with Padding Method 4, using the AES-128 algorithm according to ISO/IEC 18033-3:2010.

The OBU / OBE should be able to calculate the data attribute authenticator both using DEA (according to Security Level 1 in IAP 1) and AES (according to enhanced mechanisms), depending on the value of KeyRef that points either to an 8 octet DEA key or a 16 octet AES key stored in the OBU.

The RSE should be able to calculate Authenticators to validate data integrity and origin of the application data according to one or more of the security levels.

An OBU / OBE supporting future enhanced security, also supports IAP1 Security Level 1. This allows a seamless migration from level 1 without the need for immediate large investments in new RSE while gradually phasing in new OBU with support for enhanced security. With multiple security mechanisms present, the RSE may do an assessment on the fraud risk based on the security it uses for the tolling transaction.

The Service Provider should ensure that the value of the EFCContextMark transmitted by the OBU / OBE reflects the supported security level.

It is recommended that the RSE supports more than one level so to ensure wider interoperability.

10.2 Recommendation for other EFC standards

EN 15509 should be updated during the next revision to refer to the security levels and procedures defined in the revised EN ISO 14906.

EN ISO 12813 (CCC) is currently mandating use of EN 15509, security level 1. In a future revision, it should be to support improved security as recommended above.

EN ISO 13141 (LAC) is currently mandating use of EN 15509, security level 1. This report recommends support improved security for access credentials as recommended above.

CEN/TS 16702-1 (SM-CC) is currently mandating use of EN 15509, security level 1. In a future revision, it should be considered to support improved security as recommended above.

NOTE Other DSRC-based applications, such as e.g. EN 16312 “Interoperable application profile for AVI/AEI and ERI using DSRC”, have adopted security level 1 as defined in EN 15509. It would appear reasonable that this Technical Report and its recommendations were considered also in the reviewing and updating process of other security level 1-based standard deliverables.

10.3 New standards

There is no recommendation for new standards.

Annex A
(informative)

Current status of the DEA cryptographic algorithm

A.1 Overview

EN 15509 requires that DEA is used for MAC calculation. The DEA encryption algorithm (sometimes known as DES) is described in US FIPS 46 standards. In 2005 DEA was withdrawn from this specification and its use is discouraged.

EN 15509 requires that a MAC authenticator is calculated according to ISO/IEC 9797-1. This standard was updated in 2011 and the MAC algorithm combined with DEA, as used in EN 15509, is explicitly forbidden by the new revision. EN 15509 is compliant with the older 1999 version.

A.2 ISO/IEC 9797-1 (MAC Algorithm 1)

EN 15509:2014, B.2.1 specifies the procedure to use for calculating the MAC authenticator with the following statement: *"MAC according to* ISO/IEC 9797-1*, MAC Algorithm 1"*. When EN 15509 was first published, it was based on the 1999 edition of ISO/IEC 9797-1 and was compliant with this security standard. Over time, ISO/IEC 9797-1 has evolved. Clause 5 Requirements contains the following text in 1999 and 2011 respectively:

Table A.1 — ISO/IEC 9797-1 Recommendations for block ciphers used by MAC algorithm 1

1999 edition	**2011 edition**
"Users who wish to employ a MAC algorithm from this part of ISO/IEC 9797 shall select: • a block cipher e • a padding method from amongst those specified in Clause 6.1 • a MAC algorithm from amongst those specified in Clause 7"	"a block cipher e, either one of those specified in ISO/IEC 18033-3 or the DEA block cipher (specified in Annex A of ISO/IEC 18033-3:2005 and ANSI X3.92). **DEA may only be used with MAC Algorithms 3 and 4**: • a block cipher e • a padding method from amongst those specified in 6.3 • a MAC algorithm from amongst those specified in Clause 7"

NOTE The statement in bold (emphasis by the editors) was added in the 2011 edition. Thus the 2011 edition explicitly states that MAC algorithm 1 is not allowed to be used with DEA.

A.3 FIPS 46 (DEA Specification – DES)

DEA was published as a FIPS standard FIPS PUB 46 on 15 January 1977. The algorithm is later also specified in ANSI X3.92, NIST/SP 800-67 and ISO/IEC 18033-3.

DEA has been brute force cracked multiple times, first time publicly known in 1997. The short key length (56 bits) makes this possible. In 1999 a group organized a distributed project to publicly break a DEA key in 22 h.

This has lead to withdrawal of FIPS 46-3 by NIST on 19 May 2005. This means that DEA are no longer authorized for protection of unclassified US Federal government information.

A.4 ENISA recommendations

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU. ENISA works with these groups to develop advice and recommendations on good practice in information security.

The 2014 report on Algorithms, key size and parameters [11] recommends "minimum key size for a block cipher should be 128 bits; the minimum for the block size depends on the precise application but in many applications (for example construction of MAC functions) a 128-bit block size should now be considered the minimum" (3.2 and 3.2.3).

