ETSI TS 133 185 V14.1.0. (2017-10)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security aspect for LTE support of Vehicle-to-Everything (V2X) services
(Release 14)

Reference

Keywords
V2X,LTE,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

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

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.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the security aspects of V2X features in LTE, including security architecture, security requirements on the network entities that are used to support V2X services, as well as the procedures and solutions which are provided to meet those requirements.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.185: "Service requirements for V2X services".

[3] 3GPP TS 23 285: "Architecture enhancements for V2X services (Release 14)".

[4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[7] ETSI TS 102 226: "Smart cards; Remote APDU structure for UICC based applications".

[8] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[9] 3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications ".

[10] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[11] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)".

[12] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE): Security Architecture".

[13] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[14] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[15] 3GPP TS 33.246: "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[16] IEEE Std 1609.2-2016: "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages".

[17] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management" (V1.2.1; 2016-11).

[18] 3GPP TS 33.402: "3GPP System Architecture Evolution; Security aspects of non-3GPP accesses".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AS	Application Server
BSF	Bootstrapping Server Function
GBA	Generic Bootstrapping Architecture
GCS	Group Communication System
ITS	Intelligent Transportation System
LTE-V	LTE V2X
NAF	Network Application Function
ProSe	Proximity-based Services
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCF	V2X Control Function

4 V2X security architecture

V2X service contains three types of vehicular communication services V2V (vehicle to vehicle), V2I (vehicle to infrastructure), V2N (vehicle to network), and V2P (vehicle to pedestrian) for both safety and non-safety aspects.

The overall architecture describing LTE enhancements for V2X services is given in TS 23.285 [3]. Both LTE-Uu based architecture (e.g. eMBMS) and PC5 based architecture are used for supporting V2X services, but they may be used by a UE independently for transmission and reception, e.g. a UE can use eMBMS for reception without using LTE-Uu for transmission.

The security for interfaces given in the overall architecture (TS 23.285 [3]) is provided in clause 6, in detail these are the interfaces between network entities (clause 6.2), between UE and V2X Control Function (clause 6.3), and between V2X AS and 3GPP system (clause 6.4). Clause 6.5 discusses security of V2X application data. Clause 6.6 is providing details to privacy in V2X services.

Note: The V2 interface is not specified in 3GPP TS 23.285 [3], thus out of scope also in the present document.

5 V2X security requirements

5.1 General

The service requirements for V2X services are specified in 3GPP TS 22.185 [2]. This clause contains the security requirements for V2X.

5.2 Interfaces between network elements

The V2X network entities shall be able to authenticate the source of the received data communications.

The transmission of data between V2X network entities shall be integrity protected.

The transmission of data between V2X network entities shall be confidentiality protected.

The transmission of data between V2X network entities shall be protected from replays.

5.3 Interface between UE and V2X control function (V3)

The V2X enabled UE and its HPLMN V2X Control Function shall mutually authenticate each other.

The transmission of configuration data between the V2X Control Function and the UE shall be integrity protected.

The transmission of configuration data between the V2X Control Function and the UE shall be confidentiality protected.

The transmission of configuration data between the V2X Control Function and the UE shall be protected from replays.

The transmission of UE identity should be confidentiality protected on the V3 interface.

5.4 Interface between external provider and 3GPP network (MB2)

V2X services use the MB2 interface for GCSE. The requirements to MB2 as listed in Annex N.1.2 of 3GPP TS 33.246 shall apply.

5.5 Security requirements of V2X application data

The V2X system entities should be able to authenticate and verify that the sender of the received data communications was authorized to send the data.

The transmission of data between different V2X entities in the V2X system should be integrity protected.

The transmission of data between different V2X entities in the V2X system should be protected from replays.

The transmission of data between two different V2X entities in the V2X system should be confidentiality protected if needed for the V2X application.

NOTE: Transmission of data includes but is not limited to multicast, broadcast, unicast, or geocast.

