ICS [点击此处添加ICS号]

[点击此处添加中国标准文献分类号]

YD

中华人民共和国通信行业标准

YD/T [×××××]—[××××]

[代替YD/T]

|  |
| --- |
| 基于LTE网络的车联网通信安全总体技术要求  General technical requirements of Security for Vehicular Communication based on LTE  [点击此处添加与国际标准一致性程度的标识]  （送审稿）  （本稿完成日期：2018-8-23） |

[××××]-[××]-[××]发布

[××××]-[××]-[××]实施

中华人民共和国工业和信息化部 发 布



目　　次

[前言 IV](#_Toc522843899)

[1　范围 1](#_Toc522843900)

[2　规范性引用文件 1](#_Toc522843901)

[3　缩略语 2](#_Toc522843902)

[4　基于LTE网络的车联网通信架构（大唐） 2](#_Toc522843903)

[4.1　概述 2](#_Toc522843904)

[4.2　基于PC5和LTE-Uu的V2X通信架构（ZTE） 2](#_Toc522843905)

[4.2.1　非漫游场景下基于PC5和LTE-Uu的V2X通信架构 2](#_Toc522843906)

[4.2.2　漫游场景下基于PC5和LTE-Uu　的V2X通信架构 3](#_Toc522843907)

[4.2.3　跨PLMN场景下基于PC5和LTE-Uu　的V2X通信架构 4](#_Toc522843908)

[4.2.4　参考点 5](#_Toc522843909)

[4.3　基于MBMS和LTE-Uu的V2X通信架构 5](#_Toc522843910)

[4.4　基于LTE网络的车联网通信安全架构 6](#_Toc522843911)

[4.4.1　基于LTE网络的车联网通信安全协议架构 6](#_Toc522843912)

[4.4.2　基于LTE网络的车联网应用层通信安全架构 8](#_Toc522843913)

[5　基于LTE网络的车联网通信安全要求 8](#_Toc522843914)

[5.1　通用安全要求 9](#_Toc522843915)

[5.2　网元的安全要求 9](#_Toc522843916)

[5.2.1　V2X设备（高通） 9](#_Toc522843917)

[5.2.2　V2X　控制功能（华为） 9](#_Toc522843918)

[5.2.3　V1接口安全要求（高通） 9](#_Toc522843919)

[5.2.4　V2接口安全要求（华为） 9](#_Toc522843920)

[5.2.5　V3接口安全要求（联通） 9](#_Toc522843921)

[5.2.6　V4接口安全要求（Nokia） 10](#_Toc522843922)

[5.2.7　V5接口安全要求（大唐） 10](#_Toc522843923)

[5.2.8　MB2接口安全要求（华为） 10](#_Toc522843924)

[6　V5接口的安全过程 10](#_Toc522843925)

[6.1　概述 10](#_Toc522843926)

[6.2　安全基本元素说明 11](#_Toc522843927)

[6.2.1　编码规则 11](#_Toc522843928)

[6.2.2　数据结构定义 11](#_Toc522843929)

[6.2.3　哈希算法 12](#_Toc522843930)

[6.2.4　椭圆曲线 12](#_Toc522843931)

[6.2.5　对称加密算法 12](#_Toc522843932)

[6.2.6　签名公钥 12](#_Toc522843933)

[6.2.7　加密公钥 12](#_Toc522843934)

[6.2.8　8字节哈希值 12](#_Toc522843935)

[6.2.9　32位时间 12](#_Toc522843936)

[6.2.10　地理有效区域 12](#_Toc522843937)

[6.2.11　圆形区域 12](#_Toc522843938)

[6.2.12　矩形区域： 13](#_Toc522843939)

[6.2.13　多边形区域 13](#_Toc522843940)

[6.2.14　二维位置信息 13](#_Toc522843941)

[6.2.15　维度 13](#_Toc522843942)

[6.2.16　经度 13](#_Toc522843943)

[6.3　安全类数据结构总体要求（东软） 13](#_Toc522843944)

[6.4　公钥证书格式 14](#_Toc522843945)

[6.4.1　消息证书 14](#_Toc522843946)

[6.4.2　CA证书 14](#_Toc522843947)

[6.4.3　证书撤销列表 14](#_Toc522843948)

[6.5　消息签名流程（东软） 14](#_Toc522843949)

[6.5.1　概述 14](#_Toc522843950)

[6.5.2　签名数据结构要求 15](#_Toc522843951)

[6.5.3　签名及验签条件限定 15](#_Toc522843952)

[6.5.4　签名计算流程 16](#_Toc522843953)

[6.5.5　验签计算流程 17](#_Toc522843954)

[6.6　加密消息流程（东软） 17](#_Toc522843955)

[6.6.1　概述 17](#_Toc522843956)

[6.6.2　加密数据结构要求 18](#_Toc522843957)

[6.6.3　加密解密条件限定 19](#_Toc522843958)

[6.6.4　随机加密计算流程 19](#_Toc522843959)

[6.6.5　协商加密计算流程 20](#_Toc522843960)

[6.7　密钥协商 22](#_Toc522843961)

[6.7.1　密钥协商综述 22](#_Toc522843962)

[6.7.2　密钥协商数据结构 22](#_Toc522843963)

[6.7.3　密钥协商计算流程 23](#_Toc522843964)

[7　V3接口的安全过程（华为） 23](#_Toc522843965)

[7.1　概述 23](#_Toc522843966)

[7.2　UICC配置传输的安全流程 23](#_Toc522843967)

[7.3　数据传输的安全流程 24](#_Toc522843968)

[7.4　MB2接口的安全过程（33.246）（华为） 24](#_Toc522843969)

[附录A　（规范性附录）　算法说明 25](#_Toc522843970)

[附录B　（资料性附录）　设备授权管理 27](#_Toc522843971)

[附录C　（资料性附录）　公钥证书管理 37](#_Toc522843972)

[附录D　（资料性附录）　安全相关AID值分配建议 46](#_Toc522843973)

[附录E　（资料性附录）　密钥协商计算流程 47](#_Toc522843974)

[附录F　（资料性附录）　证书请求及应答 49](#_Toc522843975)

[附录G　（资料性附录）　V5接口数据报文 56](#_Toc522843976)

|  |
| --- |
|  |



前　　言

本标准/本部分按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准/本部分由中国通信标准化协会提出并归口。

本标准/本部分起草单位：××××、××××、××××。

本标准/本部分主要起草人：×××、×××、×××。

|  |
| --- |
|  |

基于LTE网络的车联网通信安全总体技术要求

2. 范围

本标准规定了基于LTE网络的车联网通信安全的总体技术要求、接口安全要求和安全过程。本标准适用于基于LTE网络的车联网通信系统。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD-T XXXX：基于LTE的车联网无线通信技术总体技术要求

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

3GPP TS 33.185: "Security aspect for LTE support of Vehicle-to-Everything (V2X) services"

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

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

3GPP TS 33.401: "3GPP System Architecture Evolution (SAE): Security Architecture"

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

3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2"

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

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

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

FIPS 186-4: Digital Signature Standard (DSS)

SECG: SEC 1: Elliptic Curve Cryptography

RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

ISO/IEC8825-7: ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)

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

FIPS-197: ADVANCED ENCRYPTION STANDARD

GM/T 0002：SM4分组密码算法

GM/T 0003：SM2椭圆曲线公钥密码算法

GM/T 0004：SM3密码杂凑算法

GM/T 0009：SM2密码算法使用规范

GM/T 0015：基于SM2密码学算法的数字证书格式规范

GBT XXXXX-XXXX：交通运输 数字证书格式

GBT XXXXX-XXXX：智能交通 数字证书应用接口规范

1. 缩略语

下列缩略语适用于本文件。

|  |  |  |
| --- | --- | --- |
| BM-SC | 广播多播服务中心 | Broadcast-Multicast Service Centre |
| BSF | 引导服务器功能 | Bootstrapping Server Function |
| CA | 证书管理机构 | Certificate Authority |
| E-UTRAN | 演进UTRAN | Evolved UTRAN |
| GCS AS | 组通信系统应用服务器 | Group Communication System Application Server |
| LTE | 长期演进 | Long Term Evolution |
| MBMS | 多媒体广播多播业务 | Multimedia Broadcast/Multicast Service |
| NAF | 网络应用功能 | Network Application Function |
| PLMN | 公众陆地移动网 | Public Land Mobile Network |
| USS | 用户安全设置 | User Security Setting |
| V2I | 车辆对基础设施 | Vehicle to Infrastructure |
| V2N | 车辆对网络 | Vehicle to Network |
| V2P | 车辆对行人 | Vehicle to Pedestrian |
| V2V | 车辆对车辆 | Vehicle to Vehicle |

1. 基于LTE网络的车联网通信架构（大唐）
   1. 概述

基于LTE网络的车联网通信系统支持车-车（V2V）应用、车-路（V2I）应用、车-网（V2N）应用和车-人（V2P）应用，利用这些应用可向用户提供诸如道路安全、交通效率提升和信息娱乐等各类业务。

V2X 通信有两种操作模式，基于PC5的V2X通信和基于LTE-Uu的V2X通信。

基于LTE-Uu的操作模式可以是单播或广播方式。V2X设备可以分别使用这两种操作模式进行接收和发送。例如：一个V2X设备可以使用LTE-Uu的下行广播接收V2X消息，但发送V2X消息不使用LTE-Uu。一个V2X设备也可以通过LTE-Uu下行单播来接收V2X消息。

基于PC5的V2X通信重用一对多的ProSe直接通信传输过程，邻近通信中定义的PC5-U协议栈用于基于PC5接口的V2X通信传输。

本标准针对基于PC5的V2X通信和基于LTE-Uu的V2X通信制定安全总体技术要求。

* 1. 基于PC5和LTE-Uu的V2X通信架构（ZTE）
     1. 非漫游场景下基于PC5和LTE-Uu的V2X通信架构

图1给出了非漫游场景下基于PC5和LTE-Uu的V2X通信架构。



1. 非漫游场景下基于PC5和LTE-Uu的V2X通信架构
   * 1. 漫游场景下基于PC5和LTE-Uu 的V2X通信架构

图2给出漫游场景下基于PC5和LTE-Uu的V2X架构，V2X设备 A归属PLMN A，V2X设备 B归属PLMN B， V2X设备A漫游至PLMN B ，V2X设备B非漫游。

V2X应用服务器也可以连接多个PLMN，例如：一个V2X应用服务器可以连接PLMN A中的V2X控制功能实体，也可以连接PLMN B中V2X控制功能实体。



1. 漫游场景下基于PC5和LTE-Uu 的V2X通信架构
   * 1. 跨PLMN场景下基于PC5和LTE-Uu 的V2X通信架构

图3给出跨PLMN漫游场景下基于PC5和LTE-Uu的V2X架构，V2X设备A归属PLMN A，V2X设备 B归属PLMN B，V2X设备 A漫游至PLMN C，V2X设备 B非漫游。



1. 跨PLMN场景下基于PC5和LTE-Uu的V2X架构
   * 1. 参考点

基于PC5和LTE-Uu的V2X通信架构的参考点包括：

* 1. V1: V2X应用(内置在V2X设备里)和V2X应用服务器之间的参考点。
  2. V2: V2X应用服务器和V2X控制功能之间的参考点。V2X应用服务器可以连接多个PLMN的V2X控制功能。
  3. V3: V2X设备和归属PLMN中的V2X控制功能之间的参考点，适用于基于PC5和基于LTE-Uu的V2X通信，基于LTE-Uu的V2X通信可选支持MBMS。
  4. V4: 运营商网络中HSS和V2X控制功能之间的参考点。
  5. V5: 不同V2X设备中V2X应用之间的参考点。
  6. V6: 不同PLMN中的V2X控制功能间的参考点。
  7. PC5: 使用V2X业务的V2X设备之间用户面进行ProSe直接通信的参考点。
  8. S6a: V2X场景下，在E-UTRAN附着过程中，MME可以下载V2X通信相关的签约信息，或者当HSS中的签约信息改变时通知MME 。
  9. S1-MME: 在V2X场景下，该参考点可将V2X业务授权从MME传送到eNodeB。
  10. LTE-Uu: UE和E-UTRAN之间的参考点。
  11. 基于MBMS和LTE-Uu的V2X通信架构

