ICS 33.060.99
CCS M 30

中华人民共和国国家标准

GB/T 45112—2024

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

LTE-based vehicular communication—Technical requirement of security certificate management system

2024-12-31 发布　　2025-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：中国信息通信科技集团有限公司、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、北京数字认证股份有限公司、北京信长城科技发展有限公司、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、腾讯云计算(北京)有限责任公司、北京信安世纪科技股份有限公司、上海蔚来汽车有限公司、重庆两江智慧城市投资发展有限公司、国汽智端(成都)科技有限公司。

本文件主要起草人：徐晖、周巍、房骥、葛雨明、田野、杜志敏、梁承志、吴志明、刘为华、刘献伦、郑军、李向锋、粟栗、于润东、刘建行、刘帅、潘凯、马建超、郑雪松、杨广渊、温博雪、程朝辉、张丽佳、杨行、严冬、雷艺学、张永强、王新华、张屹、张庆勇、高吉、刘鹏、陆玮瑾、郜冲、李洪桥。

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

1 范围

本文件规定了基于 LTE 的车联网安全证书管理系统架构、证书管理要求、安全认证机制要求和相关的显式证书格式及交互流程。

本文件适用于 LTE-V2X 设备和安全证书管理系统。

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 16262(所有部分) 信息技术 抽象语法记法一(ASN.1)

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 25069 信息安全技术 术语

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 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则

GB/T 32918.2 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

GB/T 32918.4 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法

GB/T 32918.5 信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

ISO/IEC 8825-7 信息技术 抽象语法记法一(ASN.1)编码规则 第 7 部分：八位字节编码规则(OER)[Information technology—ASN.1 encoding rules—Part 7：Specification of octet encoding rules (OER)]

3GPP TS 33.220 通用认证架构：通用引导架构[Generic authentication architecture (GAA)；generic bootstrapping architecture (GBA)]

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

V2X 设备 V2X equipment

车载单元、路侧设备和车联网服务提供商的安全设备。

3.2

V2X 通信证书 V2X communication certificate

证书机构签发给车联网设备的与 V2X 通信相关的数字证书。