ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0141—2024

V2X 证书认证系统检测规范

Test specification of V2X certificate authentication 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：商用密码检测认证中心、中汽研软件（测评）天津有限公司、郑州信大捷安信息技术股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、中海闻达信息技术有限公司、兴唐通信科技有限公司、中汽数据有限公司、北京中宇万通科技股份有限公司、深圳奥联信息安全技术有限公司、比亚迪汽车工业有限公司。

本文件主要起草人：肖秋林、张立花、鲍越、牛路宏、汪宗斌、罗鹏、郑军、梁承志、刘为华、马卫局、李宇宁、张绍博、侯昕田、李季、白顺东、吴永飞、李华领。

V2X 证书认证系统检测规范

1 范围

本文件规定了 V2X 证书认证系统的检测要求、送检文档和判定规则。

本文件适用于对 V2X 证书认证系统的产品检测，规范 V2X 证书认证系统中密码及相关安全技术的应用，也为该类系统的研制提供参考。

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。

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0005 随机性检测规范

GM/T 0008 安全芯片密码检测准则

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

车载设备 on board unit

安装在车辆上，负责 V2X 通信的实体。

3.2

路侧设备 road side unit

安装在路侧交通控制设备和交通信息发布设备中，负责 V2X 通信的实体。

3.3

V2X 服务提供商 V2X service provider

负责道路交通的管理机构和在车联网系统里提供某种商业服务的服务机构。

3.4

V2X 设备 V2X equipment

车载设备、路侧设备和 V2X 服务提供商的安全设备。

3.5

V2X 证书认证系统 V2X certificate authentication system

对 V2X 证书的签发、更新、下载、撤销等数字证书全生命周期进行管理的系统。

3.6

V2X 证书　V2X certificate

V2X 公钥证书　V2X public key certificate

由 V2X 证书认证系统签发的包含证书持有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注：主要应用于 V2X 直连通信场景，按应用类别分为机构证书、注册证书、应用证书、身份证书和假名证书。