图4为基于MBMS和LTE-Uu的V2X通信架构。



1. 基于MBMS和LTE-Uu的V2X架构

该架构的参考点有：

* 1. MB2:V2X应用服务器和BM-SC之间的参考点。
  2. SGmb/SGi-mb/M1/M3:MBMS系统内的SGmb/SGi-mb/M1/M3参考点。
  3. 基于LTE网络的车联网通信安全架构
     1. 基于LTE网络的车联网通信安全协议架构

基于LTE网络的车联网通信安全包括承载安全（PC安全或LTE-Uu安全）和V2X应用安全两部分，图5描述了基于PC5的V2X安全架构，图6描述了基于LTE-Uu的V2X安全架构。



1. 基于PC5的V2X通信安全协议架构

图5描述了基于PC5的V2X通信安全协议架构。邻近通信（见3GPP TS 23.303）中定义的PC5-U协议栈用于基于PC5接口的V2X通信传输。

在基于PC5的V2X通信过程中，PC5接口的PDCP安全是关闭的。



1. 基于LTE-Uu的V2X通信安全协议架构

图6描述了基于LTE-Uu的V2X通信安全协议架构，使用了LTE的协议栈，在基于LTE-Uu的V2X通信过程中，应支持LTE-Uu的安全。

* + 1. 基于LTE网络的车联网应用层通信安全架构

图7给出了基于LTE网络的车联网应用层通信安全架构。安全子系统中各功能实体的功能为：

* 1. V2X应用安全子系统：位于V2X车辆、V2X路边站、V2X服务提供商的应用服务系统中负责为V2X应用提供通信安全的功能实体。
  2. V2X应用：位于V2X车辆、V2X路边站、V2X服务提供商的应用服务系统中需要V2X应用通信安全的功能实体。
  3. V2X安全管理实体：负责对V2X应用安全子系统进行安全配置和安全数据供应的功能实体，例如，注册、授权、密钥供应和证书颁发等功能实体。
  4. V2X应用安全服务：位于V2X应用安全子系统中，与V2X应用进行交互以完成消息签名、验证、加密、解密等操作，与V2X安全管理实体进行交互完成密钥写入，证书申请与写入等操作。
  5. 安全环境：存储重要的安全数据，例如，CA证书、公私钥和加解密密钥等；为安全服务实体提供重要的安全计算服务，如数字签名、数据加密和解密等。



1. 基于LTE网络的车联网应用层通信安全架构
2. 基于LTE网络的车联网通信安全要求
   1. 通用安全要求
   2. 当V2X设备使用支持V2X通信的E-UTRAN提供的服务时，3GPP网络应提供运营商授权V2X设备进行V2X通信的方法。
   3. 3GPP网络应提供一种运营商授权V2X设备在未获得支持V2X通信的E-UTRAN服务时进行V2X通信的方法。
   4. 3GPP网络应提供一种授权V2X设备使用车到网络通信服务的方法。
   5. 3GPP网络应保护V2X设备传输的完整性。
   6. 根据监管机构的要求，3GPP网络应保护V2X设备的匿名性和隐私性，保证V2X设备在V2X应用所要求的某一段时间之内不能被其他终端追踪或识别。
   7. 根据监管机构的要求，3GPP网络应保护V2V/V2I通信终端的匿名性和隐私性，保证V2X设备不能被未经监管机构或用户授权的一方在该区域追踪。
   8. 系统应支持使用国产商用密码算法。
   9. 系统应支持安全传输通道，如https等。
   10. 系统应支持敏感信息的安全存储。
   11. 网元的安全要求
       1. V2X设备（高通）

对于PC5通信，V2X设备应支持基于证书的应用层安全机制，具体见V5接口安全。

对于Uu通信，V2X设备应支持LTE通信安全机制，包括基于EPS-AKA的双向认证、空口加密和完整性保护；V2X设备应同时支持基于证书的应用层安全机制。

为保护用户隐私，V2X用户侧设备（如车辆）可在应用层进行匿名化处理，具体见V5接口安全。当应用层指示应用层ID变化时，V2X设备应随机地改变自己的层二ID。

V2X设备应支持对敏感信息（如密钥、证书等）的保护。

* + 1. V2X 控制功能（华为）

V2X控制功能应支持7.2章定义的安全机制以保护V3接口的安全。

V2X 控制功能应支持7.1章定义的安全机制以保护其与其他网元接口的安全。

* + 1. V1接口安全要求（高通）

V1接口安全不在本标准范围内。

* + 1. V2接口安全要求（华为）

V2接口安全不在本标准范围内。

* + 1. V3接口安全要求（联通）
  1. V2X设备和其HPLMN的V2X控制功能应支持双向认证。
  2. V2X控制功能和V2X设备之间的配置数据传输应支持完整性保护。
  3. V2X控制功能和V2X设备之间的配置数据传输应支持机密性保护。
  4. V2X控制功能和V2X设备之间的配置数据传输应支持抗重放攻击。
  5. V3接口上的V2X设备身份应支持机密性保护。
     1. V4接口安全要求（Nokia）
  6. V2X网络实体应能认证所接收到的数据通信的发送方，即V2X控制功能和HSS应能认证对方。
  7. V2X网络实体之间（即V2X控制功能和HSS之间）的数据传输应受完整性保护。
  8. V2X网络实体之间（即V2X控制功能和HSS之间）的数据传输应受机密性保护。
  9. V2X网络实体之间（即V2X控制功能和HSS之间）的数据传输应支持抗重放攻击。
     1. V5接口安全要求（大唐）
  10. V2X应用之间应支持双向认证。
  11. V2X应用之间传输的数据应支持完整性保护。
  12. V2X应用之间传输的数据可支持机密性保护。
  13. V2X应用之间传输的数据应支持抗重放攻击。
      1. MB2接口安全要求（华为）

V2X业务使用GCSE的MB2接口。

MB2接口的安全需求如下：

* 1. BM-SC所处安全域的节点与GCS AS所处安全域的节点之间应进行双向认证。
  2. BM-SC和GCS AS之间MB2-C接口的信令消息应支持完整性和机密性保护。
  3. BM-SC和GCS AS之间的MB2-U接口的用户面消息应支持完整性保护。
  4. BM-SC可能对GCS AS发起的消息进行接入控制。
  5. GCS AS可能对BM-SC发起的消息进行接入控制。

1. V5接口的安全过程
   1. 概述

在V2X业务中， V2X设备间通过V5接口交互，安全通信由应用层处理。V2X设备包括V2X车辆（OBU）、V2X路边站（RSU）等。通过V5接口提供的通信完整性保护架构如图8所示，典型的安全过程如下：

* + 1. 证书管理系统向V2X设备颁发其用于签发消息的公钥证书（安全消息证书），并以安全的方式向接收消息的V2X设备提供CA公钥证书（以V2X车辆和V2X路边站通信为例，如图8中①所示，C1/C2向V2X车辆下发Co1、Co2、…，向V2X路边站下发Cca1、Cca2）。推荐证书管理系统向V2X车辆下发多个公钥证书， V2X车辆每次从这些证书中随机选取一个使用，以保证用户隐私。
    2. V2X设备利用与颁发给它的公钥证书相对应的私钥对消息进行数字签名，将签名消息连同公钥证书或证书链一同播发出去（如图8中②所示，上述消息由需要传递的内容、对内容的签名以及所使用的公钥证书/证书链构成）。此处，接收方的V2X设备可将颁发公钥证书（Co）的CA证书（Cca2）设置为可信证书， 接收方的V2X设备利用上述CA证书验证发送方的公钥证书，这样V5接口消息中可以不携带完整证书链，从而节省了空口传输资源。
    3. 作为接收方的V2X设备首先利用CA公钥证书验证消息中携带的公钥证书或证书链，然后利用公钥证书中的公钥验证签名以检查消息的完整性。接收方V2X设备成功验证对端的公钥证书（Co）后，可将该证书的hash值保存在本地，后续可以通过验证证书hash的方式验证该证书，从而减少证书验证所需的密码学操作。

V2X路边站到V2X车辆间的通信、V2X车辆到V2X车辆间的通信与上述过程类似。



1. V5接口安全流程（以V2X车辆和V2X路边站交互为例）
   1. 安全基本元素说明
      1. 编码规则
   2. 本标准使用ASN.1对数据结构进行描述，采用八位字节编码规则(OER)对数字证书格式的各项信息进行编码。
      1. 数据结构定义
   3. 数据结构定义中使用的原子类型参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
   4. 数据结构定义中使用的八位字节字符串的同义词参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
   5. 用来阐明定义的结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
      1. 哈希算法
   6. 哈希算法定义为HashAlgorithm类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
      1. 椭圆曲线
   7. 椭圆曲线定义为EccCurve类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
      1. 对称加密算法
   8. 对称加密算法定义为SymmetricAlgorithm类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
      1. 签名公钥
   9. 签名公钥定义为PublicVerifyKey类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
   10. ECC椭圆曲线上点定义为ECCPoint类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
       1. 加密公钥
   11. 加密公钥定义为PublicEncryptionKey类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
       1. 8字节哈希值
   12. 8字节哈希值定义为HashedId8类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。该哈希值用来识别证书等数据。这个数据结构包含另一个数据结构的散列。首先计算输入数据的哈希值,然后从哈希值中取8个最低有效字节。最低的八个字节是32字节的散列的最后八个字节。
       1. 32位时间
   13. 32位时间定义为Time32类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。Time32是一个32位无符号整数，高位优先编码格式，自2004年1月1日UTC 00:00:00开始，给出国际原子时间的秒数。
       1. 地理有效区域
   14. 地理有效区域定义为GeographicRegion类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。本项标识定义了证书应用地理区域，这些区域可以用来限制证书的有效性。证书所有者所包含的范围有任何一部分在规定的范围以外即为无效。
       1. 圆形区域
   15. 圆形区域定义为CircularRegion类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。本结构定义了一个圆形区域，该圆具有以米为单位的半径和中心。指定的地区参考椭球体的表面上的所有点的距离中心点在参考椭球体小于或等于半径。点包含海拔组件被认为是在圆形区域内的水平投影参考椭球体位于该地区。
       1. 矩形区域：
   16. 矩形区域定义为RectangularRegion类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。这个结构定义了一个依次由经度或维度等值线连接的矩形区域，点包含海拔组件被认为是矩形区域内的水平投影参考椭球体位于该地区。
       1. 多边形区域
   17. 多边形区域定义为PolygonalRegion类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。这个数据结构定义了一个地区使用一系列不同的地理点,定义在参考椭球体的表面。通过连接指定的地区分它们出现的顺序,每一对分通过参考椭球体上的测地线连接。完成多边形通过连接最终指向第一点。允许的地区是多边形的内部及边界。点包含海拔组件被认为是多边形区域内的水平投影参考椭球体位于该地区。一个有效的多边形区域包含至少三分。在有效多边形区域，隐含线构成的多边形不相交。
       1. 二维位置信息
   18. 二维位置信息定义为TwoDLocation类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。这个数据结构用于定义区域用于证书的有效性。纬度和经度字段包含上面定义的纬度和经度。
       1. 维度
   19. 维度定义为Latitude类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
       1. 经度
   20. 经度定义为Longitude类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。
   21. 安全类数据结构总体要求（东软）

在通过PC5接口进行安全类数据数据通信时，其安全的数据结构要求统一，其内容要求至少包含表1信息：



1. PC5接口传输的V5消息格式
   1. 信息版本：要求用于描述车辆通信采用的通信数据结构的版本。
   2. 数据类型：要求用于描述当前车辆通信采用的通信数据结构类型，其中至少包含以下三种类型表示
      1. 明文数据类型；
      2. 签名数据类型；
      3. 加密数据类型。
   3. 信息内容：要求用于表示当前信息报文的具体数据及相应的密码算法计算结果值。

