ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0138—2024

C-V2X 车联网证书策略与认证业务声明框架

Certificate policy and certification practice statement framework for C-V2X system

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京数字认证股份有限公司、商用密码检测认证中心、中国汽车技术研究中心有限公司、交通运输部路网监测与应急处置中心、交通运输部公路科学研究院、中国信息通信研究院、华为技术有限公司、中国汽车工程研究院股份有限公司、中汽研软件测评（天津）有限公司、飞天诚信科技股份有限公司、北京信安世纪科技股份有限公司、长春汽车检验中心有限责任公司、暨南大学、奇瑞新能源汽车股份有限公司、国家计算机网络与信息安全管理中心、中国工业互联网研究院、北京车网科技发展有限公司、上海伊世智能科技有限公司、襄阳达安汽车检测中心有限公司、北京理工大学、清华大学苏州汽车研究院、交通运输部科学研究院、泰尔认证中心有限公司、中汽创智科技有限公司、北京网路智联科技有限公司。

本文件主要起草人：王新华、夏鲁宁、张永强、李向锋、李广超、王本海、李国友、刘芳、肖秋林、侯昕田、倪艳、梅乐翔、齐志峰、葛雨明、于润东、房骥、张锐刚、王小军、彭宇才、朱锦涛、潘凯、陈璟、夏芹、李晓晖、李宇宁、朱鹏飞、张庆勇、吕刚、牛超、吴昊、谭武征、金飞、王永建、李邱苹、徐杰、查奇文、宋娟、高凤飞、王楠、刘虹、韩鹏、林凯、王崇文、董金聪、武俊峰、钱康、武小芳、孙圣男、杨彦召、李全发、秦建良。

引　言

C-V2X 车联网技术基于车与车、车与路侧设备、车与人及车与云平台等道路交通全要素、全时空的无线通信连接，实现智能交通管理、智能动态信息服务和自动驾驶服务，有助于降低事故发生率、提高驾驶安全、提升交通效率和节能减排。在车联网通信过程中，建立车联网通信安全身份认证体系，使用数字证书赋予车辆、路侧设备等车联网实体以可信的“数字身份”，抵御信息伪造、篡改等安全攻击，保障车联网系统安全可靠的运行。

为了规范 C-V2X 车联网电子认证服务、提升行业服务水平、促进行业健康发展，本文件从服务内容、服务质量、业务操作规范等主要方面描述了电子认证服务过程中的关键环节和操作规范。本文件能够指导证书认证机构规范开展 C-V2X 车联网领域的电子认证服务工作，也能为 C-V2X 车联网电子认证服务能力评估和监督检查工作提供依据。

C-V2X 车联网证书策略与认证业务声明框架

1 范围

本文件规定了 C-V2X 车联网领域的证书策略和认证业务声明框架，包括证书策略与认证业务声明框架结构、各章的编写要求以及编写要点。

本文件适用于开展 C-V2X 车联网领域认证服务业务的证书策略和认证业务声明的撰写，适用于指导 C-V2X 车联网证书业务的开展，也为 C-V2X 车联网证书认证服务能力评估提供依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 3957—2021 基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

C-V2X 车联网设备 C-V2X equipment

车载设备（OBU）、路侧设备（RSU）和 C-V2X 车联网服务提供商（VSP）的相关设备。

3.2

C-V2X 数字证书 C-V2X digital certificate

证书认证机构签发给 C-V2X 车联网设备的各种与 C-V2X 通信相关的数字证书。

注：包括注册证书、假名证书、应用证书、身份证书。

3.3

C-V2X 车联网服务提供商 C-V2X service provider

负责道路交通的管理机构和在 C-V2X 车联网系统里提供某种商业服务的服务机构。

3.4

证书策略 certificate policy

指定的一组规则，表明了证书在某特定范围内的、和（或）某些具有相同安全需求的应用内的使用程度。

[来源：GB/T 31508—2015，3.20]

3.5

认证业务声明 certification practice statement

证书认证机构对其签发、管理、撤销和更新证书的相关措施和实施行为的一份声明。

注：又称为电子认证业务规则。

[来源：GB/T 31508—2015，3.21]

3.6

证书认证机构　certificate authority

对数字证书进行全生命周期管理的实体。

注：也称为电子认证服务机构。本文件中特指对 C-V2X 数字证书进行全生命周期管理的实体。

3.7

注册证书认证机构　enrolment certificate authority

负责向 C-V2X 车联网设备签发注册证书的实体。

3.8

假名证书认证机构　pseudonym certificate authority

负责向 OBU 签发假名证书的实体。

3.9

应用证书认证机构　application certificate authority

负责向 OBU 签发身份证书，向 RSU 和 VSP 等 C-V2X 车联网设备签发应用证书的实体。

3.10

注册机构　registration authority

受理 C-V2X 数字证书的申请、更新和注销等业务的实体。

3.11

异常行为管理机构　misbehavior authority

能够识别潜在的异常行为或故障，确定需要撤销的证书，生成证书撤销列表的实体。

3.12

认证授权机构　authentication and authorization authority

C-V2X 车联网电子认证服务的组成部分，负责核验注册证书申请主体的实体。

3.13

注册证书　enrollment certificates

由注册证书认证机构签发给 OBU、RSU 和 VSP 的 C-V2X 数字证书，注册证书与设备唯一对应。

注：用于 C-V2X 车联网设备申请假名证书或应用证书或身份证书。

3.14

假名证书　pseudonym certificates

由假名证书认证机构签发给 OBU 的 C-V2X 数字证书，数字证书内容与设备信息无直接关联，OBU 拥有多个假名证书，用于定期切换使用。

注：OBU 使用假名证书签发其播发的主动安全消息。

3.15

身份证书　identity certificates

由应用证书认证机构签发给 OBU 的 C-V2X 数字证书。

注：用于特定的 C-V2X 车联网应用，OBU 使用身份证书向 RSU 或 VSP 证明其身份。

3.16

应用证书　application certificates

由应用证书认证机构签发给 RSU 和 VSP 相关设备的 C-V2X 数字证书。

注：RSU 和 VSP 相关设备使用应用证书签发其播发的某种应用消息。

3.17

证书撤销列表　certificate revocation list

一个经异常行为管理机构签名的列表，它指定了一系列异常行为管理机构认为无效的证书。

3.18

证书可信列表　certificate trust list

由一个认证域的 Root CA 数字签名的列表。

注：包含该认证域的根证书机构、中间证书认证机构、注册证书认证机构、假名证书认证机构、应用证书认证机构、证书注册机构、异常行为管理机构的证书集合。

3.19

密码模块　cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

[来源：GB/T 37092—2018，3.5]

3.20

订户　subscriber

接受证书认证机构提供服务的实体。

注：一般是指车企或车主。

3.21

订户协议　subscriber agreement

证书认证机构与订户共同签署，规定了双方在证书使用和管理过程中各自承担的责任和义务的文件。

[来源：GB/T 31508—2015，3.15]

3.22

依赖方协议　relying party agreement

证书认证机构在《认证业务声明》中或单独载明的与依赖方之间的协议，规定双方在证书使用和管理过程中所承担的责任和义务。

[来源：GB/T 31508—2015，3.14]

3.23

身份标识　identity

订户提供的唯一标识信息，在应用中相当于是一种“身份标识”。

注：身份标识号一般是不变的。

4　缩略语

下列缩略语适用于本文件。

CA：证书认证机构(Certificate Authority)

CP：证书策略(Certificate Policy)

CPS：认证业务声明(Certification Practice Statement)

CRL：证书撤销列表(Certificate Revocation List)

CTL：证书可信列表(Certificate Trust List)

C-V2X：蜂窝车联网(Cellular-Vehicle to Everything)