3.7

V2X 证书撤销列表　V2X certificate revocation list

由 V2X 证书认证系统签发并发布的被撤销证书的列表。

3.8

V2X 二级证书认证机构　V2X level 2 certificate authority

负责管理本级机构证书以及下一级机构证书，如中间 CA 机构证书、注册 CA 机构证书、假名 CA 机构证书、应用 CA 机构证书等。

3.9

V2X 注册证书认证机构　V2X enrollment certificate authority

负责向车载设备、路侧设备、V2X 服务提供商等车联网设备签发注册证书，由 V2X 注册证书认证系统实现证书管理功能。

3.10

V2X 假名证书认证机构　V2X pseudonym certificate authority

负责向车载设备签发假名证书，由 V2X 授权证书认证系统实现证书管理功能。

3.11

V2X 应用证书认证机构　V2X application certificate authority

负责向车载设备签发身份证书，向路侧设备和 V2X 服务提供商等 V2X 设备签发应用证书，由 V2X 授权证书认证系统实现证书管理功能。

3.12

假名证书　pseudonym certificate

签发给车载设备，包含持有者权限等但不包含持有者身份的 V2X 证书。

3.13

应用证书　application certificate

签发给路侧设备和 V2X 服务提供商，用于验证特定车联网应用消息的 V2X 证书。

3.14

身份证书　identity certificate

签发给车载设备，用于验证特定车联网应用消息的 V2X 证书。

3.15

V2X 授权证书　V2X authorization certificate

用于在 V2X 安全通信中验证消息的证书，包括：假名证书、应用证书和身份证书。

3.16

V2X 注册证书　V2X enrollment certificate

签发给车载设备、路侧设备和 V2X 服务提供商，用于验证授权证书申请和下载消息的证书。注册证书与 V2X 设备一一对应。

3.17

机构证书　authority certificate

为证书机构签发的证书，包括 V2X 二级证书认证机构的证书、V2X 注册证书认证机构的证书、

V2X 假名证书认证机构的证书、V2X 应用证书认证机构的证书等。

3.18

链接值　linkage value

利用链接种子值派生出来的值，用于假名证书的撤销。

3.19

周期链接种子　periodic linkage seed

周期链接种子基于初始链接种子派生，用于派生链接值，初始链接种子是随机数。

4　缩略语

下列缩略语适用于本文件。

ACA：V2X 应用证书认证机构（V2X Aplication Certificate Authority）

COER：正则八位字节编码规则（Canonical Octet Encoding Rules）

ECA：V2X 注册证书认证机构（V2X Enrolment Certificate Authority）

HMAC：基于杂凑的消息认证码（Hash-based Message Authentication Code）

ICA：V2X 中间证书认证机构（V2X Intermediate Certificate Authority）

OBU：车载设备（On Board Unit）

PCA：V2X 假名证书认证机构（V2X Pseudonym Certificate Authority）

PRA：假名证书注册机构（Pseudonym Certificate Registration Authority）

RSU：路侧设备（Road Side Unit）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

V2X：一种车辆与外界通信的技术（Vehicle to Everything）

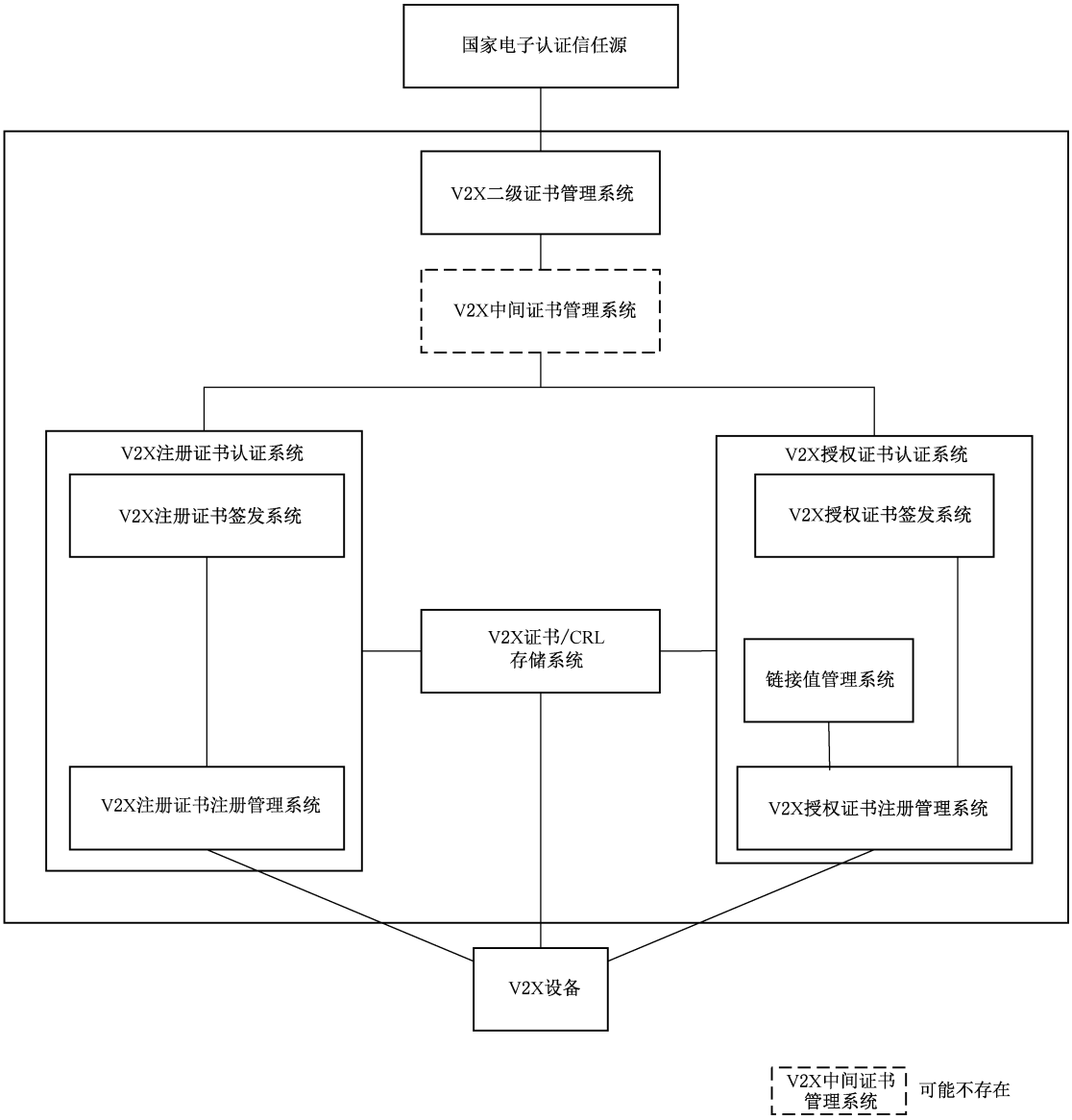
V2XCRL：V2X 证书撤销列表（V2X Certificate Revocation List）

VSP：V2X 服务提供商（V2X service provider）

5　V2X 证书认证系统

5.1　系统逻辑架构

V2X 证书认证系统由 V2X 二级证书管理系统、V2X 中间证书管理系统、V2X 注册证书认证系统、V2X 授权证书认证系统、V2X 证书/CRL 存储系统等组成，整体逻辑架构见图 1。



注 1：国家电子认证信任源和 V2X 设备，不在本文件的检测范围内。

注 2：V2X 二级证书管理系统为国家电子信任源的下一级信任。

图 1　V2X 证书认证系统逻辑架构

5.1.1　V2X 二级证书管理系统

V2X 二级证书管理系统具备接入国家电子认证信任源的功能，支持通过下一级机构证书或可信根证书信任列表的方式接入国家电子认证信任源。系统负责下一级机构（例如：ICA、ECA、PCA、ACA 等）证书的签发、更新、撤销等全生命周期管理。V2X 二级证书管理系统的下级可以有多个平行的中间证书管理系统。

5.1.2　V2X 中间证书管理系统（若有）

V2X 中间证书管理系统（若有）主要负责下一级机构（例如：ECA、PCA、ACA 等）的证书签发、更新、撤销等全生命周期管理，若不存在 V2X 中间证书管理系统，则由 V2X 二级证书管理系统直接签发其负责签发的下一级机构证书。

5.1.3 V2X 注册证书认证系统

V2X 注册证书认证系统包含 V2X 注册证书注册管理系统和 V2X 注册证书签发系统，其中 V2X 注册证书注册管理系统主要负责鉴别设备的合法性，V2X 注册证书签发系统主要负责注册证书的签发及全生命周期管理。V2X 设备通过 V2X 注册证书认证系统颁发的注册证书可以向 V2X 授权证书认证系统申请授权证书。

5.1.4 V2X 授权证书认证系统

V2X 授权证书认证系统包括 V2X 授权证书注册管理系统、链接值管理系统和 V2X 授权证书签发系统，其中 V2X 授权证书注册管理系统负责验证 V2X 设备的身份信息，处理合法设备发起的授权证书申请、下载等业务请求，并将从 V2X 授权证书签发系统获得的授权证书返回至 V2X 设备；链接值管理系统主要为授权证书中的假名证书提供链接值产生及查询服务；V2X 授权证书签发系统主要负责授权证书（假名证书、身份证书、应用证书）的签发及全生命周期管理。

5.1.5 V2X 证书/CRL 存储系统

V2X 证书/CRL 存储系统主要提供 V2X 证书/CRL 的存储、备份、查询、下载服务，也可以是具备相应功能的模块。

5.2 系统组成

5.2.1 V2X 二级证书管理系统

V2X 二级证书管理系统负责生成和签发机构证书、生成和签发证书撤销列表，其主要功能如下。

a) 机构证书生成和签发：二级证书管理系统的机构证书由国家电子认证信任源进行签发或基于可信根证书信任列表模式下由系统自签产生；下一级机构将产生的签名公钥提交给二级证书管理系统，由二级证书管理系统签发下一级机构的机构证书。
b) 机构证书撤销列表生成和签发：二级证书管理系统可签发基于证书杂凑值的 V2XCRL，并对其生命周期进行管理。
c) 安全审计：负责对二级证书管理系统的管理人员、操作人员的操作日志进行查询、审计、统计等。
d) 安全管理：对业务管理员、业务操作员和审计员登录二级证书管理系统进行安全访问控制，并对机构证书数据库进行管理和备份。

5.2.2 V2X 中间证书管理系统（若有）

V2X 中间证书管理系统属于二级证书管理系统的下一级系统，用于扩展 V2X 证书认证系统信任层级，负责生成和签发下一级机构证书、生成和签发证书撤销列表，其主要功能如下。

a) 机构证书生成和签发：下一级机构将产生的签名公钥提交给中间证书管理系统，由中间证书管理系统签发下一级机构的机构证书。
b) 机构证书撤销列表生成和签发：中间证书管理系统可签发基于证书杂凑值的 V2XCRL，并对其生命周期进行管理。
c) 安全审计：负责对中间证书管理系统的管理人员、操作人员的操作日志进行查询、审计、统计等。
d) 安全管理：对业务管理员、业务操作员和审计员登录中间证书管理系统进行安全访问控制，并对机构证书数据库进行管理和备份。

5.2.3 V2X 注册证书认证系统

5.2.3.1 V2X 注册证书注册管理系统

V2X 注册证书注册管理系统负责 V2X 设备信息管理和身份认证，其主要功能如下。

a) V2X 设备信息管理：负责 V2X 设备信息录入、核验和查询。
b) 安全审计：负责对 V2X 注册证书注册管理系统的管理人员、操作人员的操作日志进行查询、审计、统计等。
c) 安全管理：对业务管理员、业务操作员和审计员登录 V2X 注册证书注册管理系统进行安全访问控制，并对终端设备信息数据库进行管理和备份。
d) V2X 注册证书注册管理系统应具有并行处理 V2X 设备认证请求的能力。

