基于 LTE-V2X 技术的 PKI 系统架构探讨

李 峰,陈 新

(北京汽车研究总院有限公司,北京 101320)

摘 要:V2X(Vehicle to Everything)业务安全的关键在于对消息的真实性校验和个人隐私的保护,在建立身份认证体系时要合理定义各个参与方的安全边界及责任,防止来自内部及外部的攻击。在借鉴国外 SCMS、CCMS 体系的基础上,基于 LTE-V2X 技术特点和道路交通管理体系,通过分析 V2X 证书管理体系的实际需要,针对证书管理的关键过程给出相应的安全策略建议,提出面向 LTE-V2X 的 PKI 架构参考建议,可实际应用于 LTE-V2X 业务部署及相关系统的开发设计。

关键词:LTE-V2X;注册证书;DSRC;GDPR

中图分类号:TP309;U495 **文献标识码**:A DOI:10.19358/j.issn.2096-5133.2020.07.007

引用格式:李峰,陈新. 基于 LTE-V2X 技术的 PKI 系统架构探讨[J].信息技术与网络安全,2020,39(7):41-47.

PKI infrastructure architecture based on LTE-V2X

Li Feng, Chen Xin

(Beijing Automotive Technical Center Co., Ltd., Beijing 101320, China)

Abstract: A key factor to the success of V2X business lies in security: messages authentication and personal privacy protection. Therefore, it is mandatory to establish an identity authentication system based on the actual supervision system, and reasonably define the security boundaries and responsibilities of each participant. Based on existing V2X PKI systems: SCMS and CCMS, this paper analyzes the actual needs of the V2X certificate management system based on the LTE-V2X technical characteristics and domestic regulatory system, and gives corresponding solutions to several key processes of certificate management. And then it makes recommendations PKI infrastructure and security strategy for LTE-V2X business, puts forward specific security management solutions for domestic V2X business development in the future, which can actually be applied to the development and design of LTE-V2X service deployment and related systems.

Key words: LTE-V2X; enrollment certificate; DSRC; GDPR

0 引言

车辆直连通信技术 V2X(Vehicle to Everything)的应用为车辆提供了与周围道路交通参与者之间的实时通信能力,可以有效优化交通效率,降低交通事故的发生比例。但由于直连通信是以广播方式在公共频道上进行信息发送,面临着两个主要的信息安全问题:(1)消息接收者如何验证广播消息的真实性;(2)消息发送者如何有效保护隐私信息。传统的 PKI 技术的特点是为发送者提供唯一有效的身份认证凭据,能够保证消息来源的真实性,但是却无法保护发送者的隐私;同时,复杂的证书结构及算法导致过高的安全开销,也无法满足 V2X 业务的性能要求。因此,需要根据 V2X 应用的业务特点建立专用的 V2X PKI 技术体系来满足 V2X 应用的安全需求。

1 V2X PKI 认证体系现状分析

V2X 的早期标准基于 IEEE802.11 的底层通信协议,在此基础上形成了以 IEEE1609.2[1]为基础的 V2X 信息安全体系。IEEE1609.2 主要定义了 V2X 应用中的安全实体及不同安全实体之间的安全通信机制,包括针对不同实体的证书类型及安全消息的格式定义。

由于不同国家和地区在管理模式上的差异,IEEE1609.2 并没有对 V2X 证书的管理机制提出特定的建议。以政府为主导的美国和以汽车厂商为主要推动者的欧盟各自在 IEEE1609.2 的基础上发

展出了具有自身特色的 V2X PKI 管理体系：安全凭证管理系统 SCMS(Security Credential Management System)[2]和协作式智能交通系统安全证书管理系统 CCMS(Cooperative－ITS security Certificate Management System)[3]。

1.1 安全凭证管理系统 SCMS

SCMS 是由美国交通部牵头，汽车及安全行业自愿参与的针对 V2V/V2I 信息安全的技术验证项目，其主要目的是以小规模的试点来探索 V2X 证书管理中的安全流程及隐私保护机制，因此架构上考虑同时抵御来自外部及内部的攻击，确保 SCMS 系统中的任一组件都无法独立将颁发给同一设备的不同匿名证书完全关联。如图 1 所示，完整的 SCMS 架构包括 6 个主要部分：

