ETSI TR 103 630 V1.1.1 (2020-11)

Intelligent Transport Systems (ITS);
Security;
Pre-standardization Study on ITS Facility Layer Security for C-ITS Communication Using Cellular Uu Interface

Reference

DTR/ITS-00551

Keywords

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

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 Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**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

Using both short-range and wide-area communications for Cooperative ITS (C-ITS) deployment is part of the European strategy on C-ITS [i.12]. The ITS reference architecture [i.1] also specifies an access layer incorporating different access technologies for both short-range and wide-area communications. The European C-ITS certificate and security policies [i.10] and [i.11] have been defined for setting up one common C-ITS trust domain for the EU, which gives trust to ITS services using both short-range and wide-area communication technologies.

Many current ETSI ITS standards, e.g. [i.5], [i.6], and [i.7], have been developed considering short-range communications as the main access technology, though the standards of higher layers should be agnostic and flexible with the communication technologies [i.12]. Among many ITS security solutions, enabling security functions at the Facilities layer is one way of providing end-to-end ITS security in C-ITS independent from the lower layer protocols. The purpose of the present document is to investigate which amendments to existing ETSI ITS standards are needed to facilitate ITS security operations at the Facilities layer considering C-ITS deployment scenarios using wide-area communications based on mobile cellular networks. Other ITS security solutions, e.g. performing security operations at the network layer with GeoNetworking protocol, can equally provide end-to-end ITS security. Study in the present document aims at enabling ITS security at the Facilities layer while keeping compatibility with other ITS security solutions.

Wide-area cellular communications have different characteristics compared with short-range communications when supporting secured message exchange for ITS applications. The framework of mobile networks in C-ITS, including the impacts to the ITS system architecture defined in [i.1], are studied in [i.13] by ETSI ITS WG2. The present document studies the use cases and requirements of security when using wide-area cellular communications for ITS applications.

The present document also identifies standardization activities to enable ITS security at Facilities layer in ETSI ITS as one way to facilitate C-ITS deployment using wide-area cellular communications.

Since wide-area communications through cellular networks uses IP protocol at the network layer, ITS security at the Facilities layer discussed in the present document is based on IP protocol stacks and in principle can be applied to any communication channel that uses an IP-based protocol stack, e.g. communications among ITS backend systems.

NOTE: Commercial mobile cellular networks provide communication services ensuring confidentiality and integrity as well as the authentication of base stations meeting high security requirements. However, the present document focuses at the C-ITS security features following the European C-ITS certificate and security policies [i.10] and [i.11]. The intrinsic security features of mobile cellular systems can further contribute to the security of C-ITS communications, but these are out scope of the present document.

1 Scope

The present document analyses the existing solutions for secured ITS communications using wide-area cellular systems. The present document also identifies gaps in current ETSI ITS standards for enabling security features at the ITS Facilities layer, to facilitate secured C-ITS implementation using security features above the Networking & Transport layer when using wide-area cellular communications. The present document also proposes necessary standardization activities to close the identified gaps while considering interoperability and backward compatibilities with existing standards.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 (V1.1.1) (2010-09): "Intelligent Transport Systems (ITS); Communications Architecture".

[i.2] ETSI TS 102 940 (V1.3.1) (2018-04): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.3] ETSI TS 102 941 (V1.3.1) (2019-02): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[i.4] ETSI TS 103 097 (V1.3.1) (2017-10): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[i.5] ETSI TS 103 301 (V1.3.1) (2020-02): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

[i.6] ETSI EN 302 637-2 (V1.4.1) (2019-04): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[i.7] ETSI EN 302 637-3 (V1.3.1) (2019-04): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.8] ETSI TS 102 731 (V1.1.1) (2010-09): "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

[i.9] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "Standard for Wireless Access In Vehicular Environments -- Security Services for Applications and Management Messages Amendment 1".

[i.10] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1, June 2018.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf.

[i.11] Security Policy & Governance Framework for Development and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, December 2017.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf.

[i.12] EC, COM (2016) 766: "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", 2016.

[i.13] ETSI TR 102 962 (V1.1.1) (2012-02): "Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)".

[i.14] ETSI TS 136 300 (V14.2.0): "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300 version 14.2.0 Release 14)".

[i.15] 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.16] CONVERGE Project, Deliverable D4.3: "Architecture of the Car2X Systems Network", Version 1.2, 2015.

NOTE: Available at http://www.converge-online.de/doc/download/Del%2043%20Masterdocument.zip.

[i.17] ETSI EN 302 636-4-1 (V1.4.1) (2020-01), "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.18] ISO/DTS 21177: "Intelligent transport systems -- ITS station security services for secure session establishment and authentication between trusted devices".

[i.19] ETSI TS 102 943 (V1.1.1) (2012-06): "Intelligent Transport Systems (ITS); Security; Confidentiality services".

[i.20] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.21] IETF draft-msahli-ise-ieee1609-01: "TLS Authentication using IEEE 1609.2 certificate".

NOTE: Available at https://tools.ietf.org/pdf/draft-msahli-ise-ieee1609-01.pdf.

[i.22] IEEE 1609.2b™-2019: "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2 -- PDU Functional Types and Encryption Key Management".

[i.23] ETSI TR 102 893 (V1.2.1) (2017-03): "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

[i.24] SCOOP@F, C-ROADS France, InterCor: "Hybrid end-to-end security: Specification", Deliverable 2.4.4.11-H, Version 4.00, 14/11/2019.