ASN.1格式代码参考《GBT XXXXX-XXXX：智能交通 数字证书应用接口规范》第6.3.1 章节。

* 1. 公钥证书格式
     1. 消息证书
        1. 证书结构

V2X设备设备证书结构的定义参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 版本

证书的版本号Version 的值应设为2，参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 签名者信息

签名者信息定义为IssuerId类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 主题信息

主题信息定义为SubjectInfo类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 主题属性

主题属性定义为SubjectAttribute类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 有效性限定

证书有效性的相关限制定义为ValidityRestriction类型，其中应当至少包括一个time\_start\_and\_end类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + - 1. 签名

基于公钥密码算法的签名由一个容器封装，定义为Signature类型，结构参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + 1. CA证书

CA证书的的格式应符合GM/T 0015标准要求，参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* + 1. 证书撤销列表

证书撤销列表的格式参见《GB/TXXXXX—XXXX：交通运输 数字证书格式》。

* 1. 消息签名流程（东软）
     1. 概述

签名算法用于确认发送者发送信息的完整性及不可否认性，签名算法要求用于且不仅限于以下场景：

* 1. 证书链验证；
  2. 证书系统的策略配置下发；
  3. 证书系统颁发的证书撤销列表的下发；
  4. 证书请求的生成及验证；
  5. V2X设备之间数据交互。
     1. 签名数据结构要求

签名数据要求遵循6.2的数据结构，其中数据类型要求标识为签名数据类型，信息内容要求至少包含如下信息：



1. 签名数据的内容
   1. 待签名数据：要求包含所有不可更改的数据，该数据必须使用国际标准所规定的编码方式进行数据的序列化，作为最终的签名数据来源，其中待签名数据要求至少包含如下内容：
      1. 密码杂凑算法描述符，描述当前所使用的密码杂凑算法。
      2. 待签名数据类型，至少包含：（1）无加密通信消息，（2）带加密通信消息，（3）数字证书，（4）证书请求四种数据类型的标识。
      3. 待签名数据有效时间，描述当前待签名数据的有效时间范围，该时间以外被认定为数据无效。
      4. 待签名数据值，包含当前不可更改的具体数据内容。
   2. 签名者信息：描述签名者的信息，要求至少包含：（1）签名者证书摘要值，（2）签名者证书内容，（3）自我签名，三种类型来描述签名者。其中签名者证书摘要值采用的算法要求使用该报文包含的密码杂凑算法描述符指定的算法。
   3. 签名结果值：要求包含描述签名计算结果的信息，该数据要求至少包含如下内容：
      1. 签名算法描述符，表示当前签名算法及参数，具体描述内容要求满足6.4.3相关规定。
      2. 签名算法存储类型及结果值，根据不同的描述符表示当前签名算法结果采用何种方 式保存。

其ASN.1格式代码参考《GBT XXXXX-XXXX：智能交通 数字证书应用接口规范》第6.3.2.1 章节。

1. 使用国密算法时，在《GBT XXXXX-XXXX：智能交通 数字证书应用接口规范》中ECCPoint均采用x-only形式，但在本标准中，其ECCPoint可以采用ECCPointType\_x\_only，ECCPointType\_y\_0和 ECCPointType\_y\_1三种形式，以此保留对SM2快速验签算法支持的可能，具体使用规则参考 IEEE1609.2中的第6.3.23章节说明。
   * 1. 签名及验签条件限定
   1. 签名及验签计算方法需遵循相应签名算法的国际标准，椭圆曲线的参数选择中，要求至少支持NIST P-256，brainpoolP256r1及SM2三种。
   2. 密码杂凑算法要求至少支持SHA256及SM3两种算法。
   3. 数据需要包含一个被签名的数据区，该区域数据不可更改，任何需要确认且不可更改的数据均需要在该区域中。
   4. 数据需要包含一个签名者的识别信息，对于签名消息来说，其签名者信息为对应签名证书的密码杂凑值或对应的签名证书本身，对应证书来说，其签名者信息为对应颁发者证书密码杂凑值或自签标识，对于证书请求来说，其签名者信息为自签标识或者对应的准入证书。
   5. 在计算过程中，签名信息的入参数据为待签名数据编码的密码杂凑值与签名者证书编码的密码杂凑值的合并值，其中，如果签名信息为自签的准入证书请求等自签标识，其签名者信息为空，但是其摘要值仍需计算。
   6. 在签名验签计算过程中，签名算法所使用的密码杂凑算法要求与附录中的要求一致。
   7. 在基于SM2参数的椭圆曲线算法中，其签名算法要求遵循SM2签名算法规范，SM2签名用户可辨别表示要求与附录中的要求一致。
      1. 签名计算流程

签名计算流程如图9所示。



1. 签名计算流程
   * 1. 由接口触发签名流程，组织待签名数据及签名方式。
     2. 根据接口要求的签名方式确定签名者信息及签名者标识。
     3. 对签名者信息进行编码。
     4. 对编码后的签名者信息进行密码杂凑计算，如果签名者为自签标识，杂凑计算的原数据要求为空。
     5. 组织待签名数据及相关附属信息。
     6. 对待签名数据及附属信息进行编码。
     7. 对二者的摘要信息进行数据拼接并作为最终摘要值。
     8. 对待摘要值进行签名计算。
     9. 将计算结果值、待签数据、签名者信息，组成相应数据结构并进行编码。
     10. 将编码后的数据流反馈给调用接口。
     11. 验签计算流程

验签计算流程如图10。



1. 验签计算流程
   * 1. 由接口触发验签流程，对验签数据进行解码处理。
     2. 获取签发者证书信息，并判断证书是否过期，如过期，验签失败。
     3. 如果为自签证书，判断待签数据值中是否存在公钥信息，如不存在，验签失败。
     4. 获取待签数据有效时间，并判断时间是否符合要求，如不符合，验签失败。
     5. 分别对签发者证书信息和待签数据信息进行密码杂凑计算，获取其各自的摘要信息。
     6. 对二者的摘要信息进行数据拼接并作为待验签信息。
     7. 获取数据中的签名算法存储结果值，对其进行验签计算，并最终输出验签结果。
   1. 加密消息流程（东软）
      1. 概述

加密算法用于通信双方实现密文通信，实现信息的机密性，加密算法要求用于且不仅限于以下场景：

* 1. 车与车之间需要不允许被窃听的双向通信。
     1. 加密数据结构要求

加密数据要求遵循6.2的数据结构，其中数据类型要求标识为加密数据类型，信息内容要求至少包含如下信息：



1. 加密数据
   1. 对称密钥算法标识：要求描述所使用的对称加密算法，具体描述内容要求由6.5.3定义。
   2. 加密密文数据：要求包含已经加密的密文数据，其对应的明文信息内容要求包含如下信息：
      1. 原始明文数据长度，描述当前明文数据的具体长度值。
      2. 原始明文类型标识，描述当前加密数据中原始明文数据的使用类型标识，要求至少包含：（1）通信消息明文，（2）密钥协商消息明文，两种数据类型标识。
      3. 原始明文数据。
   3. 加密者：要求描述当前加密密文数据的加密者信息，其信息内容至少包含如下信息：
      1. 加密者类型，描述当前加密所使用的方法及类型，决定采用对称加密或者非对称加密中的哪种方式。
      2. 密钥数据值，表示当前加密所使用的具体密钥数据，要求至少满足可以表示如下两种情况：（1）对称密钥值情况，（2）非对称密钥值情况，具体要求如下：
   4. 对称密钥数据要求：



1. 对称加密密钥

至少包含对称密钥类型和对称密钥数据值，其中对称密钥类型要求可以标明当前使用的对称密钥表示方法，其至少包含（1）摘要表示法，（2）明文表示法，两种标识。对称密钥数据值要求根据不同的表示法包含当前密钥信息，当采用摘要表示法时，要求包含摘要算法的识别信息和摘要值。当采用明文表示时，要求包含密钥类型及具体值，同时对称密钥的明文表示方只允许由密文解密后获得。

* 1. 非对称密钥数据要求：



1. 非对称加密密钥

非对称加密密钥要求至少包含（1）非对称密钥算法标识，（2）密钥载体信息，（3）密钥密文数据。其中非对称密钥算法标识要求满足6.5.3章节中的相关规定；密钥载体信息要求至少包含载体类型及载体数据，其载体类型要求至少包含（1）以证书为载体，（2）以消息为载体，（3）以公钥数据本身为载体，三种类型标识；密钥密文数据要求仅用于保存加密后的对称密钥信息。

以上数据ASN.1格式代码参考《GBT XXXXX-XXXX：智能交通 数字证书应用接口规范》第6.3.2.1 章节。

* + 1. 加密解密条件限定
  1. 加密算法需要遵循相应的国际标准。
  2. 在使用对称加密算法时，其对称加密算法要求至少支持AES128-CCM，SM4-CBC。
  3. 在使用非对称加密算法时，其非对称加密算法要求至少支持ECIES、SM2，其中ECIES要求至少支持NIST P-256、brainpoolP256r1两种曲线参数。
  4. 加密模式要求至少包含随机加密模式、协商加密模式两种。
  5. 加密过程中椭圆曲线上的加密点均需要随机生成。
  6. 对称加密的初始化向量值要求每次均随机生成。
     1. 随机加密计算流程

随机加密要求由对称加密和非对称加密组合而成，非对称加密要求加密对称加密的秘钥，而数据则由对称密钥加密。

加密流程如图11所示。



1. 随机加密流程
   * 1. 由接口触发加密流程，组织待加密的明文数据及加密公钥的载体数据。
     2. 对公钥载体数据进行解码处理，获取对应的非对称加密密钥。
     3. 随机生成对称加密密钥及初始化向量作为对称加密参数。
     4. 用初始化向量和对称加密密钥对待加密的明文数据进行对称加密计算。
     5. 对对称加密密钥进行非对称加密计算，获得加密后的对称加密密钥密文数据。
     6. 组织对称加密密钥密文数据，初始化向量，对称加密数据，编码成相应的数据流，反馈给接口。

解密流程如图12所示。



1. 随机解密流程
   * 1. 由接口触发解密流程，对密文数据进行结构化解密操作。
     2. 从解码数据中获取非对称密文数据。
     3. 对非对称密文数据进行解密计算，获取对称加密密钥值。
     4. 从解码数据中获取初始化向量值及对称加密密文数据。
     5. 用初始化向量值和对称加密密钥值对对称加密密文数据进行解密计算，获取明文数据。
     6. 协商加密计算流程

协商加密流程如图13所示。



1. 协商加密流程
   * 1. 由接口触发协商加密流程，从已协商的对称密钥中获取可用的对称加密密钥。
     2. 对获取的对称加密密钥进行摘要计算。
     3. 生成一个随机数作为对称加密的初始化向量。
     4. 用初始化向量，对称加密密钥，对待加密数据进行加密计算，获取加密后的密文数据。
     5. 组织加密后的密文数据，对称加密密钥摘要值，初始化向量值，进行编码计算，将序列化的结果返回给接口。

协商解密流程如图14所示。



1. 协商解密流程
   * 1. 由接口触发协商加密流程，将接收到的据进行反序列化解码，获得对称密钥摘要值。
     2. 根据摘要值在已经协商的对称密钥中查找对应的对称密钥。
     3. 在解码的数据中获取初始化向量值，对称加密密文数据。
     4. 用初始化向量值和对称密钥，对对称加密密文数据进行解密计算，获取最终明文数据。
   1. 密钥协商
      1. 密钥协商综述

密钥协商用于通信者A、B双方共同建立会话密钥，密钥协商要求满足如下要求：

* 1. 密钥协商必须与协商加密流程同时存在。
  2. 协商密钥必须存在时间验证机制保障协商密钥定期更换。
  3. 通信双方必须在协商后保存两个以上协商密钥，保证通信的连续性。
  4. 密钥协商的启动条件必须满足如下条件，连接初始化或者可用密钥数量少于2个。
  5. 密钥协商的过程必须严格满足时间条件，超时或过期的协商过程均认为是失败的协商过程。
  6. 密钥协商的数据必须以密文形式传输，同时密文数据必须进行签名计算确定发起者可信。
     1. 密钥协商数据结构