5.6 Privacy related requirements

As specified in 3GPP TS 22.185 [2] the following PC5 privacy related requirements apply:

Subject to regional regulatory requirements and/or operator policy for a V2X application, the data sent in the PC5 transmission should not allow UE identity to be tracked or identified by any other UE or non-V2X entity beyond a certain short time-period required by the V2X application.

Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the data sent in the PC5 transmission should not allow a single party (operator or third party) to track a UE identity in that region.

In addition, the following PC5 related requirements are given in the present specification:

The identifiers in the V2X messages should minimize the risk of leaking the UE or user permanent identities.

UE pseudonymity should be provided to conceal personal data from attackers.

The application layer UE identity in the V2X messages should be protected from eavesdropping.

5.7 Security requirement for V2X Entities Secure Environment

For V2X services relying on access networks within the scope of TS 33.401 [12], the 3GPP authentication, key agreement, associated subscriber credentials and associated subscriber identities used to access the network should reside on USIM within the V2X enabled UE.

For V2X services relying on access networks within the scope of TS 33.402 [18], the 3GPP authentication, key agreement, associated subscriber credentials and associated subscriber identities used to access the network should reside on UICC within the V2X enabled UE, except for terminals that do not support 3GPP access capabilities and where 3GPP does not specify where the credentials used with EAP-AKA and EAP-AKA' reside.

6 V2X security solutions

6.1 General

This clause contains a description of the various security features that are available for V2X services. All V2X services do not have the same security requirements and hence may not require the use of all the described features. It is up to the deployment of the feature to ensure that all the appropriate security aspects are addressed.

6.2 V2X communication between network elements

6.2.1 General

V2X uses several interfaces between network entities as described in TS 23.285 [3]. This subclause describes the security for those interfaces.

6.2.2 Security procedures

For all interfaces between network elements,

TS 33.210 [4] shall be applied to secure signalling messages on the reference points unless specified otherwise, and

TS 33.310 [5] may be applied regarding the use of certificates with the security mechanisms of TS 33.210 [4] unless specified otherwise in the present document.

NOTE: For the case of an interface between two entities in the same security domain, TS 33.210 [4] does not mandate the protection of the interface by means of IPsec.

6.3 V2X communication between UE and V2X Control Function (V3)

6.3.1 General

The UE has interactions with the V2X Control Function over the V3 in the V2X services as described in TS 23.285 [3]. The V3 interface can be secured in the same way as the PC3 interface, as in TS 33.303 [10] clause 5.3.

6.3.2 Security procedures for configuration transfer to the UICC

After deployment of the UE the configuration parameters stored in the UICC may need to be updated to reflect the changes in the configuration applied.

In case that configuration data of V2X-enabled UE are stored in the UICC, the UICC OTA mechanism (as specified in ETSI TS 102 225 [6] / TS 102 226 [7] and 3GPP TS 31.115 [8] / TS 31.116 [9]) shall be used to secure the transfer of the configuration data to be updated in the UICC.

6.3.3 Security procedures for data transfer to the UE

This subclause describes procedures for protecting data transfer between UE and V2X Control Function.

Between the UE and network function, for UE initiated messages:

PSK TLS with GBA including the option of the co-located BSF and NAF is used as specified in TS 33.303 [10] (subclause 5.3.3.2) for UE initiated messages between the UE and ProSe Function with the V2X Control Function playing the role of the ProSe Function.

and for network initiated messages one of the following mechanisms shall be used:

If a PSK TLS connection has been established as a part of a pull message and is still available, the available PSK TLS session shall be used.

Otherwise, PSK TLS with GBA push based shared key-based mutual authentication between the UE and the network function shall be used. GBA push is specified in TS 33.223 [13]. The network function (pushNAF) shall request USSs from the BSF when requesting a GPI, and the network function shall check in the USS if the USIM is authorized to be used for V2X services. If the authorization in the network function fails, then the network function shall refrain from establishing PSK TLS with GBA push.

