# 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

# 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.

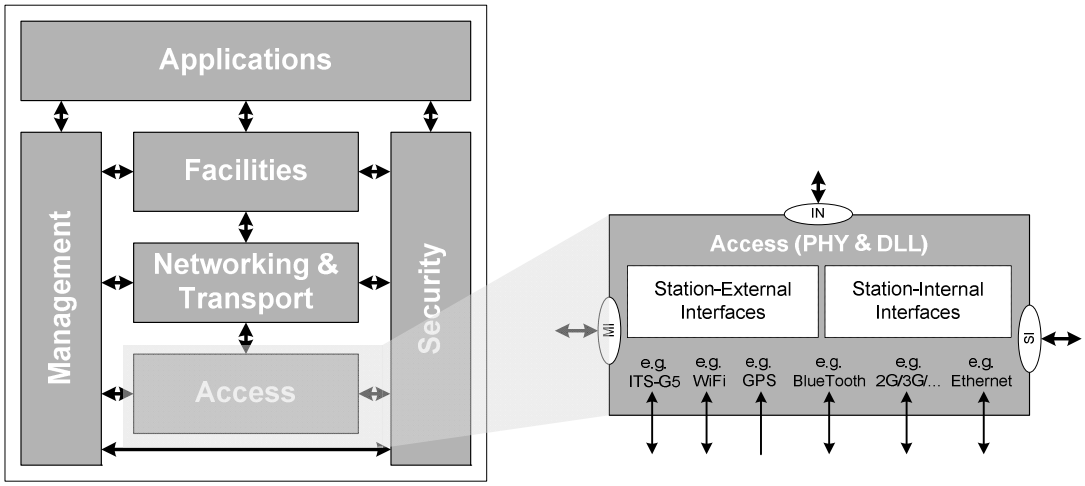


**Figure 1: Access layer of ETSI ITS station reference architecture (ETSI EN 302 665 [i.1])**

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.

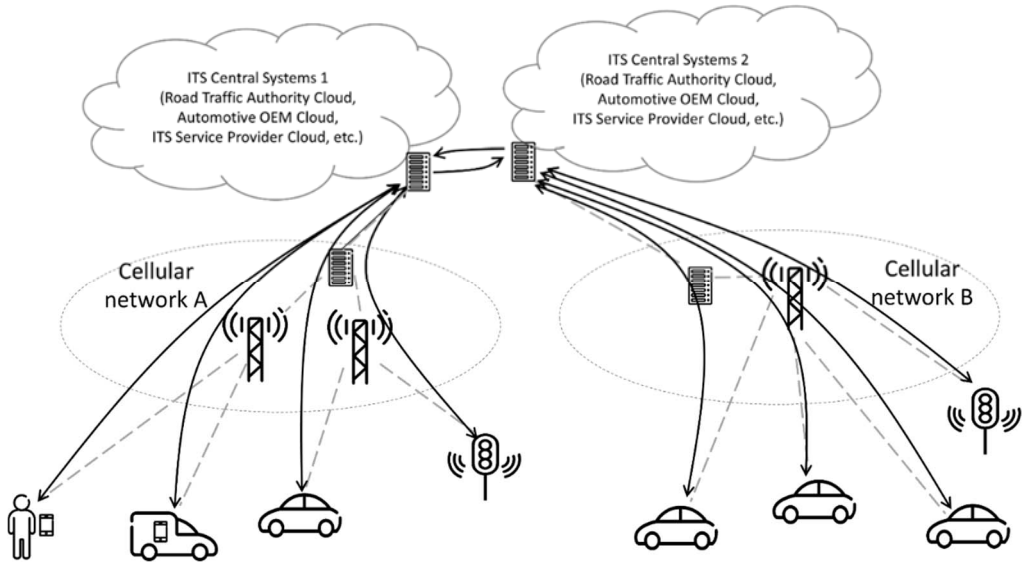


**Figure 2: Overview of ITS using wide-area cellular communications involving multiple service providers and cellular networks**

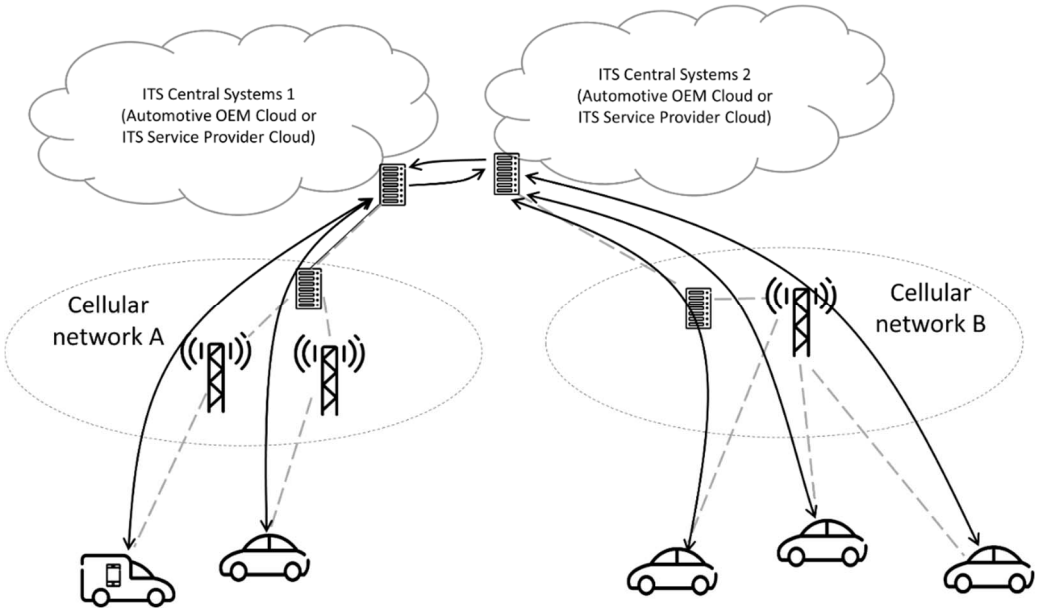


**Figure 3: Overview of V2V via cellular infrastructure using wide-area cellular communications**

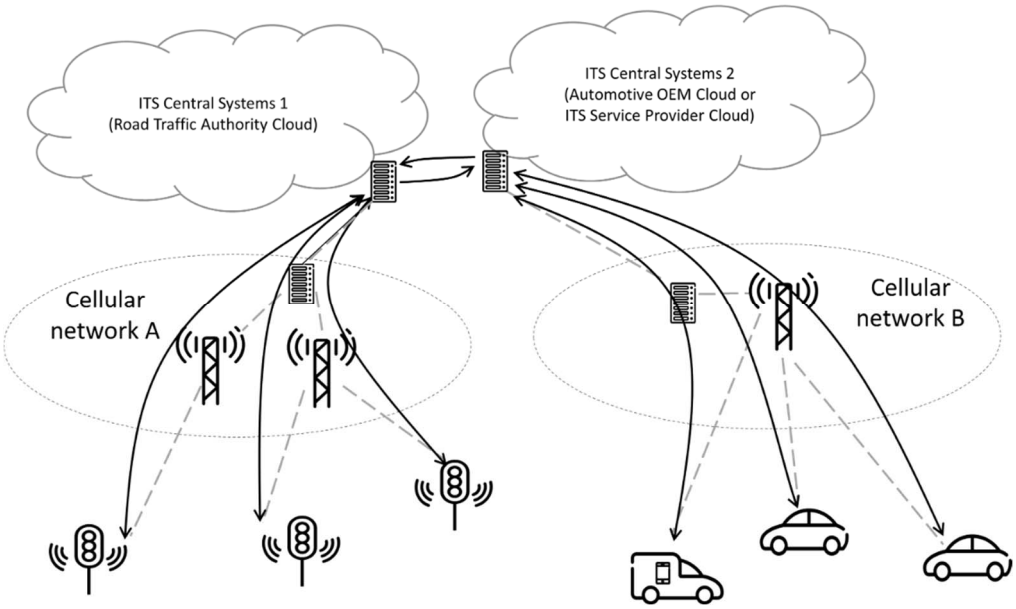


**Figure 4: Overview of V2I and I2V using wide-area cellular communications**

As shown in Figure 2 to Figure 4, mobile cellular networks support communications among vehicle, roadside, personal, and central ITS stations through the network infrastructure. The following ITS messages flows are supported by wide-area cellular communications:

- ITS messages are transmitted from ITS stations using the cellular UEs to ITS backends, where central ITS stations are located, through cellular Uu interface using uplink unicast communications and cellular core network.
- ITS messages are transmitted from the ITS backends to ITS stations using cellular UEs through cellular core network and the Uu interface using downlink unicast communications.
- ITS messages are transmitted from the ITS backends to ITS stations using cellular UEs through cellular core network and the Uu interface using downlink broadcast/multicast communications.

Combination of above ITS message flows enable communications among all ITS stations that use cellular UE and within the coverage of mobile networks.