5.2.3.2 V2X 注册证书签发系统

V2X 注册证书签发系统负责 V2X 设备注册证书生成、签发和更新，其主要功能如下。

a) 注册证书生成和签发：验证注册证书申请消息签名或接收 V2X 注册证书注册管理系统已经验证过的注册证书申请请求，生成并返回注册证书给申请实体，返回消息需通过数字签名保证完整性和来源真实性。
b) 注册证书更新：V2X 设备可利用有效的注册证书向系统申请更新注册证书，获取新的注册证书。
c) 注册证书撤销列表生成和签发：可签发基于证书杂凑值的 V2XCRL，并对其生命周期进行管理。
d) 安全审计：负责对 V2X 注册证书签发系统的管理人员、操作人员的操作日志进行查询、审计、统计等。
e) 安全管理：对业务管理员、业务操作员和审计员登录 V2X 注册证书签发系统进行安全访问控制，并对注册证书数据库进行管理和备份。
f) V2X 注册证书签发系统应具有并行签发 V2X 设备注册证书的能力。

5.2.4 V2X 授权证书认证系统

5.2.4.1 V2X 授权证书注册管理系统

V2X 授权证书注册管理系统负责链接值申请和为 V2X 设备提供授权证书的申请和下载服务。根据实际业务应用，V2X 授权证书注册管理系统包括假名证书注册系统和应用证书注册系统。其主要功能如下。

a) 授权证书申请的处理：V2X 授权证书注册管理系统解密授权证书申请消息。若 V2X 设备使用注册证书申请授权证书，则验证申请消息中携带的注册证书的有效性，并验证消息签名。验证通过则向授权证书签发系统发送授权证书签发请求消息。
b) 链接值申请：若申请实体申请的是假名证书，申请消息验证通过后，V2X 授权证书注册管理系统向链接值管理系统申请签发假名证书所需的链接值，并将链接值等信息通过授权证书签发请求消息发送至授权证书签发系统。
c) 授权证书下载请求的处理：V2X 授权证书注册管理系统解密授权证书下载消息。若 V2X 设备使用注册证书下载授权证书，则验证申请消息中携带的注册证书的有效性，并验证消息签名。验证通过后返回授权证书至申请实体。
d) 安全审计：负责对 V2X 授权证书注册管理系统的管理人员、操作人员的操作日志进行查询、审计、统计等。

e) 安全管理：对业务管理员、业务操作员和审计员登录 V2X 授权证书注册管理系统进行安全访问控制，并对授权证书数据库进行管理和备份。

f) V2X 授权证书注册管理系统宜具有并行处理 V2X 设备授权证书申请和下载请求的能力。

5.2.4.2 V2X 授权证书签发系统

V2X 授权证书签发系统负责 V2X 设备授权证书的生成、签发。根据实际业务应用，V2X 授权证书签发系统包括假名证书签发系统和应用证书签发系统。与其主要功能如下。

a) 授权证书生成和签发：验证授权证书签发请求消息的签名，然后生成并签发授权证书，其中假名证书签发系统负责签发假名证书，应用证书签发系统负责签发身份证书和应用证书。

b) 授权证书撤销列表生成和签发：可签发基于证书杂凑值的 V2XCRL 和基于链接值的 V2XCRL，并对其生命周期进行管理。

c) 安全审计：负责对 V2X 授权证书签发系统的管理人员、操作人员的操作日志进行查询、审计、统计等。

d) 安全管理：对业务管理员、业务操作员和审计员登录 V2X 授权证书签发系统进行安全访问控制，并对授权证书数据库进行管理和备份。

e) V2X 授权证书签发系统应具有并行签发 V2X 授权证书的能力。

5.2.4.3 链接值管理系统

链接值管理系统负责管理假名证书的链接值，其主要功能如下。

a) 初始链接种子生成：为新链接链随机生成初始链接种子，初始链接种子质量应符合 GM/T 0005 要求。

b) 链接标识符生成：为新链接链计算链接标识符。

c) 周期链接种子生成：根据初始链接种子，基于 SM3 密码算法计算周期链接种子。

d) 链接值生成：根据周期链接种子和周期内所需链接值数量，使用 SM4 密码算法生成一批链接值。链接值应用于假名证书标识字段，用于假名证书批量撤销。

e) 周期链接种子查询：接收来自其他系统的查询请求，根据链接值查询周期链接种子，并返回至查询者。

f) 安全审计：负责对链接值管理系统的管理人员、操作人员的操作日志进行查询、审计、统计等。

g) 安全管理：对业务管理员、业务操作员和审计员登录链接值管理系统进行安全访问控制，并对链接值数据库进行管理和备份。

5.2.5 V2X 证书/CRL 存储系统

V2X 证书/CRL 存储系统负责 V2X 证书、V2X 证书撤销列表的存储。可采用数据库或文件服务器方式，实现 V2X 证书、V2X 证书撤销列表的存储、备份和归档等功能。其主要功能如下。

a) V2X 证书存储：负责存储由 V2X 注册证书认证系统和 V2X 授权认证系统签发的注册证书和授权证书（假名证书、应用证书和身份证书）、机构证书的实体以及与证书相关设备信息、链接值信息等。

