ICS 03.220.20
CCS R 80

团 体 标 准

T/ITS 0127-2020

面向车路协同的通信证书管理技术规范

Technical specification of communication certificate management for vehicle Infrastructure cooperative system

2020-12-31 发布 2021-03-01 实施

中国智能交通产业联盟 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。

本文件由中国智能交通产业联盟（C-ITS）提出并归口。

本文件起草单位：华为技术有限公司、北京中交国通智能交通系统技术有限公司、大唐电信科技产业集团（电信科学技术研究院）、吉大正元信息技术股份有限公司、中国移动通信集团有限公司、高通无线通信技术（中国）有限公司、深圳东进技术股份有限公司、中国信息通信研究院、上海汽车集团股份有限公司、格尔软件股份有限公司、东软集团股份有限公司、深圳成谷科技有限公司、北京信安世纪科技股份有限公司、郑州信大捷安信息股份有限公司。

本文件主要起草人：潘凯、梅新明、周洲、王立岩、徐晖、周巍、才君、杜军委、田野、粟栗、陈书平、刘义鹏、于润东、葛雨明、邹清全、高吉、赵炜铭、祁帅、张宏彬、刘驰、康亮、周吉祥。

面向车路协同的通信证书管理技术规范

1 范围

本文件规定了 OBU/RSU 申请通信证书的接口规范，包括申请身份证书和应用证书的接口规范。

本文件适用于申请身份证书/应用证书的 OBU/RSU。

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 16264.8 信息技术开放系统互连目录 第 8 部分：公钥和属性证书框架

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

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 分组密钥算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GB/T 37376 交通运输 数字证书格式

YD/T 3594-2019 基于 LTE 网络的车联网通信安全技术要求

YD/T 3707-2020 基于 LTE 的车联网无线通信技术 网络层技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

合作式智能运输系统 cooperative intelligent transportation system, C-ITS

通过人、车、路信息交互，实现车辆和基础设施之间、车辆与车辆、车辆与人之间的智能协同与配合的一种智能运输系统体系。

3.2

注册证书机构 enrollment certificate authority

负责向 OBU、RSU 签发注册证书的授信机构。

3.3

应用证书机构 application certificate registration authority

验证身份证书和应用证书，并向 ACA 转发 OBU/RSU 相关请求消息的授信机构。

3.4

应用证书注册机构 application certificate authority

负责向 RSU 签发应用证书、向 OBU 签发身份证书的授信机构。

3.5

根证书机构 root certificate authority

车联网安全体系中某个 PKI 系统中最高级别的 CA，根据需要向下级 CA 签发子 CA 证书，例如 ECA、ACA 等。

3.6

身份证书 identification certificate

OBU 向 RSU 证明其身份以获得某种应用服务所使用的证书。

3.7

应用证书 application certificate

RSU 用于对其广播的某种应用消息进行签名的证书。

3.8

通信证书 communication certificate

本文件对身份证书和应用证书的统称。

4 符号和缩略语

下列缩略语适用于本文件。

AAA：认证授权机构（Authentication and Authorization Authority）

ACA：应用证书机构（Application Certificate Authority）

ARA：应用证书注册机构（Application certificate Registration Authority）

CA：证书机构（Certificate Authority）

CRA：证书撤销机构（Certificate Revocation Authority）

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

CTL：证书可信列表（Certificate Trust List）

CTRA：证书可信关系管理机构（Certificate Trust Relationship Authority）

ECA：注册证书机构（Enrolment Certificate Authority）

ICA：中间证书机构（Intermediate CA）

LA：链接机构（Linkage Authority）

MA：异常行为管理机构（Misbehavior Authority）

OBU：车载单元（On Board Unit）

PCA：假名证书机构（Pseudonym Certificate Authority）

PKI：公钥基础设施（Public Key Infrastructure）

RA：注册机构（Registration Authority）

RCA：根证书机构（Root Certificate Authority）

RSU：路边单元（Road Side Unit）

TCMF：可信证书管理功能（Trusted Certificate Management Function）

TDCL：可信域 CA 证书列表（Trusted Domain CA Certificates List）

TLS：传输层安全（Transport Layer Security）

TRC：可信根证书（Trusted Root Certificate）

TRCL：可信根证书列表（Trusted Root Certificate List）

TRCLA：可信根证书列表管理机构（Trusted Root Certificate List Authority）

5 总体架构

本文件中证书管理系统基于 PKI 实现，其架构如图 1 所示。实际应用时，图中各逻辑实体可以根据实际设备开发及部署需要合设或者分设，并可以根据政策法规，行业监管要求和业务运营需要，由不同机构分层分级部署、管理和运营。

