信大捷安

信大捷安ITS-CA解决方案

郑州信大捷安信息技术股份有限公司

目录

01 C-V2X发展现状

02 ITS-CA建设必要性和行业发展

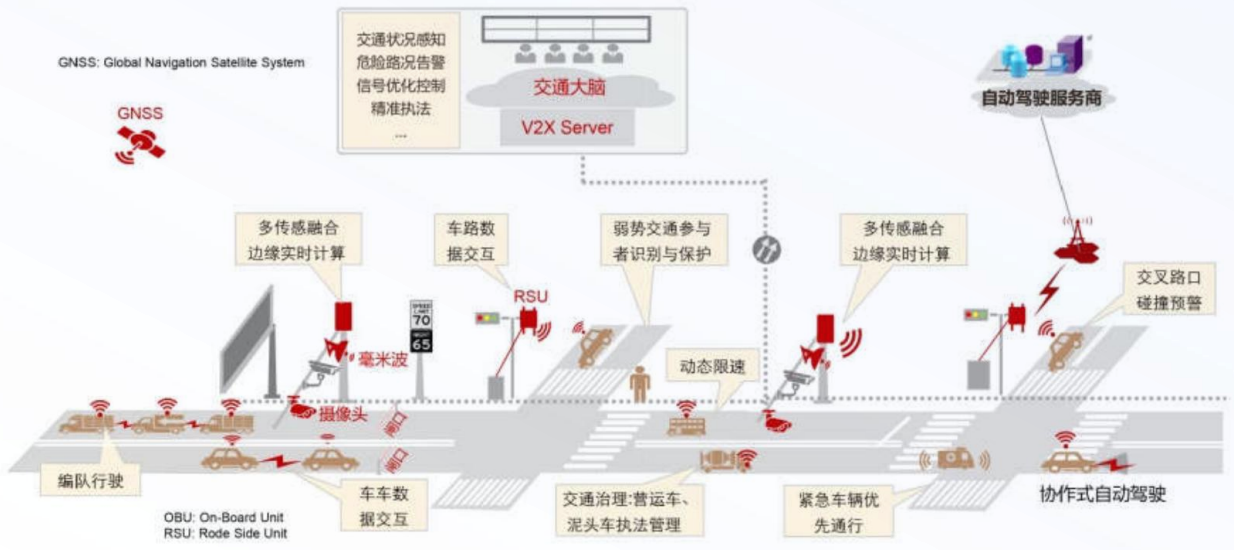
03 ITS-CA技术方案

04 关于信大捷安

信大捷安

V2X基本定义

C-V2X（Cellular- Vehicle to Everything）是将车辆与一切事物相连接的新一代蜂窝通信技术。“C”是指蜂窝通信网络，“V”代表车辆，“X”代表任何与车交互信息的对象，当前X主要包含车、人、交通路侧基础设施和服务网络。



C-V2X全场景连接

V2X使得车辆与车辆（V2V）、车辆与行人（V2P）、车辆与基础设施（V2I）（如交通信号灯、路灯、交通摄像头、路侧单元等）、车辆与接入网/核心网/云平台（V2N）之间能够通信，实时获得车、路、人、平台等交通和服务信息，进而提高驾驶安全性、提高交通效率、提供车载娱乐等智能化，甚至智慧化交通新模式，为实现客观现实世界资源的高效流通，极大化资源的价值提供支撑。

无缝的连接	高速的连接	低时延连接	高可靠连接
广域通信和直连通信	100Mbps ≥ 1Gbps	20ms ≥ 2ms	99.999%

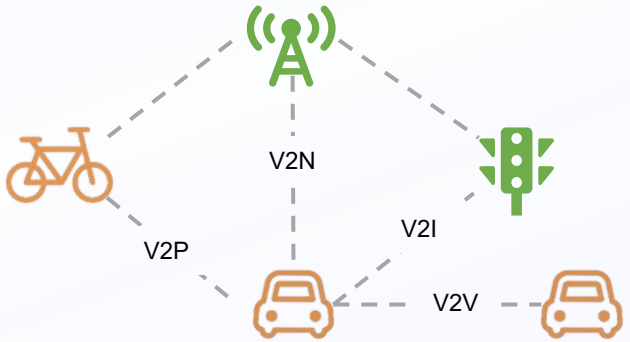
信大捷安

V2X是智能交通的重要组成部分

聪明的车

- 长距雷达
- 中短距雷达
- 激光雷达
- 摄像头
- 超声波雷达

智慧的路



车路协同 典型应用场景

类别	通信方式	应用名称
安全	V2V	前向碰撞预警
	V2V/V2I	交叉路口碰撞预警
	V2V/V2I	左转辅助
	V2V	盲区预警/变道辅助
	V2V	逆向超车预警
	V2V/Event	紧急制动预警
	V2V/Event	异常车辆提醒
	V2V/Event	车辆失控预警
	V2I	道路危险状况提示
	V2I	限速预警
	V2I	闯红灯预警
	V2P/V2I	弱势交通参与者碰撞预警
效率	V2I	绿波车速引导
	V2I	车内标牌
	V2I	前方拥堵提醒
	V2V	**紧急车辆提醒**
信息服务	V2I	汽车近场支付