(1)策略及技术管理：负责管理 PKI 系统的整体安全策略及技术路线，维护全局策略文件(GPF)以及包含所有信任证书的全局证书链文件(GCCF)。

(2)根证书管理：基于选民机制为 SCMS 系统建立可靠的信任根，并在根证书失效的情况下安全地重建系统。

(3)本地管理：基于根证书为具体的 PKI 证书域颁发本地子证书，主要包括一个中间 CA 证书以及基于此颁发的注册 CA 和匿名 CA。

(4)注册管理：由注册 CA 为 V2X 设备颁发注册证书并分配相应的业务权限。

(5)匿名证书管理：匿名 CA 基于设备注册证书 EC 的有效性及权限配置为 V2X 车载设备批量颁发匿名证书，证书密钥由系统基于设备在初次申请时提供的种子密钥进行扩展，每一批证书都会对应到一个关联值。

(6)匿名证书吊销：异常行为管理机构 MA 与 SCMS 系统内其他子系统合作确定 V2X 车载设备的异常状态。MA 将与异常设备对应的关联值发布到证书吊销列表(CRL)来实现对设备内所有未到期匿名证书的批量注销。

1.2 协作式智能交通系统安全证书管理系统 CCMS

CCMS 的架构主要考虑欧盟基于成员国的分散管理架构、V2X 业务的大规模部署要求以及欧盟

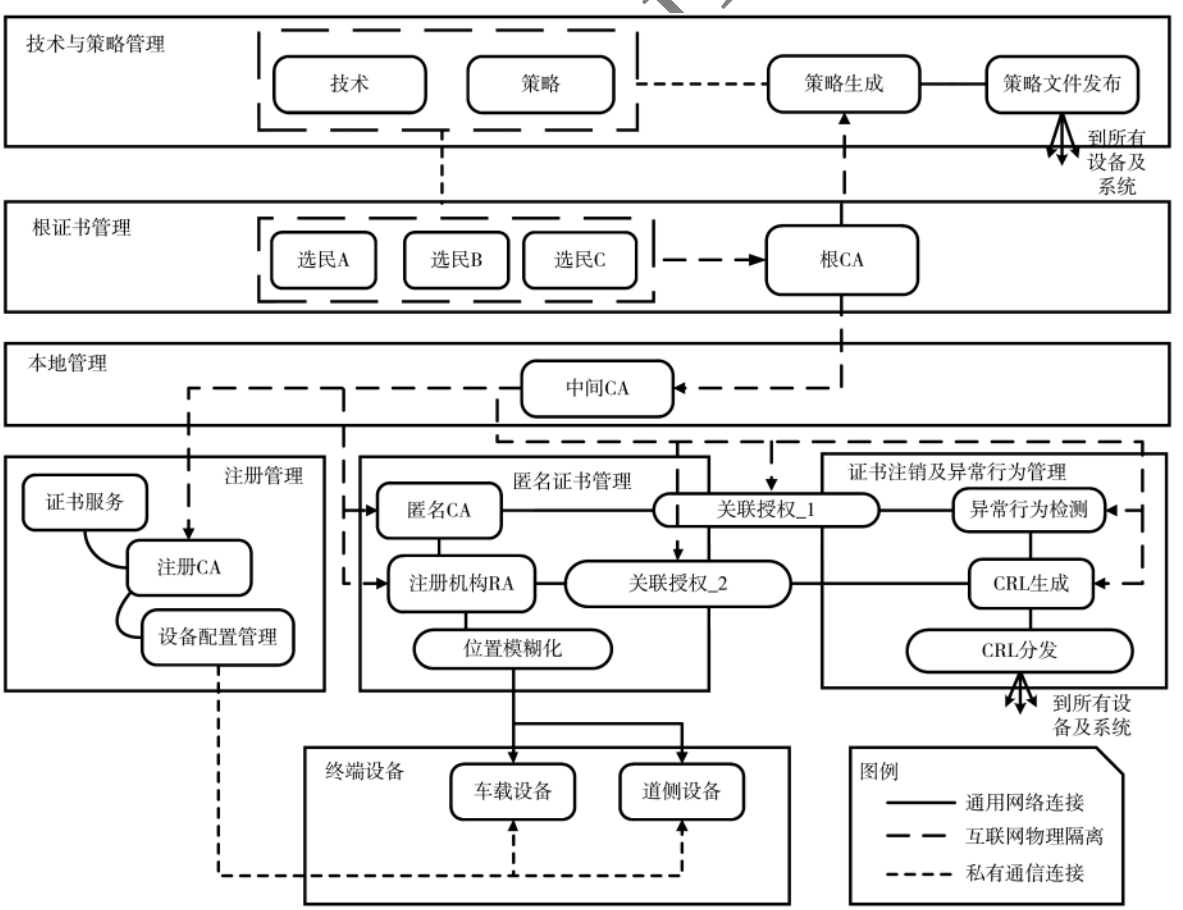

图 1 SCMS 架构

