YD

COMMUNICATION INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 33.060.99

M30

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

Issued on: November 11, 2019 **Implemented on: January 01, 2020**

Issued by: Ministry of Industry and Information Technology of PRC

Table of Contents

General technical requirements of security for vehicular communication based on LTE

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)

IEEE Std 1363 IEEE Standard Specifications for Public-Key Cryptography

IEEE Std 1363a IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques

IEEE Std 1609.2-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages

IETF RFC 5639 Elliptic Curve Cryptography (ECC) Brainpool Standard

for the operator to authorize the V2X device to perform V2X communication.

- The 3GPP network shall provide a method, for operators to authorize V2X devices to perform V2X communications, when they have not obtained E-UTRAN services that support V2X communications.

- The 3GPP network shall provide a method, to authorize V2X devices to use vehicle-to-network communication services.

- The 3GPP network shall protect the integrity of V2X device transmission.

- According to the requirements of regulatory agencies, 3GPP networks shall protect the anonymity and privacy of V2X devices; ensure that V2X devices shall not be tracked or identified by other terminals, within a certain period of time, which is required by V2X applications.

- According to the requirements of the regulatory agency, the 3GPP network shall protect the anonymity and privacy of V2V/V2I communication terminals; ensure that V2X devices shall not be tracked in this area by a party without the authorization by regulatory agency or user.

- The system shall support the use of domestic commercial cryptographic algorithms.

- The system shall support secure transmission channels, such as https.

- The system shall support the secure storage of sensitive information.

5.2 Security requirements for network elements

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 communication, V2X devices may not support air interface encryption. V2X devices shall also support certificate-based application layer security mechanisms.

To protect user privacy, V2X user-side devices (such as vehicles) can be anonymized, at the application layer. For details, see V5 interface security.

When the application layer instructs the application layer ID to change, the V2X device shall randomly change its layer 2 ID.

V2X devices shall support the protection of sensitive information (such as keys, certificates, etc.), using secure operating environments, security units, or secure processors.

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.

5.2.5 V3 interface security requirements

- V2X device and its HPLMN's V2X control function shall support mutual authentication.

- The configuration data transmission, between the V2X control function and the V2X device, shall support integrity protection

- The configuration data transmission, between the V2X control function and the V2X device, shall support confidentiality protection

- The configuration data transmission, between the V2X control function and the V2X device, shall support anti-replay attacks

- The identity of the V2X device on the V3 interface shall support confidentiality protection.

5.2.6 V4 interface security requirements

- The V2X network entity shall be able to authenticate the sender of the received data communication, that is, the V2X control function and the HSS shall be able to authenticate each other.

- Data transmission, between V2X network entities (that is, between V2X

control functions and HSS), shall be subject to integrity protection.

- Data transmission, between V2X network entities (that is, between V2X control functions and HSS), shall be subject to confidentiality protection.

- Data transmission, between V2X network entities (that is, between V2X control functions and HSS), shall support anti-replay attacks.

5.2.7 V5 interface security requirements

- The message receiver shall support the authentication of the message sender. The V2X application, on the V2X device, may be both the message sender and the message receiver. The data transmitted between the V2X applications shall support integrity protection.

- Data transferred between V2X applications can support confidentiality protection.

- Data transmitted between V2X applications shall support anti-replay attacks.

5.2.8 MB2 interface security requirements

V2X services use the MB2 interface of GCSE.

The security requirements of the MB2 interface are as follows.

- Two-way authentication shall be carried out, between the node in the security domain, where the BM-SC is located, and the node in the security domain. where the GCS AS is located.

- The signaling message of the MB2-C interface, between BM-SC and GCS AS, shall support integrity and confidentiality protection.

- The user plane message of the MB2-U interface, between BM-SC and GCS AS, shall support integrity protection.

- BM-SC may perform access control on messages, which are initiated by GCS AS.

- GCS AS may perform access control on messages, which are initiated by BM-SC

6 Security process of V5 interface

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:

The certificate management system issues its public key certificate (secure message certificate), to the V2X device for issuing messages; provides the CA public key certificate to the V2X device, which receives the message in a secure manner (taking the communication between a V2X vehicle and a V2X roadside unit as an example, as shown in ① in Figure 8, C1/C2 issues Co1, Co2, ... to V2X vehicles; it issues Cca1, Cca2 to V2X roadside units). It is recommended that the certificate management system issue multiple public key certificates to V2X vehicles; the V2X vehicles randomly select one of these certificates to use each time, to ensure user privacy.