b) V2X 证书撤销列表存储：负责存储由系统签发的基于杂凑值的 V2XCRL 和基于链接值的 V2XCRL 文件。

c) 安全审计：负责对 V2X 证书/CRL 存储系统的管理人员、操作人员的操作日志进行查询、审计、统计等。

d) 安全管理：对业务管理员、业务操作员和审计员登录 V2X 证书/CRL 存储系统进行安全访问控制，并定期对数据库和文件服务器的内容进行数据备份和归档。

5.3 互联互通

应支持接入国家密码管理部门统一规划建设的国家电子认证信任源。

5.4 V2X 证书

V2X 证书结构内容应遵循附录 A。

5.5 V2X 证书撤销列表

V2X 证书撤销列表结构内容应遵循附录 B。

6 检测要求

6.1 密码算法

6.1.1 对称密码算法正确性

检测要求：

对称密码算法应支持 SM4 密码算法，SM4 算法实现应符合 GB/T 32907。

检测方法：

a) 对给定的密钥和明文经指定的算法、工作模式和其他参数加密后，结果和给定密文完全相同；

b) 对给定的密钥和密文经指定的算法、工作模式和其他参数解密后，结果和给定明文完全相同。

结果判定：

若对应检测方法 a)和 b)项均测试通过，则该检测项为通过。

6.1.2 杂凑密码算法正确性

检测要求：

密码杂凑函数采用 SM3 密码杂凑算法，应遵循 GB/T 32905。

检测方法：

a) 送检产品使用 SM3 算法对给定的数据进行杂凑运算得到计算杂凑值；

b) 将杂凑值与预期结果数据进行比对验证，应能通过验证。

结果判定：

若对应检测方法 a)和 b)项均测试通过，则该检测项为通过。

6.1.3 非对称密码算法正确性

检测要求：

非对称密码算法应基于 SM2 算法，支持加解密和签名/验证等运算，其实现应符合 GB/T 32918、GB/T 35276。

检测方法：

a) 检测工具生成随机数据，送检产品采用指定公钥和其他参数使用 SM2 算法对随机数据进行加密运算，通过数据采集，得到密文；

b) 检测工具采用 a)中指定公钥对应的私钥和其他参数使用 SM2 算法将 a)中密文数据进行解密运算，通过数据采集，得到明文并进行比对验证；

c) 检测工具生成随机数据，检测工具采用指定公钥和其他参数使用 SM2 算法对随机数据进行加密运算，通过数据采集，得到密文；

d) 送检产品采用 c)中指定公钥对应的私钥和其他参数使用 SM2 算法将 c)中密文数据进行解密运算,通过数据采集,得到明文并进行比对验证;
e) 检测工具生成随机数据,送检产品采用指定私钥和其他参数使用 SM2 算法对随机数据进行签名运算,通过数据采集,得到签名值;
f) 检测工具采用 e)中指定私钥对应的公钥和其他参数对 e)中签名值数据进行验签运算,应能验签成功;
g) 检测工具生成随机数据,检测工具采用指定私钥和其他参数使用 SM2 算法对随机数据进行签名运算,通过数据采集,得到签名值;
h) 送检产品采用 g)中指定私钥对应的公钥和其他参数对 g)中签名值数据进行验签运算,应能验签成功。

结果判定:

若对应检测方法 a)~h)项均测试通过,则该检测项为通过。

6.1.4 非对称密钥对配对一致性

检测要求:

非对称密钥对配对应遵循 GB/T 32918.1 和 GB/T 32918.5。

检测方法:

a) 使用公钥对明文值或编码信息进行加密,并使用私钥对密文解密,检查解密的结果与原明文是否一致;
b) 使用私钥对原文进行签名,并使用公钥对签名值验证,应能验签成功。

结果判定:

若对应检测方法 a)和 b)项均测试通过,则该检测项为通过。

6.2 随机数

检测要求:

随机数应采用经检测认证合格的密码部件或模块生成,随机数质量应遵循 GM/T 0005 中的要求。

检测方法:

现场采集随机数,检测随机数的质量是否符合 GM/T 0005 中的要求。

结果判定:

若随机数采用经检测认证合格的密码部件或模块生成,且检测结果表示随机数质量符合 GM/T 0005 中的要求,则该检测项为通过。

6.3 密钥管理

检测要求:

a) V2X 证书认证系统中 V2X 二级 CA、ICA、ECA、PCA、ACA 等机构证书密钥,应使用经检测认证合格的密码设备对上述密钥涉及到的生成、存储、分发、导入与导出、使用、更新、备份与恢复、归档、销毁等环节实现安全管理,CA 密钥应支持采用(3,5)秘密共享机制进行备份与恢复;
b) V2X 设备生成的签名密钥应使用硬件密码模块或安全芯片实现密钥的安全管理,硬件密码模块应达到 GB/T 37092 二级及以上安全要求,安全芯片应达到 GM/T 0008 二级及以上安全要求;
c) V2X 证书认证系统若涉及到密钥分发,应具备身份鉴别机制保证密钥接收者身份真实性的安全措施,应采用数字签名、HMAC 等密码技术保证分发密钥的完整性,应具备保证密钥的机密

性的安全措施；

d） 密钥在导入导出时应采取加密或秘密共享机制等安全方式进行；

e） 若涉及密钥衍生机制应采用安全的算法或机制；

注：密钥衍生机制基于一个公私钥对，扩展成多个公私钥对，同时确保只有知道原始私钥的设备才能正确扩展私钥。该机制用于 V2X 设备生成一对公私钥申请多个证书，减少 V2X 设备证书请求次数。

f） 密钥应具有明确用途；密钥使用过程中应有相应安全措施，防止被非授权访问、使用和篡改；

g） V2X 证书认证系统应支持密钥的备份与恢复，应以安全形式备份到安全存储介质中，应支持以安全形式恢复备份的密钥，密钥备份或恢复应进行记录以供审计；

h） 密钥在归档过程中，应使用有效的安全措施，保证归档密钥的安全性和正确性，归档密钥应只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息，密钥归档应进行记录以供审计，归档密钥应进行数据备份，并使用有效的安全保护措施；

i） 在密钥生命周期内发生泄露或有泄露风险时应支持密钥销毁。

检测方法：

a） 核实系统使用的所有 CA 密钥是否由硬件密码设备生成并存放在该密码设备中，检测是否支持采用(3,5)秘密共享机制进行密钥备份与恢复；

b） 系统通过调用密码设备使用 CA 密钥对随机产生的一段数据进行签名，保存签名值，然后从密码设备中删除 CA 密钥；从 5 个密钥备份分量中选择任意 3 个分量，检测系统是否能够通过密码设备恢复 CA 密钥，然后用恢复的 CA 密钥，对之前保存的签名值进行验签，检测是否验签通过；使用恢复的 CA 密钥对的私钥，对之前随机产生的一段数据再次进行签名，然后利用恢复的 CA 密钥对的公钥进行验签，检测是否验签通过；上述检测通过，则认为 CA 密钥恢复成功；

c） 检测机构证书签名或加密密钥对是否由经检测认证合格的密码设备产生，支持销毁和更新；

d） 检验 V2X 设备的注册/应用/身份证书的签名密钥及用于衍生假名证书最终签名密钥的种子密钥是否由 V2X 设备中的密码模块或安全芯片产生；

e） 检查密钥衍生的方案或密钥衍生的过程，确认密钥衍生是否采用安全的算法或机制；

f） 若 V2X 设备的应用/身份证书需要加密密钥对，则证书加密密钥对是否由经检测认证合格的密钥管理系统产生并负责安全管理。

结果判定：

若对应检测方法 a)～d)项均测试通过，则该检测项为通过。若 e)和 f)为涉及项，且测试通过，则该检测项为通过。

6.4 通信安全

6.4.1 注册证书管理通信安全

检测要求：

向 V2X 注册证书认证系统申请、更新注册证书时，应采用应用层加密或 TLCP 安全通道等措施，保证通信数据的安全。

检测方法：

a） 通过抓包验证、代码审查、模拟测试等方式，检测注册证书签发系统与 V2X 注册证书注册管理系统之间、V2X 设备与 V2X 注册证书注册管理系统之间的通信是否采用应用层加密或 TLCP 安全通道等措施，通信数据是否满足机密性、完整性、真实性要求；