GBA：通用引导架构(Generic Bootstrapping Architecture)

MA：异常行为管理机构(Misbehavior Authority)

OBU：车载设备(On Board Unit)

PKI：公钥基础设施(Public Key Infrastructure)

RA：注册机构(Registration Authority)

RSU：路侧设备(Road Side Unit)

VSP:C-V2X 车联网服务提供商(C-V2X Service Provider)

5 概念

5.1 证书策略(CP)

CP 用于指明 C-V2X 数字证书在车联网领域应用的适用性,包括车联网应用使用证书的方式或方式集,并说明这些应用或使用方式需要达到一定的安全水平,以及为适用于这些应用或使用方式,设置了对 C-V2X 车联网 PKI 的要求。同时与 C-V2X 数字证书相关的各类实体,也需要按照策略进行证书解析和验证。CA 在 CP 中指明 C-V2X 数字证书签发的安全策略,如:证书签发过程中的身份确认、身份鉴别、物理设备安全、责任和赔付等,该证书策略可用于检查 CPS 是否有效支撑证书策略的实施。

5.2 认证业务声明(CPS)

CPS 由 CA 以公开声明的方式发布,内容包含证书签发、证书撤销、证书更新或密钥安全等过程的各种细节,如信息发布和信息管理、运营操作、技术安全控制等,其详细程度可有所不同。

若 CPS 包含其系统的敏感信息,CA 可选择不公布全部的 CPS,只公布一个 CPS 摘要,其中仅包含 CPS 中的部分规定,即 CA 认为与 C-V2X 车联网 PKI 参与者相关的部分。

5.3 证书策略与认证业务声明之间的关系

CP 和 CPS 所说明的是依赖方感兴趣的相同主题集合,如在何种程度上、为何种目的信任公钥证书。他们的主要不同在于其条款的针对对象不同。CP 列出了针对这些不同的主题,C-V2X 车联网 PKI 所采纳的要求和标准,其目的在于阐明各参与方所必须达到的要求。与之相应,CPS 则说明 CA 和其他参与者在给定的范围内所采取的过程和控制手段,如何满足 CP 中所提的要求,其目的在于公开各参与方如何实现各自的功能和控制。

若 PKI 体系中存在相互独立的 CA 实体,可分别制定并发布 CP 和 CPS。CP 和 CPS 也形成了一个通过审计、认可或其他方式对 CA 进行评估的基础,对于每个 CA,都可根据认为其要实现的一个或多个 CP 或 CPS,对其进行评估。

5.4 CP 和 CPS 与协议以及其他文档之间的关系

在 C-V2X 车联网 PKI 的要求与业务实践文档中,CP 和 CPS 并不是全部的文档。例如订户协议和依赖方协议,在订户和依赖方关于使用证书和密钥对的责任分配中,规定了证书签发、管理和使用的条款和条件。

订户协议、依赖方协议或者包括订户和依赖方两方的内容协议,也可作为一个 CPS。在 C-V2X 车联网 PKI 中,订户协议或依赖方协议可通过引用包含 CP 和 CPS 的部分或全部条款,也可从 CP/CPS 中提取适用于订户或依赖方的条款,形成独立的订户协议或依赖方协议。

CP 和 CPS 可通过引用包含到其他文档中,包括:

——互操作协议(包括 CA 间的交叉认证、单向认证或其他形式的互操作);

——厂商协议(在该协议下 PKI 厂商同意满足 CP 或 CPS 设置的标准);

——PKI 信息披露声明。

5.5 条款集说明

条款集覆盖了一定范围的标准主题,用于使用本文件中所描述的方法来表达 CP 或 CPS,这些描述在第 6 章至第 14 章有详细的解释。

参照 GB/T 26855—2011 描述的内容,CP/CPS 包含以下几方面:

a) 概括性描述；
b) 发布与信息管理；
c) 标识与鉴别；
d) 证书生命周期操作要求；
e) 设施、管理和操作控制；
f) 技术安全控制；
g) 证书和 CRL；
h) 一致性审计和其他评估；
i) 业务和法律事务。

CA 可在 CP 中描述以上各方面的相关策略及要求，在 CPS 中描述相应的业务规则声明。CA 还可通过上述内容撰写订户协议、依赖方协议或包括订户和依赖方的其他协议。

CA 还可根据实际情况对内容进行扩展，以满足复杂 CP 和 CPS 撰写者的要求。上述每一项都可进一步分解为子项，每个子项由多个元素组成。第 6 章至第 14 章提供了对上述每一项及其子项的详细描述，CP 和 CPS 的撰写者能够在子项下再增加新的子项，以满足其 C-V2X 车联网 PKI 的要求。

CP 或 CPS 的标题列表按照附录 A。

6 概括性描述

6.1 概述

该子项对当前撰写文档提供一个概要性介绍，对当前 CP 或 CPS 所适用的 C-V2X 车联网 PKI 提供一个大纲，例如，C-V2X 车联网 PKI 体系架构按照 YD/T 3957—2021 中 6.1 的内容进行描述，各 CA：

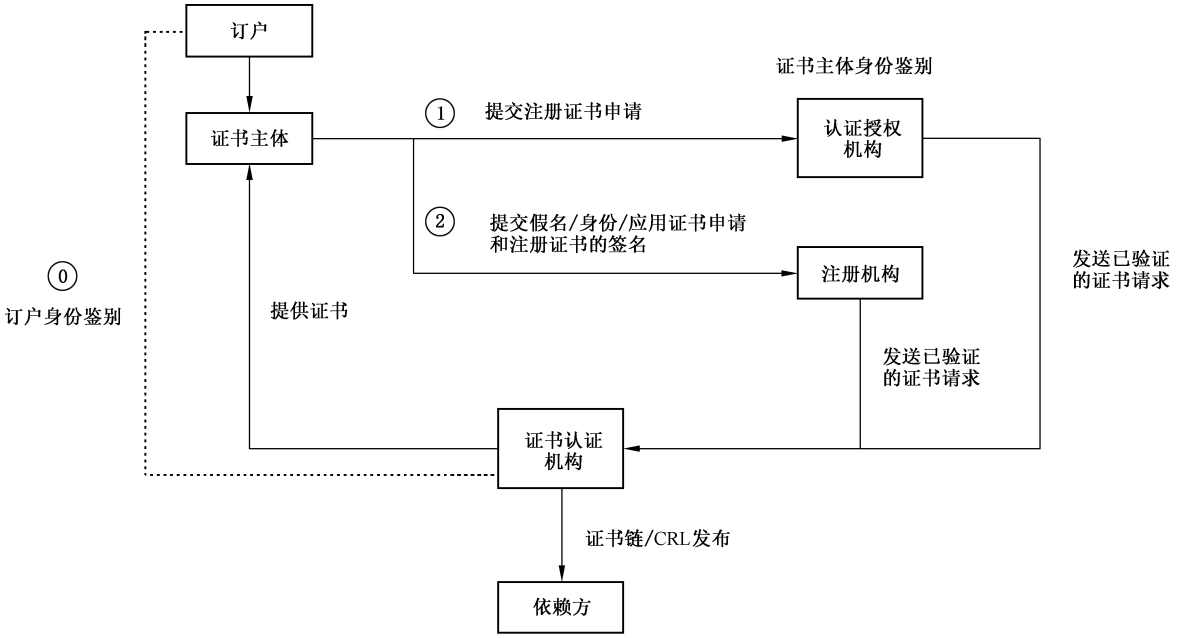
a) 根据自身情况制订 CP，并提供相应的 CPS，其 CP 符合本文件的要求，证书使用者和依赖方在处理证书时遵循本文件规定的证书处理过程；
b) 按照各自制订的 CP 进行身份的确认和证书的签发，对证书进行全生命周期管理；
c) 与证书使用者和依赖方一起借助技术或其他机制，对不同证书的具体策略达成一致。