NOTE : If a TLS connection is released, it can only be re-established by the client, i.e. UE, even though the TLS session including security association would be alive on both sides. TLS connection, in turn, is dependent on the underlying TCP connection.

6.4 Interface between V2X application server and 3GPP network (MB2)

The V2X Application Server acts as GCS AS (TS 23.468 [14]) and uses the security features as specified in Annex N of TS 33.246 [15].

6.5 Security of V2X application data

6.5.1 General

V2X application data is sent by vehicle UEs in periodic or event-driven broadcast messages, and can occur either on the PC5 interface or on the LTE-Uu interface.

V2X applications aim to improve road safety and travel mobility, by issuing timely warnings to the driver, or providing information about road hazards and congestion, emergency vehicles, etc. It is therefore of utmost importance that the safety messages broadcast by UEs are trusted as having been issued from a legitimate/well-functioning device.

For the PC5 mode, the recipients of these messages (i.e. vehicle UEs that are within communication range of the sending UE) are not known in advance to a transmitting vehicle UE, and hence a priori (e.g., network assisted) security association establishment between UEs is not feasible to be supported. This is the nature of this point to multipoint communication within a dynamically changing set of UEs. Therefore, neither current LTE security nor ProSe one-to-many communication security is applicable.

NOTE: Establishment of security association in an ad-hoc fashion between UEs over PC5, which might be needed for other applications and use cases, is not addressed in this document.

6.5.2 Security procedures

Thought the security requirements applicable to V2X communications are all satisfied by employing application-layer security as defined in other SDOs, (e.g. IEEE [16] or ETSI ITS [17]), such use of the application-layer security to secure V2X communications is outside the scope of 3GPP.

For PC5 communication, the data frames inherit the format of the PC5 one-to-many communication, although no security is applied at this layer. They contain fields relating to group keys. These fields are all set to zero for PC5 based V2X communications.

For LTE-Uu communications, the LTE security mechanism for air interface confidentiality shall be used (see TS 33.401 [12]).

NOTE: In LTE, no ciphering may be selected depending on the network policy.

6.6 Privacy in V2X services

6.6.1 General

If a UE is using the same identity in several broadcast messages, it is possible to track the vehicle and compromise its privacy. Whether such privacy concerns exist for a V2X service will likely depend on regional regulatory requirements and/or operator policy, hence the PC5 privacy feature is optional to use. For example, a service that is mandated for use by a regulator may not provide an "opt out" option.

No additional privacy features beyond the regular LTE privacy features (see TS 33.401 [12]) are supported for Uu mode V2X communications.

NOTE 1: The specification does not provide technical solutions to address any privacy concerns specific to V2X service that require privacy for a UE being attached to the network, or that due to the data traversing the network in Uu mode. However, there are general privacy principles applicable outside of 3GPP scope; data minimization and user consent if privacy impacting data collection is unavoidable for providing the V2X service.

NOTE 2: Even if out of scope of 3GPP, bilateral agreements between operator, V2X service provider, and V2X-UE might be able to address regional regulator privacy concerns.

Privacy may be supported at the application layer by employing identifiers and credentials that are not linked to long-term UE or user identifiers. These credentials would be refreshed periodically. The change of application layer identities and credentials for using the V2X service is out of scope in 3GPP.

6.6.2 Privacy procedures related to PC5 transmissions

The UE shall change and randomize the source Layer-2 ID, and the source IP address (in case of IP-based V2X communication) when indicated by the V2X application that the application layer identifier has changed. The UE shall also provide indication to the V2X application layer when the source Layer-2 ID, or/and the source IP address (in case of IP-based V2X communication) are changed.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-06	SA#76					Upgrade to change control version	14.0.0
2017-09	SA#77	SP-170643	0001	-	F	GBA use in LTE V2X	14.1.0

History

Document history		
V14.0.0	July 2017	Publication
V14.1.0.	October 2017	Publication