b） 通过检测工具、文档审查等方式，检测通信过程是否采用了符合密码相关国家标准、行业标准要求的密码算法、密码技术、密码产品。

结果判定：

若对应检测方法 a)和 b)项均测试通过，则该检测项为通过。

6.4.2 授权证书管理通信安全

6.4.2.1 假名证书管理通信安全

检测要求：

a) 向授权证书认证系统申请假名证书时，应对用户身份相关的隐私信息（例如与用户身份相关的设备标识号等）进行安全保护；

b) 在申请假名时，V2X 设备和 PRA 之间、PRA 和 PCA 之间应采用应用层加密或 TLCP 安全通道等措施，保证通信数据的安全。

检测方法：

a) 通过抓包验证、代码审查、模拟测试等方式检测是否对用户身份相关的隐私信息（例如与用户身份相关的设备标识号等）进行安全保护；

b) 通过抓包验证、代码审查、模拟测试等方式，检测在申请假名证书时，V2X 设备和 PRA 之间、PRA 和 PCA 之间是否采用应用层加密或 TLCP 安全通道等措施，通信数据是否满足机密性、完整性、真实性要求；

c) 通过检测工具检测上述通信过程是否采用了符合密码相关国家标准、行业标准要求的密码算法、密码技术、密码产品。

结果判定：

若对应检测方法 a)～c)项均测试通过，则该检测项为通过。

6.4.2.2 应用证书和身份证书管理通信安全

检测要求：

向授权证书认证系统申请应用证书和身份证书时，V2X 设备与 ARA 之间、ARA 和 ACA 之间根据系统实现方式的不同，应采用应用层加密或 TLCP 安全通道等措施，保证通信数据的安全。

检测方法：

a) 通过抓包验证、代码审查、模拟测试等方式，检测在应用证书和身份证书管理流程中，V2X 设备与 ARA 之间、ARA 和 ACA 之间是否采用应用层加密或 TLCP 安全通道等措施，通信数据是否满足机密性、完整性、真实性要求；

b) 通过检测工具检测上述通信过程是否采用了符合密码相关国家标准、行业标准要求的密码算法、密码技术、密码产品。

结果判定：

若对应检测方法 a)和 b)项均测试通过，则该检测项为通过。

6.5 使用的密码产品

检测要求：

a) 密码产品应是经检测认证合格的产品；

b) 服务器宜采用独立的物理端口与密码设备连接。

检测方法：

a) 查看密码产品是否具有商用密码产品认证证书；

b) 查看密码设备与系统服务器连接方式是否符合要求。

结果判定：

若对应检测方法 a)和 b)项测试通过，则该检测项为通过。

6.6 V2X 证书

检测要求：

a) 证书应采用 COER 编码；

b) 证书签发者使用私钥对 V2X 证书信息进行数字签名，若是自签名证书，则用户身份标识 IDA 取值为 16 字节整数：0x31，0x32，0x33，0x34，0x35，0x36，0x37，0x38，0x31，0x32，0x33，0x34，0x35，0x36，0x37，0x38；若是非自签名证书，则用户身份标识应使用签发者证书实体的杂凑值，即计算 ID_A = HashedId32(Certificate)后进行比特串到字节串的转换，比特串到字节串的转换应遵循 GB/T 32918.1；

注：ID_A 为 V2X 证书进行 SM3 杂凑计算后的杂凑值。

c) 非自签证书的签发者信息，应为签发者证书实体进行 SM3 杂凑运算结果的后 8 个字节串；

d) 假名证书的标识应包含证书所在周期和链接值；

e) 证书的版本号为 2 或 3；

f) 证书中有效期信息包含正确的证书起始时间和有效时长；

g) 证书中 cracaId 取值应为证书撤销列表签发者证书或签发者的上级 CA 证书进行 SM3 杂凑运算结果后 3 字节；

h) 证书类型应取值为 0 或 1。

检测方法：

a) 通过对证书文件进行 COER 解码，判断证书采用了 COER 编码，则测试通过；

b) 使用证书签发者的公钥验证证书签名，若验签通过，则测试通过；

c) 对证书签发者的证书使用 SM3 算法进行计算，取计算结果的后 8 个字节串，证书中签发者信息与杂凑结果的后 8 个字节串一致，则测试通过；

d) 证书公钥为 SM2 椭圆曲线上的点，则测试通过；

e) 假名证书的标识中包含证书所在周期和链接值，则测试通过；

f) 证书的版本号为 2 或 3，则测试通过；

g) 证书中有效期符合要求，则测试通过；

h) 证书中 cracaId 取值符合要求，则测试通过；

i) 证书类型取值为 0 测试通过，若取值为 1 时应提供国家密码管理部门出具的证明文件或相关技术材料以供安全性审查。

结果判定：

若对应检测方法 a)～i)项测试通过，则该检测项为通过。

6.7 V2X 证书撤销列表

检测要求：

a) V2XCRL 应采用 COER 编码；

b) V2XCRL 签发者使用私钥对 V2XCRL 进行数字签名，签名使用的 IDA 为签发者证书实体进行 SM3 杂凑运算后的杂凑值；

c) 对 V2XCRL 签发者证书或签发者的上级 CA 证书进行 SM3 杂凑运算结果后，取计算结果的后 8 个字节串作为 V2XCRL 文件中 crlCraca 信息；

d) 非假名证书撤销后，将证书实体进行 SM3 杂凑运算后，取杂凑值的后 10 个字节串作为撤销证书的标识，存入 V2XCRL 中；

e) 假名证书撤销后，将假名证书的所在周期、周期链接种子值存入到 V2XCRL 中；
f) V2XCRL 的版本号为 1 或 2；
g) V2XCRL 中应包含正确的发布时间；
h) V2XCRL 中应包含正确的下次签发时间，且该时间应在发布时间之后。

检测方法：

a) 通过对 V2XCRL 文件进行 COER 解码，判断 V2XCRL 采用了 COER 编码，则测试通过；
b) 使用 V2XCRL 签发者的公钥验证 V2XCRL 签名，若验签通过，则测试通过；
c) 对 V2XCRL 签发者证书或签发者的上级 CA 证书进行 SM3 杂凑运算后，取计算结果的后 8 个字节串，V2XCRL 中 crlCraca 信息与杂凑结果的后 8 个字节串一致，则测试通过；
d) V2XCRL 中已撤销的非假名证书的信息与其证书实体进行 SM3 杂凑运算结果的后 10 个字节串一致，则测试通过；
e) V2XCRL 中已撤销的假名证书的信息包含证书所在的周期及周期链接种子值，则测试通过；
f) V2XCRL 的版本号为 1 或 2，则测试通过；
g) V2XCRL 中发布时间符合要求，则测试通过；
h) V2XCRL 中下次签发时间在发布时间之后，则测试通过。