6.2 电子认证活动参与者

6.2.1 电子认证活动参与者关系

订户与认证授权机构、注册机构和证书认证机构之间的关系示意图见图 1。

当订户向 CA 申请 C-V2X 数字证书时，由证书认证机构完成对订户的身份鉴别，并通过证书主体申请相应的证书，认证授权机构和注册机构完成对证书主体的身份鉴别和鉴权，校验通过后，证书认证机构向证书主体签发相应的 C-V2X 数字证书。证书认证机构包括注册证书认证机构、假名证书认证机构和应用证书认证机构。



标引序号说明：

0——证书认证机构核验订户身份；

1——核验通过后，证书主体生成注册证书请求，认证授权机构鉴别证书主体身份，签发注册证书；

2——证书主体下载注册证书，生成假名/身份/应用证书请求。

注：实线代表“在线”，虚线代表“离线”。

图 1　电子认证活动参与者关系图

6.2.2　证书认证机构

该子项用于描述证书认证机构信息。证书认证机构应为依法设立的第三方电子认证服务机构。

本文件所指的证书认证机构(CA)，是指对 C-V2X 数字证书进行全生命周期管理的实体，也可称为 C-V2X CA。

6.2.3　注册机构

该子项用于描述注册机构信息。注册机构对证书申请者进行标识和鉴别，批准或拒绝证书申请。

6.2.4　认证授权机构

该子项描述认证授权机构信息。CA 可授权下属机构或委托外部机构(包括 VSP 服务商、汽车制造商、运营商等)作为认证授权机构：

a) 当 CA 授权下属机构作为认证授权机构时，VSP 服务商、汽车制造商、运营商等向 CA 提供可信的身份标识，并保证其真实有效；

b) 当 CA 授权外部机构作为认证授权机构时，其应保证身份标识的真实有效，CA 在与外部机构签署的合同中，明确双方的权利与义务，以及承担的法律责任。

6.2.5　订户

该子项用于描述目标订户。订户是指向 CA 申请证书的实体，例如，车企或车主。

6.2.6 证书主体

该子项用于描述目标证书主体。证书主体是指与证书信息绑定的实体，车联网证书中的证书主体通常是指受信任的 C-V2X 车联网设备。

6.2.7 依赖方

该子项用于描述目标依赖方。依赖方是指信赖于证书所证明的信任关系并开展业务活动的实体。

6.3 证书应用

6.3.1 适合的证书应用

该子项包括所签发 C-V2X 数字证书适用的应用类型：

a) 描述 C-V2X 证书仅可用于 C-V2X 车联网相关业务；

b) 描述不同类型的 C-V2X 证书适用于不同的业务过程，如假名证书适用于车车安全通信，注册证书适用于申请其他证书过程的身份鉴别和安全防护。

6.3.2 限制的证书应用

该子项包括所签发 C-V2X 数字证书不适用的应用类型：

a) 描述 C-V2X 证书不可用于非 C-V2X 车联网业务；

b) 描述不同类型的 C-V2X 证书在 C-V2X 车联网业务中不适用的业务过程，如注册证书不可用于车车安全通信等。

6.4 策略管理

该子项包括对 CP 和 CPS 进行制订、发布、维护和更新的组织的名称和邮件地址，还可包括联系人姓名、电话号码和传真号码等必要信息。根据业务需求，在某些情况下，组织可指定合规的联系人，独立或与其他人一起提供交流渠道。

7 发布与信息库管理

7.1 认证信息的发布

该子项用于描述公布 CP 和 CPS 及其修订信息的方式和途径。例如，CA 可通过网站公布 CP 和 CPS 及其修订等信息，供相关方下载、查阅。

CA 的信息库面向订户、证书主体及依赖方提供信息服务，提供信息服务包括但不限于以下内容：根证书、CA 证书、CPS、CP 以及 CA 不定期发布的信息。

7.2 发布时间或频率

该子项用于描述 CP 和 CPS 的发布时间或频率。例如，每年修订发布一次并保存修订发布审批记录，CP 和 CPS 可通过信息库 7×24 h 获得。

7.3 信息库访问控制

该子项用于描述对发布信息进行访问控制的措施，包括 CP、CPS、证书、证书可信列表和 CRL。

8 标识与鉴别

8.1 命名

8.1.1 名称类型

该子项描述分配给实体的名称类型。

8.1.2 对名称意义化的要求

该子项描述 C-V2X 数字证书标识名称是否一定要有意义。

8.1.3 证书主体的假名

该子项描述签发的证书是否能够使用假名，对于身份证书和应用证书不宜使用假名。

8.1.4 理解不同名称形式的规则

该子项描述签发的 C-V2X 数字证书的证书标识名称类型，用何种方式进行解析理解。

8.1.5 名称的唯一性

该子项描述 C-V2X 数字证书的名称是否需要唯一。例如，在一个认证域内签发的 C-V2X 数字证书，证书标识名称应是唯一的。

8.2 初始身份确认

8.2.1 证明持有私钥的方法

该子项描述证书主体证明持有与公钥相对应的私钥的方法。例如，证明证书主体拥有私钥的方法是通过验证证书申请所包含的数字签名来完成的。

8.2.2 订户身份鉴别

该子项用于描述对订户进行身份鉴别的过程。

8.2.3 证书主体身份鉴别

该子项用于描述对证书主体进行鉴别的过程。订户向 CA 提供证书主体的属性信息及关联关系证明。属性信息包括但不限于序列号、类型等。

8.2.4 未经验证的订户信息

该子项用于描述未经鉴别的信息的具体范围或实例，并且规定未经鉴别的信息不许写入证书。

8.3 密钥更新请求的身份标识与鉴别

8.3.1 常规密钥更新的标识与鉴别

该子项用于描述正常密钥更新中对标识和鉴别的要求。例如，在证书主体注册证书到期前，证书主体应获得新证书以保持证书使用的连续性。

8.3.2 撤销后密钥更新的标识与鉴别

该子项用于描述证书撤销后的密钥更新的标识与鉴别。例如，使用初始身份确认相同的流程。

8.4 证书撤销请求的标识与鉴别

该子项用于描述对证书主体撤销请求的标识和鉴别过程。

9 证书生命周期操作要求

9.1 证书申请

9.1.1 证书申请实体

该子项用于描述证书申请实体的信息。证书申请实体包括 OBU、RSU、VSP 等相关设备。

9.1.2 申请过程与责任

该子项用于说明实体在提交 C-V2X 数字证书申请时的过程要求。例如，实体持有认证授权机构签发的安全凭证申请注册证书，持有 CA 签发的注册证书申请假名证书或身份证书或应用证书；或符合 YD/T 3957—2021 中 6.1.3 和 6.1.4 规定的 GBA 机制和 OAuth 机制申请假名证书或身份证书或应用证书。

同时描述在此过程中各方的责任。例如，订户提供有效身份电子数据，并确保电子数据真实准确，配合认证授权机构或 RA 完成对身份信息的采集、记录和验证；认证授权机构应对订户的身份信息进行采集、记录，验证，通过鉴证后，认证授权机构向证书主体签发安全凭证；RA 应对证书主体的注册证书进行采集、记录和验证，通过鉴证后，RA 向 CA 提交证书申请。

9.2 证书申请处理

9.2.1 执行识别和鉴别功能

该子项用于描述处理 C-V2X 数字证书申请过程中对证书主体身份进行识别和鉴别的方法和流程。例如，C-V2X 车联网设备申请注册证书、假名证书、身份证书和应用证书时，认证授权机构或 RA 应遵照此流程执行。