The cellular Uu interface does not support local direct ad-hoc communications among ITS stations without involving the network infrastructure. Local direct ad-hoc communications are provided by short-range technologies, e.g. the LTE-V2X sidelink or ITS-G5. Compared with short-range communications, the cellular Uu interface offers longer communication distances.

Cellular networks support end-to-end IP-based communications, regardless of the generation of cellular communication technology and mobile communication service provider. An example of the End-to-End protocol stack for ITS applications over the 3GPP LTE network is shown in Figure 5.

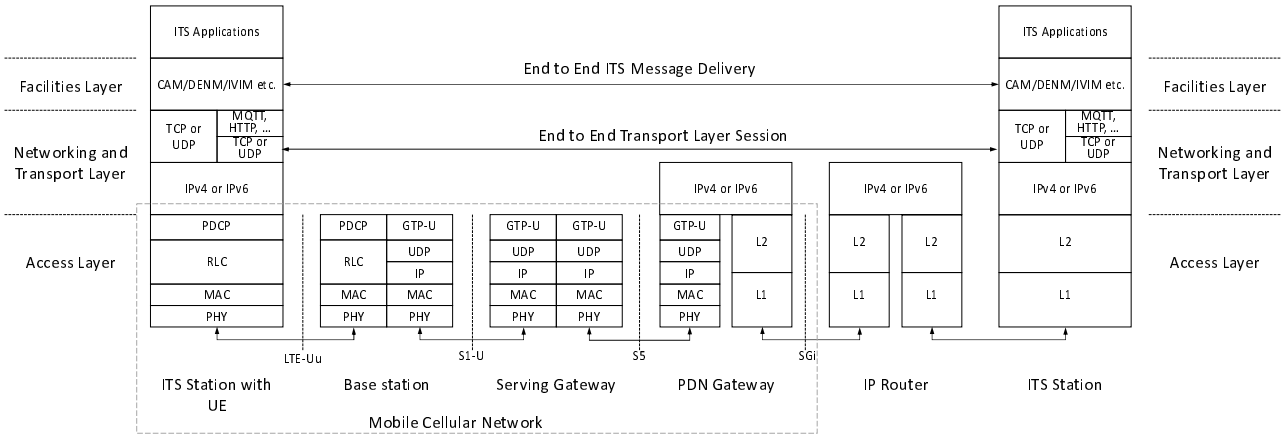


**Figure 5: Example end-to-end protocol stack of wide-area communications in ITS through the cellular Uu interface**

Observations about wide-area communications supporting ITS applications through mobile cellular networks include:

- Wide-area communications through cellular networks are based on IP protocol, either IPv4 or IPv6, at the network layer. Therefore, ITS security at the Facilities layer studied 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. the communication among ITS backend systems.

- The GeoNetworking protocol [i.17], which is designed for short-range ad-hoc communications, may be also needed in wide-area communications through cellular networks, in order to enable a fully transparent hybrid communication approach when both short-range and cellular wide area access layers are involved.

- ITS facilities layer messages can be supported by IP-based protocol stacks, e.g. TCP/IP, UDP/IP, MQTT/TCP/IP, AMQP/TCP/IP, etc., without using BTP/GeoNetworking at the Networking and Transport layer. However, the IP protocol can as well be combined with GeoNetworking, e.g. by encapsulating the GN packet (incl. payload) into an IP packet.

NOTE 2: The presence of the secured GeoNetworking header is a necessity to be able to communicate in a trusted domain with existing ITS stations (backwards compatibility) using the GeoNetworking protocol.

- ITS security entity could ensure end-to-end ITS message authentication and integrity at the facilities layer independently from the choice of lower Networking & Transport layer protocols and access technologies. However, end-to-end communication is provided by the Networking and Transport layer, therefore security can also be provided at this layer, e.g. as currently specified in the ITS station architecture. This is independent from access technologies.

- As Subscriber Identity Module (SIM) is mandatory for all UEs, access to network is always authenticated based on the SIM card for wide-area cellular communications. However, ETSI ITS message communications have additional authenticity requirements [i.23], which are not fulfilled by SIM-based solutions and still rely on ETSI ITS security solutions.

NOTE 3: The term SIM in the present document refers to the Subscriber Identity Module specified in 3GPP specifications, e.g. ETSI TS 151 011 [i.25], and its evolution used in 3G and 4G mobile networks, e.g. Universal Subscriber Identity Module (USIM) applications specified in ETSI TS 131 102 [i.26]. As for 5G communications, the 3GPP Release 15 specifications still use USIM. From the user authentication and security perspective, SIM and USIM are based on the same principles and both ensure authenticated network access and secured communication other the Uu interface.

## 4.2 ITS Application Use Cases Supported by Wide-area Cellular Communications and Security Requirements

ITS application use cases together with corresponding communication patterns and behaviour are analysed in [i.2]. Table 1 complements Table 2 in ETSI TS 102 940 [i.2] by considering wide-area communications among vehicles, roadsides, and ITS backends, which are identified as Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Infrastructure (I2I), respectively.

NOTE 1: In this context, "infrastructure" covers both the roadside infrastructure and ITS backends. So, in Table 1, I2V, V2I, I2I or V2I2V can also be interpreted as patterns implemented using cellular network infrastructure.

**Table 1: ITS applications communication behaviour**

| Use case | | Pattern | Remarks |
|---|---|---|---|
| Emergency vehicle warning | | V2V/V2I | CAM may be used |
| Slow vehicle indication | | V2V/V2I2V | CAM may be used |
| Across traffic turn collision risk warning | | V2V/V2I2V | CAM required |
| Merging Traffic Turn Collision Risk Warning | | V2V/I2V/V2I2V | CAM required |
| Co-operative merging assistance | | V2V/I2V/V2I2V | CAM required |
| Intersection collision warning | | V2V/I2V/V2I2V | CAM required |
| Co-operative forward collision warning | | V2V/V2I2V | CAM required |
| Lane Change Manoeuvre | | V2V/V2I2V | CAM required |
| Emergency electronic brake lights | | V2V/V2I2V | Low latency requirement |
| Wrong way driving warning (infrastructure based) | | I2V | |
| Stationary vehicle - accident | | V2V/V2I/V2I2V | |
| Stationary vehicle - vehicle problem | | V2V/V2I2V | |
| Traffic condition warning | | V2V/I2V/V2I2V | |
| Signal violation warning | | I2V | |
| Roadwork warning | | I2V | |
| Decentralized floating car data - Hazardous location | | V2V/I2V/V2I2V | |
| Decentralized floating car data - Precipitations | | V2V/I2V/V2I2V | |
| Decentralized floating car data - Road adhesion | | V2V/I2V/V2I2V | |
| Decentralized floating car data - Visibility | | V2V/I2V/V2I2V | |
| Decentralized floating car data - Wind | | V2V/I2V/V2I2V | |
| Vulnerable road user Warning | | V2V/I2V/V2I2V | |
| Pre-crash sensing warning | Indication | V2V/V2I2V | Low latency requirement |
| | Data exchange | V2V/V2I2V | Low latency requirement |
| Co-operative glare reduction | | V2V/I2V/V2I2V | |
| Regulatory/contextual speed limits notification | | I2V | |
| Curve Warning | | I2V | |
| Traffic light optimal speed advisory | | I2V | Some Implementation of Traffic Light Control use CAM |
| Traffic information and recommended itinerary | Advertisement | I2V | |
| | Service | I2V | |
| Public transport information | Advertisement | I2V | |
| | Service | I2V | |
| In-vehicle signage | | I2V | May require message non-repudiation |
| Point of Interest notification | Advertisement | I2V | |
| | Service | I2V | |

| Use case | | Pattern | Remarks |
|---|---|---|---|
| Automatic access control and parking management | Advertisement | I2V | |
| | Service | I2V/V2I | |
| ITS local electronic commerce | | I2V/V2I | |
| Media downloading | | I2V/V2I | |
| Insurance and financial services | | I2V/V2I | |
| Fleet management | | I2V/V2I | |
| Loading zone management | | I2V/V2I | |
| Theft related services/After theft vehicle recovery | | I2V/V2I | |
| Vehicle software/data provisioning and update | | I2V/V2I | |
| Vehicle and RSU data calibration | | I2V/V2I/I2I | |
| Traffic light priority request | | V2I | For certain fleets, there might be privacy protection requirements dependent of vehicle category |

The analysis of security requirements of ITS applications in clause 4.3 of ETSI TS 102 940 [i.2], which cover all use cases in Table 1 of the present document, is still valid for wide-area cellular communications but needs to be extended for the requirement of message signature on top of (TLS) session security. There are ITS applications that require message non-repudiation, e.g. IVS of regulatory road signs require each IVIM to be individually signed by the road authority. In certain use cases such as traffic light priority, request message signatures will be used in order to allow receivers of ITS messages to validate authenticity of the ITS message and the SSP authorization.

NOTE 2: ITS applications in Table 1 are examples that can be supported by current 3G/4G cellular mobile networks. With the deployment of 5G mobile networks, which provide enhanced latency, reliability and throughput capacities, further ITS and automotive applications are expected to be supported by cellular wide-area communications.