GDPR 隐私保护需求，在设计上加强根证书的准入机制管理，关注 V2X 功能全面部署情况下的技术限制及系统性能要求。CCMS 架构如图 2 所示，其主要包括以下几个部分：

(1)可信证书列表管理 TLM：CCMS 通过一个专门的策略机构 PA 来对 V2X 根证书进行审核并通过可信证书列表管理者 TLM 签发全局的根证书列表 CTL，对根证书的进入和退出实行严格的集中管理机制。

(2)初始安全凭证 BC：每个车载 V2X 设备在初始化过程中都会获得一个终身不变的标识 ID 并生成一对公私钥，形成一个设备自签名证书 BC。

(3)注册机构 EA：根证书直接管理注册机构 EA，减少 PKI 系统的证书层级。EA 基于对设备 BC 认证为车辆设备颁发注册证书 EC 并定义其业务权限。

(4)授权机构 AA：授权机构负责为车辆颁发用于签发消息的匿名授权证书 AT，授权机构不保存车辆的隐私信息，依赖注册机构 EA 对 AT 申请进行审核确认。

(5)匿名证书吊销：AA 必须与 EA 合作才能够共同确认异常车辆真实信息。由于在 V2X 业务大规模部署的情况下，证书撤销列表 CRL 会快速增长而导致设备验证消息签名的性能下降，因此 CCSM 主要通过对异常设备 EC 的黑名单管理机制阻止设备获得新的匿名授权证书，对异常设备内部已下载的未过期匿名证书则等待其自然过期失效，不考虑基于 CRL 的主动撤销机制。

