Electronic fee collection - Interoperability application profile for DSRC

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-EN 15509:2014 sisaldab Euroopa standardi EN 15509:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 15509:2014 consists of the English text of the European standard EN 15509:2014.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 03.09.2014.	Date of Availability of the European standard is 03.09.2014.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.240.60

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 15509

September 2014

ICS 35.240.60

Supersedes EN 15509:2007

English Version

Electronic fee collection - Interoperability application profile for DSRC

Perception de télépéage - Profil d'application d'interopérabilité pour DSRC

Elektronische Gebührenerhebung - Anwendungsprofil für DSRC Interoperabilität

This European Standard was approved by CEN on 18 July 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

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

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

Ref. No. EN 15509:2014 E

Contents

Page

Foreword 5

Introduction 7

1 Scope 9

2 Normative references 11

3 Terms and definitions 11

4 Symbols and abbreviations 14

5 Conformance 16
5.1 General 16
5.2 Base standards 16
5.3 Main contents of an EFC-DSRC-IAP 17
5.4 Conformance requirements 18
5.5 Conformation notification 18
5.6 Conformance evaluation and testing 18
5.7 Multiple IAPs 18

6 Requirements for EFC-DSRC-IAP 1 18
6.1 OBU requirements 18
6.1.1 General 18
6.1.2 DSRC requirements 18
6.1.3 DSRC L7 and EFC functions 19
6.1.4 Data requirements 19
6.1.5 Security requirements 21
6.1.6 Transaction requirements 22
6.2 RSE requirements 22
6.2.1 General 22
6.2.2 DSRC requirements 22
6.2.3 DSRC L7 and EFC functions 22
6.2.4 Data requirements 23
6.2.5 Security requirements 23
6.2.6 Transaction requirements 24

Annex A (normative) Data specification 25

Annex B (normative) Security calculations 29

B.1 General 29

B.2 Attribute authenticator 29

B.2.1 General 29

B.2.2 Authenticator using the attribute Payment Means 30

B.3 Access Credentials 32

B.3.1 General 32

B.3.2 The principle of Access Credentials 32

B.3.3 Calculation of Access Credentials 33

B.4 Key derivation 34

B.4.1 General 34

B.4.2 Calculation of derived Authentication Key 34
B.4.3 Calculation of the Access Key 34
B.5 Transaction Counter 35
Annex C (normative) Implementation conformance statement proforma 36
C.1 General 36
C.2 Guidance for completing the ICS proforma 36
C.2.1 Purposes and structure 36
C.2.2 Abbreviations and conventions 36
C.3 Instructions for completing the ICS proforma 38
C.4 ICS proforma for OBU 38
C.4.1 Identification implementation 38
C.4.2 Identification of the standard 39
C.4.3 Global statement of conformance 39
C.4.4 ICS proforma for OBU 39
C.4.5 Profile requirements list for OBU 41
C.5 ICS proforma for RSE 45
C.5.1 Identification implementation 45
C.5.2 Identification of the standard 45
C.5.3 Global statement of conformance 45
C.5.4 ICS proforma for RSE 45
C.5.5 Profile requirements list for RSE 48
Annex D (informative) IAP taxonomy and numbering 52
D.1 General 52
D.2 Contents of an Interoperable Application Profile (IAP) 52
D.3 IAP referencing and numbering 53
D.3.1 IAP numbering 53
D.3.2 Security levels numbering 53
D.3.3 Numbering and referencing examples 53
Annex E (informative) Security computation examples 54
E.1 General 54
E.2 Computation of Attribute Authenticator 54
E.3 Computation of Access Credentials 55
E.4 Key derivation 55
E.4.1 Authenticator Key 55
E.4.2 Access Credentials Key 56
Annex F (informative) Security Considerations 57
Annex G (informative) Interlayer management 58
G.1 General 58

G.2 RSE Inter Layer Management guidelines 58

G.3 OBU Inter Layer Management guidelines 58

G.4 State Transition Tables 58

Annex H (informative) Mounting guidelines for the OBU 64

H.1 General 64

H.2 OBU mounting position 64

Annex I (informative) Use of this standard for the EETS 67

I.1 General 67

I.2 Overall relationship between European standardization and the EETS 67

I.3 European standardisation work supporting the EETS 67

I.4 Correspondence between this standard and the EETS 68

Bibliography 69

Foreword

This document (EN 15509:2014) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2015 and conflicting national standards shall be withdrawn at the latest by March 2015.