密钥协商数据要求使用密文数据进行传输，在没有合规的协商密钥时其使用的加密计算流程要求使用随机加密计算流程，在存在合规的协商密钥时其使用的加密计算流程要求使用协商加密计算流程。所使用数据结构要求为加密解密数据结构，其具体数据内容要求包含在加密的信息中，标明其明文数据类型为密钥协商数据，其密钥协商数据要求至少包含表6的内容：



1. 密钥协商
   1. 协商识别号：用于确定当前数据的协商号码。
   2. 协商报文类型：表示当前密钥协商的数据结构类型标识，其中至少包含：
      1. 请求协商响应者证书，
      2. 应答协商响应者证书，
      3. 交换协商值，
      4. 交换确认值，
      5. 交换结果值。
   3. 协商报文数据：用于交换协商双方的具体数据，其中至少包含：
      1. 协商响应者证书，
      2. 协商值，
      3. 确认值，
      4. 结果值。

其中协商值为协商过程中双方的协商数据，其内容至少包含：1）协商使用的算法及参数，2）协商开始的时间及有效时间，3）协商成功的密钥值使用类型4）协商的具体数据5）协商成功后的密钥有效时间等相关内容。确认值用于交换协商的确认数据，判断双方协商密钥结果是否正确。结果值用于通知对方协商是否成功。

* + 1. 密钥协商计算流程

密钥协商计算流程参考附录E。

1. 其他接口安全过程
   1. 网元之间的V2X通信安全过程（华为）

对于网元间的所有接口：

* 1. 除非在其他章节中有明确说明，应使用3GPP TS 33.210中的机制保护信令消息；
  2. 除非在其他章节中有明确说明，应用3GPP TS 33.210中的机制时，可使用3GPP TS 33.310中的证书相关机制。

1. 相同安全域内的两个实体间的接口，3GPP TS33.210不强制通过IPsec机制保护接口安全。
   1. V3接口的安全过程（华为）
      1. 概述

在V2X业务中，V2X设备通过V3接口和V2X控制功能交互。V3接口的安全机制可以使用PC3接口的安全机制（3GPP TS 33.303，第5.3小节）。

* + 1. UICC配置传输的安全流程

V2X设备部署后，UICC上保存的配置参数可能需要更新以反映配置的更改。

当V2X设备的配置数据保存在UICC上时，应使用UICC OTA机制（ETSI TS 102 225[6]、TS 102 226[7]和3GPP TS 31.115[8]、TS 31.116[9]）保护UICC上更新的配置数据的传输。

* + 1. 数据传输的安全流程

本节了定义V2X设备和V2X控制功能之间传输数据的保护流程。

在V2X设备和网络功能之间，对于V2X设备发起的消息：

* 1. 使用V2X设备和ProSe function之间对V2X设备发起消息的保护机制（PSK TLS和GBA，3GPP TS 33.303，5.3.3.2小节）。V2X控制功能完成ProSe功能的作用。可使用BSF和NAF合设的选项。

对于网络发起的消息，应使用下列机制的其中一个：

* 1. 若之前V2X设备发送消息而建立的PSK TLS连接仍然存在，应使用已有的PSK TLS会话；
  2. 否则，应使用V2X设备和网络功能之间的PSK TLS和基于共享密钥交互认证的GBA push安全机制。GBA push在3GPP TS 33.223中定义。网络功能（pushNAF）应从BSF请求USS，网络功能还应检查USS以判断USIM是否授权获取V2X业务。如果网络功能的授权失败，则网络功能应放弃建立通过GBA push方式建立PSK TLS。

1. TLS连接释放后，只能由V2X设备重建。TLS连接依赖于下层的TC连接。
   1. MB2接口的安全过程（33.246）（华为）

应使用3GPP TS 33.246附录N中定义的安全机制。V2X应用服务器作为该机制中GCS AS的角色。

|  |
| --- |
|  |

1. （规范性附录）  
   算法说明
   1. 密码杂凑计算
      1. 概述

在本技术要求中涉及到的密码杂凑计算要求如本章节所示：

* + 1. SHA256算法

该算法存在于数据的签名计算，加密计算，密钥协商计算过程中，具体使用方式由本技术要求的第6.4章节定义，具体计算规则由标准《FIPS PUB 180：Secure Hash Standard (SHS)》定义。

* + 1. SM3算法

该算法存在于数据的签名计算，加密计算，密钥协商计算过程中，具体使用方式由本计算要求的第6.4章节定义，具体计算规则由标准《GM/T 0004：SM3密码杂凑算法》定义。

* 1. 签名计算
     1. ECDSA算法

当签名验签算法采用ECDSA算法时，其采用的密码杂凑算法规定为sha256算法，其具体计算过程由标准《FIPS PUB 186-4：Digital Signature Standard (DSS)》中的第6章节定义，选择的椭圆曲线参数NIST P-256由标准《FIPS PUB 186-4：Digital Signature Standard (DSS)》中的附录D.1.2.3 Curve P-256定义，椭圆曲线参数brainpoolP256r1由标准《RFC 5639：Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation》中的第3.4章节定义。

* + 1. SM2签名算法

当签名验签算法采用SM2算法时，其采用的密码杂凑算法规定为SM3算法，其具体计算过程由标准《GM/T 0003：SM2椭圆曲线公钥密码算法》中的第2部分定义，椭圆曲线参数采用国家密码管理局建议参数。签名用户可辨别表示IDa统一采用字符串“China”，不包括结束符，长度5字节。

* 1. 对称加密计算
     1. AES加密算法

当分组对称加密计算采用AES算法时，其计算过程及算法由标准《FIPS PUB 197：Advanced Encryption Standard》定义。当使用AES计算时，要求使用CCM模式，其计算过程及算法由标准《NIST SP 800-38C》定义。

* + 1. SM4加密算法

当分组对称加密计算采用SM4算法时，其计算过程及算法由标准《GM/T 0002：SM4分组密码算法》定义。其填充模式要求使用填充字节序列的长度（PKCS7Padding）方式。

* 1. 非对称加密计算
     1. ECIES算法

加密算法计算过程遵循标准《IEEE Std 1363a：IEEE Standard Specifications for Public-Key Cryptography—Amendment 1: Additional Techniques》，由标准《IEEE Std 1363a》中的第13章节定义其使用的密钥派生函数，由标准《NIST SP 800-56A, RECOMMENDATION FOR PAIR-WISE KEY ESTABLISHMENT》 的第5.7.1.2章节定义其使用的密钥协商函数，由标准《IEEE 1363a》中的第14.4.1章节定义其使用的消息认证码规则，其采用的密码杂凑算法为SHA256算法。具体参数选取及接口遵循《IEEE Std 1609.2™-2016》的第5.3.5章节。

* + 1. SM2加密算法

加密算法计算过程遵循标准《GM/T 0003：SM2椭圆曲线公钥密码算法》第四部分，其密钥派生函数算法，密码杂凑算法，消息认证码均由标准《GM/T 0003：SM2椭圆曲线公钥密码算法》给出。

* 1. 密钥协商计算
     1. ECDH密钥协商

ECDH密钥协商算法遵循标准《IEEE Std 1363》中的第7.2章节的相关定义。协商的确认值为双方协商后的对称密钥与对端协商信息组合的密码杂凑值。

* + 1. SM2密钥协商

SM2密钥协商算法的计算方法遵循标准《GM/T 0003：SM2椭圆曲线公钥密码算法》第三部分。

|  |
| --- |
|  |

1. （资料性附录）  
   设备授权管理
   1. 授权体系一
      1. 概述

V2X车辆V2X设备授权体系定义了一套授权机制以便将设备权限保存在相应的公钥证书中并颁发给相应设备。设备权限保存在授权机构颁发给各个设备的消息证书中，决定了车联网系统中的V2X车辆、V2X路边站或服务提供商能够发送或接收何种信息。车联网授权体系的构成如图B.1所示，其中与授权相关的实体为：

* 1. 设备生产厂商（Equipment Manufacturer，EM）：负责车联网系统相关设备的生产，如V2X车辆、V2X路边站、后台系统所使用的安全设备等。
  2. 注册机构（Enrollment Authority，EA）：负责V2X设备的认证，设备只有经过相关注册机构的认证才能在系统中使用。车联网系统中注册机构为颁发注册证书的注册CA。
  3. 授权机构（Authorization Authority，AA）：负责V2X设备的授权，设备只有经过相关授权机构的授权才能在系统中播发或接收授权许可的消息。车联网系统中授权机构为颁发安全消息证书的安全消息CA和颁发服务消息证书的服务消息CA。

1. EA可能不存在，但AA一定存在，或者EA和AA可能由同一个部门管理下的不同体系，其可能单独存在也可能合一。

本章B.2节给出了其他授权体系的实现方式作为参考。



图B.1 车联网授权体系的构成及数据流

* + 1. 设备生产厂商

设备厂商负责车联网系统相关设备的生产，如V2X车辆、V2X路边站、后台系统所使用的安全设备等。在生产过程中，可将世界范围内唯一标识该设备的ID（V2X设备International Identity）写入设备。该设备标识在设备的整个生命周期内都不会改变。在生产过程中的安全环境下，原始的设备认证和授权机制被写入设备。随后，通过该认证和授权机制可以将缺省的授信EA和授信AA信息写入设备。

在设备的生产过程中，以下数据将被在安全的环境下写入设备：

* 1. 设备的全球唯一标识；
  2. 缺省颁发的EA公钥证书，通过这些公钥证书，设备可以开始一个注册过程（当EA和AA合设时，针对全球唯一标识颁发的证书将和注册证书合一）；
  3. 缺省颁发的AA公钥证书，通过这些公钥证书，设备可以同其他　V2X设备进行通信；
  4. 针对全球唯一标识颁发的证书及其证书链（可选）。
     1. 设备注册机构

EA负责V2X设备的认证，设备只有经过相关EA的认证才能在系统中使用。EA首先验证一个V2X设备是否合法的，然后为合法的设备颁发注册证书。注册证书后续用来申请消息证书。

注册证书的主要内容为：

* 1. 设备临时标识，用以保护用户的隐私；
  2. 权限许可描述，用以限定设备可被授予的最大权限；
  3. 应用区域描述，用以限定设备的最大应用地理区域。

注册机构的主要应用特点是：

* 1. 设备可以注册到多个不同的EA；
  2. 允许多级EA体系，高级EA可授权给低级EA为设备颁发证书；
  3. EA可要求设备定期进行重注册。
     1. 设备授权机构

AA负责V2X设备的授权，设备只有经过相关AA的授权才能在系统中播发或接收授权许可的消息。AA首先验证颁发给设备的注册证书的有效性，然后为合法的设备颁发消息证书，即安全消息证书或服务消息证书。

消息证书的主要内容为：

* 1. 权限许可描述，以限定设备可发送的安全消息类别；
  2. 权限及优先级描述，以限定设备可发送的服务消息类别及其优先级；
  3. 应用区域描述，以限定该设备的应用地理区域。

AA的主要应用特点是：

* 1. 可接收来自多个EA的注册证书，此时证书的适用范围为各证书许可的交集；
  2. 允许多级AA体系，高级AA可授权给低级AA为设备颁发证书；
  3. 设备可注册至多个不同的AA；
  4. 授权机构可要求设备定期进行重授权。
     1. 根CA

所颁发的管理类证书或通信类证书及颁发这些证书的CA证书将构成一个证书层级体系。该证书体系中的信任关系将汇聚至一个最终的信任节点，即根证书。为验证一个消息的有效性，设备必须访问根证书。根证书必须以安全的方式写入设备中。

* + 1. 典型授权过程
       1. 概述

一个典型的设备注册与授权过程如图B.2所示。该过程可分概括为如下三步：

* + 1. 设备生产商在设备的生产过程中写入各种设备初始化数据，如设备ID和缺省颁发的用于设备注册或授权的公钥证书。
    2. 根据设备提出的注册申请，EA为设备颁发注册证书。
    3. 根据设备提出的授权申请，AA为设备颁发消息证书。