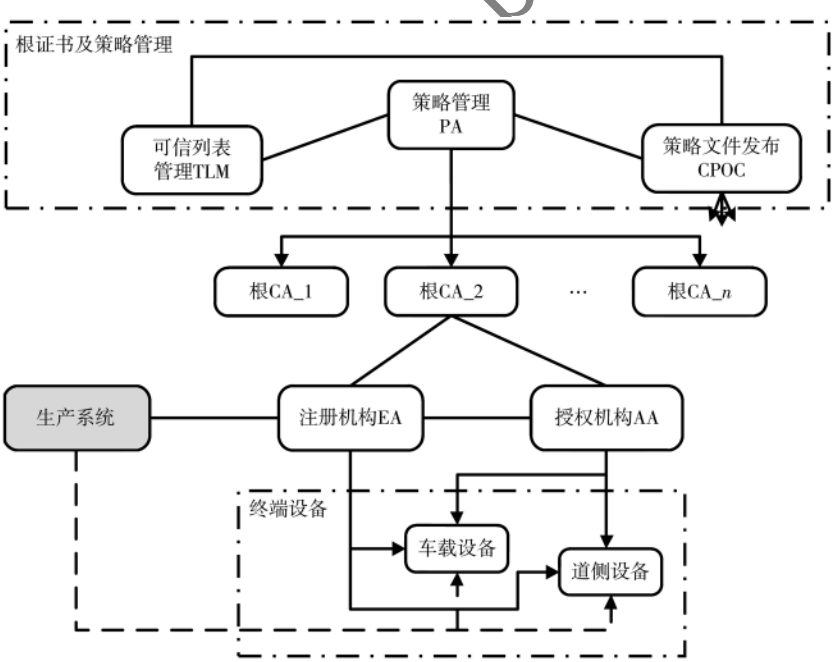

图 2 CCMS 架构

2 LTE-V2X PKI 系统架构探讨

2.1 LTE-V2X PKI 系统特点

目前用于 V2X 通信的主流技术包括专用短程通信 DSRC(Dedicated Short Range Communication)技术和基于蜂窝移动通信系统的 C-V2X(Cellular Vehicle to Everything)技术(包括 LTE-V2X 和 5G NR-V2X)，其中 LTE-V2X 是基于 4G 技术实现通信，以 LTE 蜂窝网络为 V2X 基础的车联网专有协议。美国和欧盟的 V2X 技术均基于 IEEE802.11 的 DSRC 技术，国内 LTE-V2X 系统虽然有着与其类似的消息认证及用户隐私保护需求，但是证书管理的具体实现机制有所不同：

(1)不同的通信技术体系：与 DSRC 技术相比，LTE-V2X 系统中的蜂窝移动通信技术大幅度提高了 V2X 设备与后台系统的交互能力。在 DSRC 技术中，设备与 PKI 系统之间的证书管理消息与 V2X 应用消息需要竞争相同的通信资源，因此要考虑通过证书批量颁发的方式降低设备与 PKI 系统的交互频率；在 LTE-V2X 体系中，设备通过独立的 Uu 接口与 PKI 的证书系统交互，不会与 V2X 应用消息竞争通信资源[4]，但同时 LTE-V2X 的 PKI 系统需要考虑 Uu 接口的安全保护。

(2)集中的政府管理架构：V2X PKI 系统的管理机制与道路交通的管理体系密切相关，与美国和欧盟基于州或成员国的分散管理体系不同，国内是一个相对集中的管理架构。工业与信息化部、公安部、交通部不同程度地参与到交通管理流程，其中工信部主要负责车辆及道侧设备的生产过程中的管理，公安部和交通部则负责车辆及道侧设备在使用过程中的管理。车辆及道侧设备从生产到使用的过程中存在一个管理责任的衔接，需要各方建立相互的信任机制。

(3)个人隐私保护需求：国内在车辆及个人用户隐私保护方面的焦点在于对个人用户隐私信息的搜集、存储以及分享方面的合规性

要求[5]。与此同时，严格的监管要求也需要 V2X 业务的管理方在车辆出现异常行为时能够快速定位用户的真实身份。

2.2 LTE-V2X PKI 系统架构建议

作为全球化产业体系，汽车整车业务需要考虑与国际技术的接轨，因此国内的 LTE-V2X PKI 系统也应以 IEEE1609.2 为基础，结合 LTE-V2X 的技术特点以及大规模商用的实际需求来进行规划。本文建议基于欧盟的 CCSM 架构进行相应的调整，在适应国内管理体系的同时充分利用 LTE-V2X 技术的网联能力来实现对 V2X 证书的高效管理。图 3 为建议的 V2X PKI 系统架构。

2.3 LTE-V2X PKI 系统主要流程

2.3.1 根证书管理

根证书是整个 V2X PKI 系统的可信基点，道路交通管理的参与各方需要根据实际的管理流程建立共同信任的根证书系统。SCMS 和 CCMS 都需要考虑存在不确定的 V2X PKI 的根证书提供者，地方政府、联盟成员国、安全组织以及汽车制造商都有可能独立建设 V2X PKI 根证书并为 V2X 设备颁发证书。

国内的道路交通管理部门采用全国性的集中管理模式，虽然不同的管理部门之间可能不会使用同一个根证书，但同一管理部门内部则可以建立全国性的单一根证书体系。考虑到具有根证书建设权限的管理机构基本是确定的，不会频繁增加或删除 V2X PKI 根证书信息，因此并不需要建立类似于 SCMS 的投票机制或 CCMS 的 TLM 管理机制来专门对根证书的加入与退出进行可信管理。

国内的 LTE-V2X PKI 系统可能为单一根证书模式，或包含有限的互相信任的若干根证书的多根模式，因此可以将 LTE-V2X PKI 系统的根证书管理部分简化为三个主要的机构：

(1)策略机构(PA)：策略机构负责各个根证书安全策略的管理与协调。在单根证书模式下，PA 与根证书 RCA 是合一的；在多根证书模式下，PA 由多个根证书管理机构组成，为多个根证书建立互信机制。