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.

This document supersedes EN 15509:2007.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This second edition of EN 15509 incorporates the following main modifications compared to the previous one:

— amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards;

— addition of a new clause (i.e. Clause 5) on conformance;

— amendment of the definition of vehicle licence plate number (size constraints and clarification that only Latin alphabet coding is supported)

— revision of the informative annex on security considerations (i.e. Annex F), and reference to CEN/TS 16439 on Electronic fee collection – Security framework;

— addition of a new informative annex (i.e. Annex I) on how to use this standard for the European electronic toll service;

— deletion of informative Annex H, part of the first edition, on Vehicle classification data, as it was deemed obsolete in view of EN ISO 14906:2011;

— deletion of informative Annex I, part of the first edition, on Using this European Standard for other DSRC-based transactions, as it was deemed obsolete in view of CEN ISO/TS 12813 and CEN ISO/TS 13141;

— amendments to reflect changes to the underlying base standards, with emphasis on backward compatibility with the first edition of this standard.

For the revision of this European Standard, the following principles have been used:

— take into account the evolution of some of the underlying standards and technical specifications, i.e. EN ISO 14906:2011, CEN/TS 16439, ISO/IEC 9797-1;

— maintain compatibility with the previous edition of this European Standard.

This European Standard defines an Application Profile based on a set of base standards according to the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC/TR 10000-1. The objective is to support technical interoperability between EFC DSRC-based systems in Europe. The principles of Application Profiling and relations to underlying base standards are defined in the Introduction.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

Introduction

CEN/TC 278 has produced a set of standards that supports interoperable electronic fee collection (EFC) dedicated short-range communication (DSRC)-based systems (e.g. EN ISO 14906, a “toolbox” for defining EFC-application transactions). However, these standards are necessary but not sufficient to ensure technical interoperability between DSRC-EFC-systems. This European Standard provides for a coherent set of requirements of the EFC-application and that is intended to serve as a common technical platform for EFC-interoperability.

This European Standard defines an Interoperable Application Profile for DSRC-EFC transactions. The main objective is to support technical interoperability between EFC-systems within the scope of this European Standard (as defined in Clause 1 below). A basic description of the EFC-service and an EFC System can be found in ISO 17573.

This European Standard only defines a basic level of technical interoperability for EFC equipment, i.e. on-board unit (OBU) and roadside equipment (RSE) using DSRC. It does not provide a full solution for interoperability, and it does not define other parts of the EFC-system, other services, other technologies and non-technical elements of interoperability.

The elaboration of this European Standard is based on the experiences from a vast number of implementations and projects throughout Europe. The standard makes use of the results from European projects such as CARDME, PISTA and CESARE, as they represent the fruit of European EFC harmonization and have been used as the basis for several national implementations.

The development of a common European Electronic Toll Service (EETS) as a part of the European Directive (2004/52/EC) also calls for the definition of an interoperable EFC-service. This European Standard provides for effective support for the work on the definition of EETS. After publication of EN 15509:2007 an EC-decision (2009/750/EC) on the EETS was adopted, that notes the first edition of this standard (EN 15509:2007) as a mandatory technical reference for the EETS. This has been fully maintained in this second edition of EN 15509.

Although there already are numerous existing base standards and specifications, there are specific needs that motivate this Interoperable Application Profile standard:

- Definition of the necessary and sufficient EFC-DSRC requirements to support technical interoperability;
- Provision of a crucial part of the EETS and hence support for the European Directive (2004/52/EC), the European Commission Decision (2009/750/EC of October 2009) on the definition of the European Electronic Toll Service and its technical elements complemented by the Guide for the application of the directive on the interoperability of electronic road toll systems;
- CARDME/PISTA/CESARE dialects are used in many countries but they need to converge, as the present situation is not cost effective;
- Needed additional DSRC-requirements are made;
- Choice of data elements including vehicle data;
- Extended definition of the use of some data elements, including semantics and coding;
- Clear choices for security implementation;
- It facilitates a complementing test specification (with clear relations between the conformance requirements and evaluation tests);
- Good support for procurements.