结果判定：

若对应检测方法 a)～h)项测试通过，则该检测项为通过。

6.8 系统功能

6.8.1 V2X 二级证书管理系统和中间证书管理系统

6.8.1.1 机构证书签发

检测要求：

a) 应能使用符合密码相关行业标准或国家标准的密码算法签发机构证书；
b) 下一级机构证书签名有效性应能通过上一级机构证书验证。

检测方法：

a) 查看系统签发机构证书的功能，判断是否符合检测内容的要求；
b) 验证下一级机构证书签名的有效性，判断是否符合检测内容的要求。

结果判定：

若对应检测方法 a)和 b)项测试通过，则该检测项为通过。

6.8.1.2 机构证书更新

检测要求：

系统应能为机构证书提供证书更新服务。

检测方法：

查看系统功能，并执行证书签发服务，判断是否符合检测内容的要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.1.3 机构证书撤销

检测要求：

系统应能提供证书撤销服务。机构证书撤销后，应能正确签发基于证书杂凑值的 V2XCRL。

检测方法：

查看系统功能，并执行证书撤销服务，判断是否符合检测内容的要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.2 V2X 注册证书认证系统

6.8.2.1 注册证书签发

检测要求：

a) 系统应能为身份认证通过后的 V2X 设备签发注册证书；
b) 注册证书的密钥对应由 V2X 设备产生，在申请注册证书时，应使用私钥对证书请求报文进行签名，V2X 注册证书认证系统收到报文后应验证报文的签名；
c) V2X 注册证书认证系统应对发送给 V2X 设备的包含注册证书信息的应答报文进行签名。

检测方法：

模拟执行注册证书申请流程，获取 V2X 设备与注册证书认证系统之间的报文信息进行分析，判断是否符合检测要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.2.2 注册证书更新

检测要求：

a) V2X 设备的注册证书即将到期时，V2X 设备应使用新密钥对发起注册证书更新请求，V2X 设备应对请求报文进行签名，V2X 注册证书认证系统收到报文后应对证书更新请求报文、证书撤销列表以及证书有效期进行验证，通过后，可签发新的注册证书并返回给 V2X 设备实体；
b) V2X 注册证书认证系统应对发送给 V2X 设备的包含注册证书信息的应答报文进行签名；
c) 若 V2X 设备的注册证书过期或已被撤销，V2X 设备应重新申请注册证书。

检测方法：

a) 使用有效注册证书申请更新，模拟执行注册证书更新流程，获取报文信息进行分析，判断是否符合检测要求；
b) 使用已过期的注册证书申请更新，模拟执行注册证书更新流程，判断 V2X 注册证书认证系统是否能够拒绝为其更新注册证书；
c) 使用已撤销的注册证书申请更新，模拟执行注册证书更新流程，判断 V2X 注册证书认证系统是否能够拒绝为其更新注册证书。

结果判定：

若对应检测方法 a)～c)项测试通过，则该检测项为通过。

6.8.2.3 注册证书撤销

检测要求：

a) 应能为已申请注册证书的 V2X 设备提供注册证书撤销服务；
b) 注册证书被撤销时，应签发基于证书杂凑值的 V2XCRL。

检测方法：

执行注册证书撤销流程，获取 V2XCRL，判断是否符合检测要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.3 V2X 授权证书认证系统

6.8.3.1 授权证书签发

检测要求：

a) 授权证书的签名密钥对或用于衍生最终签名密钥对的种子密钥应由 V2X 设备产生；

b) V2X 设备使用注册证书申请授权证书，授权证书认证系统的证书注册管理系统对申请信息解密后，应验证申请消息中携带的注册证书的有效性，并验证消息签名；

c) 授权证书认证系统为 V2X 设备签发假名证书时，证书标识字段应填充链接值管理系统生成的链接值，链接值应由链接值管理系统加密后传递给授权证书认证系统的证书管理系统；

d) 授权证书认证系统的授权证书签发系统返回包含假名证书的消息时，应由授权证书签发系统对消息加密并签名，消息加密密钥由 V2X 设备产生，消息签名密钥由授权证书签发系统产生；

e) 授权证书认证系统的证书注册管理系统返回给 V2X 设备的应答消息时，应由授权证书注册管理系统对应答消息签名。

检测方法：

a) 获取 V2X 设备发送给授权证书注册管理系统的证书请求报文，且送检方解析报文后提供 V2X 设备产生的公钥信息，检测公钥是否为 SM2 椭圆曲线上的点，若是则此项检测通过；

b) 使用无效的(过期、未生效或已被撤销)的注册证书去申请授权证书，模拟执行假名证书、应用证书/身份证书申请流程，判断 V2X 授权证书认证系统是否能够拒绝为其签发证书；

c) 使用有效的注册证书去申请授权证书，模拟执行假名证书、应用证书/身份证书申请流程，获取报文信息进行分析，判断是否符合检测要求。

结果判定：

若对应检测方法 a)～c)测试通过，则该检测项为通过。

6.8.3.2 授权证书下载

检测要求：

V2X 设备使用注册证书下载授权证书，授权证书认证系统的注册管理系统对下载请求消息解密后，应验证申请消息中携带的注册证书的有效性，并验证消息签名。

检测方法：

模拟执行假名证书、应用证书/身份证书下载流程，获取 V2X 设备与授权证书注册管理系统之间报文信息进行分析，判断是否满足检测要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.3.3 授权证书撤销

检测要求：

a) 应能为已经注册的 V2X 设备提供假名证书、应用证书和身份证书撤销服务；

b) 假名证书被撤销时，应签发基于链接值的 V2XCRL；

c) 应用证书和身份证书被撤销时，应签发基于证书杂凑值的 V2XCRL。

检测方法：

执行假名证书、应用证书和身份证书撤销流程，获取 V2XCRL，判断是否满足检测要求。

结果判定：

若对应检测方法通过，则该检测项为通过。

6.8.3.4 链接值

检测要求：

a) 初始链接种子应是密码设备或密码模块生成的随机数，其质量满足 6.2 的要求；

b) 通过初始链接种子、周期数以及其他固定参数因子采用 SM3 算法派生出后续的周期链接种子；

c) 通过周期链接种子、周期数及证书所在周期的顺序采用 SM4 算法可以派生出固定数量的链接值。

检测方法：

a) 验证初始链接种子是否满足 GM/T 0005 要求；

b) 现场采集 10 组初始链接种子和后续 10 个周期的链接种子数据，测试人员通过初始链接种子进行后续 10 个周期链接种子值的派生，现场计算的结果与采集的数据一致；

c) 现场采集 10 组周期链接种子和对应的链接值数据，测试人员利用周期链接种子进行派生链接值，派生出来的链接值应与采集的链接值数据一致。

结果判定：

若对应检测方法 a)～c)项测试通过，则该检测项为通过。

6.8.4 V2X 证书/CRL 存储系统

检测要求：

a) 系统应提供 V2XCRL 下载服务，并且支持通过 cracaId、crlSeries、crl 类型等条件进行组合检索，V2X 设备通过此服务下载 V2XCRL，用于验证证书的有效性；