(2)根证书(RCA)：如果存在若干个全国性 RCA，则各根证书之间通过策略机构 PA 的协调实现交叉互信。

(3)可信证书列表(CTL)：PA 定期向各个 RCA 推送可信证书列表(CTL)，由 RCA 签发给证书域内的设备或服务器站点。CTL 分为两个系列：CTL_1 包含所有可信的内部及外部根证书，发布给 PKI 架构中各服务器；CTL_2 包含可信的 V2X 根证书或次级 CA 证书，发布给 V2X 车载终端及道侧设备。

2.3.2 车辆初始化与注册

实际的车辆管理过程中，车辆的生产与注册由不同的实体进行管理。整车生产厂商负责车辆的生产和初始化；交通管理机构负责车辆的注册，为车

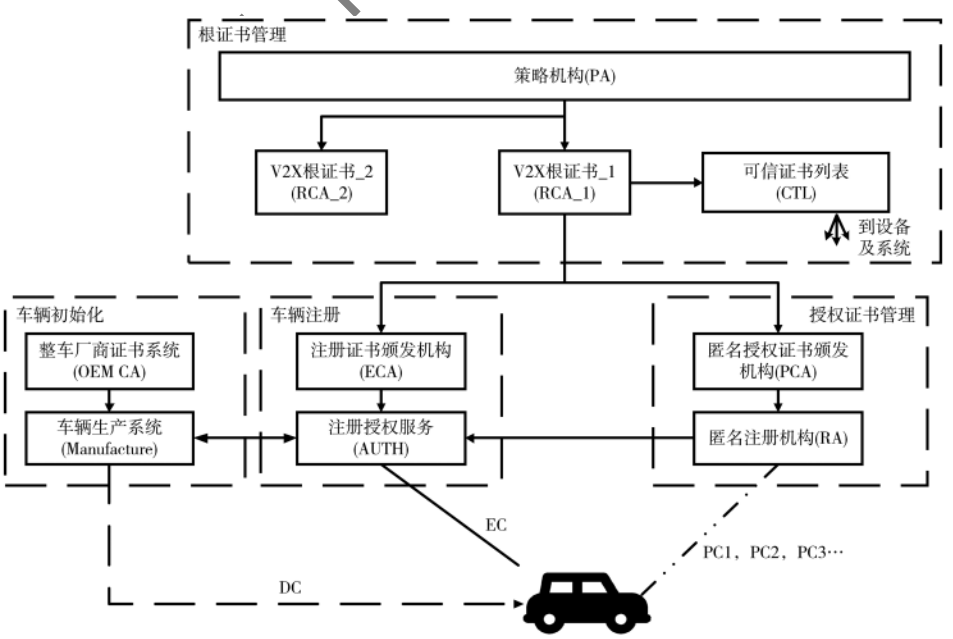

图 3 建议的 V2X PKI 系统架构

辆颁发 V2X 注册证书(EC)并分配相应的 V2X 业务权限。

SCMS 系统建议由整车厂商在生产过程中完成车辆的注册,与车辆生产与注册管理分离的管理机制不相适应;CCMS 利用设备的初始证书 BC 实现了生产与注册过程的分离,但 BC 的自签名属性决定需要额外流程才能确认未注册车辆的真实信息。同时,一旦车辆注册证书失效,需要重新进行初始化才能够下载新的注册证书,会导致产生额外的车辆召回成本。

因此,在图 3 的架构中,引入了一个独立于 V2X PKI 系统的设备证书 PKI 系统(OEMCA),整车厂商在生产过程中基于 OEMCA 为车辆颁发包含车辆 V2X 业务属性等信息在内的设备证书(DC),DC 为后续的 V2X 业务流程提供初始的信任凭证。

设备初始证书的颁发过程是一个完全定制化的过程,整车厂商确保初始化流程安全可信,并在车辆设备生命周期内负责设备证书 DC 的维护及更新。

为了确保 V2X PKI 证书系统对整车 OEMCA 的信任,策略机构 PA 需要对 OEMCA 进行审计。可信的 OEMCA 根证书会被添加到可信证书列表 CTL_1 并发布到相应的注册授权服务(AUTH),支持注册机构对车辆设备证书 DC 的认证过程。