The Application Profile is described using the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC/TR 10000-1. The ISP-concept is specifically suited for defining interoperability specifications where a set of base standards can be used in different ways. This is exactly the case in EFC, where a set of base standards allows for different choices that are not interoperable.

The principles of the ISP-concept can be summarized as follows:

- An ISP shall make references only to base standards or other ISPs;
- The profile shall restrict the choice of base standard options to the extent necessary to maximize the probability of interoperability (e.g. chosen classes, conforming subsets, options and parameter values of base standards);
- The ISP shall not copy content of the base standards (in order to avoid consistency problems with the base standards);
- The profile shall not specify any requirements that would contradict or cause non-conformance to the base standards;
- The profile may contain conformance requirements that are more specific and limited in scope than those of the base standards;
- Conformance to a profile implies by definition conformance to a set of base standards, whereas conformance to that set of base standards does not necessarily imply conformance to the profile.

The use of the Application Profiling concept also provides for a flexible framework towards adoption, migration and use of this European Standard. Toll Chargers, Toll Service Providers and Manufacturers may use this Application Profile as a basis for interoperable use of their equipment, without having to disturb or otherwise affect any EFC-system used locally.

The general requirements of the Interoperable Application Profile are set out in Clause 5, whilst the specific conformance requirements are given in Clause 6. To facilitate easy referencing, testing and look-up, these specific requirements are divided into two parts; On-Board Unit (OBU) requirements and Roadside Equipment (RSE) requirements.

In addition this European Standard also includes various annexes that provide further detailed specifications as well as background, motivation and examples for the conformance requirements. The intention is that these enhance readability and understanding of this European Standard.

The base standard EN ISO 14906:2011 has been the subject of a revision. The revision of EN 15509 takes into account the revision introduced in this base standard.

This European Standard is complemented by a set of standards defining Conformity Evaluation of the Conformance Requirements.

EN 15876 defines how to evaluate on-board and roadside equipment for conformity to EN 15509 (this European Standard). EN 15876 consists of the following parts, under the general title "*Electronic fee collection — Evaluation of on-board and roadside equipment for conformity to* EN 15509":

- Part 1: Test suite structure and test purposes;
- Part 2: Abstract test suite.

NOTE EN 15786-1 and EN 15786-2 will be subject to revision to accommodate the changes introduced in this second edition of EN 15509.

1 Scope

The scope for this European Standard is limited to:

- payment method: Central account based on EFC-DSRC;
- physical systems: OBU, RSE and the DSRC interface between them (all functions and information flows related to these parts);
- DSRC-link requirements;
- EFC transactions over the DSRC interface;
- data elements to be used by OBU and RSE used in EFC-DSRC transactions;
- security mechanisms for OBU and RSE used in EFC-DSRC transactions.

The scope of this European Standard is illustrated in Figure 1.