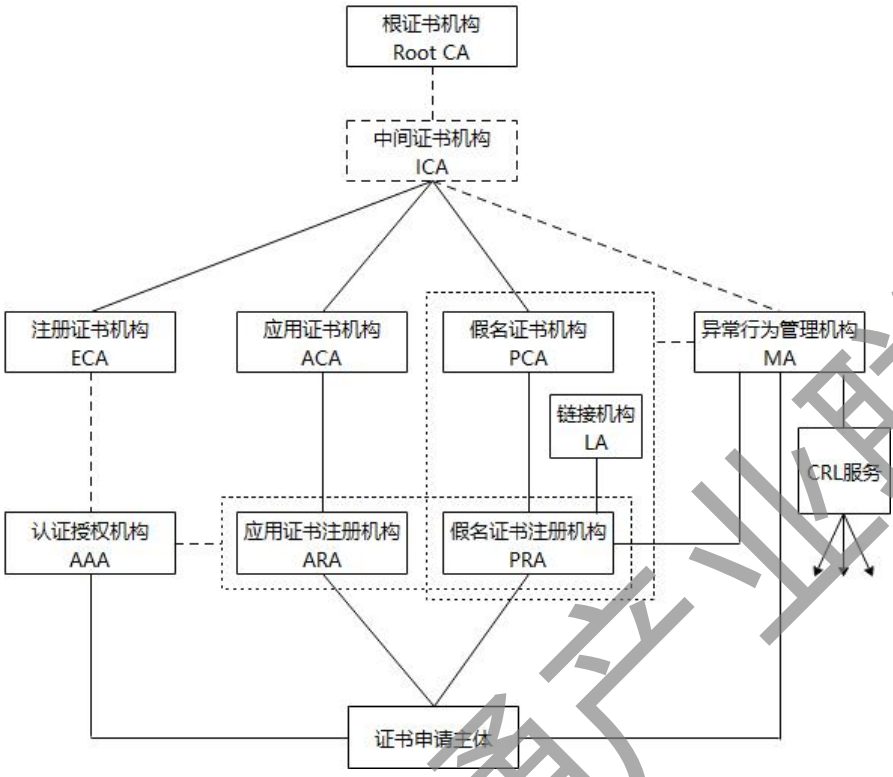

图 1 证书管理系统架构

证书管理系统架构中个单元功能如下：

- RCA：证书管理系统的信任根，负责系统根证书的管理与维护并对 CA 进行注册审批。在确认 CA 的合法性之后，根证书机构为其签发管理机构的数字证书，使其成为系统内的有效实体。
- ICA：证书管理系统可根据 PKI 部署的实际需要，在根证书机构与 CA 之间部署中间证书机构，以支持多层级 CA 部署方式。
- CA：是证书管理系统中各种证书机构的统称。根据证书类型及用途不同可分为：ECA、PCA、ACA。ECA、PCA、ACA 由 RA 和 CA 构成，前者负责证书申请主体的注册审批管理，后者负责数字证书的签发管理。与 ECA 和 PCA 相关的内容不在本文件范围内。
- LA：为假名证书生成链接值，以支持假名证书的批量撤销，不在本文件范围内。
- MA：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，不在本文件范围内。
- AAA：负责证书申请主体的身份认证和授权。在设备初始化阶段，为证书申请主体签发注册数字证书或其他类型的安全凭证，使其能够凭借获得的安全凭证与 CA 安全交互并获取相应的证书。认证授权机构还可以对证书申请主体向 CA 证书请求进行授权，不在本文件范围内。
- 证书申请主体：包括 OBU、RSU 等。