## 4.3 Related ETSI ITS Standards

ETSI ITS standards ETSI TS 102 940 [i.2], ETSI TS 103 097 [i.4], and ETSI TS 102 941 [i.3] specify the ETSI ITS security entity and corresponding operations realizing the PKI-based ITS security system according to the European Certificate Policy [i.10].

However, to enable ITS security at the facilities layer independently from BTP/GeoNetworking protocols, further evaluation of ETSI ITS standards at the Facilities layer, the Security entity, and the interfaces between them are needed. Clause 5 analyses the gaps in current ETSI ITS standards and identify the needed standardization activities to enable ITS security at the Facilities layer for ITS applications using wide-area cellular communications.

## 4.4 Solutions for secure ITS communications using wide-area cellular communications

### 4.4.1 ITS security at GeoNetworking layer

In this solution, ITS security operations of Protocol Data Units (PDU), e.g. message signing and message verification, are performed at the GeoNetworking layer. Figure 6 shows the protocol stack when the secured GeoNetworking PDU is transmitted using the cellular Uu interface.

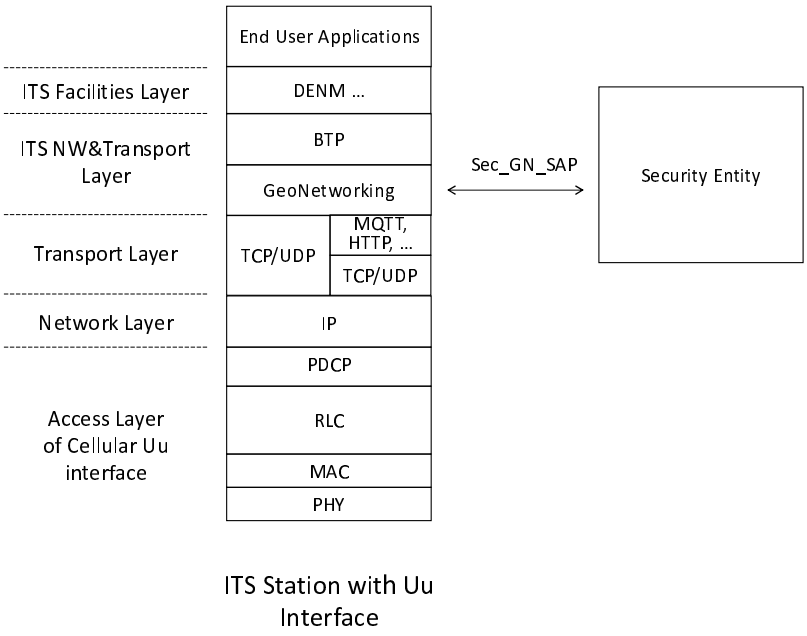


**Figure 6: Example protocol stack for ITS message delivery via the Uu interface using ITS security at the GeoNetworking layer**

This solution follows the architecture specified in ETSI EN 302 636-4-1 [i.17], as shown in Figure 7, where Sec_GN_SAP is the logical interface for the GeoNetworking layer to access security services provided by the security entity.

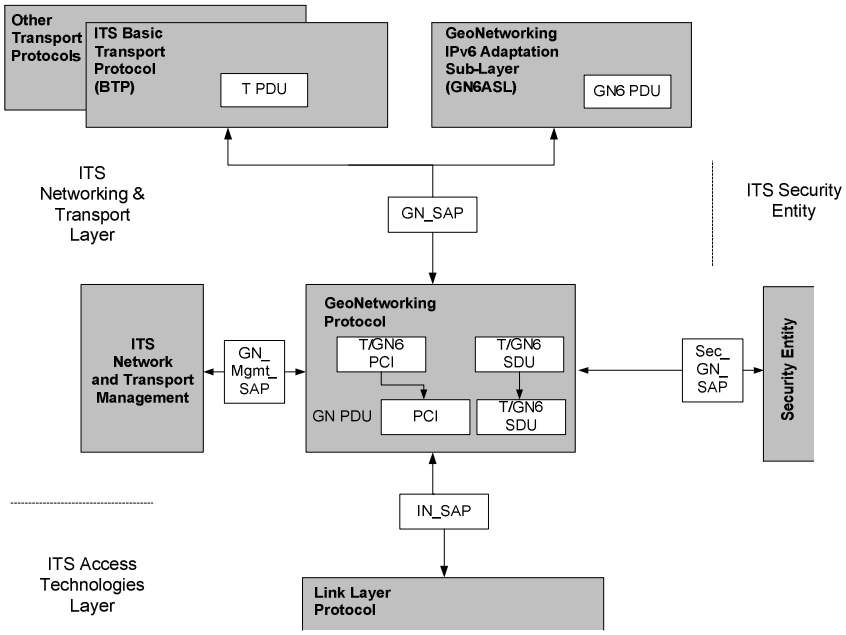


**Figure 7: Service primitives, SDUs and PDUs relevant for the GeoNetworking protocol [i.17]**

In this solution, BTP and GeoNetworking layers are encapsulated in IP based protocol stacks, e.g. TCP/IP, UDP/IP, MQTT/TCP/IP, AMQP/TCP/IP, or HTTP/TCP/IP when using the wide-area Uu interface. The receiver can in turn decapsulate the GeoNetworking message from the IP packet and obtain the same packet with the same security header as if the message would have been transmitted over a short-range communication link. This way, messages can be received and forwarded in the same way independent of the access layer without prior translation or modification. Figure 8 illustrates an example of scenario and protocol stacks for forwarding a DEN message with ITS security at the GeoNetworking layer from the wide-area channel to the short-range channel. The approach in Figure 7 has been implemented in SCOOP@F, C-ROADS France and InterCor projects [i.24].

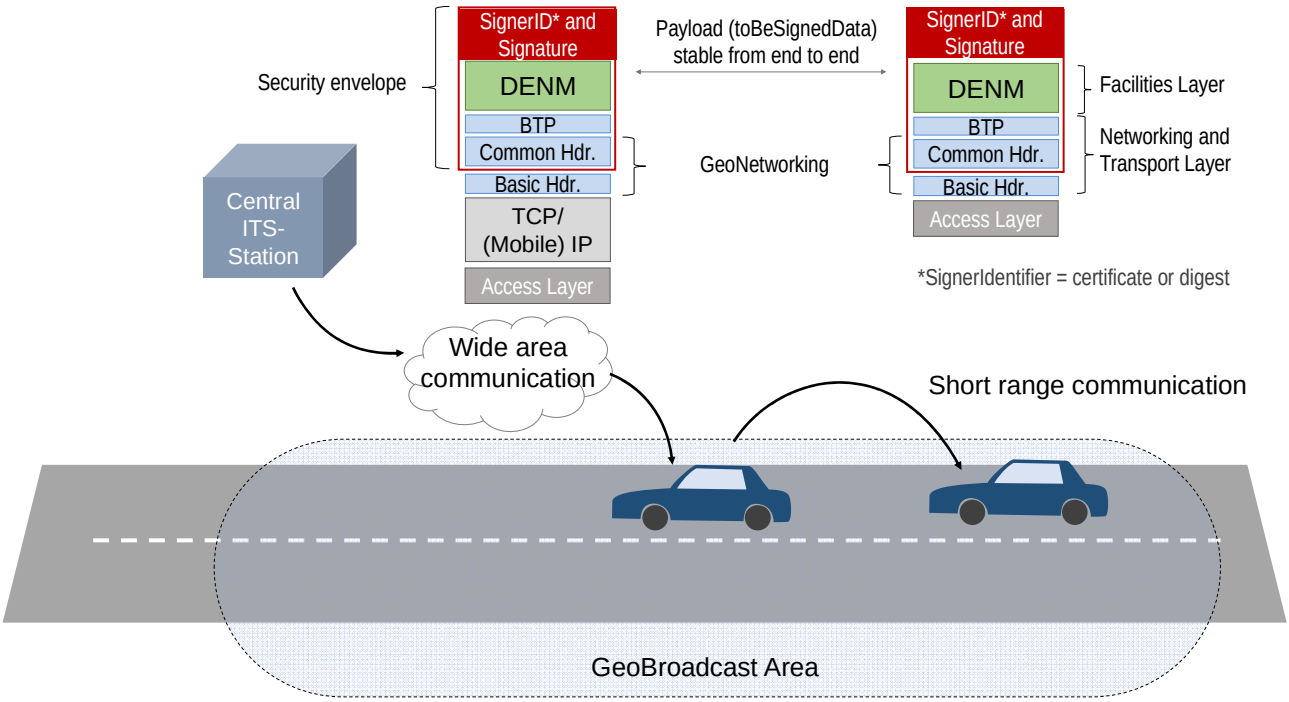


**Figure 8: I2V2V using multi-hop forwarding using cellular and short-range access layers**

NOTE: Additional transport layer and network layer security mechanisms, e.g. TLS, DTLS, and IPSec can be applied in this solution. This solution has been implemented with wide-area communications and tested in many pilot and field trial projects, e.g. the CONVERGE project [i.16], where a hybrid communication solution consisting of both short-range ITS-G5 and cellular Uu interfaces has been developed. More details about the security solution implemented in the CONVERGE project can be found in Annex A.