图B.2设备注册与授权过程

* + - 1. 设备生产过程

设备的初始化过程由设备制造厂商完成。设备制造厂商在安全的环境下对设备中与安全相关的内容进行初始化操作。设备初始化操作的主要内容为：

* 1. 写入可在世界范围内唯一标识该设备的ID，该值在设备的整个生命周期内都不会改变。
  2. 写入缺省的授信EA和授信AA的公钥证书。
  3. 写入缺省颁发的注册证书和消息证书。缺省颁发注册证书将用于申请正式的注册证书；缺省颁发的消息证书可用于发送或接收某些交通安全信息。
     + 1. 设备注册过程

设备注册的主要功能为验证设备的合法性和有效性，并为合法和有效的设备颁发相应的认证公钥证书。V2X设备的注册过程由设备发起，其通过V2X设备与EA之间的交互接口向EA发送注册请求。EA评价V2X设备的请求，并决定是否接受V2X设备的注册请求；若接受则向V2X设备颁发相应的注册证书，并将颁发的证书通过注册应答消息发送给V2X设备；若拒绝则通过注册应答消息将拒绝的原因发送给V2X设备。设备注册过程如图B.3所示，其具体过程为：

1. V2X设备生成一个“注册请求签名消息”，注册请求的主要内容见表B.1，具体过程为：
   * 1. V2X设备生成一个“待签注册请求”；
     2. V2X设备选择一个EA识别的注册证书，并用与之匹配的私钥对待签请求进行签名，从而生成一个“注册请求签名消息”。
2. V2X设备对“注册请求签名消息”进行加密，从而生成一个“签名加密消息”，具体过程为：
   * 1. V2X设备随机生成一个对称密钥，并利用该密钥加密“注册请求签名消息”；
     2. V2X设备利用EA公钥证书中的公钥加密随机生成的对称密钥；
     3. V2X设备生成一个“签名加密消息”。
3. V2X设备将生成的“签名加密消息”发送给EA。
4. EA解密并验证“签名加密消息”，具体过程为：
   * 1. EA用私钥解密加密密钥，进而用加密密钥解密收到的“签名加密消息”，从而获得“签名消息”；
     2. EA首先验证“签名消息”中签名证书的有效性，然后利用证书中的公钥验证消息签名的正确性。
5. EA根据注册请求中的内容签发相应的公钥证书。
6. EA生成一个“加密注册应答”，注册成功时注册应答的主要内容见表B.2，注册失败时注册应答的主要内容见表B.3，具体过程为：
   * 1. EA随机生成一个对称密钥，并利用该密钥加密“注册应答”；
     2. EA利用V2X设备注册请求公钥证书中的公钥加密随机生成的对称密钥；
     3. EA生成一个“加密消息”。
7. EA将生成的加密消息发送给V2X设备。
8. V2X设备解密注册应答并验证注册成功时收到的注册证书，具体过程为：
   * 1. V2X设备用私钥解密加密密钥，进而用加密密钥解密收到的“加密消息”；
     2. 注册成功时验证签发的注册证书，注册失败时验证签名消息。



图B.3设备注册过程

表 B.1注册请求的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| 申请者信息 | 签署注册申请的证书或证书链 |
| 申请证书的类型 | 注册证书 |
| 申请证书的有效期 |  |
| 申请权限描述 |  |
| 申请地理区域描述 |  |
| 公钥值 | 新申请注册证书中的公钥值 |
| 签名值 | 利用与签署注册申请证书匹配的私钥签名 |

表B.2注册成功应答的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| EA签发的公钥证书及证书链 |  |
| 证书撤销列表（CRL）路径 | 验证新签发公钥证书是否撤销的证书撤销列表（CRL）的路径 |

表B.3注册失败应答的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| 证书颁发者信息（签名者） | 签署注册应答的注册机构的证书或证书链 |
| 错误代码 |  |
| 签名值 |  |

* + - 1. 设备授权过程

设备授权的主要功能是向合法设备颁发含有授权信息的公钥证书（消息证书）。设备的授权过程由V2X设备发起，其通过V2X设备与AA之间的交互接口向AA发送授权请求。AA评价V2X设备的请求，并决定是否接受V2X设备的授权请求；若接受则向V2X设备颁发相应的消息证书，并将颁发的证书通过授权应答消息发送给V2X设备；若拒绝则通过授权应答消息将拒绝的原因发送给V2X设备。设备授权过程如图B.4所示，其具体过程为：

1. V2X设备生成一个“授权请求签名消息”，授权请求的主要内容见表B.4，具体过程为：
   * 1. V2X设备生成一个“待签授权请求”；
     2. V2X设备选择一个AA识别的注册证书，并用与之匹配的私钥对待签请求进行签名，从而生成一个“授权请求签名消息”。
2. V2X设备对“授权请求签名消息”进行加密，从而生成一个“签名加密消息”，具体过程为：
   * 1. V2X设备随机生成一个对称密钥，并利用该密钥加密“授权请求签名消息”；
     2. V2X设备利用AA公钥证书中的公钥加密随机生成的对称密钥；
     3. V2X设备生成一个“签名加密消息”。
3. V2X设备将生成的“签名加密消息”发送给AA。
4. AA解密并验证“签名加密消息”，具体过程为：
   * 1. AA用私钥解密加密密钥，进而用加密密钥解密收到的“签名加密消息”，从而获得“签名消息”；
     2. AA首先验证“签名消息”中签名证书的有效性，然后利用证书中的公钥验证消息签名的正确性。
5. AA根据授权请求中的内容签发相应的公钥证书（消息证书）。
6. AA生成一个“加密授权应答”，授权成功时授权应答的主要内容见表B.5，授权失败时授权应答的主要内容见表B.6，具体过程为：
   * 1. AA随机生成一个对称密钥，并利用该密钥加密“授权应答”；
     2. AA利用V2X设备授权请求公钥证书中的公钥加密随机生成的对称密钥；
     3. AA生成一个“加密消息”。
7. AA将生成的加密消息发送给V2X设备。
8. V2X设备解密并验证授权应答，具体过程为：
   * 1. V2X设备用私钥解密加密密钥，进而用加密密钥解密收到的“加密消息”；
     2. 注册成功时验证签发的消息证书，注册失败时验证签名消息。



图B.4设备授权详细过程

表B.4授权请求的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| 申请者信息 | 签署授权申请的证书或证书链 |
| 申请证书的类型 | 消息证书，如消息安全证书 |
| 申请证书的有效期 |  |
| 申请权限描述 |  |
| 申请地理区域描述 |  |
| 公钥值 | 新申请消息证书中的公钥值 |
| 签名值 | 利用与签署授权申请证书匹配的私钥签名 |

表B.5 授权成功应答的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| 证书颁发者信息 |  |
| AA签发的公钥证书及证书链 |  |
| 证书撤销列表（CRL）路径 | 验证新签发公钥证书是否撤销的证书撤销列表（CRL）的路径 |

表B.6 授权失败应答的主要内容

|  |  |
| --- | --- |
| 内容 | 说明 |
| 证书颁发者信息（签名者） | 签署授权应答的授权机构的证书或证书链 |
| 错误代码 |  |
| 签名值 |  |

* 1. 授权体系二
     1. V2X车辆授权

图B.5所示的是V2X车辆的授权实现，其具体过程为：

* + 1. 不同制造工厂可通过统一的工厂管理部门以安全方式向注册机构提供所生产的V2X车辆信息，同时在V2X车辆生产过程中将包括设备ID等在内的信息写入设备中；
    2. V2X车辆在向EA发起注册过程中，EA在确认V2X车辆身份信息正确后，将可用于向AA交互以获得安全消息证书的信任状下发至V2X车辆；
    3. V2X车辆利用注册证书或获得的信任状与AA交互，以便申请或更新安全消息证书，在AA完成对信任状的确认之后向V2X车辆颁发安全消息证书，并保存信任状与安全消息证书间的对应关系。

这里，EA和AA可能是同一个部门管理下的不同体系或者由不同部门管理，则V2X车辆需分别与EA和AA交互；或者EA和AA是合一的，则图中的步骤2和步骤3将合并执行。此外，V2X车辆可向多个AA请求安全消息证书，只需通过重复上述过程向其他AA请求安全消息证书。



图B.5 V2X车辆授权体系

* + 1. V2X路边站授权

V2X路边站授权体系可参考B.2.1方式实现。

图B.6给出了另一种V2X路边站授权体系，其具体过程为：

* + 1. EA及AA以安全方式向工厂管理部门提供待下发给V2X路边站的安全消息证书；
    2. 制造工厂在生产V2X路边站时将工厂管理部门获得的信任状写入V2X路边站中。

这里，AA也可以选择不将信任状事先提供给工厂管理部门，则V2X路边站后续需要通过B.2.1相应的方式向AA申请安全消息证书。



图B.6 V2X路边站授权体系

图B.7给出了又一种V2X路边站授权体系，其具体过程为：

* + 1. V2X路边站随机生成一对或多对公私钥，并将公钥通过工厂管理部门以安全的方式分别发送给EA和AA；
    2. EA和AA分别对收到的公钥签发相应的公钥证书，并通过工厂管理部门下发给V2X路边站。

这里，V2X路边站也可以选择不将公钥发给AA，则后续需要通过B.2.1相应的方式向AA申请安全消息证书。



图B.7 V2X路边站授权体系

|  |
| --- |
|  |

1. （资料性附录）  
   公钥证书管理
   1. 概述

根据公钥证书应用领域的不同可将证书分为通信类证书和管理类证书两大类，车联网公钥证书的分类如图C.1所示。

通信类证书用于V2X设备之间通信时对通信内容进行数字签名时所使用的证书。这些证书分为安全消息证书和服务消息证书，又可以统称为消息证书。

* 1. 安全消息证书：是颁发给V2X车辆和V2X路边站用于对通信内容进行数字签名的证书。例如V2X车辆利用安全消息证书对其播发的包含有车辆行驶信息的主动安全消息进行数字签名，V2X路边站利用安全消息证书对其播发的红绿灯状态信息或道路交通状态信息进行数字签名。根据其适用范围，安全消息证书又可分为全局安全消息证书和区域安全消息证书。全局安全消息证书的适用范围未做规定，例如颁发给V2X车辆的用于对主动安全消息进行数字签名的证书；区域安全消息证书的适用范围由证书中的地理区域描述域规定，例如颁发给红绿灯等路侧设备的用于对其播发的消息进行数字签名的证书。
  2. 服务消息证书：是颁发给信息服务提供商的用于对播发内容进行数字签名的证书，例如信息服务商对其通过V2X路边站播发的与本地天气，餐饮，住宿，购物，旅游等相关的广告消息进行数字签名。

管理类证书用于V2X设备向CA请求证书或CA向V2X设备颁发证书。管理类证书由注册证书、证书申请证书和CA证书组成，他们的用途是：

* 1. 注册证书：是颁发给V2X设备的用于向CA证明其身份，以便申请其他证书的证书。注册证书为设备的入网证明。一个设备首先需要获得注册证书，然后才能基于该证书申请其他与车联网应用相关的各种证书。
  2. 证书申请证书：由AA颁发给设备，后者利用其申请可签署消息的消息证书。证书申请证书用于申请和更新实际用于签发各种通信消息的消息证书。
  3. CA证书：是根CA颁发给自己或下级CA的证书，以及下级CA颁发给更下一级CA的证书。CA利用CA证书签发证书或证书撤销列表。



图C.1公钥证书的分类

车联网系统公钥证书体系中CA种类的设置及其颁发的证书如图C.2所示。它们是：

* 1. 根CA：负责颁发车联网系统里所用到的各种证书和证书撤销列表，包括向其他子CA颁发的CA证书。
  2. 注册CA：负责颁发注册证书和注册证书撤销列表。
  3. 安全消息CA：负责颁发安全消息证书申请证书、安全消息证书和证书撤销列表。
  4. 服务消息CA：负责颁发服务消息证书申请证书、服务消息证书和证书撤销列表。