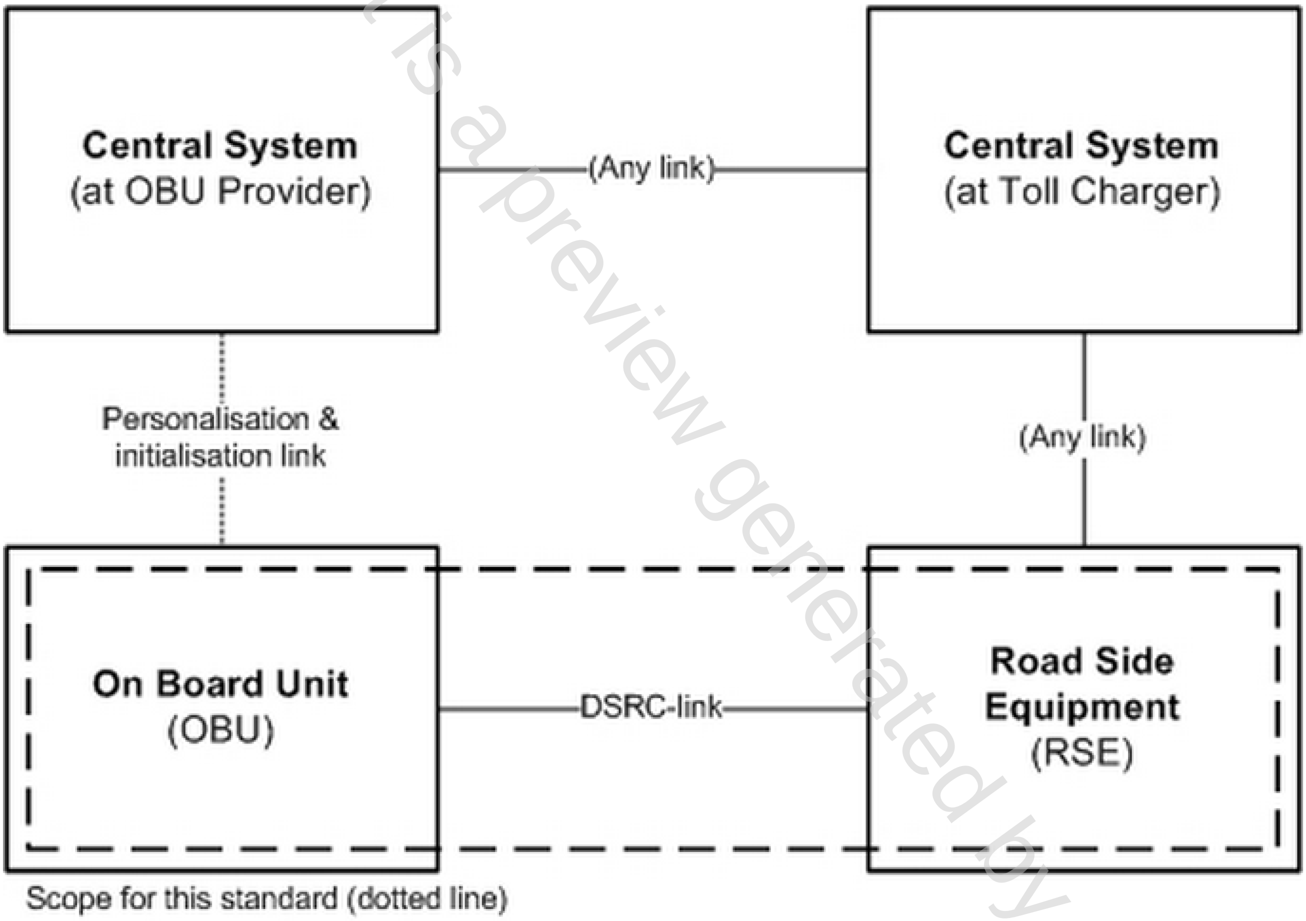

Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

It is outside the scope of this European Standard to define:

- contractual and procedural interoperability requirements (including issues related to a Memorandum of Understanding, MoU);
- conformance procedures and test specification (this is provided in a separate set of standards);

- setting-up of operating organizations (e.g. toll charger, toll service provider, trusted third party, etc.);
- legal issues;
- other payment methods in DSRC-based EFC (e.g. on-board accounts using integrated circuit cards);
- other basic technologies (e.g. GNSS/CN or video registration based EFC). However, this European Standard may be used for defining the DSRC-EFC parts for the use in applications that implement a mix of different technologies;
- non-EFC transactions over the DSRC interface (e.g. CCC and LAC communication, which is defined in other standards);
- other interfaces or functions in EFC-systems than those specified above (i.e. information flows and data exchange between operators or personalization, initialization and customization of the OBU).

Some of these issues are subject to separate standards prepared by CEN/TC 278, ISO/TC 204 or ETSI ERM.

Figure 2 shows the scope of this European Standard from a DSRC-stack perspective.