9.2.2 证书申请批准和拒绝

该子项用于描述证书申请被批准或被拒绝的决策依据。例如，如果证书主体通过身份鉴别且鉴证结果为合格，认证授权机构或 RA 批准证书申请，CA 应为证书主体制作并签发 C-V2X 数字证书。

9.2.3 处理证书申请的时间

该子项描述认证授权机构或 RA 如果收到了所有必须的相关信息，其处理证书申请的时间期限。

9.3 证书签发

9.3.1 证书签发过程中 CA 的行为

该子项描述 CA 在收到证书申请之后，所执行的证书签发行为。证书的签发意味着 CA 最终正式地批准了证书申请。

9.3.2 CA 对订户的通告

该子项描述在证书被签发前，CA 如何告知订户证书签发时间和获取证书的方式。

9.4 证书接受

该子项描述订户正式接受证书的行为。例如，证书签发完成后，CA 通告订户获取证书，在订户下载证书后，CA 认为订户接受了证书。

9.5 密钥对和证书使用

9.5.1 证书主体私钥和证书的使用

该子项用于描述与证书主体使用私钥和证书相关的订户责任。例如，证书主体在提交了证书申请并接受了 CA 签发的证书后，视为已同意遵守与 CA、依赖方有关的权利和义务的条款；订户在适用的法律、本文件指定的应用范围内使用私钥和证书，并且在证书到期或被撤销之后，订户停止使用该证书对应的私钥。

9.5.2 依赖方对公钥和证书的使用

该子项用于描述与使用证书主体公钥和证书相关依赖方的责任。例如，依赖方只能在恰当的范围内依赖于证书，此范围在 CP 中设置，可使用 CP 或 CPS 中所要求的机制来检查证书状态。

9.6 证书更新

证书更新是指在不改变证书中证书主体的公钥的情况下，为证书主体签发一张新的证书。该子项描述下列与证书更新的相关内容，具体可能包括：

a) 证书主体进行证书更新的条件，例如，证书已到期，但策略允许继续使用相同的密钥；
b) 证书主体是否可以自动请求更新证书主体证书；
c) CA 处理更新证书的过程，例如，CA 要求证书主体使用已有公钥证书对应的私钥对证书更新请求进行签名；
d) 如果 CA 不支持证书更新，CA 应明确声明。

9.7 证书密钥更新

该子项描述下列元素：

a) 证书主体的证书密钥更新条件。例如，当证书主体证书即将到期或已经到期时；或者证书主体证书密钥遭到破坏时；或者当证书主体证书或怀疑其证书密钥不安全；
b) CA 处理更新密钥的过程。例如，CA 要求证书主体使用已有私钥对包含新公钥的证书密钥更新请求进行数字签名；
c) CA 如何处理原证书。例如，在证书更新后撤销原证书。

9.8 证书撤销和挂起

9.8.1 证书撤销的情形

该子项描述证书撤销的条件。例如，订户提供的信息有误或变更时；订户没有履行双方合同规定的义务，或违反本文件；C-V2X 数字证书的安全性得不到保证；法律、行政法规规定的其他情形。

9.8.2 请求证书撤销的实体

该子项用于描述哪些实体可以请求撤销证书。例如，订户可以请求撤销证书。

9.8.3 撤销请求宽限期

该子项描述订户提出撤销请求时可用的宽限期。例如，如果出现私钥泄露等事件，撤销请求可在发现泄露或有泄露嫌疑 8 h 内提出，其他撤销原因的撤销请求可在 48 h 内提出。

9.8.4 处理撤销请求的时限

该子项描述异常行为管理机构接到撤销请求后，CA 设置处理撤销请求的时间期限。

9.8.5 依赖方检查证书撤销的要求

该子项描述依赖方如何检查证书是否撤销。如在具体应用中，依赖方使用 CRL 查询的要求。

9.8.6 CRL 和 CTL 的签发频率

该子项用于描述 CA 公布 CRL 和 CTL 的发布频率和要求。

9.8.7 证书挂起

该子项描述 CA 是否支持证书挂起以及证书挂起的条件、过程和最长时间。

9.9 证书状态服务

该子项用于描述依赖方可用的证书状态服务。例如，证书状态可通过 MA 提供的 7×24 h 的 CRL 下载服务进行状态查询。

9.10 服务终止

服务终止是指当证书有效期满或证书撤销后，该证书的服务时间结束。该子项用于描述订户终止 CA 服务时所使用的过程。例如，证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可终止服务；在证书被撤销后，可视为证书服务终止。

9.11 密钥生成、备份与恢复

该子项用于描述与密钥生成、备份和恢复相关的策略和业务实践。

9.12 跨域互信准则

在 C-V2X 车联网体系中，会存在多个独立的 CA 为订户提供证书服务，每个 CA 的服务范围称为一个认证域。跨域认证是指位于一个认证域中的证书主体能够认证由其他认证域签发给该域证书主体的证书。

该子项描述跨域互信准则。例如，为实现跨域互信，一个认证域中的证书主体可按照 YD/T 3957—2021 第 8 章的规定获取另外一个认证域签发的可信证书列表。

10 设施、管理和操作控制

10.1 物理控制

10.1.1 场地位置与建筑

该子项描述场地区域和建筑应遵循的相关标准规范。具体见附录 B 的 B.1。

10.1.2 物理访问

该子项描述物理访问采取的控制措施。具体见 B.2。

10.1.3 电力与空调

该子项描述机房受到保护以有效应对停电或其他电力异常情况，应有双路电源保障等保障措施。

10.1.4 水患防治

该子项描述水患防治的控制要求。应有充分保障，防止水侵蚀。

10.1.5 火灾预防和保护

该子项描述火灾预防和保护的措施。具体见 B.3。

10.1.6 介质存储

该子项描述 CA 机房的介质存储类型。例如，硬盘、软盘、磁带、光盘等，介质存储地点和 CA 机房系统分开并且保证物理安全，能够防磁、防静电干扰、防火、防水，由专人管理。

10.1.7 废物处理

该子项用于描述作废数据的处理方法。例如，当 CA 机房存档的敏感数据或密钥已不再需要或存档的期限已满时，将这些数据进行销毁；写在纸张之上的，切碎或烧毁；或保存在磁盘中的，多次重写覆盖磁盘的存储区域。

10.1.8 异地备份

该子项描述异地备用的地点，CA 主机房的电子认证数据应实时传输到容灾备份中心，用于容灾备份系统应急恢复。

10.2 程序控制

10.2.1 可信角色

该子项描述定义可信角色的要求，以及各个角色的责任。CA、RA、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，应由可信人员担任。具体见 B.4。

10.2.2 每个角色的识别和鉴别

该子项描述对不同角色进行识别以及在其相关活动中进行鉴别的机制。例如，进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。

10.2.3 需要职责分割的角色

该子项描述对角色定义的责任分离，CA 遵循可信角色分离的原则，进行角色的职责分离。

例如，对于根密钥的操作，有 3 名以上的根密钥管理员同时到场，才能进行有关的操作；CA 在遇到紧急情况需要联合抢修时，至少有 1 名 CA 人员在场，抢修人员在 CA 人员的陪同下，执行许可的操作，所有操作、修改都保留记录；非 CA 人员因物理修理、消防、强电故障等情况，需要进入 CA 机房实施修理时，需经同意后，首先认证修理者的身份，然后由 CA 指定的人员始终陪同和监护，完成约定部位的修理。

10.3 人员控制

10.3.1 资格、经历和无过失要求

该子项描述对可信角色的审查要求。包括资格、经历和无过失的要求。对于充当可信角色或其他重要角色的人员，应具备一定的资格，具体要求在人事管理制度中规定。CA 要求充当可信角色的人员至少具备忠诚、可信赖及工作的热诚度、无影响 CA 运行的其他兼职工作、无同行业重大错误记录、无违法记录等。