车辆在注册 V2X 业务时,首先通过 LTE 网络 Uu 接口向 AUTH 提交设备证书 DC 进行认证并建立安全通信通道,注册授权服务(AUTH)基于此安全通道搜集并保存车辆及用户的隐私信息,校验注册请求的有效性并向证书注册机构(ECA)为车辆申请注册证书(EC)。在 EC 过期或更换 ECA 时,车辆基于同样的流程重新注册,无需对车辆重新进行初始化。

由于 OEMCA 和注册系统均采集了车辆设备的隐私信息,因此二者应基于具有高安全防护能力的私有云系统进行部署。

2.3.3 授权证书管理

匿名授权证书主要在具有隐私保护需求的场景下实现对车辆隐私的保护,V2X PKI 系统会为车辆在同一个时间段颁发多个同时有效的无关联的匿名授权证书,车辆通过不断切换证书进行 V2X 消息签发的方式来隐藏自己的真实信息,避免车辆被跟踪并重建轨迹。V2X 证书管理流程中一个重要的隐私安全就是要避免单个系统可以将匿名证书与实际车辆进行关联,SCMS 及 CCMS 在流程上都对此做出了有针对性的设计,本文中的架构采用与 CCMS 一致的机制。

由于匿名授权证书短期性的特点,需要在设备上预先保存可用于多个连续时间段的证书来保证业务的连续性。预存证书的时间跨度越长,设备与后台的交互所占资源越低,但设备被侵入的风险也越大,因此需要基于相应的 V2X 技术实现来选择最佳的证书预存策略。在 DSRC 技术体系中,由于证书的申请和下载需要与 V2X 应用消息竞争无线通道资源,导致业务上的互相干扰,因此 SCMS 及 CCMS 都推荐设备内预置较长时间所需的匿名授权证书,二者的推荐配置如表 1 所示。

表 1 SCMS 与 CCSM 的匿名授权证书安全配置

	SCMS	CCMS
匿名授权证书有效期	1 周	1 周
每周的匿名授权证书数量	20	20
设备内匿名授权证书数量	3 000(3 年)	240(3 个月)[6]
CRL 更新	1 周	无
逾期的 CRL 容忍度	2 周	无
CRL 系统要求	链接值管理能力	无

由表 1 可以看到,在确认设备异常之后,SCMS 系统的安全目标是在不超过三周之内基于 CRL 更新的机制完成对被侵入设备上所有证书的注销,这种机制存在两个主要的问题:(1)需要建立链接值管理机制实现匿名授权证书的批量注销,增加额外的系统成本;(2)在 V2X 设备大规模部署的情况下,CRL 长度的快速增长会导致设备安全性能的下降。为避免这两个问题,CCMS 限定 CRL 仅用于特定证书的注销管理,对于大量的短期有效的匿名授权证书则等待其自然过期。但在当前配置条件下,设备在确认异常后仍然可以在长达数月的时间内签发消息,虽然可以利用业务层的消息真实性校验机制来进行风险缓冲,V2X 业务仍然存在较大的安全隐患,因此需要进一步对预置匿名证书的数量进行优化配置。

LTE-V2X 技术所提供的网联能力上的优势,使得对匿名授权证书的安全优化成为可能。根据 LTE-V2X 技术的 Uu 接口性能的发展,可以分两个阶段来优化匿名授权证书的安全机制:长期而言,随着车辆网联能力的进一步提高,在 5G 网络下采用实时的在线证书状态协议(OCSP)方案与 CRL 相结合的机制,在控制设备本地 CRL 长度的同时,实

时撤销设备异常后本地存储的未过期匿名授权证书；在目前阶段，建议利用 LTE 网络高速可靠的处理能力，优化匿名授权证书的配置策略，将风险控制在可接受的水平。

在不使用 CRL 进行匿名授权证书注销的情况下，如果要达到与 SCMS 相当的安全目标，车载OBU 设备内预置的匿名授权证书的数量应当压缩到两周的使用量，从而将设备被侵入后 V2X 系统面临安全风险的窗口时间控制在两周以内。在这一配置策略下，车辆必须每周都向 PKI 系统预先申请下周所需的匿名授权证书，系统应具备足够的处理能力以支持 V2X 的大规模商业应用。按照目前国内 1.8 亿的私家车保有量考虑，由表 2 可见即使在所有车辆都具备 V2X 功能的极端情况下，证书系统平均每秒处理的证书申请也低于 6 000 个。参考同样具有高安全要求并采用分布式混合云部署方式的银行业务系统，招商银行目前已经可以达到每秒 3.2 万笔的峰值处理能力[7]。通过合理规划 PKI 系统的部署方案及车辆匿名证书的更新策略，完全可以满足车辆按周进行匿名授权证书更新的业务模式。