### 4.4.2 ITS security at Facilities layer

The logical interface Security Facilities Service Access Point (SF-SAP) defined in the DEN service specification [i.7] provides another way for securing ITS communications when using wide-area communications. As the SF-SAP interface provide access to ITS security services, Facilities layer ITS messages can be signed and verified at the Facilities layer without relying on underlying ITS networking and transport layers, e.g. BTP and GeoNetworking.

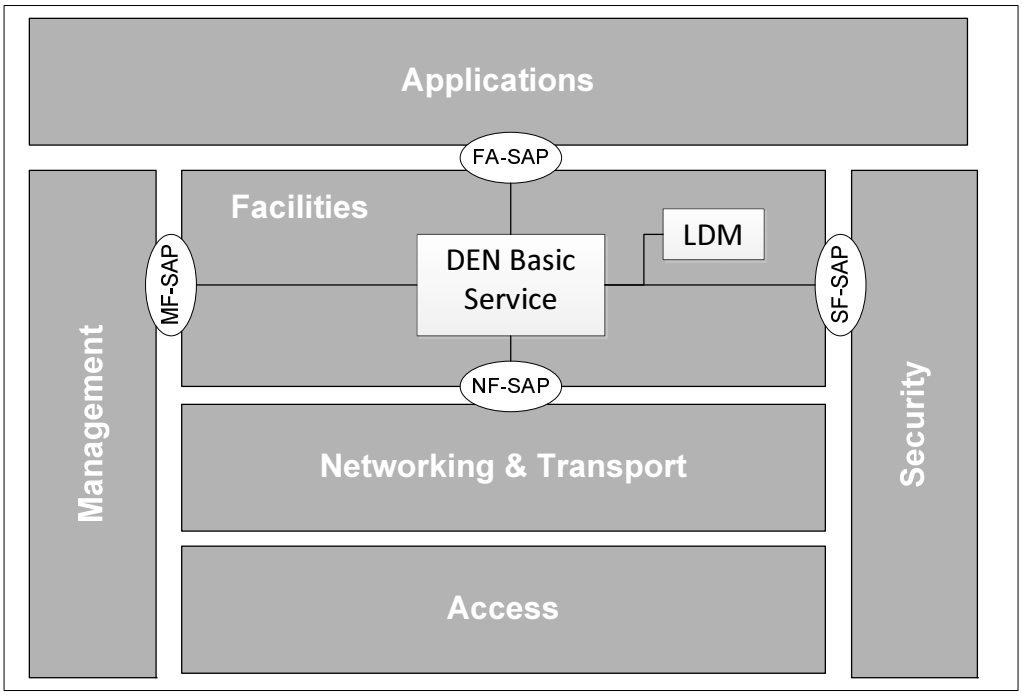


**Figure 9: DEN basic service and logical interfaces [i.7]**

As a result, the protocol stack, as shown in Figure 10, can be used at ITS stations, where secured ITS facilities layer messages are transmitted directly over the IP based protocol stacks, e.g. TCP/IP, UDP/IP, MQTT/TCP/IP, HTTP/TCP/IP, etc.

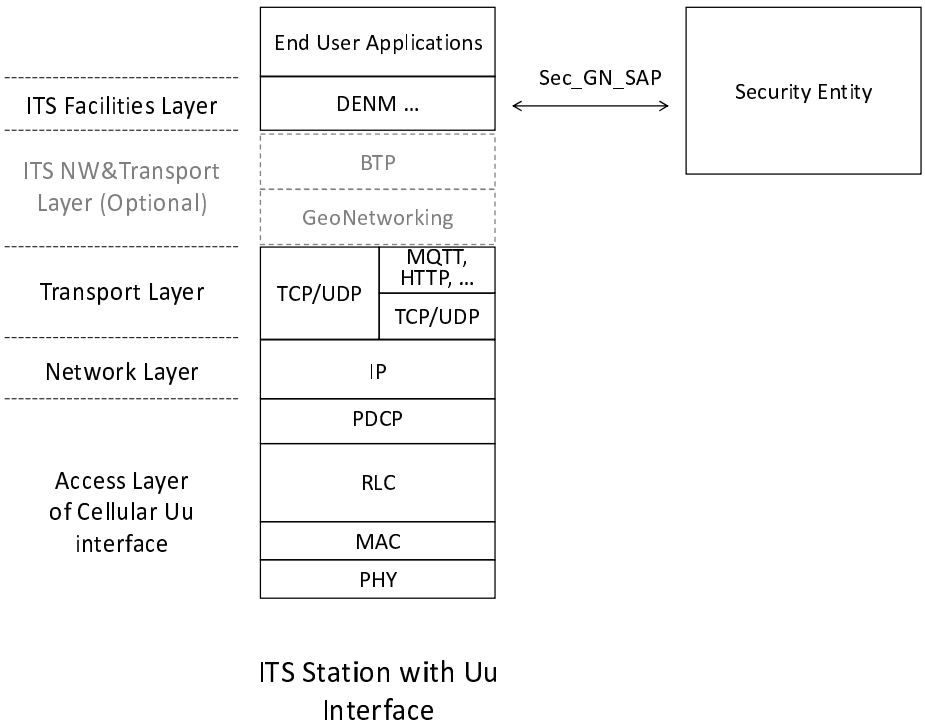


**Figure 10: Example protocol stack for ITS message delivery via the Uu interface using ITS security at the Facilities layer**

In addition to the SF-SAP interface that needs to be specified, other ETSI ITS facilities layer and security standards also need to be updated to enable this solution, as discussed in clause 5.

NOTE: Additional transport layer and network layer security mechanisms, e.g. TLS, DTLS, and IPSec, may be applied in this solution.

The secured message structures are shown in Figure 11 for the ITS security solutions at the GeoNetworking layer and at the Facilities layer respectively, considering the scenario in Figure 8. In the former solution, as detailed in clause 4.4.1, the ITS security envelope covers the GeoNetworking common head, BTP, and the Facilities layer message. In this case, BTP and GeoNetworking protocols are mandatory. In the latter solution, i.e. ITS security solution at the Facilities layer, only the Facilities layer message is included in the ITS security envelope. In this solution, BTP and GeoNetworking protocols are optional for the transport and networking layers. In both cases, TCP/IP could be substituted by other protocols e.g. UDP/IP, MQTT/TCP/IP, AMQP/TCP/IP, or HTTP/TCP/IP. Depending on the protocol used, the port number at the transport layer can be used to differentiate between the secured and unsecured Facilities layer messages, as analysed in clause 5.2.1.

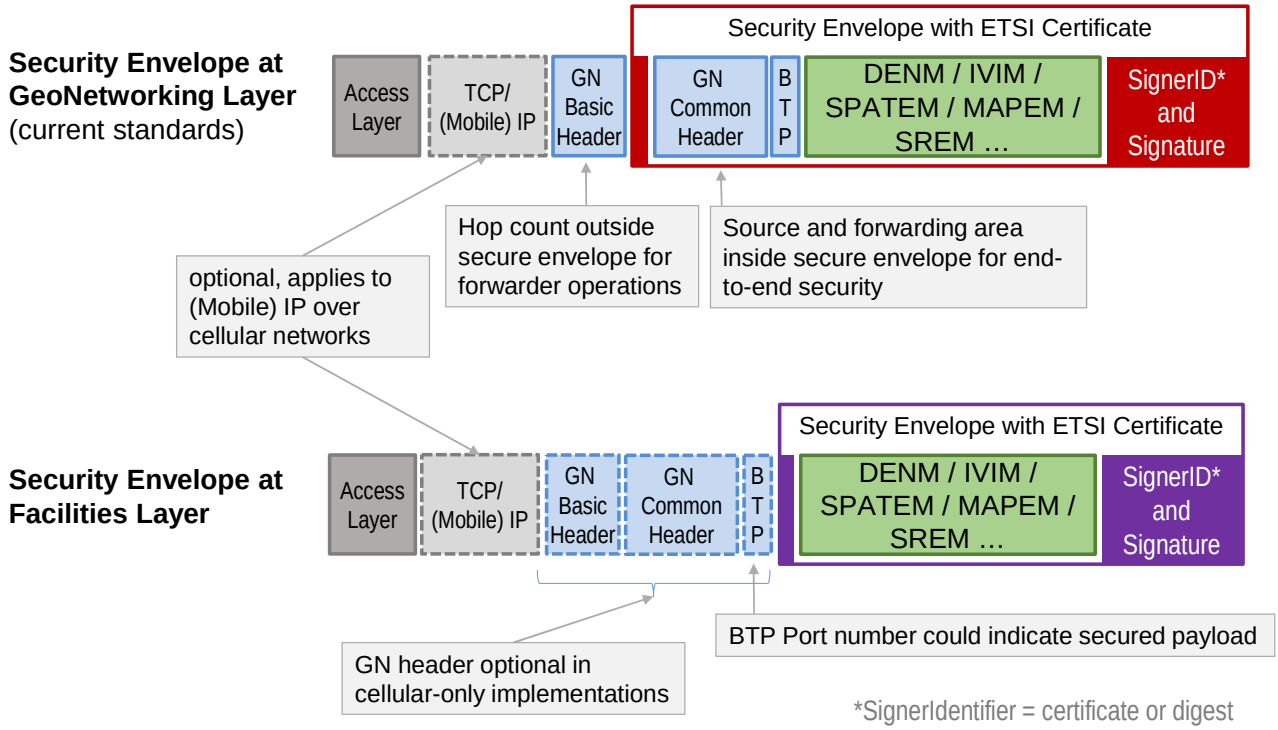


**Figure 11: Secured message structure for ITS security at the GeoNetworking layer and at the Facilities layer**

Clause 5 of the present document analyses the existing ETSI ITS standards and identify further standardization activities to enable ITS security at the Facilities layer.