6 OBU/RSU 申请通信证书的流程

6.1 总则

本节主要介绍申请通信证书时所涉及到的流程，如图 2 所示，主要包括申请通信证书、更新通信证书和申请 CRL 的流程。

6.2 通信证书申请流程

申请通信证书前，OBU 或 RSU 应与 ARA 采用安全环境、应用层加密、TLS 安全通道等措施建立安全连接。

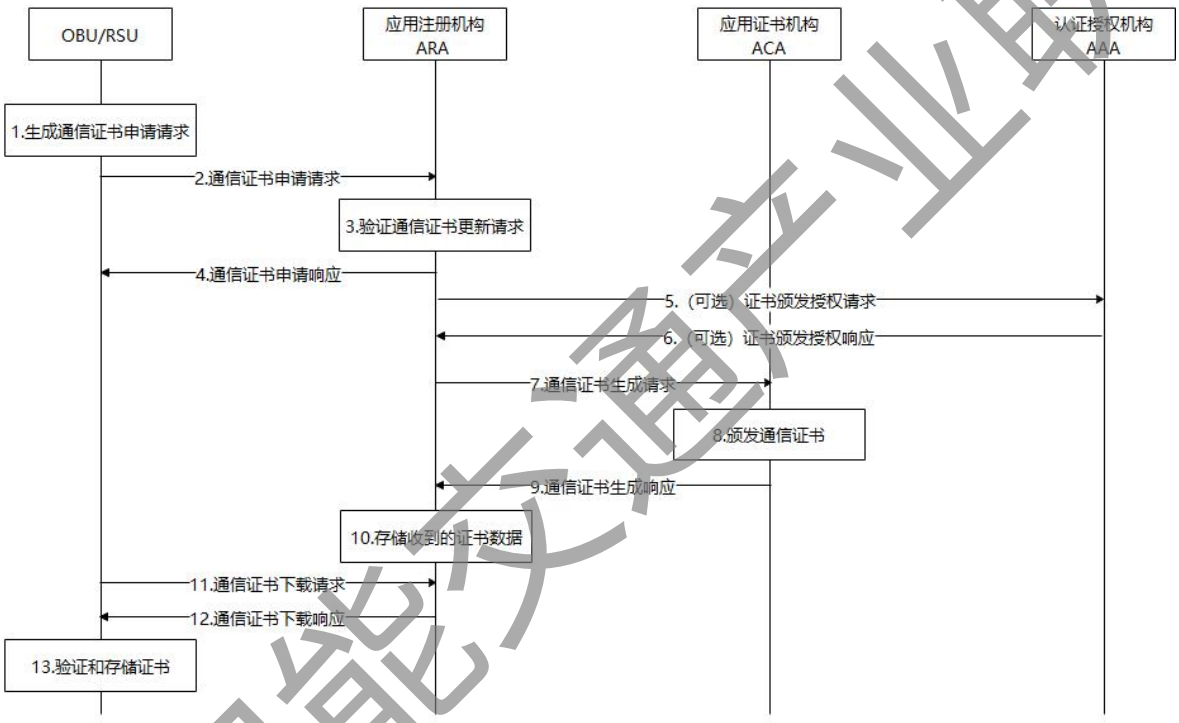

图 2 OBU/RSU 请求通信证书的过程

1. OBU/RSU 为所申请证书生成用于签名功能的公私密钥对，并生成通信证书请求消息，并使用其注册证书的私钥对上述消息进行签名。若所申请证书中应包含有专门用于数据加密的加密公钥，则还应生成一个用于数据加密的公私密钥对。基于具体的安全需求，可对通信证书申请消息提供机密性保护。机密性保护应使用接收方的公钥证书中的公钥对通信证书申请请求消息进行公钥加密保护。若接收方公钥证书中包含有加密公钥，则应优先使用该加密公钥。
2. OBU/RSU 将签名的通信证书请求消息连同注册证书发送给 ARA。
3. ARA 首先验证注册证书的有效性，例如有效期和是否已被撤销等，然后使用 OBU/RSU 注册证书中的公钥验证通信证书请求消息签名的正确性。若该消息为加密消息，则在验证消息签名之前使用与加密公钥对应的私钥对加密消息进行解密。
4. ARA 向 OBU/RSU 返回应用证书申请响应。响应中包含所申请证书的下载时间和与所下载证书相

关的标识等信息。

5. 若此证书颁发过程需要具有证书颁发授权能力的 AAA 的授权，则 ARA 应向该 AAA 发送证书颁发授权请求。授权请求中应包含有该 OBU/RSU 标识和代表证书应用领域的应用标识信息，并可包含有描述证书具体适用领域权限的应用描述信息和描述该应用对 OBU/RSU 本身需求的设备需求描述信息。若 OBU/RSU 证书请求消息中包含有 OBU/RSU 提供给 AAA 的数据，则应在该授权请求中包含有该数据。AAA 的地址可由 OBU/RSU 通过其证书申请消息提供，或由 ARA 本地配置的数据确定。
6. AAA 检查 ARA 发送的授权请求，包括包含在授权请求中的由 OBU/RSU 生成的车辆和/或设备描述信息，确定是否允许向该 OBU/RSU 颁发所申请的应用证书。若允许，则 AAA 应为该 OBU/RSU 颁发一个经其数字签名的授权令牌，并将该授权令牌发送给 ARA。
7. ARA 基于本地证书颁发策略确定是否向该 OBU/RSU 颁发证书。若允许，则为该 OBU/RSU 生成一个通信证书生成请求，并将该请求发送给 ACA
8. ACA 基于 ARA 发送的证书生成请求为该 OBU/RSU 生成一个通信证书。
9. ACA 将生成的通信证书通过证书生成响应发送给 ARA。
10. ARA 使用接收到的 OBU/RSU 应用证书数据生成证书下载包，并存储证书下载包以供 OBU/RSU 下载。
11. OBU/RSU 向 ARA 发送应用证书下载请求，其中包含有与下载证书相关的标识信息。
12. ARA 依据下载请求中的标识信息，获取存储在本地的 OBU/RSU 应用证书数据，生成应用证书下载包，然后通过应用证书下载响应发送给 OBU/RSU。
13. OBU/RSU 验证应用证书下载响应，并存储颁发的应用证书。