图C.2 CA及其颁发的公钥证书

如果使用在线方式申请证书时，车联网系统公钥证书的申请及使用过程可分为如下四个步骤：

* + 1. V2X设备经EA的认证后获得EA颁发的注册证书。
    2. V2X设备利用注册证书向AA申请证书申请证书。
    3. V2X设备利用证书申请证书向AA申请消息证书。
    4. V2X设备利用消息证书签发相应的消息。

某些情况下，上述机构可能合设，则此时相应的证书也将合一（如，EA和AA合设时，注册证书和证书申请证书将合一）。

证书根据其类别还可能包含如下信息：

* 1. 主题类型：描述证书的类别，例如，根CA证书，注册CA证书，授权CA证书，或消息证书等。
  2. 主题类型描述：规定了CA所能颁发证书的类型。CA不能颁发超出该主题类型描述中所规定的证书种类。
  3. 安全消息权限描述：规定了CA颁发的安全消息证书所能拥有的最大权限。CA签发的安全消息证书不能超出这些安全消息权限描述所规定的范围。
  4. 服务消息权限描述：规定了CA颁发的服务消息证书所能拥有的最大权限及其最高优先级。CA签发的服务消息证书不能超出这些服务消息权限描述所规定的范围。
  5. 地理区域描述：描述了该CA颁发证书的最大地理应用区域。CA签发证书中的地理应用区域描述范围不能超出该地理区域描述所规定的区域。

本规范所定义的各类证书中应包含如下信息：

* 1. 根CA证书应包含：主题类型，主题类型描述，安全消息权限描述，服务消息权限描述，地理区域描述。
  2. 注册CA证书应包含：主题类型，主题类型描述，安全消息权限描述，服务消息权限描述，地理区域描述。
  3. 安全消息CA证书应包含：主题类型，主题类型描述，安全消息权限描述，地理区域描述。
  4. 服务消息CA证书应包含：主题类型，主题类型描述，服务消息权限描述，地理区域描述。
  5. 安全消息证书应包含：主题类型，主题类型描述，消息权限描述，地理区域描述。
  6. 服务消息证书应包含：主题类型，消息权限描述，地理区域描述。
  7. 公钥证书体系

车联网系统中的CA依据其完成的具体功能可以分为3类：注册CA，安全消息CA和服务消息CA。车联网系统可以根据行政管理的特点和车联网系统的实际需要采用一个证书体系，也即注册证书体系，安全消息证书体系和服务消息证书体系拥有共同的根CA。车联网系统也可以采用多个独立的证书体系，通过CA交叉认证技术实现互操作。例如，注册证书体系，安全消息证书体系和服务消息证书体系分别拥有各自的根CA，然后通过将不同证书体系中的CA证书安全地配置到需要互操作的设备中，从而实现这些证书体系的互操作。

* 1. 公钥证书管理
     1. 注册证书管理
        1. 注册证书产生

注册CA证书颁发给注册CA。注册CA可以是最高级CA，也可以是子CA。若注册CA是最高级CA，则其证书是自签发的，那么它需要被安全地传送到需要它的每个设备中并且存储在安全存储区中；若注册CA是子CA，那么它就可以按普通证书那样管理，即不必传送到每个需要它的设备中。注册CA证书中规定了该CA所能颁发证书的最大权限。

设备注册证书由注册CA颁发给设备。设备首先产生密钥对，然后向注册CA申请注册证书。注册CA首先对设备进行验证，然后为其颁发相应的证书，并在安全的环境下将该证书写入设备中。注册证书中规定了该设备所能拥有的最大权限。当设备通过LTE网络与注册CA连接时建议支持安全传输机制，如https等。

* + - 1. 注册证书更新

在旧的注册CA证书到期之前，注册证书应该更新。若注册CA为根CA，则证书更新重复注册证书第一次产生时的操作，即产生新的自签名证书。若注册CA为子CA，则证书的更新有两种方式。一种是重复注册证书第一次产生时的操作；另一种是利用即将到期的注册证书向上一级证书颁发机构申请新的证书。这种更新需要在旧证书过期前完成。

在旧的注册证书到期之前，注册证书应该更新。注册证书的更新有两种方式。一种是重复注册证书产生时的操作；另一种是利用即将到期的注册证书向注册CA申请新的证书。这种更新需要在旧证书过期前完成。

* + - 1. 注册证书撤销

若注册CA密钥对受到损害，则该注册CA的证书需要被撤销，同时由此CA签发的旧证书也应该停止使用，而且还要在相应的CRL中列出这些被撤销的证书。若注册证书是自签发的，就应该从每个使用它的设备中将其移除。CRL列表应采用适当的方法通知给使用这些证书但不能实时联网检测相应CRL列表的设备，如V2X车辆。

若设备注册证书的密钥对受到损害，则该注册证书需要被停止使用，并且还要在相应的CRL中列出被撤销的证书。

* + 1. 证书申请证书管理
       1. 证书申请证书产生

证书申请证书包括安全消息证书申请证书和服务消息证书申请证书，证书申请证书由AA颁发给设备用于申请相应的消息证书。证书申请过程由设备发起，设备首先生成密钥对，然后利用其注册证书向AA申请相应的证书申请证书。AA首先验证设备的注册证书，然后根据本地的授权策略向申请设备颁发证书申请证书。证书申请证书中规定了该设备在该AA所能申请的最大权限。当设备通过LTE网络与授权机构连接时建议支持安全传输机制，如https等。

* + - 1. 证书申请证书更新

在旧的证书申请证书到期之前，证书申请证书应该更新。证书申请证书的更新是重复证书申请证书产生时的操作。这种更新需要在旧证书过期前完成。

* + - 1. 证书申请证书撤销

若设备证书申请证书的密钥对受到损害，则该证书申请证书需要被停止使用，并且还要在相应的CRL中列出被撤销的证书。或者被撤销的证书由相应的机构秘密保存，仅在被设备用来申请消息证书时验证其合法性。

* + 1. 消息证书的管理
       1. 消息证书产生

消息证书包括安全消息证书和服务消息证书，消息证书由AA颁发给设备。证书申请过程由设备发起，设备首先生成密钥对，然后利用其证书申请证书向AA申请相应的消息证书。AA首先验证设备的证书申请证书，然后根据本地的授权策略向申请设备颁发消息证书。消息证书中规定了该设备所能执行权限。当设备通过LTE网络与授权机构连接时建议支持安全传输机制，如https等。

* + - 1. 消息证书更新

在旧的消息证书到期之前，消息证书应该更新。消息证书的更新是重复消息证书产生时的操作。这种更新需要在旧证书过期前完成。

* + - 1. 消息证书撤销

若设备消息证书的密钥对受到损害，则消息证书需要被停止使用，并且还要在相应的CRL中列出被撤销的证书。CRL列表应采用适当的方法通知给使用这些证书但不能实时联网检测相应CRL列表的设备，如V2X车辆。或者，由于消息证书通常生命周期比较短，也可以不使用CRL的模式撤销，而使用被动的撤销模式。

* 1. 设备特权管理
     1. 设备特权管理概述

车联网系统中发送或接收消息的设备有V2X车辆、V2X路边站和服务提供商。

车联网系统中播发的消息有两种：

* 1. 安全消息：用于V2X车辆或V2X路边站向周围播发与交通安全相关的广播信息。
  2. 服务消息：用于服务提供商通过V2X路边站向周围播发各种服务广告信息。

V2X设备能够发送或接收什么消息由所拥有的特权决定。设备特权主要由以下四个要素描述：

* 1. 消息类别：消息类别为车联网系统中安全或服务消息的标识，设备根据该标识可确定应该发送或接收什么消息。
  2. 有效时间：有效时间规定了设备能够发送或接收消息的时间范围，有效时间由消息证书的有效期决定。
  3. 有效地理区域：有效地理区域规定了设备能够发送或接收消息的地理区域，有效地理区域由消息证书的有效期决定。
  4. 优先级：优先级决定了设备处理多条服务消息的先后顺序。

描述安全消息的特权要素有：

* 1. 消息类别，
  2. 有效时间，
  3. 有效地理区域。

描述服务消息的特权要素有：

* 1. 消息类别，
  2. 有效时间，
  3. 有效地理区域，
  4. 优先级。

V2X设备的特权管理是通过控制设备所能发送或接收的消息来实现的。设备的特权由AA决定，并且以消息证书的形式授予相关设备。其中V2X车辆的特权存储在安全消息证书中，服务提供商的特权存储在服务消息证书中。车联网系统通过CA证书、注册证书、证书请求证书和消息证书四个层次来实现特权管理。以下各节分别从证书的颁发和应用角度描述车联网特权管理和控制机制。

* + 1. 证书颁发中的特权管理
       1. CA颁发证书中的特权管理

CA负责颁发车联网系统中所用到的各种证书和证书撤销列表。根CA可将其特权分发给各种子CA以代替其完成某些证书或撤销列表的颁发工作。子CA亦可将其特权分发给更下一级的子CA以代替其完成某些证书或证书撤销列表的颁发工作。CA证书描述了该CA所能颁发证书的种类及限制条件。CA证书中与特权管理相关的信息有：

* 1. 证书有效期：CA所颁发证书的有效期不能超出CA证书的有效期；
  2. 主题类型描述：其中规定了CA所能颁发证书的类型，该CA不能颁发超出该主题类型描述中所规定的证书种类；
  3. 安全消息特权描述：若安全消息特权描述为空，则该CA所能签发的安全消息许可证书没有限制；若安全消息特权描述不为空，则该CA签发的安全消息证书不能超出这些安全消息特权描述所规定的范围；
  4. 服务消息特权描述：若服务消息特权描述为空，则该CA所能签发的服务消息许可证书没有限制；若服务消息特权描述不为空，则该CA签发的服务消息证书不能超出这些服务消息特权描述所规定的范围，且这些服务消息的优先级不能高于对应许可中的优先级；
  5. 地理区域描述：若地理区域描述域的值为“none”，则该CA证书的应用没有区域限制，并且可为任意地理区域签发证书；若该域不为空，者该CA所签发证书的应用范围不能超出该地理区域描述所规定的区域。

车联网系统颁发给设备的证书有注册证书、安全消息证书申请证书、服务消息证书申请证书、安全消息证书和服务消息证书。据此，CA的种类可细分为：根CA、注册CA、安全消息CA、服务消息CA。这些CA及其颁发的证书和特权描述如表C.1所示。

表C.1 CA及其颁发的证书和特权描述

|  |  |  |
| --- | --- | --- |
| 子CA | 颁发的证书 | 特权描述 |
| 根CA | 注册证书  安全消息证书申请证书  服务消息证书申请证书  安全消息证书  服务消息证书  证书撤销列表 | 证书有效期  主题类型描述  特权描述  特权及优先级描述  地理区域描述 |
| 注册CA | 注册证书  证书撤销列表 | 证书有效期  主题类型描述  特权描述  特权及优先级描述  地理区域描述 |
| 安全消息CA | 安全消息证书申请证书  安全消息证书  证书撤销列表 | 证书有效期  主题类型描述  特权描述  地理区域描述 |
| 服务消息CA | 服务消息证书申请证书  服务消息证书  证书撤销列表 | 证书有效期  特权及优先级描述  地理区域描述 |

根CA可将其特权分发给各种子CA，子CA又可将其特权分发给更下一级的子CA。在这种特权的分发过程中，CA所颁发的证书种类及其特权都不能超出其CA证书中描述特权的范围。

车联网系统中CA的设置可以有多种方案，如单根CA方案或多根CA方案。在多根CA方案中即可采用注册根CA与授权根CA不同，也可采用注册根CA、安全消息根CA和服务消息根CA均不同的方案。

* + - 1. 证书申请过程中的特权管理

用于申请证书的证书分为注册证书和消息证书申请证书两类，其中注册证书用于申请消息证书申请证书。消息证书的颁发分两步：第一步是AA根据注册证书向设备颁发消息证书申请证书，第二步是AA根据消息证书申请证书向设备颁发可用于签发消息的消息证书。消息证书申请证书又分为安全消息证书申请证书和服务消息证书申请证书，它们分别用于申请安全消息证书和服务消息证书。证书申请证书的颁发者、特权描述和用途如表C.2所示。