Characteristics of ITS security solutions at the GeoNetworking layer and at the Facilities layer are summarized in Annex B.

### 4.4.3 Transport layer security for IP based ITS communications

For ITS communications based on IP-protocol stacks over cellular Uu interface, the ETSI TS 102 941 [i.3] and ETSI TS 102 943 [i.19] standards specify solutions for establishing Security Associations in unicast, multicast/broadcast communication modes. As specified in ETSI TS 102 941 [i.3], different security protocols can be used, e.g. IPsec, TLS.

As shown in Figure 12, Facilities layer messages can be sent after establishing a secure association using TLS or DTLS to ensure the authenticity and confidentiality of messages and then secured messages are transmitted over the IP based protocol stacks, e.g. TCP/IP or UDP/IP. This provides a potential solution for securing ITS communications when using the wide-area cellular Uu interface. However, it should be noted that TLS secure session does not provide E2E authentication of the exchanged messages when there is a chain of successive communication links from the ITS-S to the cloud or service provider server.

ISO/DTS 21177 [i.18] also specifies secure session establishment and authentication to exchange information in a secure and trusted way between ITS-S applications (see clause 4.4.4).

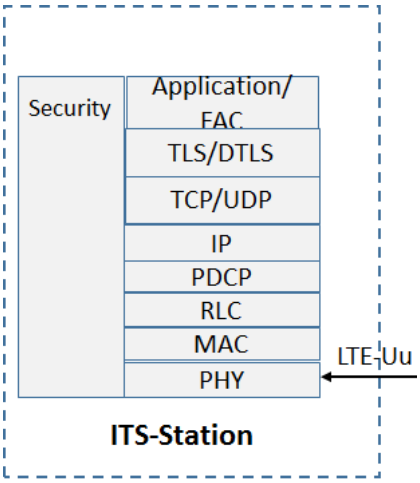


**Figure 12: ITS station with cellular Uu interface (TLS secure connection)**

### 4.4.4 ISO/DTS 21177 ITS-station security services for secure session establishment and authentication between trusted devices

For ITS applications and automotive services that require secure communication session, ISO/DTS 21177 [i.18] specifies a set of ITS security services for authentication and secure session establishment.

An example protocol stack using ISO/DTS 21177 [i.18] security service is shown in Figure 13. The security subsystem uses inputs from the Access Control Policy block and applies security mechanisms to determine the permission of the peer. It also applies appropriate security processing for outgoing communication from the application, e.g. signing ITS facilities layer messages. For incoming communications, the security subsystem receives input commands and data from the Security Adaptor Layer and applies the appropriate access control policy, e.g. verify the signature of the received data messages. Moreover, the security subsystem defined in ISO/DTS 21177 [i.18] can communicate with the peer instance of security subsystem using session control commands, which also go through the Security Adaptor Layer.

ISO/DTS 21177 [i.18] Security Adaptor Layer serves as a multiplexer/demultiplexer allowing both data, which are communicated between the Applications, and session control commands, which are communicated between peer instances of Security Subsystem or Security Adaptor Layer, to be exchanged over the same secure session. Security Session provides confidentiality, integrity, authentication, guaranteed in-order delivery, and replay protection on the datagrams that are passed over it.

NOTE: As currently specified in ISO/DTS 21177 [i.18], the only supported secure session mechanism is TLS 1.3 specified in [i.20] amended with [i.21] to enable the use of certificates specified in IEEE 1609.2 [i.9] with the amendment IEEE Std. 1609.2b [i.22].

Besides, the Security Subsystem can also configure the Security Adaptor Layer and the Secure Session.

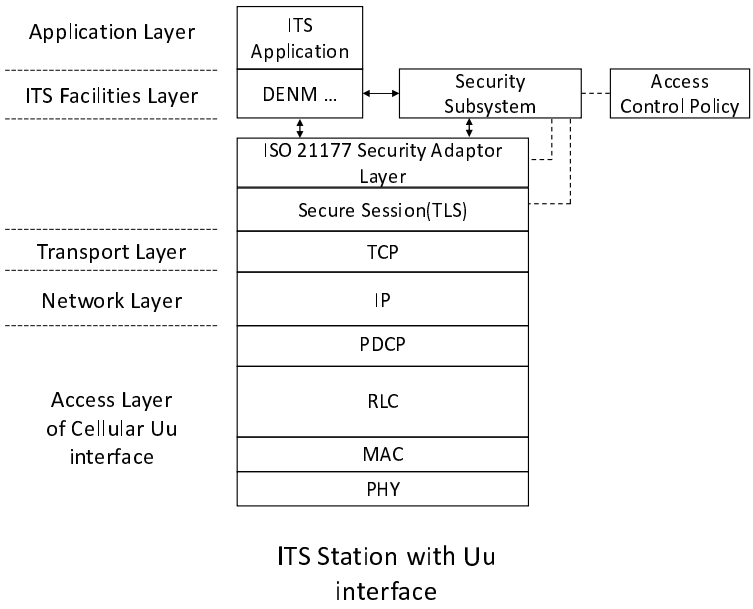


**Figure 13: Example protocol stack of ITS communication over security session established**

# 5 Gap analysis of ETSI ITS standards to enable ITS security at the facilities layer

## 5.1 Security Entity

### 5.1.1 ETSI TS 102 940 ITS communication security architecture and security management

#### 5.1.1.1 Scope of the standard

ETSI TS 102 940 [i.2] specifies a security architecture for ITS communications. Based on the security services defined in ETSI TS 102 731 [i.8], it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [i.1].

ETSI TS 102 940 [i.2] also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces, as well as basic policies and guidelines for trust establishment.

#### 5.1.1.2 Identified gaps and proposed standardization activities

##### 5.1.1.2.1 Missing wide-area communications in ITS applications communication characteristics description

**Gap:** ITS communications should cover both short-range local ad-hoc communication and wide-area cellular infrastructure-based communications. However, the ITS applications communication behaviour and corresponding characteristics description of ITS applications specified in clause 4.2 of ETSI TS 102 940 [i.2] consider only single- or multi-hop short-range communications among vehicles (V2V) or between vehicle and roadside infrastructure (V2I/I2V).

**Proposal:** It is proposed to consider wide-area communications based on IP protocol stacks between vehicles and network, e.g. V2I/I2V using the cellular Uu interface, in clause 4.2 of ETSI TS 102 940 [i.2], and to consider whether this extends the group of distributed (networked) services, which should be revised in the next update of ETSI TS 102 940 [i.2]. However, these proposed changes do not necessarily impact the security requirements specified in ETSI TS 102 940 [i.2].

**Consideration on backward compatibility:** The proposed changes add V2N/N2V wide-area communications in the ITS applications communication behaviour and security requirements without affecting the specifications related to short-range V2V and V2I/I2V communications.

#### 5.1.1.2.2 Placement of security services "Authorize Single Message" and "Validate Authorization on Single Message" at the facilities layer

**Gap:** Security services "Authorize Single Message" and "Validate Authorization on Single Message" secure the sending or receiving of a single message (like a CAM or DENM) [i.2]. However, these security services are missing in the Facilities layer in Figure 5 "the placement of security services within the ITS station architecture" of ETSI TS 102 940 [i.2].

**Proposal:** It is proposed to add security services "Authorize Single Message" and "Validate Authorization on Single Message" in the Facilities layer of Figure 5 of ETSI TS 102 940 [i.2].

**Consideration on backward compatibility:** ETSI TS 102 940 [i.2] supports one security service and operates in multiple ITS architectural layers. For example, in Figure 5 of [i.2] security service "Manage Security Association" is placed in both Facilities and Networking&Transport layers. From the standardization point of view, adding "Authorize Single Message" and "Validate Authorization on Single Message" services at the Facilities layer does not intervene with similar services, e.g. "Authorize Message", "Sign Message", "Validate message authorization", and "Validate message integrity" at the Networking&Transport layer, as they are performed at different ITS architectural layers. From the deployment point of view, implementing the same security services at different ITS architectural layers at the same ITS station introduces redundancy, low efficiency, and potentially increased processing delay of ITS messages. It needs to be addressed in system architecture or profile specifying the settings and configurations of ITS standards to avoid duplicated ITS security services at multiple layers. The system architecture or profile should also ensure that implementation of ITS stations according to the new version of ITS standards, which are capable of "Authorize Single Message" and "Validate Authorization on Single Message" at the Facilities layer", can also perform secured ITS message communication with ITS stations implemented according to the old version of ITS standards, where the message signing and validating services are implemented only at the Networking&Transport layer.