10.3.2 背景审查程序

该子项描述对可信角色进行背景审查的程序。如 CA 可与有关的政府部门和调查机构合作，完成对 CA 可信任员工的背景调查，所有可信任员工和申请调入的可信任员工都书面同意对其进行背景调查。

10.3.3 培训与考核要求

该子项描述对运营人员按照其岗位和角色进行培训的要求和过程。例如，对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 CA 组织培训与考核；技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

10.3.4 再培训周期和要求

该子项描述对每个角色进行再培训的周期和要求。例如，对于充当可信角色或其他重要角色的人员，每年至少接受一次 CA 组织的培训。对于认证策略调整、系统更新时，对全体人员进行再培训，以适应新的变化。

10.3.5 工作轮换周期和顺序

对于可替换的角色，根据业务说明工作轮换机制。轮换的周期和顺序，视业务的具体情况而定。

10.3.6 对未授权行为的处罚

该子项描述对未授权行为进行处罚的机制。例如，当 CA 员工被怀疑，或者已进行了未授权的操作，CA 得知后立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施；对情节严重的，依法追究相应责任。

10.3.7 独立合约人的要求

该子项描述对独立合约人而非实体内部人员的控制要求。

10.3.8 提供给员工的文档

为使得系统正常运行，说明员工完成其工作所必须提供的文档。

10.4 审计日志程序

10.4.1 记录事件的类型

该子项描述 CA 记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

如果 CA 记录的事件内容包含敏感信息，CA 应说明对敏感信息的防护措施。

10.4.2 处理或归档日志的周期

该子项用于描述处理或归档日志的周期。例如，CA 建有的日志收集分析系统，实时收集应用日志并归档保存。

同时说明审计日志的处理或归档日志的保存期。如每星期，或用于审计日志的可用磁盘空间低于一周内预期产生的审计日志数据量时。

审计日志处理包括对审计日志的审查、对日志未遭到篡改的验证、对所有日志条目的检查以及对日志中任何警报或违规行为的调查。

10.4.3 审计日志的保存期限

该子项用于描述审计日志的保存期限，如保存到证书失效后 5 年，法律法规另有规定的，按照相关法律法规执行。

10.4.4 审计日志的保护

该子项描述审计日志的保护措施。具体可能包括：

a) 对当前和归档的审计日志的修改或非授权销毁的保护；

b) 明确对审计日志的操作权限。如更改、删除。

10.4.5 审计日志备份程序

该子项描述审计日志备份程序。例如，具备数据库自身备份程序，根据记录的性质和要求，按照实时、每日、每周等策略进行备份。

10.4.6 审计日志收集系统

该子项描述 CA 审计日志收集的工具，审计日志信息包含系统登录日志、业务操作日志等。

10.4.7 对导致事件实体的通告

该子项描述是否对导致事件的实体进行通告。例如，CA 发现被攻击现象，记录攻击者的行为，在法律许可的范围内追溯攻击者，CA 保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

10.4.8 脆弱性评估

该子项用于描述 CA 对系统进行脆弱性评估的措施。例如，定期对系统进行漏洞扫描和渗透测试等脆弱性评估，以降低系统运行的风险。

10.5 记录归档

10.5.1 归档记录的类型

该子项描述归档记录的类型，例如所有审计数据、证书申请信息、与证书申请相关的信息等。

10.5.2 归档记录的保存期限

该子项描述设置归档记录的保存期限，例如所有归档记录的保存期为证书失效后五年。

10.5.3 归档文件的保护

该子项描述归档文件保护措施。例如，存档内容采用物理安全措施和密码技术保护，只有经过授权

的工作人员按照特定的安全方式才能查询。

10.5.4 归档文件的备份程序

该子项描述归档文件的备份机制。例如，所有存档的文件和数据库除了保存在CA主机房的存储库，还在异地保存其备份；存档的数据库应采取物理或逻辑隔离的方式，与外界不发生信息交互；只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。

CA在安全机制上应禁止对档案及其备份进行删除、修改等操作。

10.5.5 记录时间戳要求

该子项描述对记录加盖时间戳的要求，所有记录都要在存档时添加准确的时间标识以表明存档时间。

10.5.6 获得和检验归档信息的程序

该子项用于描述获得和验证归档信息的程序，如由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。

CA应定期验证归档信息的完整性。

10.6 CA密钥更替

该子项用于描述CA密钥更替的策略。例如，在证书到期前，CA按照CP的规定对根密钥进行更换，生成新的证书；在进行密钥的生成时，严格按照CA关于密钥管理的规范执行。

10.7 损害和灾难恢复

10.7.1 事故和损害处理程序

该子项用于描述对事故和损害进行处理的过程。

10.7.2 计算资源、软件和/或数据被破坏

该子项用于描述对被破坏的计算资源、软件和(或)数据进行恢复的过程。具体可能包括：

a) 证书是否要被撤销；

b) 证书主体签发新证书的过程。

10.7.3 实体私钥损害处理程序

该子项用于描述对被损害实体私钥的处理过程。

10.7.4 灾难后的业务连续性能力

该子项用于描述在发生自然或其他不可抗力性灾难后，CA应采用哪些措施对运营进行恢复。

10.8 CA或RA终止

该子项用于描述当CA或RA终止运营时，终止通告的相关过程要求。

CA和RA按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

11 技术安全控制

11.1 密钥对的生成和安装

11.1.1 密钥对的生成

该子项用于描述CA、RA和证书主体的密钥的生成方式和实现方式。例如，对于注册证书、身份证书、应用证书，密钥由证书主体的密码模块生成；对于假名证书，证书主体密钥由终端的密钥因子和私钥重构值运算产生，其中证书主体的密钥因子由密码模块（如OBU或RSU的安全密码模块）生成，私钥重构值由CA在假名证书申请过程中产生并发送给证书主体，由证书主体计算最终签名私钥的数据。

11.1.2 私钥重构值传给证书主体

该子项用于描述私钥重构值如何安全地传递给实体。

11.1.3 公钥传送给证书签发机构

该子项用于描述证书主体的公钥安全地提供给证书认证机构的方法。例如，当需要通过网络传送时应使用安全传输层协议或其他安全加密方式。

11.1.4 证书认证机构公钥传送给依赖方

该子项用于描述依赖方获取CA公钥的方式和途径。例如，依赖方可从CA指定的位置下载证书可信列表，从而得到CA的公钥。

11.1.5 密钥的长度

该子项用于描述密钥的长度。

11.1.6 公钥参数的生成和质量检查

该子项用于描述公钥参数的生成方，在必要时说明如何对公钥参数质量进行检查。

11.1.7 密钥使用目的

该子项用于描述证书主体的证书密钥的使用目的，如身份鉴别、不可抵赖性和信息的完整性等。

11.2 私钥保护和密码模块工程控制

11.2.1 密码模块标准和控制

该子项用于描述CA、RA和证书主体所使用的密码模块需要符合哪些标准。例如，CA所用的密码模块是否需要通过商用密码产品认证，是否存在与密码模块相关的其他工程或控制，如接口安全、协议安全、密钥安全、物理安全、软件安全、算法一致性、操作系统安全等。