表C.2 证书申请证书的颁发者、特权描述和用途

|  |  |  |  |
| --- | --- | --- | --- |
| 子CA | 证书颁发者 | 特权描述 | 用途 |
| 注册证书 | 注册CA | 证书有效期  主题类型描述  特权描述  特权及优先级描述  地理区域描述 | 用于设备签署向授权机构申请消息申请证书的请求。 |
| 安全消息证书申请证书 | 安全消息CA | 证书有效期  主题类型描述  特权描述  地理区域描述 | 用于设备签署向授权机构申请安全消息证书的请求。 |
| 服务消息证书申请证书 | 服务消息CA | 证书有效期  特权及优先级描述  地理区域描述 | 用于设备签署向授权机构申请服务消息证书的请求。 |

表C.2中特权描述项在相应证书颁发过程中的具体应用为：

* 1. 设备所申请证书的有效期不能超出证书申请证书的有效期。
  2. 安全消息证书申请证书主题类型描述域不能为空，设备申请的证书必须符合证书申请证书中所列的主题类型。
  3. 设备申请的安全消息证书不能超出安全消息证书申请证书中所列的特权。
  4. 设备申请的服务消息证书不能超出服务消息证书申请证书中所列的特权和优先级。
  5. 设备申请的证书中的地理区域描述不能超出证书申请证书中所列的区域。
     1. 消息证书中的特权管理
        1. 全局安全消息证书中的特权管理

全局安全消息的发布特权保存在全局安全消息证书中，安全消息证书中与特权相关的数据域有：

* 1. 证书有效期
  2. 特权描述
  3. 全局安全消息证书在消息发布过程中的具体应用为：
  4. 设备只能在证书有效期内发布特权描述域中规定的安全消息；
  5. 全局安全消息证书的应用没有地域限制。
     + 1. 局部安全消息证书中的特权管理

局部安全消息的发布特权保存在局部安全消息证书中，安全消息证书中与特权相关的数据域有：

* 1. 证书有效期
  2. 特权描述
  3. 地域限制描述

局部安全消息证书在消息发布过程中的具体应用为：

* 1. 设备只能在证书有效期内发布特权描述域中规定的安全消息；
  2. 局部安全消息证书的应用有地域限制，设备只能在地域限制描述中所规定的区域内发布消息。
     + 1. 服务消息证书中的特权管理

授予服务提供商发布消息的特权保存在服务消息证书中，服务消息证书中与特权相关的数据域有：

* 1. 证书有效期
  2. 特权及优先级描述
  3. 地域限制描述

服务消息证书在消息发布过程中的具体应用为：

* 1. 设备只能在证书有效期内发布特权描述域中规定的服务消息，并且赋予消息的优先级不能大于证书中所规定的值；
  2. 服务消息证书的应用有地域限制，设备只能在地域限制描述中所规定的区域内发布消息。
     + 1. V2X车辆特权管理

根据地方法律的规定，车辆在道路上行驶的优先级是不同的，如公共汽车或校车的通行优先级高于普通车辆，而消防车或救护车又具有更高的通行优先级。但这些有特殊通行优先权的车辆在非执行公务时又应被视为普通车辆。为适应这种应用情况，这些拥有特殊通行权的车辆应被授予多张证书。车辆在不同应用场景使用不同的安全消息证书播发消息。当车辆使用这些特殊证书播发消息时，其他车辆会获知这些特殊车辆的存在，从而为其让开行驶道路。

V2X车辆播发消息的类型由颁发给该设备的安全消息证书中的特权描述域决定。在V2X车辆同时拥有多个安全消息证书时，其所拥有的特权将是这些证书所授特权的集合。

这些颁发给V2X设备的安全消息证书只有处于激活状态才能用来播发消息。颁发给所有车辆的普通消息证书将一直处于激活状态，其他证书将由应用系统决定是否处于激活状态。播发消息时，V2X车辆将选择当前处于激活状态的且具有最高通行优先级的证书播发安全消息。

* + - 1. V2X路边站特权管理

V2X路边站完成的功能可分为三大类：

* 1. 安全消息广播，例如，广播限速信息，广播道路维护信息，广播红绿灯信息等；
  2. 服务消息广播，例如，广播交通信息，广播本地服务信息，数据发布等；
  3. 交通数据收集，例如，交通流量的监控，交通违法监控等。

在车联网系统中，只有被授予了安全消息证书的V2X路边站才能播发证书特权描述域中所规定的消息。当V2X路边站可以播发多种安全消息时，这些特权既可以放在一张证书中，也可以放在不同的证书中。

V2X路边站播发消息的类型由颁发给该设备的安全消息证书中的特权描述域决定。在V2X路边站同时拥有多个安全消息证书时，其所拥有的特权将是这些证书所授特权的集合。

|  |
| --- |
|  |

1. （资料性附录）  
   安全相关AID值分配建议

根据标准《合作式智能运输系统 专用短程通信 第3部分：网络层和应用层规范》中第5.2.3章节及附录B的资料，建议将AID取值0xa000-0xa7ff共2048个AID值作为安全专用功能。其具体功能定义如下：

|  |  |  |
| --- | --- | --- |
| AID 取值 | 类型名称 | 描述 |
| 0xa000（40960） | 安全功能预留 | 预留 |
| 0xa001（40961） | 通用注册证书申请 | 用于标识设备第一次申请注册证书的数据结构 |
| 0xa002（40962） | 通用注册证书应答 | 用于标识设备申请的注册证书应答数据结构 |
| 0xa003（40963） | 通用非注册证书申请 | 用于标识设备申请非注册类证书的数据结构 |
| 0xa004（40964） | 通用非注册证书应答 | 用于标识设备申请非注册类证书的数据结构 |
| 0xa100（41216） | 证书吊销列表 | 用于标识当前数据为证书吊销列表数据结构 |
| 0xa200（41472） | 密钥协商 | 用于标识当前报文结构为密钥协商类数据 |

|  |
| --- |
|  |

1. （资料性附录）  
   密钥协商计算流程

密钥协商计算流程如图15所示。



图E.1 密钥协商流程

* + 1. 协商发起者A通过随机生成函数生成一个基于椭圆曲线参数的公私钥对Ra，ra。
    2. 协商发起者A将该随机的公钥Ra信息通过签名过程发送给协商接收者B。
    3. 协商接收者B通过随机生成函数同样生成一个基于椭圆曲线参数的公私钥对Rb，rb。
    4. 协商接收者B将随机公钥Rb信息通过随机加密过程对数据加密并发送给协商发起者A。
    5. 协商发起者A及接收者B通过密钥协商算法利用自身生成的私钥和对方的公钥进行密钥协商计算，获得协商密钥K1及K2，其计算规则及算法满足加解密条件限定中的规则。
    6. 协商接收者B在密钥协商计算完毕后，将对应的密钥与公钥组合的数据的密码杂凑结果值S2发送给协商发起者A。
    7. 协商接发起者A在接收到协商接收者计算的密码杂凑结果S2值后，判断协商结果，并且返馈给协商接收者B，如果正确则反馈给协商接收者B自身计算的密码杂凑结果值S1。
    8. 协商接收者B在接收到结果值S1后，与自身密码杂凑值进行判断确定最终结果。并将最终协商结果发送给协商发送者A。

1. 协商发起者A的协商值报文必须带有加密公钥，协商接收者B反馈的协商值报文必须带有加密公钥，协商双方在协商过程中使用的加密计算均使用对端协商值报文中的加密公钥。协商接收者B要求拥有拒绝协商请求的能力。

|  |
| --- |
|  |

1. （资料性附录）  
   证书请求及应答
   1. 证书请求结构

该附录定义了证书请求内包含数据的具体结构。

CertRequest ::= SEQUENCE {

version Uint8,

currentTime Time32,

tbsCertData TbsCert,

encryptionKey PublicEncryptionKey OPTIONAL

}

version ：证书请求版本号。Uint8定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。

Time32：当前请求时间。Time32定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。

tbsCertData：证书请求的具体内容。TbsCert定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。

encryptionKey:证书请求应答加密公钥，PublicEncryptionKey定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。当该项存在时，其返回的证书请求应答为加密数据。

* 1. 注册证书
     1. 注册证书请求数据格式

注册证书是终端的第一个证书，其申请采用自签名模式，注册证书请求的数据格式为SecureMessage结构，其具体定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。数据具体构成如下：

EnrollmentCertRequestData ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS {

self

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(40961),

hashAlg PRESENT,

genTime PRESENT,

expiryTime ABSENT,

digest ABSENT,

encKey ABSENT

}),

data(CONTAINING CertRequest(WITH COMPONENTS { ...,

version(2),

tbsData(WITH COMPONENTS { ...,

subjectAttributes(WITH COMPONENTS { ...,

assuranceLevel ABSENT,

itsAidList ABSENT,

itsAidSspList ABSENT

}),

validityRestrictions(WITH COMPONENTS { ...,

region PRESENT

})

}),

encryptionKey PRESENT

})),

extHash ABSENT

})

})

})

})

在生成注册证书请求时，申请者共生成两对公私钥，签名公私钥和加密公私钥，签名公私钥使用方法参考附录C.3.1.1章节，加密公钥用于加密由证书系统反馈生成的注册证书数据，私钥用于解密注册证书数据，注册证书请求生成过程及数据组织计算方法如下：



* + 1. 注册证书应答数据格式

注册证书应答的数据文件名称为其证书请求的哈希值，格式为SecureMessage结构，其具体定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。数据具体构成如下：

EnrollmentCertResp ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS {

certificate(SequenceOfCertificate(SIZE(1)))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(40962),

hashAlg PRESENT,

genTime PRESENT,

expiryTime ABSENT,

digest ABSENT,

encKey ABSENT

}),

data(CONTAINING EnrollmentCertRespData),

extHash ABSENT

})

})

})

})

EnrollmentCertRespData ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

encData(WITH COMPONENTS { ...,

recipients(SequenceOfRecipientInfo (SIZE(1)) (CONSTRAINED BY {

RecipientInfo(WITH COMPONENTS {

signedDataRecipInfo

})

}))

})

})

})

CA在颁发证书后，使用注册证书请求中的EnrollmentCertRequestData->payload->signedData->tbs->data(CertRequest)->encryptionKey对颁发的证书进行随机加密计算，根据证书请求EnrollmentCertRequestData->payload->signedData->tbs->data(CertRequest)中的CertRequest数据的OER编码做HashID8计算并对EnrollmentCertRespData->payload->encData->recipients->signedDataRecipInfo->recipientId赋值，终端在做EnrollmentCertResp数据验签后，获取其EnrollmentCertRespData数据并对其中的EnrollmentCertRespData->payload->encData->cipherText解密，获取最终的注册证书数据。

* 1. 非注册证书
     1. 非注册证书请求数据格式

非注册证书的申请是通过已授权证书实现的，其数据为SecureMessage嵌套结构，其外部为SecureMessage签名，内部为SecureMessage加密，其具体定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。数据具体构成如下：

NormalCertRequestSign ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS {

SequenceOfCertificate(SIZE(1))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(40963),

hashAlg PRESENT,

genTime PRESENT,

expiryTime ABSENT,

digest ABSENT,

encKey ABSENT

}),

data( CONTAINING NormalCertRequestEnc ),

extHash ABSENT

})

})

})

})

其签名数据NormalCertRequestEnc构成如下：

NormalCertRequestEnc ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

encData(WITH COMPONENTS { ...,

recipients(SequenceOfRecipientInfo (SIZE(1)) (CONSTRAINED BY {

RecipientInfo(WITH COMPONENTS {

certRecipInfo

})

}))

})

})

})

在NormalCertRequestEnc中，加密使用的公钥为需要对数据解密的CA的证书中的加密公钥，密文数据对应的明文为NormalCertRequest的OER编码值，具体数据构成如下：