6.3 通信证书更新流程

当 OBU/RSU 所使用的通信证书不再有效（包括过期、被吊销等）时，需要执行通信证书更新流程。流程同 6.2。

6.4 CRL 申请流程

当 OBU/RSU 收到对端发来的消息时，首先需要确认对端所使用的通信证书是否已经被撤销，在确定通信证书没有被撤销时再对通信证书和消息签名进行验证。OBU/RSU 通信证书的撤销，主要基于不当行为机制实现。当 MA 收到针对某 OBU/RSU 的不当行为上报信息后，根据 MA 的不当行为决策策略，判断该 OBU/RSU 通信证书是否需要撤销。当判断该 OBU/RSU 通信证书需要撤销时，由 MA 负责该设备应用证书、身份证书 CRL 的签发。同时，ARA 也可将注册证书加入黑名单，当收到通信证书申请时，拒绝该申请。

当通信证书的撤销列表过大时，可根据实际需求，针对不同的设备类型、证书类型、地理区域的证

书，签发不同的 CRL，以减小单个 CRL 文件的大小。本文件支持全量和增量 CRL，CRL 签发机构可根据实际情况，签发全量和增量 CRL。

证书撤销列表相关应用使用的 AID，其应用标识取值为十进制 3628。

在下载 CRL 前，OBU/RSU 应和 ARA 建立 TLS 安全通道，如图 3 所示，OBU/RSU 获取证书撤销列表的过程如下：

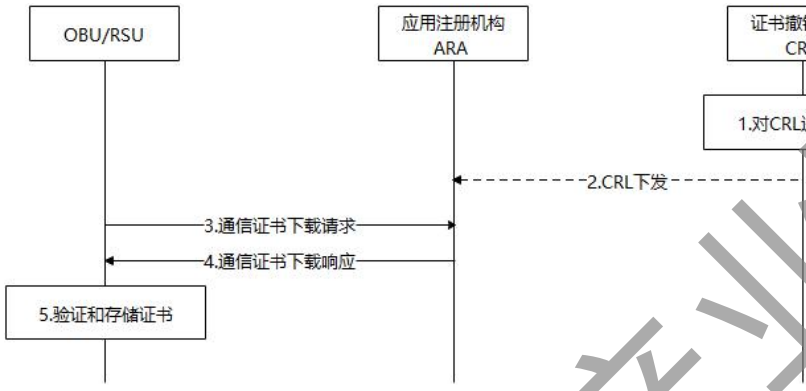

图 3　OBU/RSU 请求 CRL 的过程

1. 证书撤销机构 CRA（可与 ACA 合并设置）根据 CRA 的证书撤销列表更新策略，定期更新 CRL，并使用 CRA 的私钥对 CRL 签名。
2. CRA 将生成的 CRL 下发至 ARA。
3. OBU/RSU 根据设备的 CRL 更新策略，向 ARA 发送 CRL 下载请求。
4. ARA 将向 OBU/RSU 发送 CRL 下载应答。
5. OBU/RSU 先验证 CRL 的签名有效性和内容完整性，然后判断是否更新本地 CRL，若需要更新，则将 CRL 写入本地安全存储中。

7　OBU/RSU 与 ARA 间的接口要求

7.1 通信证书申请接口要求

以下接口用于 OBU/RSU 向 ACA 申请通信证书。

- 证书申请请求类型：HTTP POST 或 HTTPS POST
- HTTP Content-Type: application/octet-stream

HTTP request body 中包含版本信息、时间、公钥等参数，具体如下：

- version：包含结构的当前版本，在本文件中此处版本号为 1。
- generationTime：包含通信证书请求生成时间。
- type：指示 OBU/RSU 申请的证书类型。
- cracaId：指示颁发此证书的 CRL CA 的证书的哈希值，本文件置为全 0。
- crlSeries：指示 CRL 序列号，本文件中取值为 0。