11.2.2 私钥的多人控制

该子项用于描述私钥是否由多人控制，以及控制方法。

11.2.3 私钥托管

该子项用于描述CA、RA和证书主体私钥是否托管。

11.2.4 私钥备份

该子项用于描述CA、RA和证书主体私钥是否备份，以及备份方式。

11.2.5 私钥归档

该子项用于描述对CA、RA和证书主体私钥归档的要求。例如，CA私钥过期后，CA对CA私钥的归档保存周期至少是十年；归档加密保存在外部存储介质中并存放在安全区域。

11.2.6 私钥导入或导出密码模块

该子项用于描述CA、RA和证书主体私钥如何导入或导出密码模块。例如，在需要备份或迁移CA私钥时，从密码模块中由多人控制导出。

CA不应提供从硬件密码模块中导出证书主体私钥的方法。

11.2.7 私钥在密码模块中的存储

该子项用于描述CA、RA和证书主体私钥如何在密码模块中存储。例如，CA使用通过商用密码产品认证合格的密码模块，密码模块内置的协议、算法等均符合国家密码标准要求。

11.2.8 激活私钥的方法

该子项用于描述CA、RA和证书主体激活私钥的方法和过程。例如，对于CA私钥的激活，由具有激活私钥权限的管理员使用安全介质（如：USB-Key）登录，启动密钥管理程序，进行激活私钥的操作，有不少于3名管理员同时在场；对于证书主体私钥的激活，在申请假名证书的情况下，使用CA传递的私钥重构值，激活并派生签名私钥。

11.2.9 解除私钥激活状态的方法

该子项用于描述CA、RA和证书主体解除私钥激活的方法和过程。例如，对于CA私钥，由具有解除私钥权限的管理员使用安全介质（如：USB-Key）登录，启动密钥管理程序，进行解除私钥激活状态的操作，有不少于3名管理员同时在场。

11.2.10 销毁私钥的方法

该子项用于描述CA、RA和证书主体销毁私钥的实体及过程。例如，当CA私钥生命周期结束后，通过私钥归档的方法进行CA私钥归档，其他的CA私钥备份应被安全销毁；在CA私钥归档期结束后，具有销毁密钥权限的管理员，启动密钥管理程序，进行销毁密钥的操作，有不少于3名管理员同时在场。

11.2.11 密码模块的评估

该子项用于描述密码模块的指标。如密码模块的接口安全、协议安全、密钥安全、物理安全、软件安全、算法一致性、操作系统安全等。

CA应使用通过商用密码产品认证合格的密码模块。

11.3 密钥对管理的其他方面

11.3.1 公钥归档

该子项用于描述对CA、RA和证书主体公钥进行归档的安全控制要求，包括公钥归档的操作过程、安全措施、保存期限以及保存策略。

11.3.2 证书操作期和密钥对使用期限

该子项描述 C-V2X 数字证书的有效期和其对应的密钥对的有效期。

11.4 激活数据

11.4.1 激活数据的产生和安装

该子项用于描述 CA、RA 和证书主体生成和安装激活数据的安全控制的机制，避免激活数据被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

11.4.2 激活数据的保护

为了防止对 CA、RA 和证书主体私钥的非授权使用，说明如何保护激活数据。例如，CA 按照可靠的方式将激活数据分割后由不同的可信人员掌管。

11.5 计算机安全控制

该子项用于描述对计算机安全控制的方法和措施。例如采用自主访问控制、强制访问控制、审计、标识与鉴别、安全测试等方法。也可说明 CA 使用的涉及安全的网络设备、主机、系统软件等应属经正式验收测试合格的产品。

11.6 生命周期技术控制

11.6.1 系统开发控制

该子项描述系统开发控制的要求。包括开发环境的安全、开发人员的安全、产品维护期的配置管理安全、系统模块化、系统层次化、多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

11.6.2 安全管理控制

该子项描述安全管理控制的要求，包括操作系统、网络设置和系统配置安全。

11.6.3 生命周期安全控制

该子项描述生命周期安全控制的要求。整个系统从设计到实现应重点保证系统的安全性，充分考虑人员权限、系统备份、密钥恢复等安全运行措施，使整个系统安全可靠。

11.7 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。说明系统网路安全的相关控制，例如，采用防火墙、病毒防治、入侵检测、入侵防御、漏洞扫描、数据备份、灾难恢复等安全防护措施。

11.8 时间信息

该子项用于描述不同数据使用时间信息相关的要求或业务实践。例如，证书、CRL、CTL、电子认证服务系统日志是否包含时间信息，如果是，该时间信息应来源于国家的标准时间源。

12 证书和 CRL

12.1 证书

12.1.1 版本号

该子项用于描述 CA 签发的证书版本信息。

12.1.2 证书结构类型

该子项用于描述签发证书的结构类型。例如，证书基本结构按照 YD/T 3957—2021 中 6.2 的内容说明。

12.1.3 证书签发者

该子项用于描述签发者 CA 证书的标识信息。例如，标识信息按照 YD/T 3957—2021 中 6.2 的内容说明。

12.2 证书撤销列表

12.2.1 版本号

该子项用于描述 CA 签发的 CRL 版本信息。

12.2.2 CRL 结构

该子项用于描述 CRL 的内容结构。例如，CRL 基本域内容按照 YD/T 3957—2021 中 6.2.6 的内容说明。

13 一致性审计和其他评估

该子项用于说明一致性审计和评估的条件和内容，具体可能包括以下几项。

a) 审计或评估的提供者及其人员的身份及资质。
b) 审计或评估的触发条件，例如定期触发或事件触发。
c) 审计或评估涵盖的内容及相关实体，审计和评估内容应至少包括如下：
   1) 人事审查；
   2) 物理环境建设及安全运营管理规范审查；
   3) 系统结构及其运行审查；
   4) 密钥管理审查；
   5) 客户服务及证书处理流程审查。
d) 审计或评估的依据，例如相关的法律、法规、标准和规范等。
e) 审计和评估中发现的问题的处置措施。
f) 审计和评估结果对各相关方的可见性。

14 业务和法律事务

14.1 费用

该子项用于描述电子认证服务向订户收取费用的相关事项，包括以下内容。

a) 电子认证活动服务过程中的收费项及收费标准，其中可能包括：
   1) 证书签发或更新费用；
   2) 证书访问费用；
   3) 证书吊销或状态信息访问费用。
b) 电子认证活动中证书退订、订户取消服务相关的退款策略和退款手续。

14.2 财务责任

该子项用于描述电子认证服务活动各参与实体的资源可用性，包括：

a） 各参与实体对其他参与实体所负有的责任保险范围声明；

b） 各参与实体利用其他资源支持其运营的情况，包括利用其他资源对潜在责任进行赔付的声明。

14.3 业务信息保密

该子项用于描述电子认证服务活动中各参与实体对保密商业信息进行处理的相关规定，包括：

a） 被认为属于保密信息的范围；

b） 保密信息之外的信息类型；

c） 各参与方防止信息泄漏的责任，例如参与实体不应将信息发布给未被授权的其他实体等。

具体内容见附录 C 的 C.1。

14.4 用户隐私保护

该子项用于描述电子认证服务活动中各参与实体的用户隐私保护事项，包括：

a） 适用于电子认证服务活动的用户隐私法律和法规要求，并依据法规明确各参与实体的用户隐私保护责任；

b） 对车辆真实标识的保护、车辆不可跟踪、车辆证书不可链接等要求；

c） 在电子认证服务活动中需要使用用户隐私信息时，单独征得用户授权的要求；

d） 各参与实体实施用户隐私信息保护的方案和措施，包括对车辆真实标识的保护、车辆不可跟踪、车辆证书不可链接等要求的实现方法；

e） 包含用户隐私信息内容的公开条件。

14.5 知识产权

该子项用于描述电子认证服务活动中涉及的知识产权事项，包括：

a） 电子认证服务活动中所提供的 C-V2X 数字证书、文件与手册中、软件与服务相关的知识产权归属，例如版权、专利、商标、商业秘密等；

b） 电子认证服务活动相关的知识产权转让情况。

14.6 陈述与担保

该子项用于描述证书认证机构对各种实体所作的陈述和担保。或者 CPS 包含一个较有限的担保：在执行了某种身份鉴别过程后，就 CA 所掌握的信息而言，证书中的信息是真实的。还可要求在某些协议中要包含陈述和担保条款，如订户或依赖方协议。CA、RA、认证授权机构、订户、依赖方和其他参与者都可制定自己的陈述和担保。参见 C.2。