紧急车辆提醒（EVW）

信大捷安

V2X安全威胁的严重性

不仅仅经济损失--

---------财产安全

人员伤亡----------

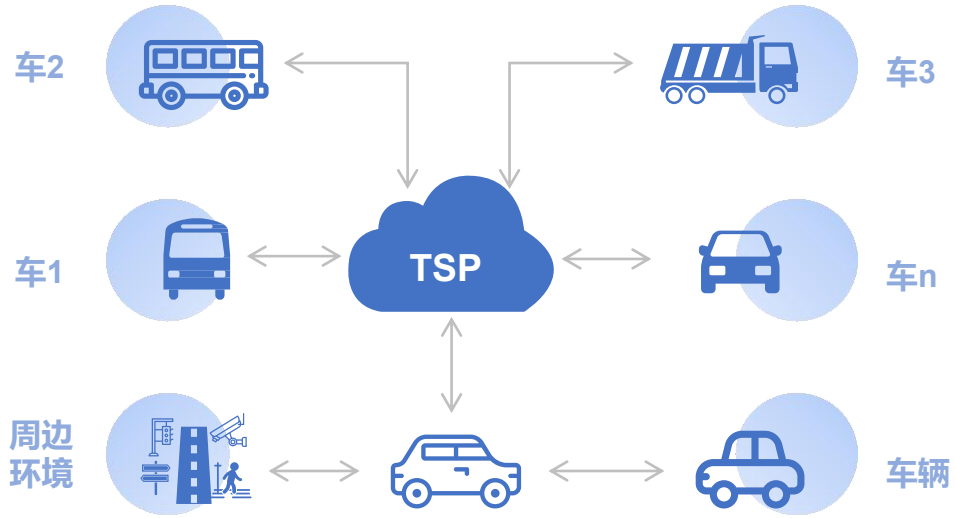
---------人身安全

恐怖袭击----------

---------国家安全

我国处于智能网联汽车高速发展阶段，智能网联汽车也存在安全风险，智能网联汽车安全事件不仅会影响到财产、人身安全，甚至会威胁到国家安全。

车路协同（C-V2X）终端或云端系统一旦被黑客攻击，有可能造成大规模交通事故，影响到国家安全；



当车辆运行周边环境存在安全问题，固定区域的车辆会造成安全事件。

信大捷安

目录

01 C-V2X发展现状

02 ITS-CA建设必要性和行业发展

03 ITS-CA技术方案

04 关于信大捷安

信大捷安

ITS-CA 是C-V2X安全的关键基础设施

C-V2X系统可以分为车辆网设备层、车联网网络层和车联网应用层，不同的层面临的安全风险和挑战不尽相同。为了应对车联网设备、网络、应用层的安全风险和挑战，需要构建面向C-V2X的ITS-CA车联网网络信任支撑平台，实现了车、路、云、端通信过程中的身份认证，保障车联网及智慧交通场景下通信数据的机密性和完整性、车辆信息的私密性。

保障车路协同V2X安全

- 认证
- 隐私保护
- 不当行为管理

传统X.509证书不适合V2X场景

- 不支持V2X场景下的特定功能需求
- 无隐私保护
- 无防跟踪能力
- 证书太大

专门为V2X场景设计的全新ITS-CA

- 支持应用权限、应用地理区域管理
- 支持隐私保护
- 支持防跟踪
- 证书足够小，满足高频率交互带宽需求

符合国家战略和市场需求

- 国家发改委、中央网信办、科技部、工信部等11个国家部委联合发布了《智能汽车创新发展战略》标志着未来几年中国智能汽车将进入高速发展的黄金时期。
- V2X-CA是保障V2X安全的基础，已经上升到国家战略层面。

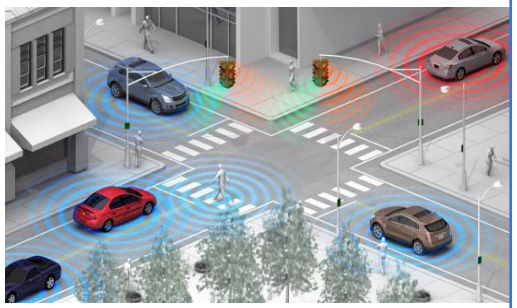
取得市场先机

- V2X安全涉及面广，技术要求高，需要提前做技术储备
- 各单位V2X-CA最后需要接入国家部委根CA，才能实现商用。提前部署，国家根CA发布后可第一时间接入，抢占V2X市场先机

信大捷安

ITS-CA 证书需求

- **应用权限** 管理能力
- **应用地理区域** 管理能力



攻击场景：

- 车辆伪装RSU发送交通信号灯信息等
- 某路口RSU私自拆卸安装到其他区域路口
- 车辆伪装警车进入事故区域等

功能性需求

- **车辆证书不带车主身份信息**
- **CA机构不知道车主身份**

攻击场景：

- 攻击者通过证书信息，知道车主是谁、什么时候去了哪里、出行习惯等隐私信息
- 攻击分类：路边攻击者、CA机构内部攻击者

隐私保护需求

- **多张假名证书随机替换**
- **假名证书生命周期尽量短**

攻击场景：

- 虽然不知道车主身份，但能够辨别是否同一辆车辆发出，从而跟踪、绘制车辆行驶轨迹，反向识别车主身份和活动路线。

防跟踪需求

- **带宽资源有限/验签速率要求高**
- **V2X证书需要尽可能的小/V2X安全芯片性能要高**

场景：

- 车辆每秒广播10条BSM消息
- 车辆每秒接收2000条数据

证书大小需求

信大捷安

ITS-CA安全规范

国内标准

《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》

《C-V2X 异常行为管理技术要求》

美国标准

《IEEE Std 1609.2™-2016/1609.2a-2017/1609.2b-2019 IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applicatiosn and Management Messages》

《A Security Credential Management System for V2X Communications》

欧洲标准

《ETSI TS 102 941 V1.3.1 (2019-02) Intelligent Transport Systems (ITS);Security;Trust and Privacy Management》