The report summarizes properties of various block ciphers by this table:

Table A.2 — Block Cipher Summary (adopted from Table 3.2 in ENISA report)

Primitive	Classification	
	Legacy	Future
AES	Ok	Ok
Camellia	Ok	Ok
Three-key-3DES	Ok	No
Two-key-3DES	Ok	No
Kasumi	Ok	No
Blowfish	Ok	No
DES	No	No

The report also gives advice on Message Authentication Codes (MAC). It does in particular mention the MAC truncation procedure: "a MAC function with security 2^s should have an output size of at least s bits; and for a well-designed MAC function the output size should be exactly s bits. If we truncate a MAC output by e percent, then the security drops to 2^{e*s} for a well-designed MAC function". This means that by applying EN 15509 and keeping the 32-bit MAC, we only get an effective key length of 32 bits with reduced non-repudiation properties.

Annex B
(informative)

Security considerations regarding DSRC in EFC Standards

B.1 Security vulnerabilities in EN 15509 and EN ISO 14906

EN 15509 and EN ISO 14906 defines security procedures for EFC with DSRC. The relatively weak DEA cipher together with possible known plain text attacks enables brute force attack to recover MAC and AC keys.

It is possible for an attacker with access to a customized RSE to create and send an appropriately chosen GET_STAMPED request and examine the GET_STAMPED response from the OBU / OBE. By requesting an empty list of attributes the response will be known, with the MAC authenticator added. RndRSE is chosen by the attacker and known. By applying the GET_STAMPED response with only 6 octets of payload the procedure in EN 15509:2014 (B.2) has only one iteration and the result is predictable. By examining repeated responses with different RndRSE, the authentication key can be recovered. The access credential key can be recovered in a similar attack, requiring a customized OBU / OBE.

Leaked credential keys enables an attacker to access application attributes in many OBUs / OBE in the same way a legitimate RSU has access to the attributes.

Leaked authentication keys enables an attacker create transaction with a valid MAC attribute authenticator undistinguishable from a valid OBU / OBE. This enables drivers to have faked or clonedOBU / OBE and avoids paying tolls. It enables modification of transaction while in transit to the TSP or TC.

EN 15509:2014, B.5, requires a transaction counter in the OBU / OBE. EN ISO 14906 defines the EquipmentStatus attribute. EN 15509 requires that 12 bits (of a total of 16) are reserved for use as a transaction counter. The counter is initialized to a known value during personalization, and it is incremented by the RSE after each transaction. This allows the RSE to detect OBUs / OBE that have gaps in the transaction counter. The semantics of the EquipmentStatus is also described in EN ISO 14906:2011, B.3.3.5 with the following statement: “The transaction counter also helps identifying instances when cryptographic security is broken”. It should be noted that also the transaction counter may be manipulated and its effectiveness may be reduced if cryptographic security is broken.

When using EN 15509 with security level 0, any RSE can write arbitrary values into the EquipmentStatus without any access control. RSE cannot trust the values found in this attribute.

B.2 Security vulnerabilities in EN ISO 12813 (CCC)

Security procedure in EN ISO 12813 Compliance check communication for autonomous systems follows EN 15509 security level 1, without support for the transaction counter. It is exposed to the same key recovery attacks as described for EN 15509.

It may be possible for a customized OBU (with a cloned security key) to comply with CCC procedures by providing false attribute values to a RSE. This may mislead the RSE to conclude that the passing vehicle is equipped with an authentic and activated functional OBU even then it is not.

Furthermore, the CCC security procedures assume that privacy protection requirements are covered by the access credentials mechanism. It may be possible for a perpetrator to listen in on the

communication between the RSE and OBU from a distance, without knowledge of the AC key. This type of attack has been demonstrated for ISO/IEC 18000-6C compliant tags [10].

Criminals may get monetary profit from the CCC security attacks by circumventing compliance check procedures and thus avoid the computed charge when using a non-compliant GNSS OBU / OBE.

B.3 Security vulnerabilities in EN ISO 13141 (LAC)

Security procedures in EN ISO 13141 Localisation augmentation communication for autonomous systems are designed to ensure that the OBU receives legitimate LAC information from the RSE. Access credentials provide for protection against unauthorized writing of LAC data, and hence for authentication of the LAC RSE. It is exposed to the same key recovery attacks as described for EN 15509 in preceding clauses.

The specification defines two 8 octet data fields (mAC-TC and mAC2) in the LACData attribute. This mechanism allows the producer of the LACData to sign the data before it is distributed to the RSE. Combined with lacTime it prevents an attacker to record a valid LACData attribute and later replay it at a different location. However, it does not protect against online attacks, where real LAC data are recorded at one location and immediately replayed at another location.

The RSE should use one of the following algorithms for calculating the MAC1:

1) CBC-DES according to ISO/IEC 9797-1:2011 MAC algorithm 1 using the DEA algorithm according to ISO/IEC 18033-3:2010 with a LAC authentication key of 8 octets;

2) CMAC according to ISO/IEC 9797-1:2011 MAC algorithm 5 using AES-128 according to ISO/IEC 18033-3:2010 with a LAC authentication key of 16 octets.