b) 操作员登录系统后，通过管理界面可以检索已存储的证书及 V2XCRL；

c) 系统应提供可信域证书的下载服务，V2X 设备通过此服务下载所需的可信域证书；

d) 系统应记录操作日志，日志应包含操作人员、操作时间、操作行为、操作结果等内容，并通过密码算法保障日志的完整性；

e) 业务管理员、业务操作员、审计员登录系统时，应采用包含数字签名技术等的双因素模式；

f) 业务管理员、业务操作员、审计员在进行系统管理时，应对自己发起的请求报文进行数字签名。

检测方法：

a) 界面输入查询条件进行证书检索，若能响应检索结果则通过测试；

b) 通过调用 V2XCRL 下载接口，若可以正常下载 V2XCRL 文件则通过测试；

c) 界面输入查询条件进行 V2XCRL 检索，若能响应检索结果则通过测试；

d) 若通过日志管理界面可以查询到相关的证书操作记录且能正确校验日志是否被篡改，则测试通过；

e) 若是独立系统需检查系统登录过程是否符合双因素要求，若符合则测试通过；

f) 若是独立系统需现场获取系统管理请求报文，并对请求报文进行验签，若通过验签，则测试通过。

结果判定：

若对应检测方法 a)～f)项测试通过，则该检测项为通过。

6.8.5 授权证书签发性能

6.8.5.1 应用/身份证书签发性能

检测要求：

应测试从 V2X 设备发送应用/身份证书申请到接收到包含应用/身份证书实体响应的时间差。

检测方法：

a) 记录从 V2X 设备发送应用/身份证书证书请求到 ARA 的时间点，记录为 T_1；

b) 记录 V2X 设备接收到应用/身份证书响应的时间点，记录为 T_2；

c) 记录从 ARA 发送应用/身份证书证书请求到 ACA 的时间点，记录为 T_3；

d) 记录 ARA 接收到应用/身份证书响应的时间点，记录为 T_4；

e) 记录 V2X 设备发送应用/身份证书下载证书请求到 ARA 的时间点，记录为 T_5；

f) 记录 V2X 设备接收到应用/身份证书证书实体响应的时间点，记录为 T_6；

g) 计算应用/身份证书签发耗时 $T=(T_2-T_1)+(T_4-T_3)+(T_6-T_5)$的时间。

结果判定：

(T_2-T_1)、(T_4-T_3)、(T_6-T_5)的值不超过 20 s，T 的值不超过 30 s，则通过此项检测。

6.8.5.2 假名证书签发性能

检测要求：

应测试从 V2X 设备发送假名证书申请到接收到包含假名证书实体响应的时间差。

检测方法：

a) 记录从 V2X 设备发送假名证书请求到 PRA 的时间点，记录为 T_1；

b) 记录 V2X 设备接收到假名证书响应的时间点，记录为 T_2；

c) 记录从 PRA 发送假名证书证书请求到 PCA 的时间点，记录为 T_3；

d) 记录 PRA 接收到假名证书响应的时间点，记录为 T_4；

e) 记录 V2X 设备发送到假名证书下载证书请求到 PRA 的时间点，记录为 T_5；

f) 记录 V2X 设备接收到假名证书证书实体响应的时间点，记录为 T_6；

g) 计算假名证书签发耗时 $T=(T_2-T_1)+(T_4-T_3)+(T_6-T_5)$的时间。

结果判定：

(T_2-T_1)、(T_4-T_3)、(T_6-T_5)的值不超过 20 s，T 的值不超过 30 s，则通过此项检测。

6.9 互联互通

检测要求：

V2X 证书认证系统产品应支持接入国家密码管理部门统一规划建设的电子认证信任源。

检测方法：

a) 检测是否支持配置国家根证书；

b) 检测是否支持配置国家根签发的二级 CA 证书；

c) 检测是否支持加入国家根签发的可信根证书列表。

结果判定：

若对应检测方法 a)测试通过，且 b)或 c)测试通过，则通过此项检测。

7 送检文档要求

按照检测认证机构要求提交相关文档资料，作为送检产品的检测依据。文档资料包括但不限于包

括 V2X 证书认证系统的技术工作总结报告、安全性设计报告、用户手册文档，主要描述内容如下：

a） 技术工作总结报告：描述 V2X 证书认证系统研制的背景和意义、研制过程、设计原则、逻辑结构、系统工作原理、工作流程、通信设计、密钥管理、关键技术及创新点、主要技术指标、印制版图及实物图等；

b） 安全性设计报告：描述 V2X 证书认证系统的需求分析、安全性设计、安全性分析与评估等；

c） 用户手册：描述用户对 V2X 证书认证系统使用和操作的技术手册。

8 判定规则

合格判定应满足如下要求：任何一项检测结果不符合相应检测要求的，即判定为不合格，否则判定为合格。

附 录 A
（规范性）
V2X 证书结构

附录 A 给出了 V2X 证书格式基本结构、CA 证书结构、RA 证书结构、注册证书结构、假名证书结构、应用证书/身份证书结构。

V2X 证书格式基本结构见表 A.1。

表 A.1 V2X 证书格式基本结构

字段项	数据域 1	数据域 2	说明
版本		version	证书结构版本，取值为 2 或 3
类型		type	证书结构类型取值为 0 或 1
签发者		issuer	自签证书，取值为 Hash 算法类型值； 非自签证书，取值为签发此证书的 CA 证书的 HashedId8 值，采用 SM3 密码算法
签名数据	toBeSigned	id	证书标识
		cracaId	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3，若不使用设置为全零
		crlSeries	CRL 系列号，若不使用设置为全零
		validityPeriod	有效期
		region	有效地理范围
		assuranceLevel	保证级别
		appPermissions	应用数据签名权限（例如 OBU/RSU 签名的应用消息类型）
		certIssuePermissions	适用于 CA 证书，描述可签发的证书种类和权限范围
		certRequestPermissions	适用于 RA 证书和注册证书，描述可申请的证书种类、权限范围
		canRequestRollover	是否能够用于请求同等权限的证书
		encryptionKey	加密公钥，默认采用 SM2 密码算法，用于加密会话密钥及消息
		verifyKeyIndicator	type 为 0 时，取值为签名公钥； type 为 1 时，取值为公钥重构值。 默认采用 SM2 密码算法 用于对消息的签名验签，对应私钥存储在密码模块或安全芯片中
签名值		signature	type 为 0 时，用于存储证书的签名值； type 为 1 时，此字段不存在。 默认采用 SM2 和 SM3 密码算法

CA 证书结构见表 A.2。

表 A.2 CA 证书结构

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	证书结构版本，取值为 2 或 3
类型		type	是	证书结构类型取值为 0
签发者		issuer	是	自签证书，取值为 Hash 算法类型值； 非自签证书，取值为签发此证书的 CA 证书的 HashedId8
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3，若不使用设置为全零
		crlSeries	是	CRL 系列号，若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	保证级别
		appPermissions	是	应用数据签名权限、撤销权限等
		certIssuePermissions	是	适用于 CA 证书，描述可签发的证书种类和权限范围
		canRequestRollover	否	是否能够用于请求同等权限的证书
		encryptionKey	否	加密公钥
		verifyKeyIndicator	是	签名公钥
签名值		signature	是	签名值