14.7 赔偿责任限制

该子项用于描述在电子认证服务活动中赔偿责任的限制。包含了关于 CA 责任限制和订户责任限制的规定。参见 C.3。

14.8 担保免责

该子项用于描述担保免责的规定，或者包含一项要求，规定担保免责条款要出现在相关协议当中，如订户或依赖方协议。参见 C.4。

14.9 有限责任

该子项用于描述订户、依赖方因 CA 提供的电子认证服务从事民事活动遭受到的直接损失，CA 根据其 CP 的规定向订户、依赖方承担的有限责任。

14.10 赔偿

该子项用于描述在电子认证服务活动中，由于一方的行为导致另一方遭受损失的情况下进行赔偿的相关事项，具体包括：

a) CA 对何种情况需要承担何种赔偿责任，具体内容见 C.3；
b) 证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致 CA 和 RA 产生损失，订户和依赖方对 CA 的赔偿要求，具体内容见 C.5。

14.11 争议处理

该子项用于描述电子认证服务活动中出现争议的解决机制，包括：

a) 解决争议的负责者；
b) 解决争议的流程；
c) 争议协调无效的情况下的处置方法。

14.12 管辖法律

该子项用于描述法律法规对证书策略、认证业务声明的作用，其内容至少包括《中华人民共和国电子签名法》。

14.13 与适用法律符合性

该子项用于描述各参与者需要遵守的法律和法规，包括：

a) 密码硬件和软件相关的法律法规；
b) 数据安全需要遵守的法律法规；
c) 其他法律法规，如《电子认证服务管理办法》。

附 录 A
（规范性）
条款集框架

本附录包含条款集的标题列表，可作为全部标题的一览表或 CP、CPS 编写者的标准模板。

标题列表如下：

1 概括性描述
1.1 概述
1.2 电子认证活动参与者
1.2.1 电子认证活动参与者关系
1.2.2 证书认证机构
1.2.3 注册机构
1.2.4 认证授权机构
1.2.5 订户
1.2.6 证书主体
1.2.7 依赖方
1.3 证书应用
1.3.1 适合的证书应用
1.3.2 限制的证书应用
1.4 策略管理
2 发布与信息管理
2.1 认证信息的发布
2.2 发布时间或频率
2.3 信息库访问控制
3 标识与鉴别
3.1 命名
3.1.1 名称类型
3.1.2 对名称意义化的要求
3.1.3 证书主体的假名
3.1.4 理解不同名称形式的规则
3.1.5 名称的唯一性
3.2 初始身份确认
3.2.1 证明持有私钥的方法
3.2.2 订户身份鉴别
3.2.3 证书主体身份鉴别
3.2.4 未经验证的订户信息
3.3 密钥更新请求的身份标识与鉴别
3.3.1 常规密钥更新的标识与鉴别
3.3.2 撤销后密钥更新的标识与鉴别
3.4 证书撤销请求的标识与鉴别
4 证书生命周期操作要求
4.1 证书申请

附 录 B
（资料性）
设施、管理和操作控制

B.1 场地位置与建筑建设要求

场地位置与建筑可参考以下建设标准。

a） CA 机房的建筑物和机房建设按照下列标准实施：

1） GB 50174—2008 《电子信息系统机房设计规范》；

2） GB/T 2887—2011 《计算机场地通用规范》；

3） GB/T 9361—2011 《计算机场地安全要求》；

4） GB/T 36340—2018 《防静电活动地板通用规范》；

5） GB 50034—2013 《建筑照明设计标准》；

6） GB 50054—2011 《低压配电设计规范》；

7） GB 50019—2015 《工业建筑供暖通风与空气调节设计规范》；

8） GB 50057—2010 《建筑物防雷设计规范》；

9） GB 50689—2011 《通信局站防雷与接地工程设计规范》。

b） CA 机房的功能区域可划分为六个层次，四个区域。

六个层次由外到里分别是：入口、办公、敏感、数据中心、屏蔽机房和保密机柜。

四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

B.2 物理访问控制要求

物理访问控制包括如下几个方面。

a） 门禁系统：控制各层门的人员进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

b） 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c） 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 h 不间断录像。所有录像资料应保留不少于 6 个月，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 h 的不间断供电。

B.3 火灾预防与保护要求

火灾预防包括以下内容。

a） 敏感区（物理三层）、高度敏感区域（物理四、五、六层），其建筑物的耐火等级应符合 GB 50016—2014 中规定的二级耐火等级。

b） CA 机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。

c） 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。CA 机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

d) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

e) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 h，吊顶的耐火极限不得低于 15 min。

f) 在非敏感区及敏感区的办公区域内，应设置紧急出口，紧急出口应设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

g) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。CA 机房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用电动、手动、紧急启动三种方式。

a) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

B.4 可信角色划分

可信角色包括以下内容。

a) 系统管理员

系统管理员负责对 C-V2X 数字证书服务体系进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b) 安全管理员

安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c) 审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d) 密钥管理员

密钥管理员负责管理 CA 的密钥相关设备，进行 CA 密钥的生成、备份、恢复、销毁等操作。

e) 证书业务管理员

证书业务管理员对 RA 操作员进行管理，并对 RA 业务进行管理。

附 录 C
（资料性）
业务和法律事务

C.1 业务信息保密

C.1.1 保密信息范围

保密的业务信息包括但不限于以下方面：

a） 在双方披露时标明为保密（或有类似标记）的；

b） 在保密情况下由双方披露的或知悉的；

c） 双方根据合理的商业判断应理解为保密数据和信息的；

d） 以其他书面或有形形式确认为保密信息的；

e） 或从上述信息中衍生出的信息。

对于 CA 来说，保密信息包括但不限于以下方面：

a） C-V2X 车联网应用的各参与方的签名密钥都是保密的；

b） 保存在审计记录中的信息；

c） 年度审计结果也同样视为保密；

d） 除非有法律要求，由 CA 掌握的，除作为证书、CRL、CTL、认证策略被清楚发布之外的个人和公司的信息需要保密。

除非法律明文规定，CA 没有义务公布或透露订户 C-V2X 数字证书以外的信息。

C.1.2 保护保密信息的责任

各参与方在接收到保密信息时有责任对信息保密。

a） 各方有保护自己和其他人员或单位的机密信息并保证不泄露给第三方的责任。不将机密数据和信息（也不会促使或允许他人将机密数据和信息）用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接收方不得复印、复制或储存机密数据和信息。

b） 当 CA 在任何法律、法规或规章的要求下，或在法院的要求下应提供其 CP 和 CPS 中具有保密性质的信息，CA 应按照要求，向执法部门公布相关的保密信息，CA 无须承担任何责任。这种提供不被视为违反保密的要求和义务。

C.2 陈述与担保

C.2.1 证书认证机构的陈述与担保

CA 在提供电子认证服务活动过程中的服务要求。

a） CA 应遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的 C-V2X 数字证书承担相应的法律责任。

b） CA 应保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c） 除非已通过 CA 的 CRL 发出了 CA 的私钥被破坏或被盗的通知，CA 应保证其私钥是安全的。

d） CA 签发给订户的证书应符合 CA 的 CPS 所有实质性要求。

e) CA 应向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。
f) CA 应及时撤销证书。
g) CA 拒绝签发证书后，应立即向证书订户归还所付的全部费用。
h) 证书公开发布后，CA 应向证书依赖方证明，C-V2X 数字证书中载明的订户信息都是准确的。
i) CA 不负责评估证书是否在适当的范围内使用。
j) 所有证书不应用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，因为任何潜在的、或有的故障都可能导致死亡、人员伤害或环境破坏。

