ETSI TS 102 723-9 V1.1.1 (2021-03)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
OSI cross-layer topics;
Part 9: Interface between security entity and facilities layer

Reference

DTS/ITS-00553

Keywords

adaption, addressing, interface, ITS, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

The present document is part 9 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.2].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The communications architecture standard ETSI EN 302 665 [i.1], clause 4.4 describes the reference architecture of ITS station, which includes the following internal functional blocks:

- ITS-S Access layer;
- ITS-S Networking & Transport layer;
- ITS-S Facilities layer;
- ITS-S Applications;
- ITS-S Management entity;
- ITS-S Security entity;

and the interfaces between these blocks.

The present document specifies interfaces between the security entity and facilities layer of ITS-S from a functional point of view. Access control to the Service Access Point and further definitions of station internal signals are out of scope of the present document.

The SAP specification is specific to the ITS architecture but generic to the concrete technologies used.

The present document is structured in the following way:

- First, the architecture integration is outlined.
- Secondly, functionalities are collected from related standards and mapped to service primitives.
- Finally, the use of service primitives in procedures is described.

1 Scope

The present document specifies interfaces between the ITS Security entity and the ITS Facilities layer including interface services and service primitives which are extensible in order to achieve general applicability. Additionally, it specifies related procedures and common parameters.

The SF-SAP description in the present document is from a functional point of view according to the ISO model modified by ETSI EN 302 665 [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.2] ETSI TS 102 723-1: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 1: Architecture and addressing schemes".

[i.3] ISO 24102-3: "Intelligent transport systems -- Communications access for land mobiles (CALM) -- ITS station management -- Part 3: Service access points".

[i.4] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[i.5] ETSI TS 102 637-1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements".

[i.6] ETSI TS 101 539-2: "Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification".

[i.7] ETSI TS 101 539-3: "Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification".

[i.8] PRESERVE Deliverable D1.3: "V2X Security Architecture V2", January 2014.

NOTE: Available at https://www.preserve-project.eu/www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf.

[i.9] H. Schweppe, B. Weyl, Y. Roudier, M.S. Idrees, T. Gendrullis, M. Wolf: "Securing car2X applications with effective hardware-software co-design for vehicular on-board networks". In 27th Joint VDI/VW Automotive Security Conference, Berlin, Germany, October 2011. VDI Berichte 2131.

NOTE: Available at https://evita-project.org/Publications/SGIR11.pdf.

[i.10] ETSI EN 302 663: "Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.11] ETSI EN 303 613: "Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.12] ETSI TS 101 539-1: "Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 302 665 [i.1], ETSI TS 102 940 [1] and the following apply:

security association: addressing information and 'security material' for connecting to the 'security management entity'

NOTE: This corresponds to 'enrolment authorities' and 'authorization authorities'.

security entity: functional entity inside an ITS station which offers 'security mechanisms'

security protocol: protocol used to encode and decode 'security material' and messages between ITS Stations

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 302 665 [i.1], ETSI TS 102 940 [1] and the following apply:

SAP	Service Access Point
SF-SAP	Security entity - Facilities layer SAP

4 Architecture

4.1 General

4.1.1 Introduction

Figure 1 shows the ITS station reference architecture, as defined in ETSI EN 302 665 [i.1]. The present document contains the specification of the Service Access Points (SAP), connecting the security entity and the facilities layer, i.e. SF-SAP.

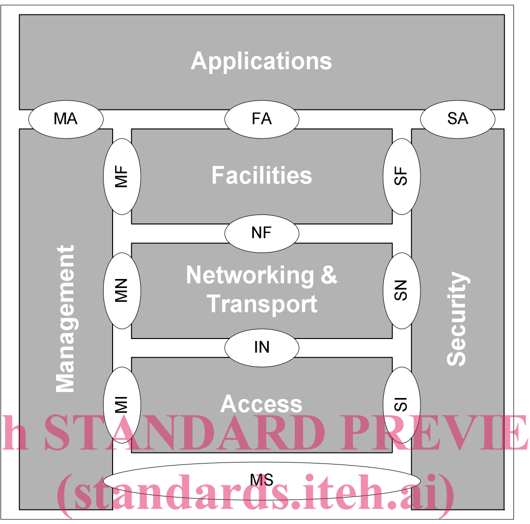

Figure 1: ITS station reference architecture

Interaction between the security entity and the layers may follow two principles. First, the vertical message flow through the layers from top to bottom or vice versa. Secondly, the horizontal control communication from the security entity towards the corresponding layer. Both are described in clauses 4.1.2 and 4.1.3.