MAC2 is left open to private use.

In the first case mAC-TC is vulnerable to the same key recovery attacks as described in this document.

There is no immediate way for criminals get monetary profit from the LAC security attacks. It may be possible to create problems for the operations of the GNSS tolling system if perpetrators replay authentic (or disseminate false) LAC data from unauthorized RSE at chosen locations.

B.4 Security vulnerabilities in CEN/TS 16702-1 (SM-CC)

Security procedures in CEN/TS 16702-1 Secure monitoring for autonomous toll systems – Part 1: Compliance checking are designed to provide the Toll Charger and the Toll Service Provider with means to detect manipulation, fraud or OBU malfunction for EFC schemes using autonomous OBU / OBE.

SM-CC enables readout of Context Independent Itinerary Record by using procedures described in EN 15509, security level 1. It is exposed to the same key recovery attacks as described for EN 15509 in preceding clauses.

The SM-CC security procedures assume that privacy protection requirements are implemented effectively by the access credentials mechanism. It may be possible for a perpetrator to listen in on the communication between the RSE and OBU from a distance, without knowledge of the AC key. This type of attack has been demonstrated for ISO/IEC 18000-6C compliant tags (see CEN/TR 16670).

The security functions that protect the itinerary freezing process are based on modern strong cryptographic algorithms SHA-256, AES-128, and ECDSA. There is no reason to believe they are vulnerable.

There is no immediate way for criminals to get monetary profit from the SM-CC security attacks, but it may be possible to circumvent DSRC SM-CC IIR security procedures and thus avoid the GNSS computed charge.

Bibliography

[1] Gautam Korlam, Department of Computer Science, UC Santa Barbara, *Password Cracking in the Cloud,* http://cs.ucsb.edu/~koc/ns/projects/12Reports/GautamKorlam.pdf

[2] KLEINJUNG T., LENSTRA A.K., PAGE D., SMART N.P. École Polytechnique Fédérale de Lausanne and University of Bristol, *Using the Cloud to Determine Key Strengths*, http://www.cs.bris.ac.uk/~nigel/Cloud-Keys/, http://eprint.iacr.org/2011/254.pdf

[3] BIHAM E. Fast Software Encryption, Lecture Notes in Computer Science Volume 1267, 1997, pp 260-272, Springer-Verlag, *A Fast New DES Implementation in Software*

[4] KWAN M. *Cryptology ePrint Archive, Report 2000/051*. Reducing the Gate Count of Bitslice DES, 2000

[5] CEN/TR 16670:2014, *Information technology - RFID threat and vulnerability analysis*

[6] NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security Recommendations of the National Institute of Standards and Technology

[7] ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*

[8] ETSI/TS 102 165-1, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis*

[9] ETSI/TR 102 893, *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*

[10] ISO/IEC 18000-6:2013, *Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*

[11] European Union Agency for Network and Information Security, *Algorithms, key size and parameters, report*, Nov 2014

[12] The European Electronic Toll Service (EETS) - Guide for the application of Directive 2004/52/EC of The European Parliament and of the Council and of Commission Decision 2009/750/EC

[13] EN 16312:2013, *Intelligent transport systems - Automatic Vehicle and Equipment Registration (AVI/AEI) - Interoperable application profile for AVI/AEI and Electronic Register Identification using dedicated short range communication*

[14] ISO/IEC 29167-10, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*

[15] ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[16] EN ISO 14906:2011, *Electronic fee collection — Application interface definition for dedicated short-range communication*

[17] EN 15509:2014, *Electronic fee collection - Interoperability application profile for DSRC*

[18] CEN ISO/TS 19299:2015, *Electronic fee collection — Security framework (ISO/TS 19299:2015)*

[19] EN ISO 12813:2015, *Electronic fee collection — Compliance check communication for autonomous systems (ISO 12813:2015)*

[20] EN ISO 13141:2015, *Electronic fee collection — Localisation augmentation communication for autonomous systems (ISO 13141:2015)*

[21] CEN/TS 16702-1, *Electronic fee collection - Secure monitoring for autonomous toll systems - Part 1: Compliance checking*

[22] ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[23] CEN/TR 16152:2011, *Electronic fee collection - Personalisation and mounting of first mount OBE*

[24] ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[25] EN ISO 17575-1:2016, *Electronic fee collection - Application interface definition for autonomous systems - Part 1: Charging (ISO 17575-1:2016)*

[26] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[27] CEN ISO/TS 17574:2009, *Electronic fee collection - Guidelines for security protection profiles (ISO/TS 17574:2009)*

[28] EN ISO 12855:2015, *Electronic fee collection - Information exchange between service provision and toll charging (ISO 12855:2015)*

[29] CEN ISO/TS 14907-1:2015, *Electronic fee collection - Test procedures for user and fixed equipment - Part 1: Description of test procedures (ISO/TS 14907-1:2015)*

[30] ISO 17573:2010, *Electronic fee collection — Systems architecture for vehicle-related tolling*

[31] ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[32] ISO/IEC 29167-10:2015, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.