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]