《ETSI TS 102 731 V1.1.1 (2010-09) Intelligent Transport Systems (ITS);Security;Security Services and Architecture》

《ETSI TS 103 097 V1.3.1 (2017-10) Intelligent Transport Systems (ITS);Security;Security header and certificate formats》

《ETSI TS 102 940 V1.3.1 (2018-04) Intelligent Transport Systems (ITS);Security;ITS communications security architecture and security management》

目录

01 C-V2X发展现状

02 ITS-CA建设必要性和行业发展

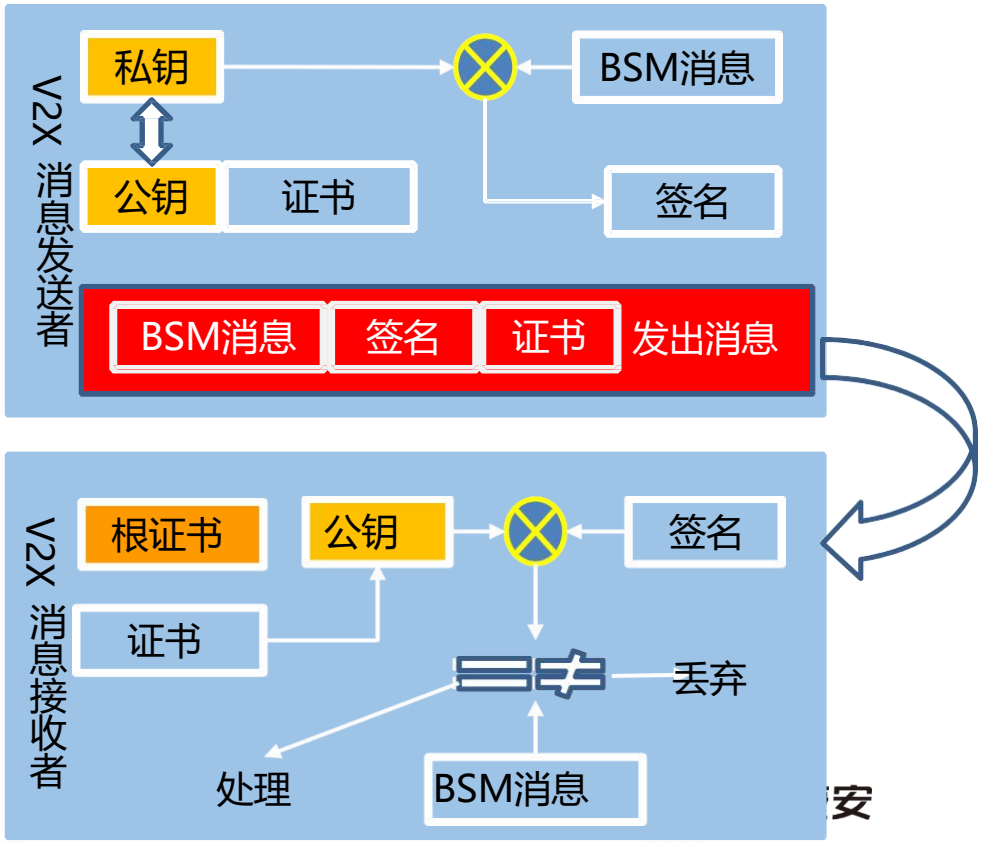
03 ITS-CA技术方案

04 关于信大捷安

信大捷安

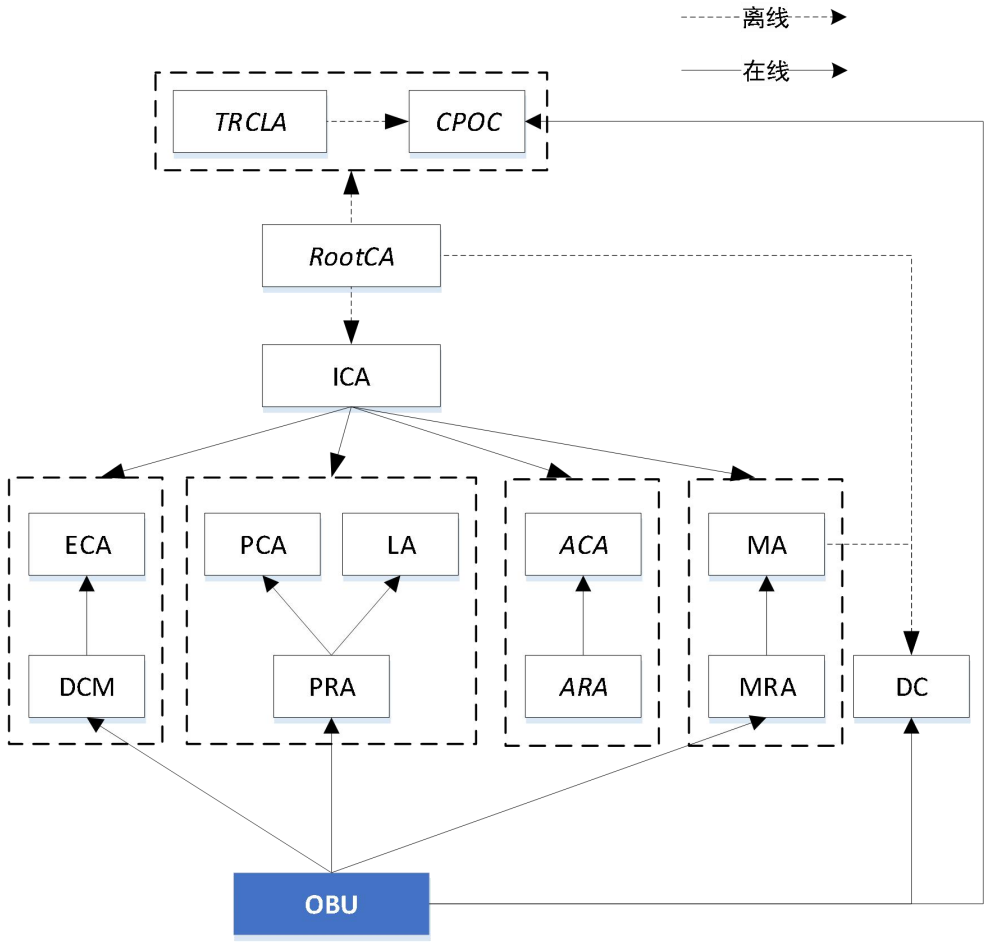
ITS-CA应用-保障V2X通信（PC5口通讯）安全

以**安全芯片、ITS-CA（PKI）**为基础，向参与车路协同的车辆和基础设施节点发布数字证书，对V2X消息进行签名和签名认证，能够有效解决V2X车联网系统面临的虚假信息、假冒终端、信息篡改/重放、隐私泄露等安全风险，同时实现不同企业的车辆通信过程中的互通互认。



系统总体结构

序号	系统构件名称	功能说明
1	TRCLA	根证书信任列表管理机构，签发可信根CA的TRCL。
2	CPOC	中心联系点，负责TRCLA签发的TRCL的发布。
3	RootCA	根证书机构，通过离线形式签发下级CA证书；签发TDCL。