RA 证书结构见表 A.3。

表 A.3 RA 证书结构

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	证书结构版本，取值为 2 或 3
类型		type	是	证书结构类型取值为 0
签发者		issuer	是	签发此证书的 CA 证书的 HashedId8 值
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3，若不使用设置为全零
		crlSeries	是	CRL 系列号，若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	保证级别

表 A.3　RA 证书结构（续）

字段项	数据域 1	数据域 2	是否必选	说明
签名数据	toBeSigned	appPermissions	是	应用数据签名权限(例如 OBU/RSU 签名的应用消息类型)
		certRequestPermissions	是	适用于注册证书,描述可申请的证书种类、权限范围
		canRequestRollover	否	是否能够用于请求同等权限的证书
		encryptionKey	是	加密公钥
		verifyKeyIndicator	是	签名公钥
签名值		signature	是	签名值

注册证书结构见表 A.4。

表 A.4　注册证书结构

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	证书结构版本,取值为 2 或 3
类型		type	是	证书结构类型取值为 0
签发者		issuer	是	签发此证书的 CA 证书的 HashedId8 值
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3,若不使用设置为全零
		crlSeries	是	CRL 系列号,若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	保证级别
		appPermissions	是	应用数据签名权限(例如 OBU/RSU 签名的应用消息类型)
		certRequestPermissions	是	适用于 RA 证书和注册证书,描述可申请的证书种类、权限范围
		canRequestRollover	否	是否能够用于请求同等权限的证书
		encryptionKey	否	加密公钥
		verifyKeyIndicator	是	签名公钥
签名值		signature	是	签名值

假名证书结构见表 A.5。

表 A.5　假名证书结构

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	证书结构版本，取值为 2 或 3
类型		type	是	证书结构类型，取值为 0 或 1
签发者		issuer	是	签发此证书的 CA 证书的 HashedId8 值
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3，若不使用设置为全零
		crlSeries	是	CRL 序列号，若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	保证级别
		appPermissions	是	应用数据签名权限（例如 OBU/RSU 签名的应用消息类型）
		canRequestRollover	否	是否能够用于请求同等权限的证书
		encryptionKey	否	加密公钥
		verifyKeyIndicator	是	type 为 0 时，取值为签名公钥； type 为 1 时，取值为公钥重构值
签名值		signature	否	type 为 0 时，用于存储证书的签名值； type 为 1 时，此字段不存在

应用证书/身份证书结构见表 A.6。

表 A.6　应用证书/身份证书结构

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	证书结构版本，取值为 2 或 3
类型		type	是	证书结构类型，取值为 0 或 1
签发者		issuer	是	签发此证书的 CA 证书的 HashedId8 值
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId3，若不使用设置为全零
		crlSeries	是	CRL 系列号，若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	保证级别
		appPermissions	是	应用数据签名权限（例如 OBU/RSU 签名的应用消息类型）

表 A.6　应用证书/身份证书结构（续）

字段项	数据域 1	数据域 2	是否必选	说明
签名数据	toBeSigned	canRequestRollover	否	是否能够用于请求同等权限的证书
		encryptionKey	否	加密公钥
		verifyKeyIndicator	是	type 为 0 时，取值为签名公钥； type 为 1 时，取值为公钥重构值
签名值		signature	否	type 为 0 时，用于存储证书的签名值； type 为 1 时，此字段不存在

附 录 B
（规范性）
V2X 证书撤销列表结构

安全的证书撤销列表结构——SecuredCrl 见表 B.1。

表 B.1 安全的证书撤销列表结构——SecuredCrl

字段项	数据域 1	数据域 2	数据域 3	数据域 4	数据域 5	数据域 6	数据域 7	数据域 8	说明
协议版本	protocol Version								协议版本号为 3
协议内容	content								包含安全协议数据的内容
签名结构		signed Data							签名结构
杂凑算法			Hash Algorithm						默认采用国密 SM3 算法
签名数据			toBe Signed Data						包含生成或验证签名时要进行哈希处理的数据
				Signed Data Payload					包含 ToBeSignedData 的数据载荷
					data				承载在数据结构中明确传输的数据
						protocol Version			协议版本号为 3
						content			包含安全协议数据的内容
							unsecured Data		指示用八位字节串表征的无安全处理数据
								Crl Contents	详情见表 B.2，证书撤销列表内容结构
				header Info					包含插入的附加数据指示
					aid				发送方宣称的与有效负载相关联的应用领域，此处取值 3628
签名者			Signer Identifier						签发此 V2XCRL 的签发者证书或证书的 HashedId8 值，默认采用 SM3 密码算法
签名值			signature						用于存储 V2XCRL 的签名值，默认采用 SM2 和 SM3 密码算法

证书撤销列表内容结构——CrlContents 见表 B.2。

表 B.2　证书撤销列表内容结构——CrlContents

字段项	数据域 1	数据域 2	是否必选	说明
版本		version	是	version 是 CRL 的版本号，取值为 1 或 2
V2XCRL 系列号		crlSeries	是	CRL 系列号
授权签发 V2XCRL 的 CA		crlCraca	是	V2XCRL 签发者证书或签发者上级 CA 证书的 HashedId8 值
V2XCRL 签发时间		issueDate	是	CRL 的发布时间
预期下次 V2XCRL 签发时间		nextCrl	是	包含预期发出具有相同 crlSeries 和 crlCraca 的下一个 CRL 的时间
优先级		priorityInfo	是	所包含的信息可协助存储空间有限的设备确定要保留哪些撤销信息以及丢弃哪些撤销信息
V2XCRL 正文选择结构体	typeSpecific	fullHashCrl	4 选 1	包含一个基于杂凑值的全量 CRL，即包含所有已撤销证书的杂凑值列表
		deltaHashCrl		包含基于杂凑值的增量 CRL，即所有增量的已撤销证书的杂凑值列表
		fullLinkedCrl		包含一个基于 Linkage ID 的全量 CRL，即包含所有已撤销证书的个体和/或群组链接数据的列表
		deltaLinkedCrl		包含基于 Linkage ID 的增量 CRL，即包含所有增量的已撤销证书的个体和/或群组链接数据的列表

参 考 文 献

[1] GB/T 16262(所有部分) 信息技术抽象语法记法一(ASN.1)
[2] GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范
[3] GB/T 37376 交通运输 数字证书格式
[4] GB/T 38636 信息安全技术 传输层密码协议(TLCP)
[5] 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

中华人民共和国密码
行业标准
V2X证书认证系统检测规范
GM/T 0141—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 2.25　字数 45 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39092　定价 59.00 元

GM/T 0141-2024