#### 5.1.1.2.3 The role of central ITS station in ITS security function model

**Gap:** The role of central ITS station is missing in the ITS security function model specified in clause 5.3 of [i.2].

**Proposal:** It is proposed to add central ITS station in the ITS security function model in clause 5.3 of [i.2].

**Consideration on backward compatibility:** The amendment of central ITS station that communicates with other ITS stations using wide-area communications in the security function model does not affect the existing security function model.

#### 5.1.1.2.4 Pseudonym identity management for ITS stations using wide-area cellular communication

In wide-area cellular ITS implementations there is an important role for central ITS stations. In principle a central ITS station is an [Itss_NoPrivacy] [i.2] just like a typical Roadside ITS station. There may be exceptions depending of the role of a central ITS station in its implementation.

A central ITS station may be the originator of an ITS message (ITS station that generates ITS Application Data Unit) or it may relay an ITS message originating from another ITS station (vehicle, personal, roadside, central ITS station) that it is connected to by wide-area cellular communications. In the second case when the central ITS station is to relay a message of another ITS station, the other ITS station is the originator signing it with its own authorization ticket (certificate).

In the first case the central ITS station is the originator of the ITS message and will sign the message with its authorization ticket (certificate). When a central ITS station generates ITS messages, which are usually generated by individual vehicle ITS stations as [Itss_WithPrivacy], this central ITS station can be an [Itss_WithPrivacy], depending on the content and context of the message. This scenario applies when central ITS station acts as an ITS-S gateway to non-ITS systems, as defined in clause 4.5.2.3 of ETSI EN 302 665 [i.1].

**Gap:** Mechanisms as ID-change and ID-lock as defined in ETSI TS 102 723-8 [i.27] should be applicable on the facility layer to central ITS stations.

**Proposal:** ID-change and ID-lock will need to be specified. See also clause 5.3.

**Consideration on backward compatibility:**

1) The proposed change has no impact on the existing requirements for [Itss_WithPrivacy] and [Itss_NoPrivacy] in ETSI TS 102 941 [i.3].

For wide-area connected roadside units the case is simpler as privacy of these devices is not an issue.

#### 5.1.1.2.5 Communication between vehicle ITS station and central ITS station in PKI architecture illustration

**Gap:** Central ITS stations are missing in the PKI architecture illustration, i.e. Figure 6 of ETSI TS 102 940 [i.2]. In order to be applicable to C-ITS, which consist of different types of ITS stations including central ITS stations, [i.2] should not preclude the central ITS station in the PKI architecture.

**Proposal:** To add central ITS station in the PKI architecture illustration, i.e. Figure 6 of [i.2].

NOTE: ETSI TS 102 940 [i.2] is based upon the security services defined in ETSI TS 102 731 [i.8], which specifies mechanisms at the stage 2 level for secure and privacy-preserving communication in ITS environments. As ETSI TS 102 731 [i.8] specifies security services implementing the countermeasures identified by the ETSI TR 102 893 [i.23] for security threats of 5,9 GHz radio communications in ITS, the Threat, Vulnerability and Risk Analysis (TVRA) in ETSI TR 102 893 [i.23] needs to be first updated taking into account central ITS stations that may not use 5,9 GHz communications, before [i.3] adding central ITS station in the PKI architecture illustration, i.e. Figure 11 of [i.2].

**Consideration on backward compatibility:** The amendment of central ITS station in Figure 6 of [i.2] complements the illustration of the PKI architecture without affecting the existing PKI architecture and operations, as central ITS station is another type of ITS station to be enrolled into the PKI similar to vehicle or roadside ITS stations.

## 5.1.2 ETSI TS 102 941 Trust and Privacy Management

### 5.1.2.1 Scope of the standard

ETSI TS 102 941 [i.3] specifies the trust and privacy management for ITS communications. Based on the security services defined in ETSI TS 102 731 [i.8] and the security architecture defined in ETSI TS 102 940 [i.2], it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [i.1].

ETSI TS 102 941 [i.3] identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in ITS. Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS.

### 5.1.2.2 Identified gaps and proposed standardization activities

#### 5.1.2.2.1 ITS-S is limited to "Single-hop and relayed broadcast message"

**Gap:** Table 1 of ETSI TS 102 941 [i.3] the description of "Sending ITS-S", "Relaying ITS-S", and "Receiving ITS-S" only cover "Single-hop and relayed broadcast message". However, ITS-S should also be able to send and receive unicast message using wide-area communications, e.g. the ITS message sent by central ITS station to roadside ITS station.

**Proposal:** To remove "single-hop" and "broadcast" in the description of "Sending ITS-S", "Relaying ITS-S", and "Receiving ITS-S" in Table 1 of ETSI TS 102 941 [i.3].

**Consideration on backward compatibility:** The proposed modifications generalize the description of "Sending ITS-S", "Relaying ITS-S", and "Receiving ITS-S" and also cover the case of "single-hop and relayed broadcast message" in the original description.

### 5.1.3 ETSI TS 103 097 Security header and certificate formats

#### 5.1.3.1 Scope of the standard

ETSI TS 103 097 [i.4] specifies the secure data structure including header and certificate formats for ITS. ETSI TS 103 097 [i.4] provides these definitions as a profile of the base standard IEEE 1609.2 [i.9] and its amendment IEEE 1609.2a [i.9].

#### 5.1.3.2 Identified gaps and proposed standardization activities

The secure data structure and security profile for ITS messages are communication layer agnostic and can be applied to ITS Facilities layer messages. Therefore, no gap is identified in ETSI TS 103 097 [i.4].

## 5.2 Facilities Layer Standards

### 5.2.1 ETSI EN 302 637-3 Specifications of Decentralized Environmental Notification Basic Service

#### 5.2.1.1 Scope of the standard

ETSI EN 302 637-3 [i.7] provides specification of the DEN basic service, which is in support of the RHW application. It specifies the syntax and semantics of the "Decentralized Environmental Notification Message" (DENM) and the DENM protocol handling. The DEN basic service may be implemented in a vehicle ITS-S, a roadside ITS-S, a personal ITS-S, or a central ITS-S.

#### 5.2.1.2 Identified gaps and proposed standardization activities

##### 5.2.1.2.1 Interface to the ITS security entity

**Gap:** Interface between ITS security entity and DEN basic service is not specified. Instead DEN basic service relies on BTP/GeoNetworking protocols at the Networking & Transport layer for security operation.

**Proposal:** To specify interface between ITS security entity and DEN basic service for ITS security operation, e.g. signing DENM and validating signed DENM, at the Facilities layer.

NOTE 1: The existing interface between the GeoNetworking layer and security entity stays untouched.

NOTE 2: The interface between DEN basic service and ITS security entity is already illustrated in Figure 2 and Figure 3 of ETSI EN 302 637-3 [i.7] but not referenced to the correct SF-SAP specification. See clause 5.3 of the present document.

NOTE 3: The interface may be implemented by calling the proposed Secure Facilities layer PDU service, as analysed in clause 5.2.1.2.2. That means the facilities layer PDU is the payload component of the signedData structure defined in clause 5.2 of ETSI TS 103 097 [i.4].

**Consideration on backward compatibility:** The proposed change complements the existing specification of ETSI EN 302 637-3 [i.7] without affecting the architecture and interfaces defined in the existing standard. The proposed change introduces an additional way of implementing ITS security at the Facilities layer, which is different from the message structure following the ITS security implementation at the GeoNetworking layer. As a result, existing ITS station implementation following ITS security at the GeoNetworking layer cannot decode or authenticate a received message that follows the ITS security implementation at the Facilities layer.

#### 5.2.1.2.2 No specification of secured message format and security operation for DENM at the Facilities layer

**Gap:** Message format of secured DENM at the Facilities layer and the protocol operations of signing DENM and validating signed DENM are not specified in ETSI EN 302 637-3 [i.7].

**Proposal:** To specify secured ITS message format at the Facilities layer, and to specify security operations, e.g. signing DENM and validating signed DENM, at the Facilities layer.

NOTE 1: The existing ITS PDU header as well as DEN message format specified in ETSI EN 302 637-3 [i.7] stays unchanged.

**Consideration on backward compatibility:** Introducing security operation at the Facilities layer in a new revision of DENM standard will prevent the DEN basic service implementation, which follows the current version of the standard, from decoding the received secured DENM at the Facilities layer, because such a secured DENM may have a message structure different from the traditional DENM without ITS security at the Facilities layer. Current implementations following ETSI EN 302 637-3 V1.3.1 [i.7] without Facilities layer security will not be able to process secured DEN message at the Facilities layer. For future implementations to handle DEN message both with and without ITS security at the Facilities layer, the following approach is suggested.

A new ITS Facilities layer service for secure Facilities layer PDU, i.e. Secure Facilities layer PDU service, is defined:

- The process of transmitting secured DEN should be identical to the existing DEN service without ITS security at the Facilities layer, except that the DEN message is passed to the Secured Facilities layer PDU service, which calls the security services via the SF-SAP interface to sign the Facilities layer DEN PDU including the ITS PDU Header and the DEN payload before passing it to the transport layer.