- appPermissions：指示所具有的应用数据签名权限（例如 OBU/RSU 签名的应用消息类型）。
- verifyKeyIndicator：包含 OBU/RSU 发送的公钥信息。

HTTP response body 中包含版本信息、证书下载时间等参数，具体如下：

- version：包含结构的当前版本，在本文件中此处版本号为 1。
- generationTime：包含通信证书响应生成时间。
- requestHash：包含对应的通信证书申请的哈希值。
- nextDlTime：在此时间之后，OBU/RSU 可以连接到 ARA 以下载通信证书。

以下接口用于 OBU/RSU 从 ARA 下载通信证书。

- 证书下载请求类型：HTTP GET 或 HTTPS GET
- 响应中包含通信证书等参数。

7.2 CRL 申请接口要求

以下接口用于 OBU/RSU 申请证书撤销列表。

- 证书撤销列表申请请求类型：HTTP GET 或 HTTPS GET
- 响应中包含证书吊销列表等参数。

8 互信机制

8.1 互信架构

车联网安全系统可能由多个独立 PKI 系统构成，此时这些 PKI 系统之间可以根据需要构建可信关系，以便实现证书互认，实现多 PKI 体系可信关系的原理如图 4 所示。多个车联网 PKI 系统之间的可信关系是通过一个 CTL 实现的。该可信列表由 CTRA。CTL 的存在与否不会影响各个独立 PKI 系统的运行，但会影响不同 PKI 系统证书之间是否能够互认。车联网系统可以根据需要动态地向 CTL 添加或从 CTL 中移除根 CA 证书。当新 CTL 列表产生后，旧 CTL 列表自动作废。关于 CTL 列表的添加、移除等操作不在本文件范围内。

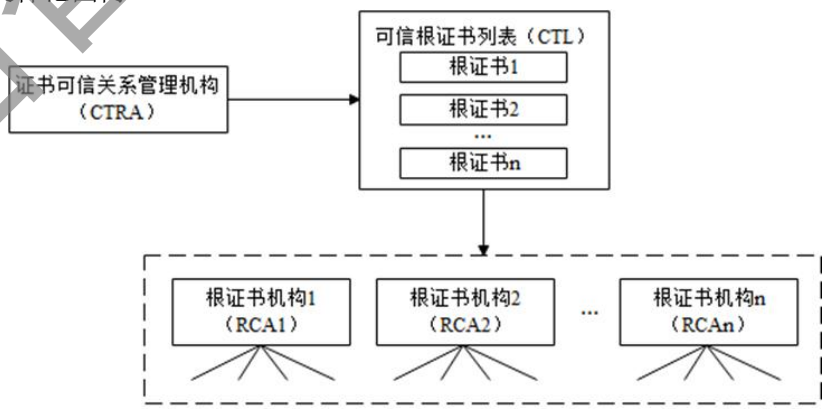

图 4 构建多个 PKI 系统之间的可信关系

为实现跨域认证，一个认证域中的设备需要获取另一个认证域签发证书的 CA 证书或证书链。本文件将一个认证域提供给另一个认证域的用于互信操作的顶级 CA 证书为 TRC。该顶级 CA 证书可以是该认证域的自签名的根 CA 证书，也可以是该认证域的非自签名的子 CA 证书。PKI 互信架构如图 5 所示。