4.1.2 Vertical message flow

Figure 2 extends the ITS station reference architecture by illustrating the overall information flow through the layers, from originating application on the left hand side, to the receiving application on the right hand side.

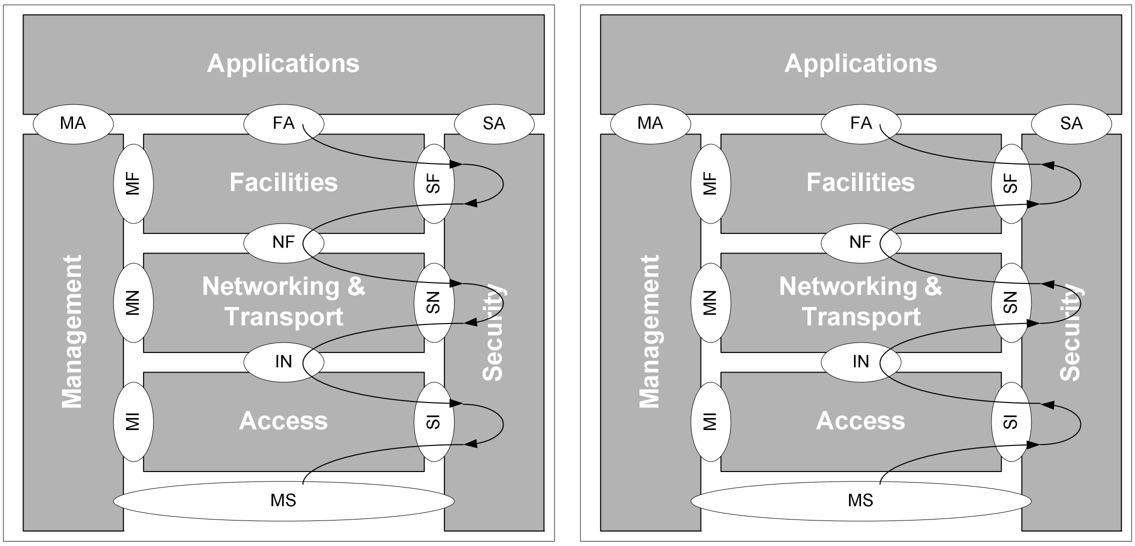

Figure 2: TX (left) and RX (right) information flow through the ITS station

The present document specifies only the SF-SAP, therefore only a subset of the ITS station reference architecture has to be taken into account. Figure 3 shows the typical information flow between any sending (TX) and receiving (RX) party, with regard to the SF-SAP only. The Security entity acts like a layer inside the Facilities layer, i.e. it is called during the processing of messages traversing the Facilities layer. The security entity will however not act as a layer above or below the Facilities layer. This means that interactions with Applications and Network & Transport layers are achieved via other means, i.e. the FA-SAP is used for the interaction between the Facilities and Applications layers, whereas the NF-SAP is used for the interaction between the Networking & Transport layers and Facilities layers.