表 2 LTE-V2X PKI 系统处理能力要求

V2X 车辆占比/%	每周每车发证数量	系统每秒证书处理量
30	20	1 785.71
50	20	2 976.19
80	20	4 761.90
100	20	5 952.38

基于分布式云平台部署的匿名授权系统在带来性能优势的同时也引入了一定的用户隐私保护上的安全风险[8]，V2X PKI 在整体架构上应尽可能避免匿名授权系统对用户隐私数据的直接访问及存储。因此，在分布式混合云的部署架构中，匿名授权证书管理系统应性能优先，部署在分布式的公有云；注册证书管理系统应安全优先，建议基于私有云进行部署。在匿名授权证书的申请中，注册证书管理系统直接对匿名授权证书申请中的设备信息及业务权限进行审核，阻止非法越权的证书申请行为，同时避免匿名授权证书管理系统对车辆隐私信息的访问和处理。

2.3.4 证书类型

在上文提到的架构中，V2X 终端设备中需要安装三类证书：

(1)设备证书(DC)：此证书为传统的 X.509 格式证书，用于车辆与注册系统之间的身份认证及通信保护，同时为 V2X 系统提供可信的设备身份信息及 V2X 业务能力配置参数，有效期通常大于 5 年。

(2)注册证书(EC)：IEEE1609.2 格式证书，定义车辆的 V2X 业务权限，用于匿名授权证书的申请，有效期 1 年。

(3)匿名授权证书(PC)：IEEE1609.2 格式证书，用于签发 V2X 消息，有效期 1 周。

其中设备证书 DC 为新引入的证书，整车厂商负责设备证书的初始化及更新维护。三种证书的下载流程和相互关系如图 4 所示。

3 结束语

与 DSRC 系统相比，LTE-V2X 技术的特点在于

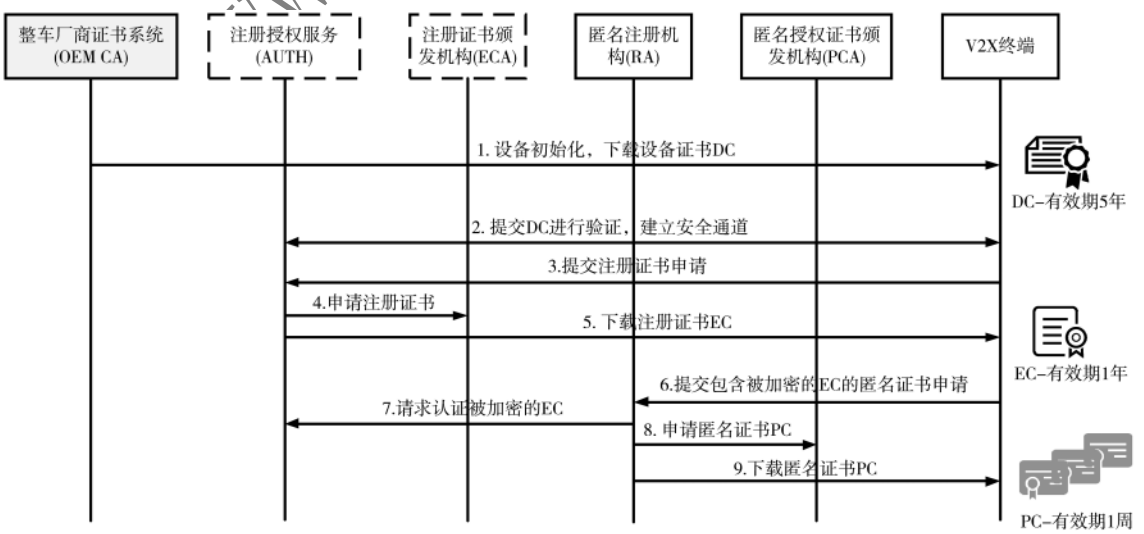

图 4 证书类型及下载流程

车辆与云端的高可靠以及低时延的连接能力，因此可以利用云平台计算能力在简化系统架构的同时为 V2X 业务提供较高的安全防护能力。本文建议以分布式的混合云架构作为 LTE－V2X PKI 系统的基础架构：CTL 与根证书处在一个不提供联网功能的高安全域；整车厂商的安全系统及 V2X 注册系统处于一个具有严格访问控制的私有云系统，为车辆及用户的隐私信息提供全生命周期的高安全保护；匿名授权系统以公有云或边缘云的方式为车辆提供短时有效的匿名授权服务，基于 LTE 的高可靠低时延网络能力确保海量匿名证书处理的服务质量。

V2X 业务的复杂性决定了 V2X 的 PKI 安全系统流程的复杂性。本文基于 CCMS 架构，结合 LTE－V2X 技术特点及国内的交通管理体系与合规要求，针对具有隐私安全需求的车辆的 V2X 证书管理流程进行分析，通过对系统架构、管理流程以及配置参数的优化，在适应国内业务需要的基础上充分利用 LTE－V2X 技术优势简化系统架构，并同时提升整体的安全防护能力。但是，由于未来 V2X 业务管理体系的不确定性，这一架构仍然存在需要进一步细化和优化的地方：

(1)策略机构(PA)：在多根证书的机制下，如何建立 PA，以何种机制在不同的根证书中建立相互信任机制还需要根据具体的管理模式来细化。

(2)整车厂商证书系统(OEMCA)：部分整车厂商并不具备建立自主证书系统的能力，这一能力的建设还存在不确定性。在这一方面，运营商基于 LTE－UICC 的 GBA 认证服务也是一个可选的替代方案。