- Upon reception of a secure Facilities layer message from the transport layer, the Secure Facilities layer PDU service first verifies the message by calling the ITS security service via the SF-SAP interface. The DEN message is passed to the Facilities layer DEN service, only when its signature is verified, and the security envelope is removed by the Secure Facilities layer PDU service.

Figure 14 shows the proposed transmission flow of the secure DEN message at the Facilities layer.

NOTE 2: Implementations that do not have a secured Facilities layer PDU service cannot transmit or receive such secured messages at the Facilities layer.

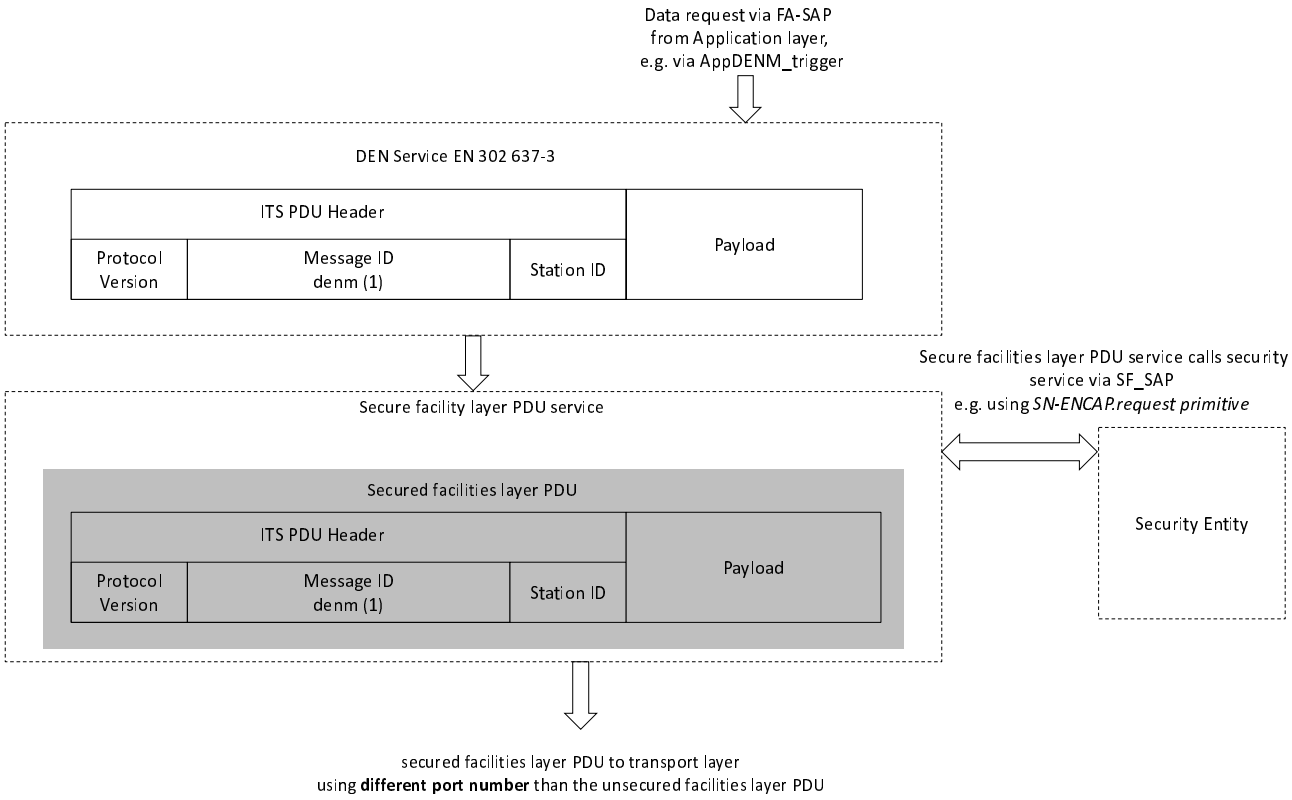


**Figure 14: Transmission flow of the secure DEN message at the Facilities layer**

In order to differentiate secure and unsecure facilities layer messages, the secure facilities layer message can be assigned with a new transport layer port, different from all other facilities layer messages without ITS security at the facilities layer.

This approach does not impact the existing specification of DEN service for DEN message without ITS security at the Facilities layer. It complements the DEN standard with the capability of handling DEN messages with ITS security at the Facilities layer. It signs and/or encrypts the entire Facilities layer PDU including the ITS PDU Header.

NOTE 3: If BTP is used as the transport layer protocol, the "destination port info" field of BTP-B header format may be considered for differentiating secured and unsecured Facilities layer message.

## 5.2.2 ETSI TS 103 301 Facilities layer protocols and communication requirements for infrastructure services

### 5.2.2.1 Scope of the standard

ETSI TS 103 301 [i.5] provides specifications of infrastructure related ITS services to support communication between infrastructure ITS equipment and traffic participants using ITS equipment (e.g. vehicles, pedestrians). It defines services in the Facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity.

### 5.2.2.2 Identified gaps and proposed standardization activities

#### 5.2.2.2.1 Interface to the ITS security entity

**Gap:** Interface between ITS security entity and infrastructure-based services is not specified in clause 4.4.3 of ETSI TS 103 301 [i.5].

**Proposal:** To specify interface between ITS security entity and infrastructure-based services for ITS security operation, e.g. signing and validating signed IVIM, at the Facilities layer.

NOTE 1: The existing interface between the GeoNetworking layer and security entity stays untouched.

NOTE 2: The interface between Infrastructure services and ITS security entity is already illustrated in Figure 1 of ETSI TS 103 301 [i.5] but not referenced to the correct SF-SAP specification. See clause 5.3 of the present document.

NOTE 3: The interface may be implemented by calling the proposed Secure Facilities layer PDU service, as analysed in clause 5.2.1.2.2. That means the Facilities layer PDU is the payload component of the signedData structure defined in clause 5.2 of ETSI TS 103 097 [i.4].

**Consideration on backward compatibility:** The proposed change complements the existing specification of ETSI TS 103 301 [i.5] without affecting the architecture and interfaces defined in the existing standard. The proposed change introduces additional way of implementing ITS security at the Facilities layer, which is different from the message structure following the ITS security implementation at the GeoNetworking layer. As a result, existing ITS station implementation following ITS security at the GeoNetworking layer cannot decode or authenticate a received message that follows the ITS security implementation at the Facilities layer.

#### 5.2.2.2.2 No specification of secured message format and security operation for infrastructure-based services at the Facilities layer

**Gap:** Format of secured messages for Infrastructure-based services at the Facilities layer and the protocol operations of signing and validating secured messages for Infrastructure-based services are not specified in ETSI TS 103 301 [i.5].

**Proposal:** To specify secured ITS message format at the Facilities layer, and to specify security related protocol operations, e.g. signing and validating signed messages for Infrastructure-based services.

**Consideration on backward compatibility:** Introducing security operation at the Facilities layers in a new revision of ETSI TS 103 301 [i.5] standard will prevent the implementation, which follows the current version of the standard, from decoding the received secured messages for Infrastructure-based services at the Facilities layer, because secured message may have a structure different from the traditional message without ITS security at the Facilities layer. In order to avoid this incompatibility, the approach discussed in clause 5.2.1.2.2 should be followed when specifying Facilities layer services with ITS security.

NOTE: Implementations that do not have a Secured Facilities layer PDU service cannot transmit or receive such secured messages at the Facilities layer.

### 5.2.3 ETSI EN 302 637-2 Specification of Cooperative Awareness Basic Service

#### 5.2.3.1 Scope of the standard

ETSI EN 302 637-2 [i.6] provides the specifications of the Cooperative Awareness basic service (CA basic service), which is in support of the BSA road safety application. This includes definition of the syntax and semantics of the Cooperative Awareness Message (CAM) and detailed specifications on the message handling.

#### 5.2.3.2 Identified gaps and proposed standardization activities

##### 5.2.3.2.1 Interface to the ITS security entity

**Gap:** Interface between ITS security entity and CA basic service is not specified. Instead CA basic service relies on BTP/GeoNetworking protocols at the Networking & Transport layer for security operation.

**Proposal:** To specify interface between ITS security entity and CA basic service for ITS security operation, e.g. signing CAM and validating signed CAM, at the Facilities layer.

NOTE 1: The existing interface between the GeoNetworking layer and security entity stays untouched.

NOTE 2: The interface between CA basic service and ITS security entity is already illustrated in Figure 1 and Figure 2 of ETSI EN 302 637-2 [i.6] but not referenced to the correct SF-SAP specification. See clause 5.3 of the present document.

NOTE 3: The interface may be implemented by calling the proposed Secure Facilities layer PDU service, as analysed in clause 5.2.1.2.2. That means the Facilities layer PDU is the payload component of the signedData structure defined in clause 5.2 of ETSI TS 103 097 [i.4].