4	ICA	中间CA，位于根CA与注册证书、各种授权证书CA之间，用于扩展PKI体系的层级。
5	ECA	注册证书机构，提供V2X设备注册证书签发、查询等管理功能。
6	DCM	设备配置管理机构，受理EC申请、更新请求，并验证授权请求的有效性。
7	PCA	假名证书机构，提供V2X设备假名证书签发、查询等管理功能。
8	PRA	假名证书注册机构，为PC申请提供受理、验证、密钥衍生、混淆、批量下载功能。
9	LA	链接值管理机构，为V2X设备证书供应链接值，以支持假名证书的批量撤销。
10	ACA	提供V2X设备应用/身份证书签发功能
11	ARA	用于受理应用/身份证书申请请求
12	MA	异常行为管理机构，提供不当行为管理和设备证书撤销功能。
13	MRA	异常行为注册机构，为MA提供在线受理服务
14	DC	分发中心，为RCA所签发的TDCL、MA签发的CRL提供数据分发的功能。

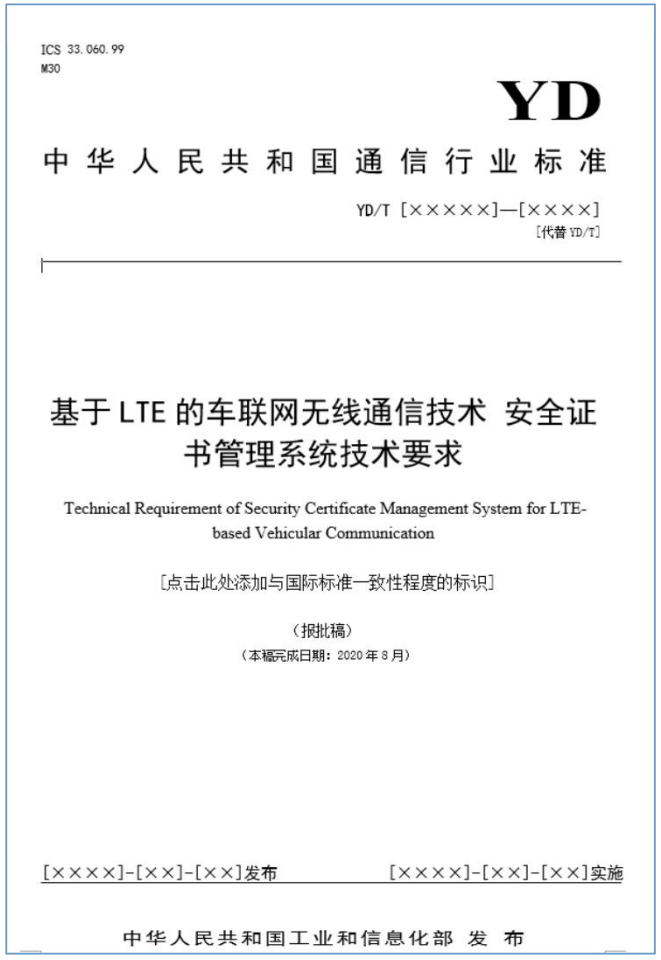


信大捷安

ITS-CA 功能列表

- **支持设备管理**，包括设备初始信息录入，设备的应用权限、应用区域管理，设备冻结；
- **支持基于DCM架构的V2X设备证书申请**，包括EC、PC、应用/身份证书在线申请，其中PC的申请支持密钥衍生、链接值、批量下载；
- **支持MA和不当行为在线上报功能**；
- **支持证书撤撤销功能，**其中PC的CRL支持基于LV的高效撤销；
- **支持EC的黑名单管理功能；**
- **支持安全审计功能；**
- **ECA与PCA支持分机构部署和管理**，保证V2X设备证书使用者的身份隐私安全；
- **支持单LA**，支持单LA的独立部署，提供可信的防跟踪能力；
- **根CA支持离线部署**，保证根CA的安全性；
- **支持TDCL**，保证相同RCA体系中，不同PCA/ACA下的V2X设备的互认；
- **支持对接国家级的TRCL**，保证不同RCA下的V2X设备互认。

