ICS 33.060.99
CCS M30

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45112-2024

LTE-based vehicular communication - Technical requirements of the security certificate management system

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

Issued on: December 31, 2024 **Implemented on: April 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part

1.Structure and drafting rules for standardization documents" Drafting. Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents. This document was proposed by the Ministry of Industry and Information Technology of the People's Republic of China. This document is under the jurisdiction of the National Communications Standardization Technical Committee (SAC/TC485). This document was drafted by: China Information and Communications Technology Group Co., Ltd., China Academy of Information and Communications Technology, China Mobile Communications Group Co., Ltd. China Automotive (Beijing) Intelligent Connected Vehicle Research Institute Co., Ltd., Huawei Technologies Co., Ltd., Qualcomm Wireless Communications Technologies (China) Ltd. Ltd., Neusoft Group Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Volkswagen (China) Investment Co., Ltd., BMW (China) Service Co., Ltd., General Motors (China) Investment Co., Ltd., Beijing Digital Certification Co., Ltd., Beijing Xinchangcheng Technology Development Shenzhen Aolian Information Security Technology Co., Ltd., Shanghai Automotive Group Co., Ltd., Beijing Qihoo Technology Co., Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Beijing Xin'an Century Technology Co., Ltd., Shanghai Weilai Automobile Co., Ltd., Chongqing Liangjiang Zhi Huicheng City Investment Development Co., Ltd. and Guoqi Zhiduan (Chengdu) Technology Co., Ltd. The main drafters of this document are. Xu Hui, Zhou Wei, Fang Ji, Ge Yuming, Tian Ye, Du Zhimin, Liang Chengzhi, Wu Zhiming, Liu Weihua, Liu Xianlun, Zheng Jun, Li Xiangfeng, Su Li, Yu Rundong, Liu Jianxing, Liu Shuai, Pan Kai, Ma Jianchao, Zheng Xuesong, Yang Guangyuan, Wen Boxue, Cheng Zhaohui, Zhang Lijia, Yang Xing, Yan Dong, Lei Yixue, Zhang Yongqiang, Wang Xinhua, Zhang Yi, Zhang Qingyong, Gao Ji, Liu Peng, Lu Weijin, Tai Chong, and Li Hongqiao. Wireless communication technology for Internet of Vehicles based on LTE

Technical requirements for security certificate management system

1 Scope

GB/T 45112 specifies the security certificate management system for LTE-V2X, the vehicle-to-everything technology China has standardised on. Every message a vehicle broadcasts to another vehicle or to the roadside has to be signed, or the channel becomes an attack surface; but the signature also has to be anonymous, or the system becomes a national vehicle tracking network. Resolving that tension is what a V2X PKI does, and this document specifies it: the architecture of the certificate management system and the roles within it, the enrolment of a device, the issue and use of the short-lived pseudonym certificates a vehicle rotates through, the linkage authorities that make misbehaviour traceable without making ordinary traffic identifiable, the certificate revocation list and its distribution, the trust relationships between certificate authorities, and the interfaces and the security requirements at each of them. At 90,000 words it is one of the largest documents in the Chinese connected vehicle system. For a carmaker, a Tier 1 or a roadside unit supplier entering the Chinese V2X market, this is the text a security design has to satisfy.

This document specifies the architecture of the LTE-based Internet of Vehicles security certificate management system, certificate management requirements, security authentication mechanism requirements and related The explicit certificate format and interaction process related to it. This document applies to LTE-V2X devices and security certificate management systems.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 16262 (all parts) Information technology Abstract syntax notation

GB/T 25056 Information security technology certificate authentication system password and related security technical specifications

GB/T 25069 Information security technical terms

GB/T 32905 Information security technology SM3 cryptographic hash algorithm

GB/T 32907 Information security technology SM4 group key algorithm

GB/T 32918.1-2016 Information security technology SM

3 Terms and definitions

The terms and definitions defined in GB/T 25069 and the following apply to this document.

3.1 V2X equipment Safety equipment for vehicle-mounted units, roadside equipment and connected vehicle service providers.

3.2 A digital certificate related to V2X communication issued by a certificate authority to a connected vehicle device.

4 Public key encryption algorithm

GB/T 32918.5 Information Security Technology SM

5 Parameter Definition

GB/T 36624 Information technology security technology identifiable encryption mechanism ISO / IEC 8825-