**Consideration on backward compatibility:** The proposed change complements the existing specification of ETSI EN 302 637-2 [i.6] without affecting the architecture and interfaces defined in the existing standard. The proposed change introduces additional way of implementing ITS security at the Facilities layer, which is different from the message structure following the ITS security implementation at the GeoNetworking layer. As a result, existing ITS station implementation following ITS security at the GeoNetworking layer cannot decode or authenticate a received message that follows the ITS security implementation at the Facilities layer.

#### 5.2.3.2.2 No specification of security message format and security operation for CAM at the Facilities layer

**Gap:** Message format of secured CAM at the Facilities layer and the protocol operations of signing CAM and validating signed CAM are not specified in ETSI EN 302 637-2 [i.6].

**Proposal:** To specify secured ITS message format at the Facilities layer and to specify security operations, e.g. signing CAM and validating signed CAM, at the Facilities layer.

**Consideration on backward compatibility:** Introducing security operation at the Facilities layers in a new revision of ETSI EN 302 637-2 [i.6] standard will prevent the implementation, which follows the current version of the standard, from decoding the received secured messages for CA services at the Facilities layer, because secured message may have a structure different from the traditional message without ITS security at the Facilities layer. To avoid this incompatibility, the approach discussed in clause 5.2.1.2.2 should be followed when specifying Facilities layer services with ITS security.

NOTE: Implementations that do not have a Secured Facilities layer PDU service cannot transmit or receive such secured messages at the Facilities layer.

## 5.3 Interface between Security Entity and Facilities Layer

**Gap:** The interface specification between Security Entity and ITS Facilities Layer has not been defined yet.

**Proposal:** To specify the interface between Security Entity and ITS Facilities Layer.

**Consideration on backward compatibility:** The proposed action completes the planned specifications of cross-layer interfaces. Existing ITS stations implementation following ITS security at the GeoNetworking layer cannot decode or authenticate a received message that follows the ITS security implementation at the Facilities layer.

# 6 Conclusions

The present document analyses the existing ETSI ITS standards for the purpose of enabling ITS security operation at the ITS Facilities layer. Gaps in current ITS standards for performing ITS security operation at the ITS facilities layer are identified. To close these gaps while maintaining backward compatibility with existing standards, standardization activities for each related ETSI ITS standard are proposed.

CAM as a type of Facilities layer message can be transmitted over cellular wide-area communications for different use cases, e.g. probe vehicle data, or traffic light priority request, which needs SREM and SSEM but also CAM to track the requesting vehicle for a limited time window. Therefore, transmitting CAM over wide-area communications is discussed in the present document from the view point of Facilities layer security. However, it has to be noted that requirements, e.g. the generation frequency and latency of transmitting CAM over cellular wide-area communication for those use cases may be different from requirements of transmitting CAM over short-range communications for cooperative awareness service. Such requirements need to be further investigated. Another open issue is personal data protection and the impact of GDPR when CAM is transmitted over cellular wide-area communications. A Data Protection Impact Assessment (DPIA) is needed to address this issue. Resolving these open issues require dedicated studies out of scope of the present document which only focuses at enabling ITS security at Facilities layer for CAM from a specification point of view.

The need for ITS applications for E2E security is another important topic for wide-area ITS communications that involve a chain of successive communication links. For example, requirements for specific ITS applications for authentication/non-repudiation should be reviewed as part of the TVRA review, as such security features are standardized for short-range ITS communications but not for wide-area ITS communications.

Moreover, it has to be noted that the network capacity requirements are out of scope of the present document. Large scale deployments of ITS services over cellular networks, in particular with the support of CAM, will increase the bandwidth usage and the number of parallel active radio connections. While 5G networks support per design massive parallel connections, the impact of a large-scale deployment on 4G networks needs to be studied. Interoperability of ITS security solutions in hybrid environments, where both short-range and wide-area cellular technologies are used in the E2E communication supporting C-ITS services, has not been addressed in the present document. It has to be noted that the alignment of IP based communication with short-range communications for secure C-ITS communication can be facilitated by alternative solutions, e.g. GeoNetworking over IP as outlined in clause 4.4.1. The present document pays special attention to maintaining compatibility of different alternative solutions in related ETSI standards.

Nevertheless, a dedicated study on E2E security solution for C-ITS services, especially when ITS messages are forwarded between different communication channels that may use different alternative ITS security solutions, is needed.

# Annex A:
# Security solutions for cellular based ITS in pilot and field trial projects

## A.1 CONVERGE project

In the CONVERGE project [i.16], hybrid communication solution using both short-range ITS-G5 and wide-area cellular communication are tested. Section 4.1.6 of CONVERGE project deliverable D.4.3 gives an overview of the security concept, as well as corresponding message flows and communication protocols stacks using both short-range and wide-area communication channels in the Car2X system developed in the project.

# Annex B: Comparison of ITS security solutions for C-ITS over IP based cellular communication

Table B.1 provides a comparison of ITS security solutions at the GeoNetworking layer and at the Facilities layer, which are respectively described in clauses 4.4.1 and 4.4.2 of the present document. In the table different aspects for the end-to-end delivery of an ITS message involving both short-range and wide-area communications are considered, e.g. as shown in Figure 8.

NOTE: Other solutions described in clauses 4.4.3 and 4.4.4 are not included in Table B.1.

**Table B.1: Comparison of ITS security solutions at GeoNetworking layer and at the Facilities layer**

| Comparison of ITS security solutions at GeoNetworking layer and at the Facilities layer | Solution 1: (clause 4.4.1) ITS security at GeoNetworking layer | Solution 2: (clause 4.4.2) ITS security at Facilities layer |
|---|---|---|
| Security | GN header, BTP header and the payload (CAM, DENM, IVIM, etc.) are protected for integrity and authenticity<br>Additional security mechanisms, e.g. TLS, can be applied at the TCP/IP layer. | This solution only covers the Facilities layer PDU (payload) and does not cover the network and transport layers.<br>Additional security mechanisms, e.g. TLS, can be applied at the TCP/IP layer. |
| Case 1 Multi-hop/re-forwarding of message, e.g. DENM (V2I2V) (See note) | The geonet signature is verified by all ITS stations that process the payload of the message (E2E verification). The geonet signature can be used to verify the message by intermediate ITS stations.<br>On the wide area links standard session security may be applied for message integrity checking, e.g. TLS. | N/A.<br>In case of forwarding an ITS message, e.g. DENM, which is received from a vehicle using wide area communication, to other ITS stations using short-range communication, adding facility layer security does not add value on top of standard session security e.g. TLS. |
| Case 2 Forwarding message, e.g. IVIM (I2V2V/I2I2V):<br>Central ITS station creating IVIM message sends this message to another ITS station that forwards the message to vehicles either via cellular or short range | I2V2V:<br>In case of forwarding an ITS message, which is received by a vehicle using wide area communication from the central ITS station and further forwarded to other ITS stations using short-range communication, the message can be forwarded without changing the geonet and security headers from the originating central ITS station (one E2E security header at the GeoNetworking layer).<br>Geonet signature provides originator non-repudiation of messages.<br>I2I2V:<br>Central ITS station adds geonet header to the payload and signs the message on geonet layer. This offloads the functionality of generating the geonet headers and signatures from a RSU.<br>In this case, RSUs act as geo-routers. The geonet signature is only verified by vehicles receiving the message over short range. Intermediate central and roadside stations receiving the message over wide area communications can verify the geonet signature. They may also rely on session security e.g. TLS for message integrity verification. | I2V2V/I2I2V:<br>Central ITS station may sign message on facility layer on top of session security (e.g. TLS). Facilities layer signature provides originator non-repudiation of the message.<br>The facility layer signature may be verified by all receiving and forwarding stations that process the facilities layer message. Forwarding stations do not change the facility layer signature.<br>In case of a message needs to be delivered to short range communication vehicles, the forwarding station needs to sign the message with the geonet header according to the current geonet security standards. |

| Comparison of ITS security solutions at GeoNetworking layer and at the Facilities layer | Solution 1: (clause 4.4.1) ITS security at GeoNetworking layer | Solution 2: (clause 4.4.2) ITS security at Facilities layer |
|---|---|---|
| | Geonet signature provides originator non-repudiation of messages.<br>RSUs forward this I2V message to short range communication vehicles.<br>RSUs do not sign the message as it is already signed on the geonet layer. | |
| Implementation | May require using a messaging protocol such as MQTT or AMQP. | May require using a messaging protocol such as MQTT or AMQP. |
| Standard | GeoNetworking protocol is on the local "short-range" communication with geographical information dissemination. In this scenario, messages secured at the GeoNetworking layer are transmitted over the IP protocol stack.<br>BTP/GeoNetworking over TCP/IP has not been standardized.<br>Need to include this solution in TVRA [i.23]. | Require changing the standard to include security in facilities layer.<br>Need to specify the SF-SAP interface.<br>Need to include this solution in TVRA [i.23]. |
| NOTE: "I" in "V2I2V" refers to the central ITS station. | | |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | November 2020 | Publication |
| | | |
| | | |
| | | |
| | | |