遵循标准



ICS 33.060.99
M30

YD

中华人民共和国通信行业标准

YD/T [×××××]—[××××]
[代替 YD/T]

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

Technical Requirement of Security Certificate Management System for LTE-based Vehicular Communication

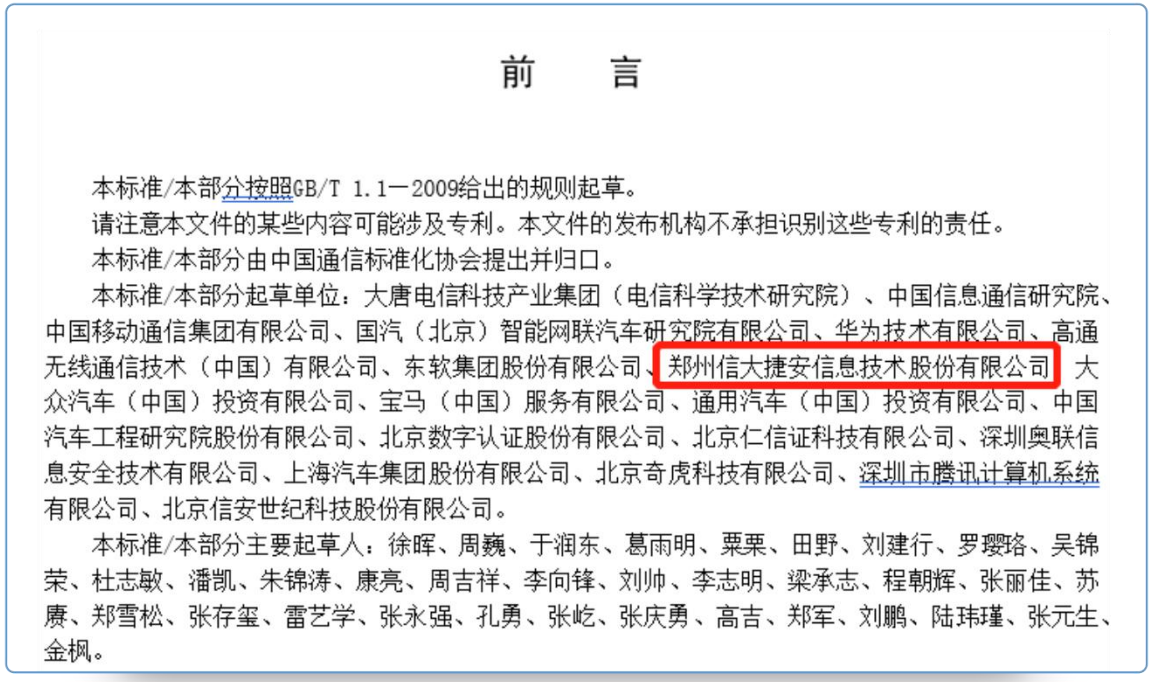
[点击此处添加与国际标准一致性程度的标识]

（报批稿）
（本稿完成日期：2020 年 8 月）

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部 发布

支持国内CCSA《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》标准，后期根据客户需求扩展支持IEEE1609.2和ETSI证书标准。



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。

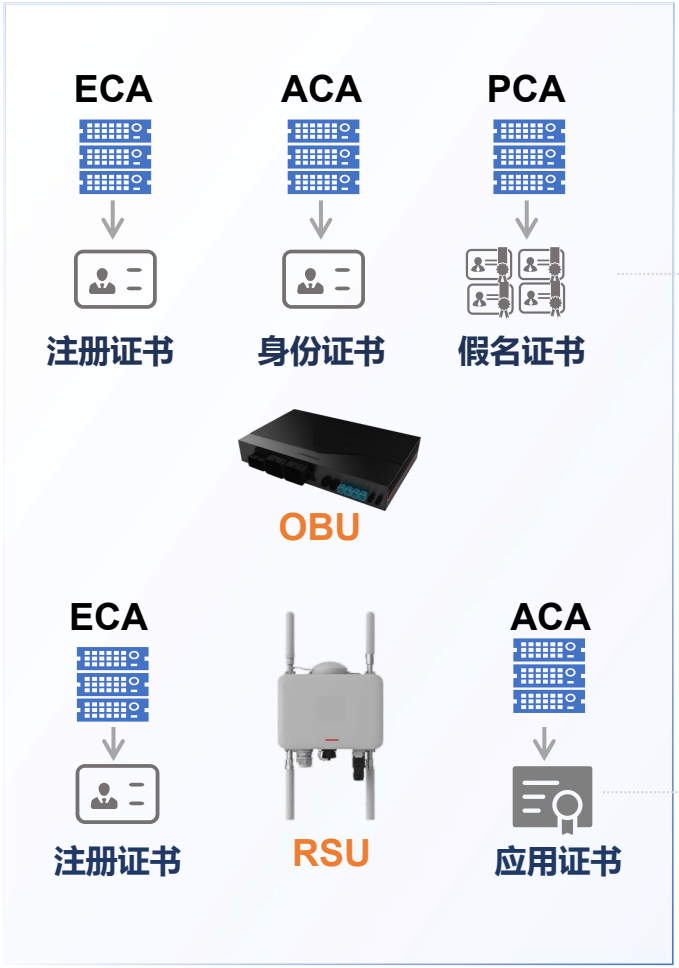
本标准/本部分由中国通信标准化协会提出并归口。

本标准/本部分起草单位：大唐电信科技产业集团（电信科学技术研究院）、中国信息通信研究院、中国移动通信集团有限公司、国汽（北京）智能网联汽车研究院有限公司、华为技术有限公司、高通无线通信技术（中国）有限公司、东软集团股份有限公司、郑州信大捷安信息技术股份有限公司、大众汽车（中国）投资有限公司、宝马（中国）服务有限公司、通用汽车（中国）投资有限公司、中国汽车工程研究院股份有限公司、北京数字认证股份有限公司、北京仁信证科技有限公司、深圳奥联信息安全技术有限公司、上海汽车集团股份有限公司、北京奇虎科技有限公司、深圳市腾讯计算机系统有限公司、北京信安世纪科技股份有限公司。