(3)注册授权服务(AUTH)：注册授权服务在车辆的注册过程中会搜集、存储以及处理用户和车辆的隐私数据，一旦系统被侵入，用户隐私就面临被泄露的风险。因此未来需要进一步加强注册授权服务系统的安全防护能力。

(4)匿名授权证书注销：如何确认 V2X 设备是否出现异常，对于及时的证书注销至关重要，这一机制本身的复杂性决定需要一个持续的设计及优化过程。

本文中的系统架构主要从主机厂商角度出发，基于 LTE－V2X 业务管理的流程及场景对已有的成熟架构进行优化，能够有效解决传统 PKI 体系面临的发送者隐私保护和计算开销太大的问题。随着 LTE－V2X 业务场景的逐步落地、管理模式的不断成熟以及技术能力的进一步提升，这一安全架构还存在进一步的优化可能。

参考文献

[1] IEEE Vehicular Technology Society. IEEE 1609.2－IEEE standard for wireless access in vehicular environments－security service for applications and management messages[S]. New York：IEEE Standards Association，2016.

[2] BRECHT B，THERRIAULT D，ANDRÉ W，et al. A security credential management system for V2X communications[J]. IEEE Transactions on Intelligent Transportation Systems，2018，19(12)：3850－3871.

[3] ETSI TS WG5.TS 102 940：Intelligent Transport Systems(ITS)；Security；ITS communications security architecture and security management，V1.3.1[S].2018.

[4] 鲍海森.浅析下一代车联网 V2X 技术[J].信息技术与信息化，2017(9)：111－114.

[5] 斐卢冉·热依木江.大数据时代我国个人信息保护现状及建议[J].江苏科技信息，2019，36(19)：19－21.

[6] European Commission. Certificate policy for deployment and operation of European cooperative intelligent transport systems(C－ITS) release 1.1[R]. European Commission，2018.

[7] 招商银行.招商银行 2018 年度报告 A 股[R].深圳：招商银行，2019：47.

[8] 吴延顺.基于云计算的大数据安全隐私保护的研究[J].电子技术与软件工程，2016(4)：199.

(收稿日期：2020－04－01)

作者简介：

李峰(1974－)，男，硕士，高级工程师，主要研究方向：计算机应用及信息安全。

陈新(1981－)，男，硕士，高级工程师，主要研究方向：汽车工程。

版权声明