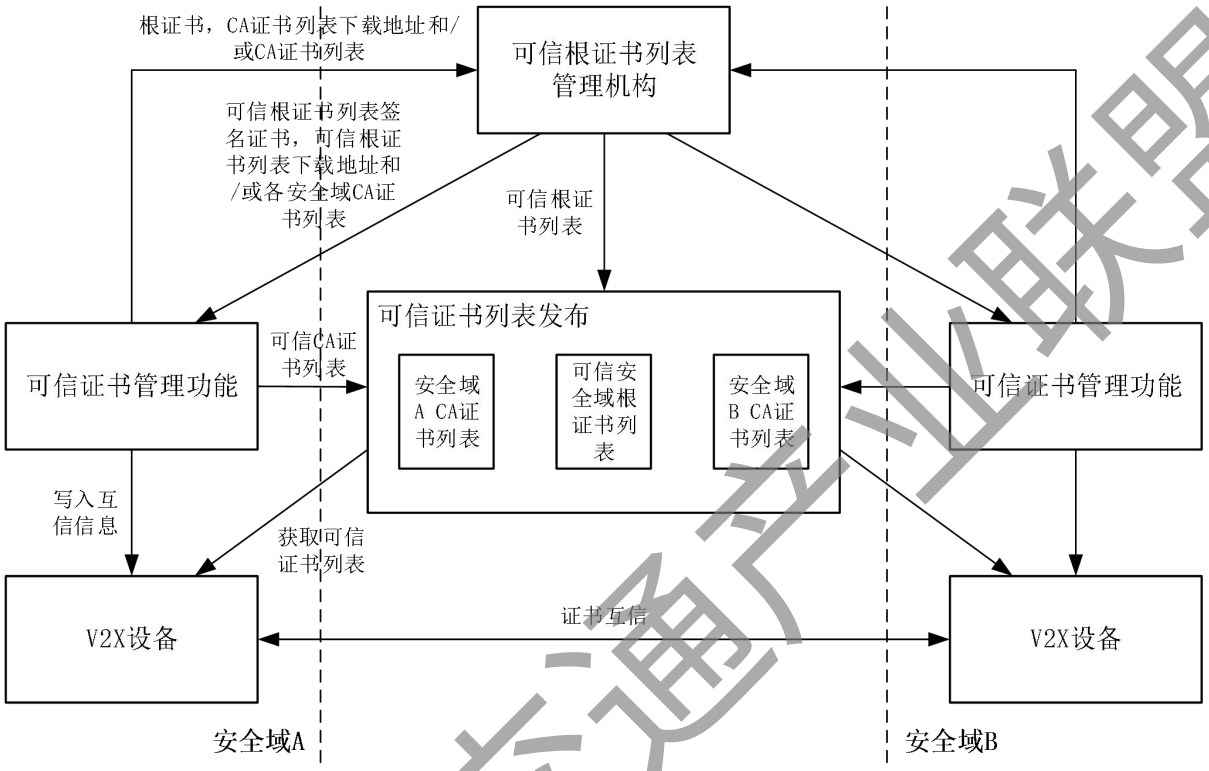

图 5 PKI 互信架构

该架构由如下功能实体和数据构成：

- TRCLA：负责颁发可信根证书列表。
- TRCL：由可信的 PKI 系统的根证书、可信的 PKI 系统的可信域 CA 证书列表下载地址和保护可信根证书列表的安全机制构成。保护可信根证书列表的安全机制为数字签名技术。
- 可信根证书列表签名证书：用于对可信根证书列表提供数字签名保护的公钥证书。该证书可以是符合本文件定义的车联网证书，也可以是符合 X.509 证书规范的证书。
- TCMF：在一个 PKI 系统内负责与可信根证书列表管理机构交互，向可信根证书列表管理机构提供本 PKI 系统与互信操作相关的数据，从可信根证书列表管理机构获取实现 PKI 互信所需要的数据和向本 PKI 系统内的 OBU/RSU 提供实现 PKI 互信所需要的数据。
- TDCL：由一个 PKI 系统颁发的包含有其他 PKI 系统验证本 PKI 系统所颁发证书时需要 CA 证书的列表和保护可信域 CA 证书列表的安全机制构成。列表中的 CA 证书应为从相关 CA 至该 PKI 根的证书链。保护可信域 CA 证书列表的安全机制为数字签名技术。

TRCL 和 TDCL 的发布可以分为集中式和分布式两种。集中式发布方式是指 TRCLA 将 TRCL 和各个安全域的 TDCL 发送给各个安全域，然后由各个安全域确定如何分发给域内的 OBU/RSU。分布式发

布方式是指向 OBU/RSU 提供下载 TRCL 和各个安全域的 TDCL，然后由 OBU/RSU 自行下载交叉认证时需要的各个认证域的 CA 证书。

8.2 可信根证书列表结构

可信根证书列表结构及各字段的用途如表 1 所示。

表 1 可信根证书列表结构

数据域 1	数据域 2	数据域 3	是否必选	说明
版本		version	是	描述列表结构的版本，与本文件对应的版本号为 1
颁发者		issuer	是	签发此列表的证书的低位 8 字节哈希值（HashedId8）
序列号		series	是	每次更新列表，序列号应较上一次更新加 1
颁发时间		issueDate	是	颁发时间
下次颁发时间		nextRootCtl	是	预计下次颁发时间
根证书列表	某可信 PKI 系统相关的数据	rootCertificate	是	某 PKI 系统的可信根 CA 证书
		caListUrl	否	某可信 PKI 系统的可信域 CA 证书列表下载地址
	……	……		
签名值		signature	是	可信根证书列表的签名值