本标准/本部分主要起草人：徐晖、周巍、于润东、葛雨明、粟栗、田野、刘建行、罗璎珞、吴锦荣、杜志敏、潘凯、朱锦涛、康亮、周吉祥、李向锋、刘帅、李志明、梁承志、程朝辉、张丽佳、苏赓、郑雪松、张存玺、雷艺学、张永强、孔勇、张屹、张庆勇、高吉、郑军、刘鹏、陆玮瑾、张元生、金枫。

信大捷安

签发证书类型



对应私钥签名

BSM消息：车辆基本安全消息，用来在车辆之间交换安全状态数据，包括车辆身份信息、实时定位和运动状态信息、车身状态信息、轨迹信息、类别信息以及灯光等辅助信息等。

对应私钥签名

MAP消息：地图消息，用来定义一定区域内的地图信息，描述道路位置、连接关系以及属性等。消息内容包括路口信息、路段信息、车道信息等。

SPAT消息：信号灯消息，用于传递一个或多个路口信号灯的当前状态信息，包括信号灯当前工作状态、相位列表以及各相位状态配时等。

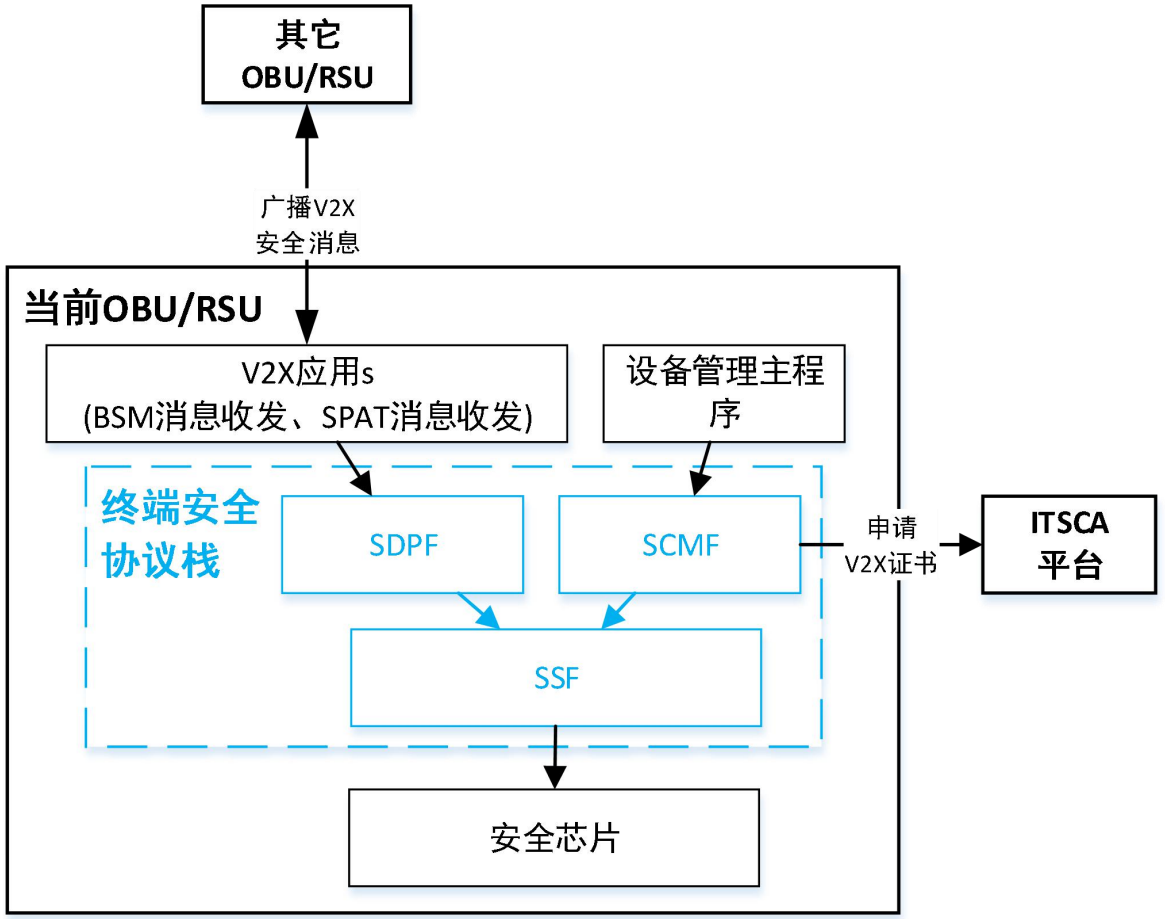
RSI消息：路侧交通信息消息，由路侧单元向周围车载单元发布的交通事件消息以及交通标志与标线信息。