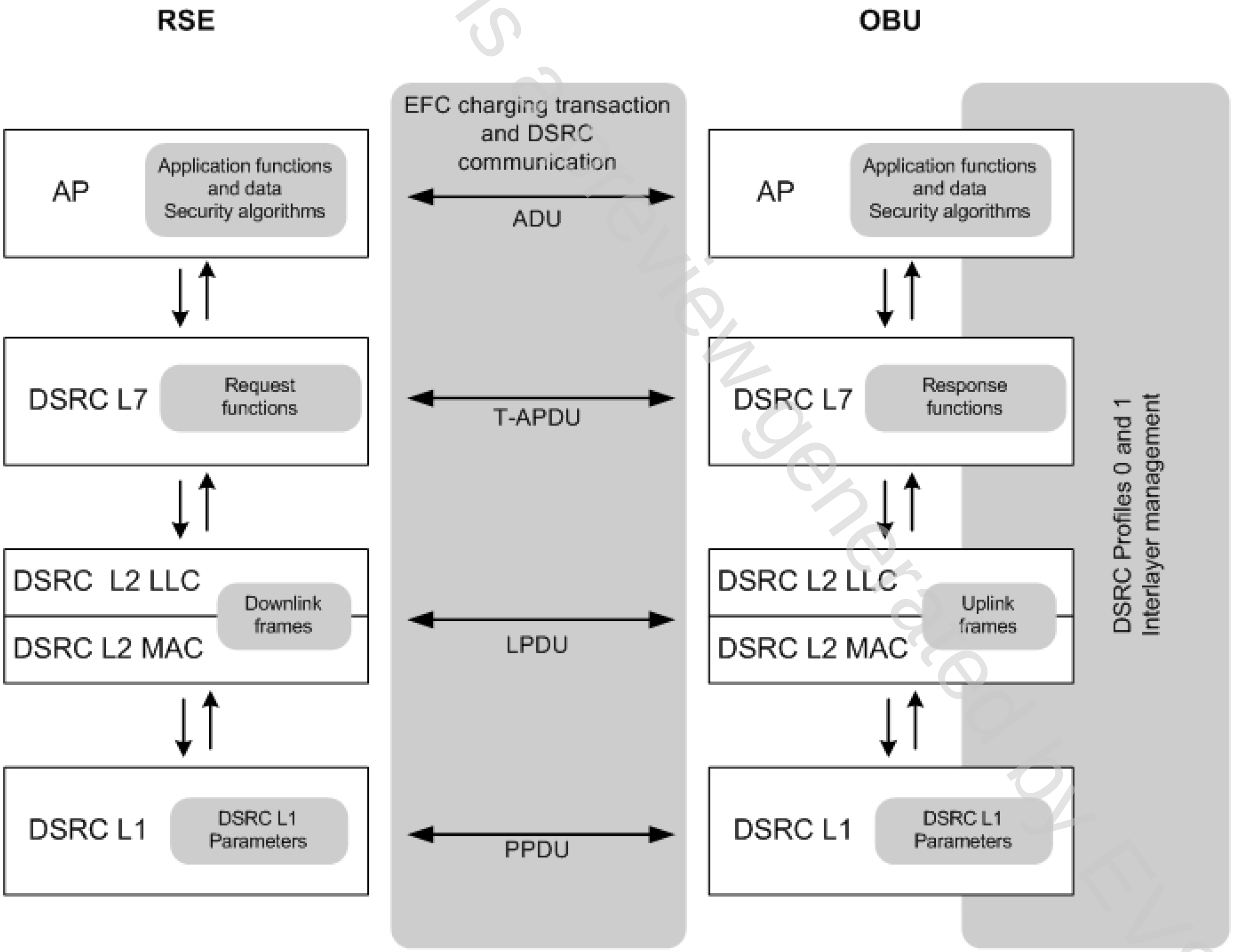

Figure 2 — Relationship between this European Standard and DSRC-stack elements

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 12834:2003, *Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) - DSRC application layer*

EN 13372:2004, *Road Transport and Traffic Telematics (RTTT) - Dedicated short-range communication - Profiles for RTTT applications*

EN ISO 14906:2011, *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)*

ETSI/TS 102 486-1-1 V1.1.1 (2006-03), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

ETSI/TS 102 486-2-1 V1.2.1 (2008-10), *Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

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

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

3 Terms and definitions

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

3.1
access credentials
trusted attestation or secure module that establishes the claimed identity of an object or application

Note 1 to entry: The access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

3.2
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

3.3
authenticator
data, possibly encrypted, that is used for authentication

3.4
base standard
approved international standard or ITU-T Recommendation