NormalCertRequest ::= CertRequest(WITH COMPONENTS { ...,

version(2),

tbsCertData(WITH COMPONENTS { ...,

subjectAttributes(WITH COMPONENTS { ...,

assuranceLevel ABSENT,

itsAidList ABSENT,

itsAidSspList ABSENT

}),

validityRestrictions(WITH COMPONENTS { ...,

region PRESENT

})

}),

encryptionKey PRESENT

})

在生成非注册证书请求时，申请者共生成两对公私钥，签名公私钥和加密公私钥，签名公私钥使用方法参考附录C.3.2.1章节，加密公钥用于加密由证书系统反馈生成的非注册证书数据，私钥用于解密非注册证书数据，非注册证书请求生成过程及数据组织计算方法如下：



* + 1. 非注册证书应答数据格式

非注册证书应答的数据文件名称为其证书请求中NormalCertRequest的OER编码值的哈希值，非注册证书的应答数据格式为SecureMessage结构，其具体定义参考《GB/TXXXXX—XXXX：交通运输 数字证书应用接口规范》。数据具体构成如下：

NormalCertResp ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS {

SequenceOfCertificate(SIZE(1))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(40964),

hashAlg PRESENT,

genTime PRESENT,

expiryTime ABSENT,

digest ABSENT,

encKey ABSENT

}),

data( CONTAINING NormalCertRespData ),

extHash ABSENT

})

})

})

})

NormalCertResp的签名数据NormalCertRespData构成如下：

NormalCertRespData ::= SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

encData(WITH COMPONENTS { ...,

recipients(SequenceOfRecipientInfo (SIZE(1)) (CONSTRAINED BY {

RecipientInfo(WITH COMPONENTS {

signedDataRecipInfo

})

}))

})

})

})

CA在颁发证书后，使用非注册证书请求中的NormalCertRequest->encryptionKey对颁发的证书进行随机加密计算，根据证书请求对NormalCertRequest数据的OER编码做HashID8计算并对NormalCertRespData->payload->encData->recipients->signedDataRecipInfo->recipientId赋值，终端在做NormalCertResp数据验签后，获取其NormalCertRespData数据并对其中的NormalCertRespData->payload->encData->cipherText解密，获取最终的证书数据。

|  |
| --- |
|  |

1. （资料性附录）  
   V5接口数据报文
   1. 签名报文

签名报文数据结构参考本标准的第6.5.2章节，该章节数据结构参考《智能交通 数字证书应用接口规范》第6.3.2.1 章节，其数据格式如下：

SignedMessage ::= SecureMessage(WITH COMPONENTS {...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS { ...,

certificate(SequenceOfCertificate(SIZE(1))),

certificateDigest

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

hashAlg PRESENT,

genTime PRESENT

}),

extHash ABSENT

}),

sign(WITH COMPONENTS { ...,

r(WITH COMPONENTS {...,

x-only,compressed-y-0,compressed-y-1

})

})

})

})

})

在生成签名报文时，其数据，签名公钥及证书，签名私钥等数据的使用流程参考本标准的第6.5.4章节，具体数据数据组织计算方法如下：



* 1. 加密报文
     1. 概述

加密报文数据结构参考本标准的第6.6.2章节，该章节数据结构参考《智能交通 数字证书应用接口规范》第6.3.2.3 章节，其数据格式分为随机加密报文和协商加密报文两种，一般情况下加密报文不允许单独使用，要求与签名报文组合成签名加密报文，具体组合说明参考附录F.3章节：

* + 1. 随机加密报文

随机加密报文结构参考本标准的第6.6.2章节，该章节数据结构参考《智能交通 数字证书应用接口规范》第6.3.2.3 章节，其数据格式如下：

EphemeralEncryptMessage ::= SecureMessage(WITH COMPONENTS {...,

version(2),

payload(WITH COMPONENTS { ...,

encData(WITH COMPONENTS { ...,

recipients(SequenceOfRecipientInfo (SIZE(1)) (CONSTRAINED BY {

RecipientInfo(WITH COMPONENTS {

certRecipInfo,signedDataRecipInfo

})

}))

})

})

})

在生成随机加密报文过程中，其数据，非对称加密公钥，对称加密密钥等数据的使用流程参考本标准的第6.6.4章节，具体数据的组织计算方法如下：



* + 1. 协商加密报文

协商加密报文结构参考本标准的第6.6.2章节，该章节数据结构参考《智能交通 数字证书应用接口规范》第6.3.2.3 章节，其数据格式如下：

StaticEncryptMessage ::= SecureMessage(WITH COMPONENTS {...,

version(2),

payload(WITH COMPONENTS { ...,

encData(WITH COMPONENTS { ...,

recipients(SequenceOfRecipientInfo (SIZE(1)) (CONSTRAINED BY {

RecipientInfo(WITH COMPONENTS {

pskRecipientInfo

})

}))

})

})

})

在生成协商加密报文过程中，其数据，对称加密密钥等数据的使用流程参考本标准的第6.6.5章节，具体数据的组织计算方法如下：



* 1. 签名加密报文

签名加密报文结构为组合结构，其外部为签名数据结构，内部为加密数据结构，该章节数据结构参考《智能交通 数字证书应用接口规范》第6.3.2 章节，其数据格式如下：

SignEncryptMessage ::= SignedMessage(WITH COMPONENTS {...,

version(2),

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

tbs(WITH COMPONENTS { ...,

data(CONTAINING SecureMessage(WITH COMPONENTS {...,

version(2),

payload(WITH COMPONENTS { ...,

encData

})

}))

})

})

})

})

在生成加密签名报文过程中，其加密数据，加密密钥处理，参考本标准的第6.6章节，签名密钥，签名公钥及证书等数据的使用流程参考本标准的第6.5章节，具体数据的组织计算方法如下：



* 1. 密钥协商报文
     1. 密钥协商数据结构
        1. 密钥协商数据统一结构

ECDHMessage::=SEQUENCE {

version Uint8,

hashAlg HashAlgorithm,

curve EccCurve,

dhID OCTET STRING (SIZE(16)),

dhStartTime Time32 OPTIONAL,

dhExpireTime Time32 OPTIONAL,

dhData ECDHContent

}

version:协商数据版本号，为符合当前文档该值应设为2。

hashAlg:摘要算法ID，描述当前使用的摘要算法，为本标准第6.2章节的HashAlgorithm原子类型定义。

curve:协商使用的椭圆曲线算法，为本标准第6.2章节的椭圆曲线定义，满足EccCurve类型定义。

dhID:协商过程ID号码，随机生成，且在协商未完成的列表中唯一，用于归纳同一组协商过程。

dhStartTime:协商开始时间，为本标准第6.2章节的Time32定义。

dhExpireTime:协商超时时间，为本标准第6.2章节的Time32定义。

协商开始时间与协商超时时间用于判断协商状态在时间上是否仍然有效。

dhData:协商内容，其内部包含密钥协商所使用的数据，具体结构如附录F.4.1.2。

* + - 1. 密钥协商数据内容

ECDHContent::=CHOICE {

exchangeData ECDHData,

exchangeConfirm ECDHConfirm,

exchangeResult ECDHResult,

...

}

exchangeData:用于双方交换椭圆曲线参数，进而实现椭圆曲线密钥协商。

exchangeConfirm:用于双方交换椭圆曲线密钥协商过程中的确认值。

exchangeResult:用于应答对方密钥协商的结果和交换证书ID的结果。

* + - 1. 协商值

ECDHData ::= SEQUENCE {

keyStartTime Time32,

keyExpireTime Time32,

dhKey ECCPoint,

...

}

keyStartTime:协商密钥的开始使用时间，为本标准第6.2章节的Time32定义。

keyExpireTime:协商密钥过期时间，为本标准第6.2章节的Time32定义。

dhKey:协商用椭圆曲线点数据，为本标准第6.2章节的ECCPoint定义。

* + - 1. 确认值

ECDHConfirm ::= SEQUENCE {

confirmDataS OCTET STRING (SIZE(32)),

...

}

confirmDataS:双方密钥协商计算确认值，详见附录A3.3和附录A3.4章节。

* + - 1. 结果值

ECDHResult ::= SEQUENCE {

result DHResult,

...

}

Result：反馈协商结果和证书ID绑定的结果。

DHResult ::= ENUMERATED{

success,

refuse,

stateError,

timeOut,

...

}

success:密钥协商成功。

refuse:对端设备拒绝相应通讯。

stateError:通讯中途发生计算异常。

timeOut:协商已经超时。

* + 1. 密钥协商数据格式
       1. 协商请求发起者协商值数据格式

发起者协商值数据格式为签名报文数据格式，其格式同附录G.1章节，其AID值由附录D定义。

ECDHRequestData ::= SignedMessage(WITH COMPONENTS {...,

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS { ...,

certificate(SequenceOfCertificate(SIZE(1)))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(41472),

encKey PRESENT

}),

data(CONTAINING SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

unSecuredData(CONTAINING ECDHExChangeData)

})

}))

})

})

})

})

数据ECDHRequestData->payload->signedData->tbs->headerInfo->encKey为本次密钥协商过程生成的临时公钥，该公钥用于协商响应方对响应数据做随机加密处理，协商请求的待签数据为非密文数据的OER编码，非密文数据结构参考标准《智能交通 数字证书应用接口规范》第6.3.2章节。非密文数据内容为ECDHExChangeData数据的OER编码。

ECDHExChangeData ::= ECDHMessage(WITH COMPONENTS { ...,

dhStartTime PRESENT,

dhExpireTime PRESENT,

dhData(WITH COMPONENTS { ...,

exchangeData

})

})

在协商发起者生成协商值通讯报文时，其协商用随机数据，报文签名公私钥，接收端协商响应的加密公钥等数据组织计算方法如下：



* + - 1. 协商请求响应者协商值数据格式

响应者协商值数据格式为签名加密报文数据格式，其格式同附录G.3章节，其AID值由附录D定义。

ECDHResponseData ::= SignedMessage(WITH COMPONENTS {...,

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS { ...,

certificate(SequenceOfCertificate(SIZE(1)))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(41472),

encKey PRESENT

}),

data(CONTAINING SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

encData

})

}))

})

})

})

})

其中数据ECDHResponseData->payloa->signedDat->tbs->data数据为OER编码的随机加密数据格式，其对应的明文数据格式为ECDHExChangeData。

在协商响应者在收到协商发起者的报文后，验签计算确定其数据可信，并从发起者报文中获取相应的非对称加密公钥，采用随机加密方式对协商响应数据进行随机加密流程计算，报文签名公私钥，反馈给协商发起者的加密公钥等数据组织计算方法如下：



* + - 1. 确认值、结果值数据格式

确认值及结果值的通信数据格式为签名加密报文数据格式，其格式同附录G.3章节，其AID值由附录D定义。

ECDHConfirmOrResultData ::= SignedMessage(WITH COMPONENTS {...,

payload(WITH COMPONENTS { ...,

signedData(WITH COMPONENTS { ...,

signer(WITH COMPONENTS { ...,

certificate(SequenceOfCertificate(SIZE(1)))

}),

tbs(WITH COMPONENTS { ...,

headerInfo(WITH COMPONENTS { ...,

itsAid(41472),

encKey ABSENT

}),

data(CONTAINING SecureMessage(WITH COMPONENTS { ...,

version(2),

payload(WITH COMPONENTS { ...,

encData

})

}))

})

})

})

})

其中数据ECDHConfirmOrResultData->payloa->signedDat->tbs->data数据为OER编码的随机加密数据格式，其对应的明文数据格式为ECDHExChangeConfirmOrResult。

ECDHExChangeConfirmOrResult ::= ECDHMessage(WITH COMPONENTS { ...,

version(2),

dhStartTime PRESENT,

dhExpireTime PRESENT,

dhData(WITH COMPONENTS { ...,

ECDHConfirm,ECDHResult

})

})

在协商进入到交换确认值和结果值阶段，系统从协商请求发起者报文及协商请求响应者报文中获取相应的非对称加密公钥，采用随机加密方式对确认值及结果值数据进行随机加密流程计算，其数据组织计算方法如下。



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_