[i.25] ETSI TS 151 011 (V4.15.0): "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011 version 4.15.0 Release 4)".

[i.26] ETSI TS 131 102 (V15.10.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 15.10.0 Release 15)".

[i.27] ETSI TS 102 723-8 (V1.1.1) (2016-04): "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer".

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] and the following apply:

ITS backend: centralized system in the backend providing ITS services

EXAMPLE: Systems at traffic control, traffic management, ITS application suppliers, or automotive OEMs.

NOTE: A central ITS station may be part of an ITS backend.

ITS-G5: access technology according to ETSI EN 302 663 [i.15]

LTE-V2X Sidelink: access technology using V2X sidelink communication according to ETSI TS 136 300 [i.14]

Uu interface: interface between user equipment and base station in 3GPP systems

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
5G	5th Generation
AMQP	Advanced Message Queuing Protocol
BSA	Basic Set of Applications
BTP	Basic Transport Protocol
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
C-ITS	Cooperative - ITS
DEN	Decentralized Environments Notification
DENM	Decentralized Environments Notification Message
DPIA	Data Protection Impact Assessment
DTLS	Datagram Transport Layer Security
E2E	End-to-End
EU	European Union
GDPR	General Data Protection Regulation
GN	GeoNetworking
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
I2I	Infrastructure-to-Infrastructure
I2V	Infrastructure-to-Vehicle
IP	Internet Protocol
IPSec	IP Security
ITS	Intelligent Transport Systems
IVIM	Infrastructure to Vehicle Information Message
IVS	In-Vehicle Signage
MQTT	Message Queuing Telemetry Transport
N2V	Network-to-Vehicle
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
PDU	Packet Data Unit

PKI	Public Key Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SF-SAP	Security Facilities Service Access Point
SIM	Subscriber Identity Module
SREM	Signal Request Extended Message
SSEM	Signal request Status Extended Message
SSP	Service Specific Permissions
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TVRA	Threat, Vulnerability and Risk Analysis
UDP	User Datagram Protocol
UE	User Equipment
USIM	Universal Subscriber Identity Module
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2V	Vehicle-to-Vehicle

4 Background

4.1 ITS architecture and wide-area cellular communications for ITS

4.1.1 ITS station architecture

ETSI EN 302 665 [i.1] describes an ITS station reference architecture based on the following four processing layers:

- Access Layer;
- Networking & Transport Layer;
- Facilities Layer; and
- Application Layer.

The Access Layer in the ETSI ITS station reference architecture represents the OSI layer 1 and 2 of the ITS station and can be implemented with various communication technologies, including both short-range and wide-area communications, as shown in Figure 1.

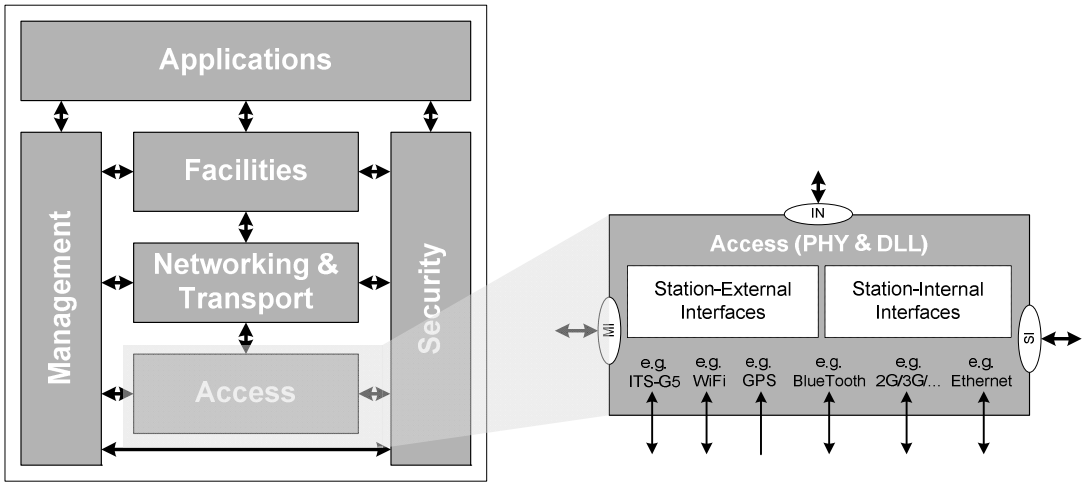

Figure 1: Access layer of ETSI ITS station reference architecture (ETSI EN 302 665 [i.1])

Cellular 2G/3G/4G/5G networks provide wide-area communications between User Equipment (UE) and base station, which is known as the Uu interface in the 3GPP architecture of 3G, 4G, and 5G networks, supporting ITS applications.

The framework of mobile networks in C-ITS, including the impacts to the ITS system architecture defined in ETSI EN 302 665 [i.1], have been studied in ETSI TR 102 962 [i.13]. The present document studies the use cases and requirements of security at the facilities layer when using wide-area cellular communications for ITS applications.

4.1.2 Wide-area Communications for ITS Applications through Mobile Cellular Networks

The framework of 3G/4G cellular networks in Cooperative ITS (C-ITS) is described in ETSI TR 102 962 [i.13].

NOTE 1: A revision of [i.13] is under development to include the 5G cellular network for support of day one ITS applications and other advanced automotive and ITS applications.

Figure 2 shows an overview of ITS using wide-area cellular communications, where the dashed lines indicate links at the access layers and solid lines show the path of ITS message communication with the arrows indicating the direction of information flows.