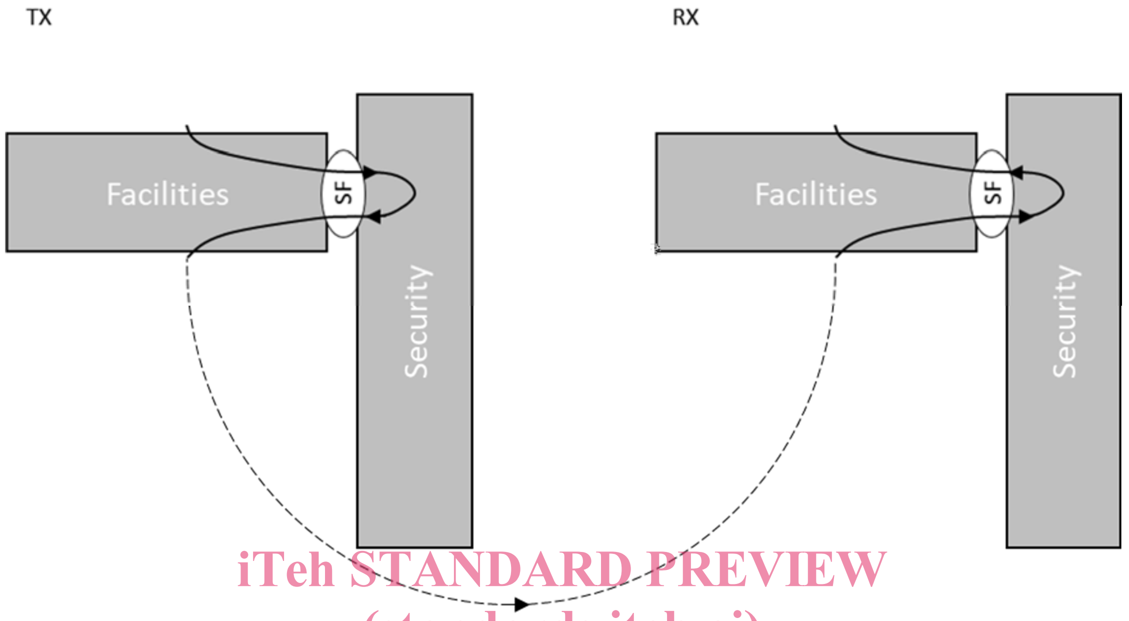

Figure 3: SF-SAP centric Information flow

4.1.3 Horizontal control communication

Figure 4 outlines the second communication principle. There is a horizontal control communication between the security entity and the corresponding communications layer, facilities layer in this case. This is needed for the ID change functionality introduced later. In general, the security entity will be able to indicate an ID change to the corresponding layer and some additional ID change related calls.

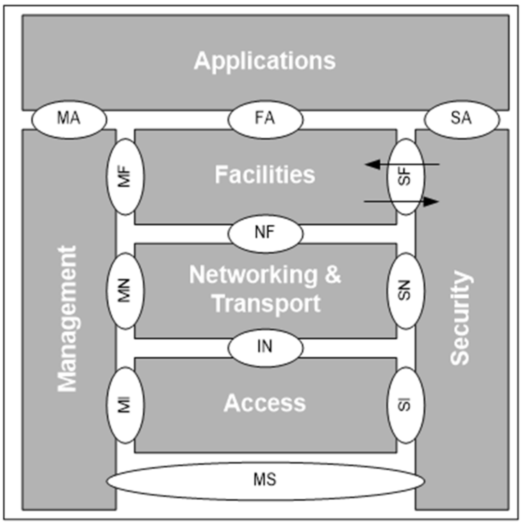

Figure 4: Horizontal Control Communication

4.1.4 Protocol work split

The SF-SAP provides a set of primitive Security functions to the Facilities layer.

Figure 5 shows how a protocol entity within the Facilities layer handles the sending and receiving of information but uses some security extensions to invoke the primitive functions of the Security entity in order to meet the security requirements of this layer. They are supported by the Identity Management Capabilities, specified in ETSI TS 102 940 [1], clause 6, necessary to apply the Atomic Security Capabilities.

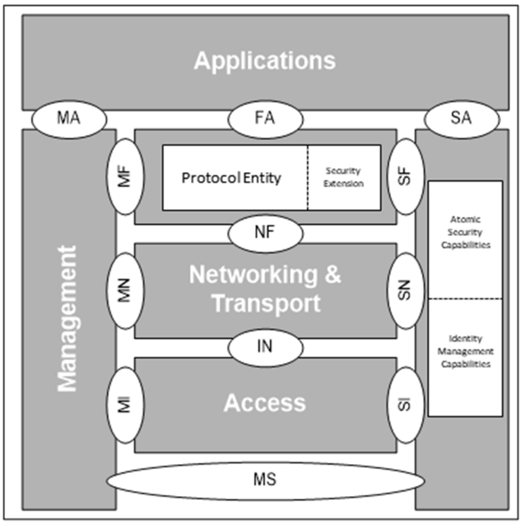

Figure 5: Protocol work split

4.1.5 Multiple instances

The present document does not discuss architecture. However, the SF-SAP can support different permissions. The management of different credential sets at the same time can be implemented by using multiple instances of the Security entity at the same time. Different or same components in the Facilities layer might use multiple instances of the Security entity using the service primitives described in clause 5. Handling and access control of those is out of scope of the present document.

4.1.6 Error handling

The present document does not make assumptions on implementation specific error handling for using the described services. This means that, if a call of any of the described services fails for some reason, the present document does not specify if this should be handled using exceptions or any other error handling technique.

However, the present document does specify the behaviour of services that can have a positive or negative result. For instance, a SF-VERIFY can be SUCCESSFUL if the verification was successful or it can be unsuccessful, if the signature was invalid (FALSE_SIGNATURE). This is considered to be within normal operation conditions, and therefore not an error.

4.2 Security services

The required ITS security services are identified as the first level security services in ETSI TS 102 940 [1], clause 5.2. In addition to those, security services used in the research projects PRE-DRIVE C2X and EVITA were adopted and fitted to the existing services. See PRESERVE Deliverable D1.3 [i.8] and [i.9] for documentation on the research project services.

Table 1 summarizes the security services to be specified in the present document, clause 5. These security services shall be invoked directly by applications or other components and layers according to ETSI TS 102 940 [1]. A "security service group" is introduced to ease the readability of the table.