8.3 可信域 CA 证书列表结构

可信域CA证书列表结构及各字段的用途如表2所示。

表 2 可信域 CA 证书列表结构

数据域 1	数据域 2	数据域 3	是否必选	说明
版本		version	是	描述列表结构的版本，与本文件对应的版本号为 1
颁发者		issuer	是	签发此列表的证书的低位 8 字节哈希值（HashedId8）
序列号		series	是	每次更新列表，序列号应较上一次更新加 1
颁发时间		issueDate	是	颁发时间
下次颁发时间		nextPkiCtl	是	预计下次颁发时间
可信域 CA 证书列表	可信 CA 证书	certificateChain	是	可信 CA 证书的证书链
		crlUrl	否	该 CA 所颁发证书的 CRL 列表下载地址
		maUrl	否	该 CA 所颁发证书不端行为上报地址
	… …	… …		
签名值		signature	是	可信域 CA 证书列表的签名值

8.4 PKI 互信管理过程

8.4.1 分布式 PKI 互信管理过程

分布式 PKI 互信管理的一般过程如图 6 所示。

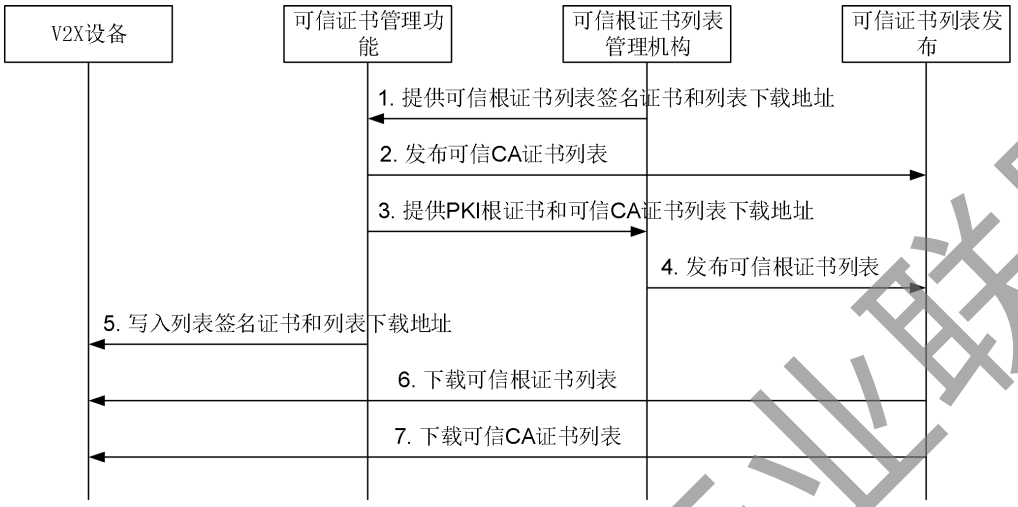

图 6　分布式 PKI 互信管理的一般过程

分布式 PKI 互信管理过程如下：

1. 可信根证书列表管理机构将可信根证书列表签名证书和可信根证书列表下载地址提供给一个可信 PKI 系统中的可信证书管理功能。
2. 一个可信 PKI 系统的可信证书管理功能生成并发布可信 CA 证列表。该列表的管理和发布应符合相关规范。
3. 可信证书管理功能向可信根证书列表管理机构提供其根证书和可信域 CA 证书列表下载地址。
4. 可信根证书列表管理机构利用各可信 PKI 系统提供的根证书和可信域 CA 证书列表下载地址生成一个可信根证书列表并将该列表发布至可公开下载的网络上。
5. 在一个可信 PKI 系统内，可信证书管理功能以安全的方式向其域内的 OBU/RSU 写入可信根证书列表签名证书和可信根证书列表下载地址。
6. OBU/RSU 首先依据可信根证书列表下载地址下载可信根证书列表，然后使用可信根证书列表签名证书验证可信根证书列表的数字签名。
7. 基于下载的可信根证书列表，OBU/RSU 执行如下操作：
   - 获取可信根证书列表中的某个列项；
   - 使用该列项中的可信域 CA 证书列表下载地址下载可信域 CA 证书列表；
   - 使用该列项中的根证书验证下载的可信域 CA 证书列表的数字签名；
   - 使用该列项中的根证书验证可信域 CA 证书列表中证书链的正确性。
   - 若可信域 CA 证书列表提供了 CRL 下载地址，则还应下载相应的 CRL。