C.2.2 注册机构的陈述与担保

CA 的注册机构在参与电子认证服务过程中的服务要求如下。
a) 提供给证书订户的申请过程应完全符合 CA 的 CPS 所有实质性要求。
b) 在 CA 生成证书时，不能因为注册机构的失误而导致证书中的信息与证书申请方的信息不一致。
c) 注册机构应按 CPS 的规定，及时向 CA 提交证书申请、更新等服务请求。当订户以书面形式通知注册机构其申请证书时提供的声明或信息发生改变时，注册机构无正当理由未及时提供相关证书服务的，由此给订户造成的损失由注册机构自行承担全部法律责任。

C.2.3 认证授权机构的授权与担保

认证授权机构在参与电子认证服务过程中的服务要求如下。
a) 提供给证书订户的注册过程应完全符合 CA 的 CPS 所有实质性要求。
b) 在 CA 生成证书时，不能因为认证授权机构的失误而导致证书中的信息与证书申请方的信息不一致。
c) 认证授权机构应按 CPS 的规定，及时向 CA 提交证书申请服务请求。

C.2.4 订户的陈述与担保

订户一旦接受 CA 签发的证书，就被视为向 CA、注册机构及信赖证书的有关当事人做出以下承诺。
a) 订户确认已知悉并接受了 CPS 及相关规定的全部内容，且同意受其 CPS 条款的约束，同意其中赔偿责任限制的规定。
b) 订户在申请证书时提供的所有声明和信息应是完整、真实和正确的，可供 CA 或注册机构检查和核实。如果前述声明或信息发生任何改变应及时通知 CA 或注册机构。如因订户故意或过失提供虚假、伪造等信息资料或陈述，或前述提供的声明或信息发生改变时未及时以书面形式通知 CA 或注册机构的，由订户承担全部法律责任。
c) 订户应当妥善保管私钥，订户的密码安全设备应符合安全技术标准，具备足够的安全防护能力来防止证书私钥的遗失、泄露和被篡改等事件的发生。
d) 私钥为订户自身访问和使用，订户对使用私钥的行为负责。

C.2.5 依赖方的陈述与担保

依赖方知悉其 CPS 的条款以及和订户 C-V2X 数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的 C-V2X 数字证书前，应采取合理步骤，查证订户 C-V2X 数字证书及数字签名的有效性。当依赖方未尽到前述查证义务时，依赖方愿意赔偿由此给 CA 造成的全部损失，并且自行承担由此给自身或他人造成的损失。

所有依赖方应承认，他们对证书的信赖行为就表明他们承认了解其 CP 及 CPS 的有关条款，同意其

中赔偿责任限制的规定。

C.2.6 其他参与者的陈述与担保

其他参与者的陈述与担保同依赖方的陈述与担保。

C.3 赔偿责任限制

以下情况是对赔偿责任限制的条件。

a) 除非有另行的规定或约定，对于非 CPS 下的认证服务而导致的任何损失，CA 不向订户或依赖方承担任何赔偿和/或补偿责任。

b) 订户或依赖方进行 C-V2X 车联网应用，因 CA 提供的认证服务而遭受的直接损失，应依据 CPS 的相关条款给予相应的赔偿。

c) 如果 CA 能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、CA 向主管部门备案的 CPS 实施的，则视为 CA 不具有任何过错，CA 不对订户或依赖方承担任何赔偿或补偿责任。

d) 无论 CA 的 CPS 是否有相反或不同规定，就以下损失或损害，CA 不承担任何赔偿和/或补偿责任：

   1) 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损失、任何商机或契机损失、失去项目，以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

   2) 由上述第 1 项所述的损失相应生成或附带引起的损失或损害；

   3) 非 CA 行为而导致的损失；

   4) 因不可抗力而导致的损失，如罢工、战争、灾害、恶意病毒代码等。

e) 无论其 CPS 是否有相反或不同规定，如果 CA 根据 CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，CA 应按照相关法律法规的规定、仲裁机构的裁决或法院的裁判承担相应的赔偿责任。

f) CA 对于任何证书或依赖方等实体的证书赔偿合计责任不得超出证书市场购买价格。

C.4 担保免责

有下列情况之一的，应当免除 CA 责任，包括但不限于赔偿责任及补偿责任。

a) 如果订户故意或过失地提供了不完整、不可靠、已过期或无效的信息，又根据正常的流程提供了必须的审核文件，得到了 CA 签发的 C-V2X 数字证书，由此引起的经济纠纷应由订户全部承担，CA 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

b) CA 不承担任何其他未经授权的人或组织以本 CA 名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c) CA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

d) CA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

e) CA 和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。CA 和证书持有人间的关系以及 CA 和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让 CA 承担信托责任。

f) CA 与授权的认证授权机构签署合同，合同条款中明确认证授权机构负责并承担订户身份鉴别责任。对于由认证授权机构的行为所产生的法律与赔偿责任由 CA 授权的认证授权机构承

担，并且认证授权机构应当使 CA 免于第三方的索赔。

g) 若 C-V2X 数字证书被超出范围或者以非预期的方式使用(如应用领域不被 CA 认可等)，CA 不向任何方承担赔偿和/或补偿责任。

h) 由于客观意外或其他不可抗力事件原因而导致 C-V2X 数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。

i) 因 CA 的设备或网络故障等技术故障而导致 C-V2X 数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起的原因包括但不限于：

   1) 不可抗力；
   2) 关联单位如电力、电信、通信部门而致；
   3) 黑客攻击；
   4) 设备或网络故障。

j) CA 已谨慎地遵循了国家法律、法规规定的 C-V2X 数字证书认证业务规则，而仍有损失产生的。

C.5 赔偿

订户或其管理者接受证书就表示同意在以下情况下承担赔偿责任。

a) 未向 CA 提供真实、完整和准确的信息，而导致 CA 或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知 CA，并终止使用该证书，而导致 CA 或有关各方损失。

d) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户应对这种行为的后果负责。

e) 证书的非法使用，即违反 CA 对证书使用的规定，造成了 CA 或有关各方的利益受到损失。

参 考 文 献

[1] GB/T 2887—2011 计算机场地通用规范
[2] GB/T 9361—2011 计算机场地安全要求
[3] GB/T 26855—2011 信息安全技术 公钥基础设施 证书策略与认证业务声明框架
[4] GB/T 36340—2018 防静电活动地板通用规范
[5] GB 50016—2014 建设设计防火规范
[6] GB 50019—2015 工业建筑供暖通风与空气调节设计规范
[7] GB 50034—2013 建筑照明设计标准
[8] GB 50054—2011 低压配电设计规范
[9] GB 50057—2010 建筑物防雷设计规范
[10] GB 50174—2008 电子信息系统机房设计规范
[11] GB 50689—2011 通信局站防雷与接地工程设计规范
[12] 中华人民共和国工业和信息化部令第1号《电子认证服务管理办法》
[13] IEEE 1609.2 Security Services for Applications and Management Messages
[14] BS PD CEN ISO/TR 21186-1—2021 Cooperative intelligent transport systems (C-ITS)—Guidelines on the usage of standards—Part 3:Security
[15] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1.1
[16] UNE-CEN ISO/TS 21177—2019 Intelligent transport systems—ITS station security services for secure session establishment and authentication between trusted devices

中华人民共和国密码
行业标准
C-V2X 车联网证书策略与认证业务声明框架
GM/T 0138—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.75　字数 69 千字
2025 年 6 月第 1 版　2025 年 6 月第 1 次印刷
*
书号:155066·2-39030　定价 70.00 元

GM/T 0138-2024