RSM消息：路侧安全消息，由路侧单元向周围车载单元广播其自身和周边交通参与者的实时状态信息，交通参与者包括车辆、行人、非机动车等。

信大捷安

终端安全协议栈

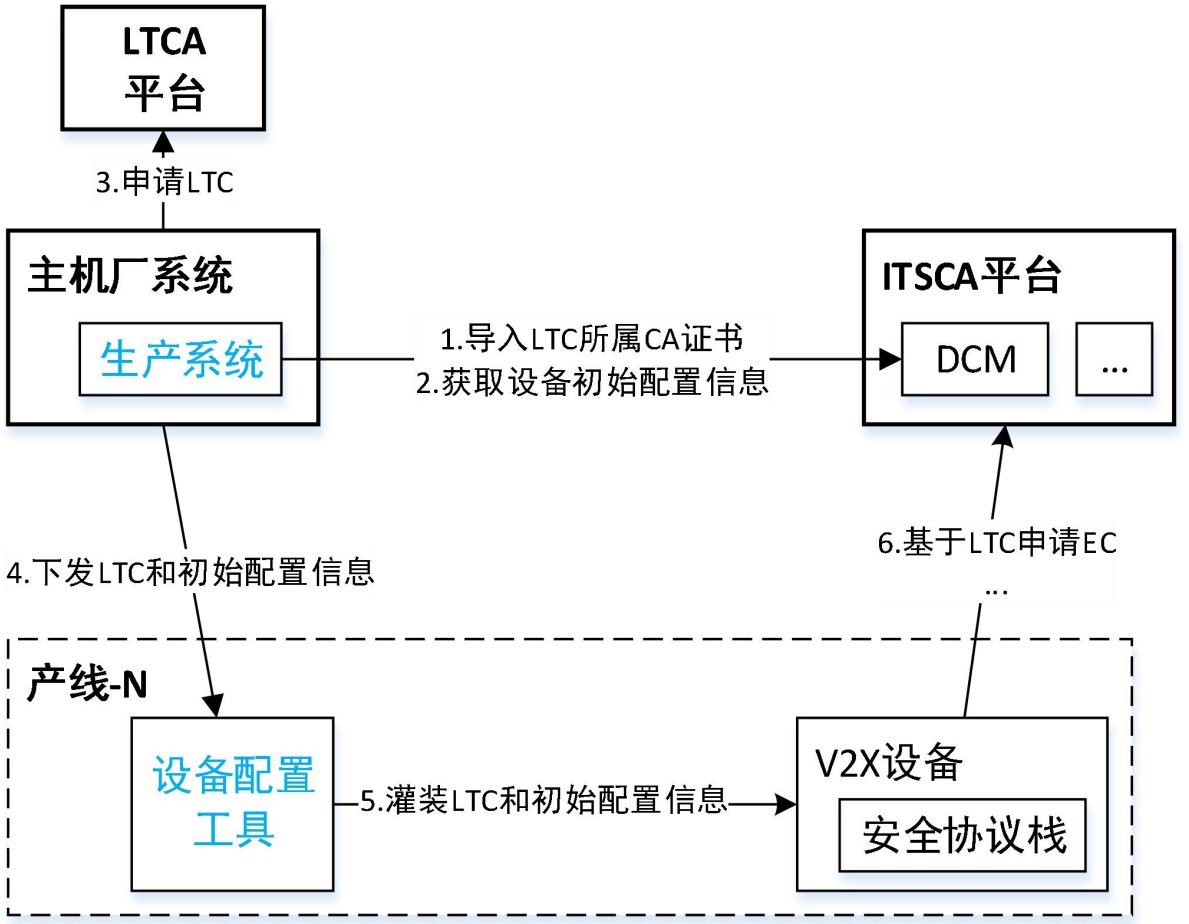
- SCMF：安全凭证管理功能，负责与ITSCA平台进行远程交互，为OBU/RSU申请V2X证书。
- SDPF：安全数据处理功能，负责为V2X应用提供数据处理接口，包括V2X消息的签名/验签、加密/解密，支撑V2X设备间的安全通信。
- SSF：安全服务功能，基于安全芯片为SCMF/SDPF提供基础的密钥对生成、原始数据的签名/验签、加密/解密等功能。



信大捷安

产线集成

1. 生产系统将LTC所属的CA证书导入DCM系统；
2. 生产系统从DCM获取初始配置信息，包括TRCL、TDCL、ECA证书、PCA证书、DCM地址、PRA地址、LPF文件等（可选的，获取离线的EC/PC）；
3. 生产系统向LTCA申请LTC；
4. 生产系统基于原LTC下发机制，连同初始配置信息一起下发至设备配置工具；
5. 设备配置工具将LTC和初始配置信息一同灌装至V2X设备内；
6. 安全协议栈基于LTC向DCM申请EC。



信大捷安

ITS-CA系统部署

信大捷安

信大捷安ITS-CA优势

最新标准制定方、系统功能最完善

信大捷安作为CCSA的《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》标准的主要制定方之一，《C-V2X 异常行为管理技术要求》标准立项主要发起方之一，ITS-CA系统在同期竞品中功能最为完善和全面。

丰富的实施经验

包括北汽、宇通等国内车企，也包括上海临港、机西高速等车路协同示范点。是国内最早为主机厂提供ITS-CA整体解决方案的供应商。

建设周期短、灵活部署

1. 信大捷安全程参与CCSA标准制定工作，系统可在较短时间内满足CCSA的标准要求，建设周期极短；
2. 信大捷安ITS-CA系统可根据客户需求，通过配置灵活增删功能模块，实现定制化快速部署。

众多的产业链合作伙伴

信大捷安是最早参与V2X安全领域产品研发的企业，已于恒润、雅讯、东软、大唐、金溢、万集、华砺智行、华为等主流的路侧设备及车载单元设备厂商建立良好的合作关系，ITS-CA系统可快速适配各大厂商的产品并提供服务。

