

ICS 33.060.99
CCS M 30

YD

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

YD/T 3594-2019

**General technical requirements of Security for Vehicular
Communication based on LTE**

基于LTE的车联网通信安全技术要求

(English Translation)

Issued on: November 11, 2019

Implemented on: January 1, 2020

Issued by: Ministry of Industry and Information Technology of PRC

Table of Contents

Foreword...	4
1 Scope...	5
2 Normative references...	5
3 Abbreviations...	6
4 LTE-based vehicular communication architecture...	7
4.1 Overview...	7
4.2 PC5 and LTE-Uu based V2X communication architecture...	7
4.3 MBMS and LTE-Uu based V2X communication architecture...	11
4.4 LTE-based vehicular communication security architecture...	11
5 Requirements for LTE-based vehicular communication security...	13
5.1 General security requirements...	13
5.2 Security requirements for network elements...	14
6 Security process of V5 interface...	17
6.1 Overview...	17
6.2 Description of security basic elements...	18
6.3 General requirements for security data structure...	21
6.4 Public key certificate format...	22
6.5 Message signing process...	23
6.6 Message encryption process...	28
6.7 Key negotiation...	34
7 Security procedures of other interfaces...	36
7.1 V2X communication security process between network elements...	36
7.2 Security process of V3 interface...	36
7.3 Security process of MB2 interface...	38
Appendix A (Normative) Algorithm description...	39
Appendix B (Informative) Device authorization management...	41
Appendix C (Informative) Public key certificate management...	55
Appendix D (Informative) Data message of V5 interface...	70
Appendix E (Informative) Key negotiation calculation process...	84
Appendix F (Informative) Certificate request and response...	86

1 Scope

This standard specifies the overall technical requirements, interface security requirements, security procedures for LTE-based vehicular communication security.

This standard applies to LTE-based vehicular communication systems.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this standard.

GB/T 37376-2019 Transportation - Digital certificate format

GB/T 37374-2019 Intelligent transport - Digital certificate application interface

3GPP TS 33.210 3G security; Network Domain Security (NDS); IP network layer security)

3GPP TS 33.223 Generic Authentication Architecture (GAA); Generic

Bootstrapping Architecture (GBA) Push function)

3GPP TS 33.246 3G Security; Security of Multimedia Broadcast/Multicast

Service (MBMS)

3 Abbreviations

The following abbreviations apply to this document

BM-SC. Broadcast-Multicast Service Center

BSF. Bootstrapping Server Function

CA. Certificate Authority

E-UTRAN. Evolved UTRAN

GCS AS. Group Communication System Application Server

LTE. Long Term Evolution

MBMS. Multimedia Broadcast / Multicast Service

NAF. Network Application Function

PLMN. Public Land Mobile Network

USS. User Security Settings

4.1 Overview

The LTE-based vehicular communication system supports vehicle-to- Vehicle (V2V) applications, vehicle-to-infrastructure (V2I) applications, vehicle-to- network (V2N) applications, vehicle-to-pedestrian (V2P) applications. These applications can provide users with various businesses, such as road security, transportation efficiency improvement, infotainment.

4.2.1 PC5 and LTE-Uu based V2X communication architecture in non-roaming scenarios

Figure 1 shows the PC5 and LTE-Uu based V2X communication architecture in

4.2.2 PC5 and LTE-Uu based V2X communication architecture in roaming scenarios

4.2.3 PC5 and LTE-Uu based V2X communication architecture in cross-PLMN scenarios

4.2.4 Reference point

The reference points of the PC5 and LTE-Uu based V2X communication architecture include the following points.

4.4.1 Security protocol architecture of LTE-based vehicular communication

4.4.2 Communication security architecture of LTE-based Internet of Vehicles application layer

Figure 7 shows the communication security architecture of LTE-based Internet of Vehicles application layer. The functions of each functional entity, in the security subsystem, include the following points.

5 Requirements for LTE-based vehicular

communication security

5.1 General security requirements

- When a V2X device uses the service, which is provided by E-UTRAN that supports V2X communication, the 3GPP network shall provide a method

5.2.1 V2X device

For PC5 communication, V2X devices shall support certificate-based application layer security mechanisms. See V5 interface security for details.

For the Uu communication, V2X devices shall support LTE communication security mechanisms, including EPS-AKA-based mutual authentication, air interface encryption, integrity protection of signaling messages. Among the, for the air interface encryption, the V2X device and the LTE network shall, through negotiation, determine whether to enable it. For MBMS-based Uu

5.2.2 V2X control function

The V2X control function shall support the security mechanism, which is defined in Chapter 7.2, to protect the security of the V3 interface.

The V2X control function shall support the security mechanism, which is defined in Chapter 7.1, to protect the security of the interface with other network elements.

5.2.3 V1 interface security requirements

The security of the V1 interface is outside the scope of this standard.

5.2.4 V2 interface security requirements

The security of the V2 interface is outside the scope of this standard.

6.1 Overview

In V2X services, V2X devices interact through V5 interfaces; secure communication is handled by the application layer. V2X device includes V2X vehicles (OBU), V2X roadside units (RSU), etc. The communication integrity protection architecture, which is provided through the V5 interface, is as shown in Figure 8. The typical security process is as follows.

6.2.1 Encoding rules

This standard uses ASN.1 to describe the data structure; uses octet encoding rules (OER) to encode various information, in the digital certificate format.

6.2.2 Definition of data structure

The atomic types, which are used in the data structure definition, shall meet the relevant requirements of GB/T 37376-2019.

The synonyms of the octet string, which are used in the data structure definition, shall meet the relevant requirements of GB/T 37376-2019.