The V2X device uses the private key, corresponding to the public key certificate, which is issued to it, to digitally sign the message; broadcasts the signed message together with the public key certificate or certificate chain (as shown in ② of Figure 8, the above message is composed of the content to transmit, the signature of the content, the public key certificate/certificate chain used). Here, the receiver's V2X device can set the CA certificate (Cca2), that issues the public key certificate (Co), as a trusted certificate; the receiver's V2X device uses the above CA certificate, to verify the sender's public key certificate, so that the V5 interface message may not necessarily carry the complete certificate chain, thereby saving air interface transmission resources.

The V2X device, as the receiver, first uses the CA public key certificate, to verify the public key certificate or certificate chain, which is carried in the message; then uses the public key, in the public key certificate, to verify the signature, to check the integrity of the message. Optionally, after the recipient's V2X device successfully verifies the peer's public key certificate (Co), the hash value of the certificate can be stored locally; the certificate can be verified later, by verifying the certificate hash, thereby reducing the cryptography operations, which are required for certificate verification.

The communication between the V2X roadside equipment and the V2X vehicle, as well as the communication between the V2X vehicle and the V2X vehicle, are similar to the above process.

6.2.4 Elliptic curve

The elliptic curve is defined as the EccCurve type. The structure shall meet the relevant requirements of GB/T 37376-2019.

6.2.5 Symmetric encryption algorithm

The symmetric encryption algorithm is defined as the SymmetricAlgorithm type. The structure shall meet the relevant requirements of GB/T 37376-2019.

6.2.6 Signature public key

The signature public key is defined as the PublicVerifyKey type. The structure shall meet the relevant requirements of GB/T 37376-2019.

The point on the ECC elliptic curve is defined as the ECCPoint type. The structure shall meet the relevant requirements of GB/T 37376-2019.

6.2.7 Encrypted public key

The encrypted public key is defined as the PublicEncryptionKey type. The structure shall meet the relevant requirements of GB/T 37376-2019.

6.2.8 The 8-byte hash value

The 8-byte hash value is defined as the HashedId8 type. The structure shall meet the relevant requirements of GB/T 37376-2019. The hash value is used to identify data, such as certificates. This data structure contains a hash of another data structure. First calculate the hash value of the input data; then take the 8 least significant bytes from the hash value. The lowest eight bytes are the last eight bytes of the 32-byte hash.

6.2.9 The 32-bit time

The 32-bit time is defined as the Time32 type. The structure shall meet the relevant requirements of GB/T 37376-2019. Time32 is a 32-bit unsigned integer, in high-end first encoding format; starting from January 1, 2004 UTC 00:00:00, it gives the number of seconds in the international atomic time.

6.2.10 Geographic effective region

The geographic effective region is defined as the GeographicRegion type. The structure shall meet the relevant requirements of GB/T 37376-2019. This identification defines the geographical region, where the certificate is applied; these regions can be used to limit the validity of the certificate. Any part of the scope included by the certificate owner, if outside the specified scope, is invalid. It includes the following 4 types: circular region, rectangular region, polygonal region, recognized region.

6.2.11 Circular region

The circular region is defined as the CircularRegion type. The structure shall meet the relevant requirements of GB/T 37376-2019. This structure defines a circular region, which has a radius and center in the unit of meters. For the distance between all points on the surface of the reference ellipsoid in the specified region, the center point is less than or equal to the radius on the reference ellipsoid. The point, which contains the elevation component, is considered that the reference ellipsoid of horizontal projection, in the circular region, is located in that region.

6.2.12 Rectangular region

The rectangular region is defined as a RectangularRegion type. The structure shall meet the relevant requirements of GB/T 37376-2019. This structure defines a rectangular area, which is connected by contours of longitude or latitude in turn. The point, which contains the elevation component, is considered that the reference ellipsoid of horizontal projection, is within the rectangular region.

6.2.13 Polygonal region

The polygonal region is defined as PolygonalRegion type. The structure shall meet the relevant requirements of GB/T 37376-2019. This data structure defines a region, which uses a series of different geographic points, defined on the surface of the reference ellipsoid. Distinguish the order in which they appear by connecting the specified locations; each pair is connected by a geodesic on the reference ellipsoid. The completed polygon will eventually point to the first point, through the connection. The allowed region is the interior and boundary of the polygon. The point, which contains the elevation component, is considered that, the polygonal region of horizontal projection, is within the reference ellipsoid, which is located in that region. A valid polygon region contains at least three parts. In the effective polygon region, the polygons, which are formed by the hidden lines, do not intersect.

6.2.14 Recognized region

The recognized region is defined as an IdentifiedRegion type. The structure shall meet the relevant requirements of IEEE Std 1609.2-2016. This structure defines a series of region identifiers, to indicate the validity of the certificate. Its structure includes Region and SubRegion. Region represents one or more regions within a country, such as a provincial administrative unit; SubRegion represents one or more sub-regions within a Region, such as cities, counties, districts, etc.

6.2.15 Two-dimensional location information

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------