端到端解决方案

ITS-CA结合自主研发的V2X高性能安全芯片以及终端安全协议栈，提供V2X端到端安全解决方案

支持多种运营模式

可为国家部委ITS-CA运营中心提供完整的系统；可为有自建ITS-CA能力的企业，提供满足需求的独立ITS-CA系统，并签发子CA；可为没有自建ITS-CA的企业，提供OBU证书签发服务；可为车路协同试验场提供安全测试平台。

信大捷安

信大捷安ITS-CA行业影响力

为加速我国车联网和智能网联汽车产业发展，进一步促进汽车、信息通信、交通、安全等行业的跨界协同，2020智能网联汽车C-V2X“新四跨”暨大规模先导应用示范活动在上海举办，加速了C-V2X规模化商用步伐。此次共有来自整车、芯片模组、终端、安全等130余家企业共同参与，活动中共计有62支队伍参与了互联互通测试，**信大捷安提供的安全产品和CA服务，市场渗透率超过60%。**

信大捷安

目录

01 C-V2X发展现状

02 ITS-CA建设必要性和行业发展

03 ITS-CA技术方案

04 关于信大捷安

信大捷安

关于信大捷安

郑州信大捷安信息技术股份有限公司成立于2004年，注册资本14727万元，是一家专业从事**国密安全芯片创新设计、云安全服务平台研发，为移动互联网、物联网提供信息安全服务**的智力密集型高新技术企业。

科技奖项

- 国家企业技术中心
- 移动信息安全关键技术国家地方联合工程实验室
- 河南省大数据安全防护产业技术研究院
- 河南省移动信息安全工程技术研究中心
- 移动信息安全河南省工程实验室
- 河南省企业技术中心
- ……

知识产权

国家科技进步奖二等奖

国家级

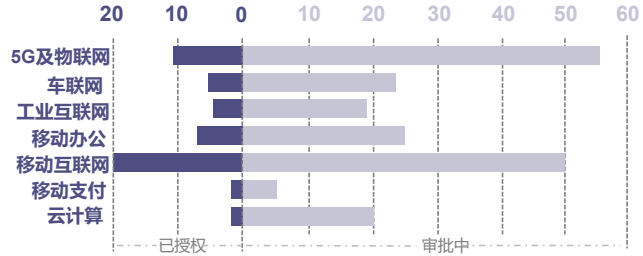
· 国家科技进步奖二等奖**1**项

省部级

· 国家教育部技术发明奖一等奖**1**项

· 党政密码科学技术进步三等奖**3**项

· 河南省科技进步奖**7**项



已授权专利**85**项（发明专利**53**、实用新型**32**）

计算机软件著作权**111**项，集成电路布图设计**6**项

参与国家（行业）标准规范

全国汽车标准化技术委员会 （汽标委）TC114

- 信息安全工作组
- 网联应用工作组

全国信息安全标准化技术委员会成员（信安标委）

中国智能网联汽车产业创新联盟成员

中国通信标准化协会CCSA TC485

- WG1总体工作组 车联网子组
- WG1 总体工作组 移动互联网+汽车子组

中国智能交通产业联盟

- 车载信息服务与安全工作组
- 交通运输信息安全工作组

信大捷安

公司产品资质及参与国家级保障活动

公司服务资质

ISO9001质量管理体系认证证书

IEC27001信息安全管理体系认证证书

ISO14001环境管理体系认证证书

CMMI3能力成熟度等级证书

国家信息安全测评服务资质-安全工程类一级

河南省大数据安全防护产业技术研究院

业务领域

警务

（2004年至今 ）

从2004年至今先后参与建设、服务20个省份移动警务平台。

政务

（2009年至今）

从2009年至今已服务市场监督、税务、财政、检察院、法院、司法、纪委监察委、国家电网等政府部门。

物联网

（2014年至今）

从2014年服务领域延伸至物联网，比如：奥迪下一代V2X智能网联汽车、比亚迪云轨、美的智能家电、新潮传媒户外多媒体屏媒等领域。

智能家居　**轨道交通**

智能网联汽车　**数字屏媒**

梯联网　工业互联网

智能交通

5G基础设施

（2018年至今）

从2018年底开始与华为车联网团队交流V2X，并制订对应的C-V2X的研发计划；

公司**自主研发的5G通信基础安全单元**，作为5G通信基础设施核心组件，可应用于智慧交通、智慧城市、智慧农业等产业互联网应用场景，服务万物互联。

信大捷安

技术专业能力

A

公司

综合实力强，行业地位领先。

B

团队

具备独立的车联网实施团队，从售前、方案、产品、嵌入式研发到实施与运维，支持覆盖项目完整生命周期。

C

方案

深入了解智能网联汽车生产过程、车联网业务安全应用，能结合生产过程及业务场景设计完整、合理的技术方案。

D

产品

智能网联汽车安全应用需求实现依赖的产品线齐全，涉及系统、芯片、协议栈等，且产品合规有资质。

E

经验

具备丰富的车联网项目案例与实施、集成经验，案例有量产车型。

F

服务

具备科学化的项目管理和服务方法论，完善的项目服务及运维管理流程，同时保障系统的稳定运行、项目的持续性和系统的先进性。

信大捷安

信大捷安整体解决方案优势

自主研发**国家密码算法安全芯片，以及片上操作系统（COS）；**

国家密码管理局
商用密码产品生产定点单位
承建工信部公共安全服务平台

提供**“芯-端-管-云”一体化的信息安全解决方案；**

比亚迪秦100、宋MAX、唐**已量产**
宇通新能源大巴**已批量装车**
业务覆盖**研发-测试-生产-验收-售后各环节**

众多知名的**Tier1合作伙伴**

信大捷安

生活，本应安全

www.safecenter.com