8.4.2 集中式 PKI 互信管理过程

集中式 PKI 互信管理的一般过程如图 7 所示。

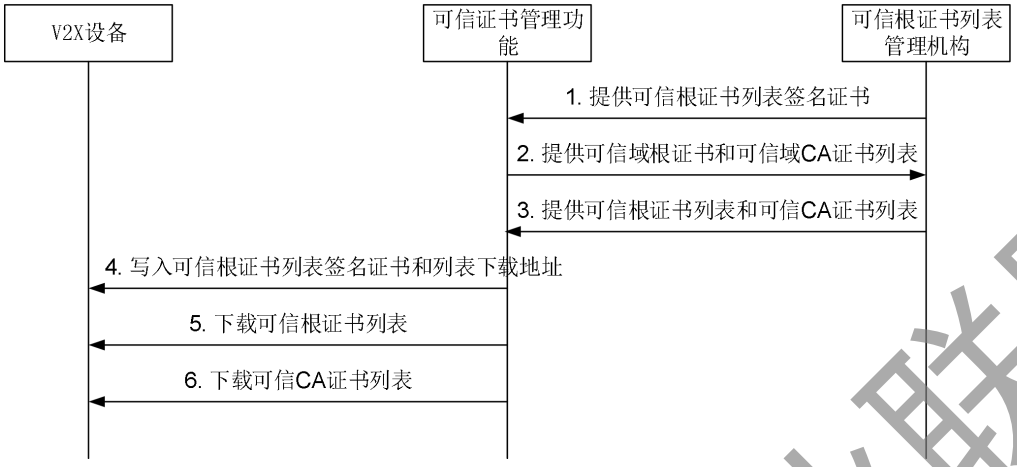

图 7 集中式 PKI 互信管理的一般过程

集中式 PKI 互信管理过程如下：

1. 可信根证书列表管理机构将可信根证书列表签名证书提供给一个可信 PKI 系统中的可信证书管理功能。
2. 可信证书管理功能向可信根证书列表管理机构提供其根证书和可信域 CA 证书列表。
3. 可信根证书列表管理机构生成一个可信根证书列表，并将该列表和其他可信域的可信域 CA 证书列表提供可信 PKI 系统的可信证书管理功能。
4. 可信 PKI 系统的可信证书管理功能以安全的方式向其域内的 OBU/RSU 写入可信根证书列表签名证书和各可信列表的下载地址。
5. OBU/RSU 依据提供的可信根证书列表下载地址下载可信根证书列表，然后使用可信根证书列表签名证书验证可信根证书列表的数字签名。
6. OBU/RSU 依据提供的可信 CA 证列表下载地址下载可信域 CA 证书列表，然后利用可信根证书列表中相应的可信域根证书验证下载的列表。

证书撤销列表使用的 AID 应为十进制 3628。

8.5 PKI 互信认证过程

PKI 互信认证的一般过程为：

1. OBU/RSU 接收其他 OBU/RSU 播发的签名消息。
2. OBU/RSU 获取签名消息中携带的签名证书。
3. OBU/RSU 获取签名证书中证书颁发者标识。
4. OBU/RSU 利用获取的证书颁发者标识与本 PKI 系统的 CA 证书和其他可信 PKI 系统的 CA 证书的低位 8 字节哈希值（HashedId8）相比较，若有匹配，则利用相应的 CA 证书验证消息签名证书，并检查相应的 CRL，以确定该证书是否已被撤销。
5. OBU/RSU 利用通过验证的消息签名证书验证消息签名。

9 异常行为检测和上报

本文件不涉及系统中各实体如何实现本地异常行为检测、全局异常行为检测，也不涉及具体执行相关检测的实体如何在当前 PKI 架构中的映射和定义关系。异常行为的上报流程示例见附录 A。

附 录 A

（资料性）

异常行为检测上报流程

异常行为是指在直连通信中，部分节点由于有意或无意的原因，对外发送包含虚假或错误内容的信息，从而对于直连通信自组网络中其它的通信节点造成影响其进行业务判断的行为。其中恶意的攻击者可能对于整体直连通信自组网络的运转效率和安全性带来严重的影响。因此，需要考虑在直连通信自组网中实现异常行为检测的能力。

异常行为检测，通常包括如下过程：

1. 本地异常行为检测：终端设备根据接收到的周边消息，以及本地的检测算法，判断消息是否异常；
2. 上报：对于确定的终端设备异常行为，需要上报给专门的异常行为检测中心 MA 进行进一步的检测；
3. 全局异常行为检测：MA 根据收到的多方上报的本地异常行为检测报告信息，汇总并决策是否确实是异常行为；
4. 证书吊销：对于确认为异常行为的终端设备，需要对其证书进行吊销。

中国智能交通产业联盟
标准

面向车路协同的通信证书管理技术规范

T/ITS 0127-2020

北京市海淀区西土城路 8 号（100088）
中国智能交通产业联盟印刷
网址：http://www.c-its.org.cn

2021 年 1 月第一版　2021 年 1 月第一次印刷