ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43694-2024

Cybersecurity technology - Certificate application integrated service interface specification

网络安全技术 证书应用综合服务接口规范

Issued on: April 25, 2024 **Implemented on: November 1, 2024**

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 and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260): This document was drafted by: Beijing Digital Certification Co:, Ltd:, Boya Zhongke (Beijing) Information Technology Co:, Ltd:, Beijing Qihoo Technology Co:, Ltd:, Shandong De'an Information Technology Co:, Ltd:, China Electric Power Research Institute, Beijing Xin'an Century Technology Co:, Ltd:, Wuxi Jiang South China Information Security Engineering Technology Center, China Electronics Technology Standardization Institute, Geer Software Co:, Ltd:, China Electronics Technology Network Security Technology Co:, Ltd:, Shenzhen Real Estate Registration Center, Zhengzhou Xindajiean Information Technology Co:, Ltd:, Alibaba Cloud Computing Co:, Ltd:, Zhejiang Jiang Jiuzhou Quantum Information Technology Co:, Ltd:, Aerospace Information Co:, Ltd:, Digital Security Times Technology Co:, Ltd:, Zhixun Password (Shanghai) Hai) Testing Technology Co:, Ltd:, China Science and Technology Information Security Common Technology National Engineering Research Center Co:, Ltd:, China Automotive Engineering Research Institute Co:, Ltd: Ltd: The main drafters of this document are: Liu Wei, Zhao Yongsheng, Xia Luning, Li Shusheng, Liu Zhong, Cheng Kewei, Pu Yusan, Zhang Yi, Zhang Zhilei, Ma Hongfu, Yuan Zhonglin, Li Zhihu, Jiao Jingwei, Liu Ping, Huang Jingjing, Tan Wuzheng, Kou Jianbo, Yan Hailong, Liu Xianlun, Liu Weihua, Xiao Shuting, Zhang Wenke, Yang Qianmei, Dong Liangliang, Zhou Weilin, Han Wei, Gao Zhenpeng, Hu Jianxun, Liu Chong, and Mou Jie: Network Security Technology Certificate Application Comprehensive Service Interface Specification

1 Scope

GB/T 43694-2024 specifies the integrated service interface through which a Chinese application obtains and uses digital certificates. China runs its own public key infrastructure on its own cryptographic algorithms, and an application that has to sign, verify, encrypt or decrypt using a certificate needs a defined interface to the certificate service; without one, every certificate authority and every middleware vendor invents their own, which is what this standard puts an end to. It sets the classification of the interface into client-side and server-side services, the identifiers and data structures with their definitions and format requirements, and then the interface definitions themselves in detail, the client COM component interface among them, covering certificate application, issuance, query, update, revocation and status checking, together with the signing, verification and envelope operations that an application actually calls. For any software vendor, integrator or certificate authority operating inside the Chinese PKI, this is the interface contract, and for a foreign supplier it is the document that says exactly what a Chinese customer will expect their product to implement.

This document specifies the requirements and definitions of the comprehensive service interface for certificate applications and describes the corresponding verification methods: This document is applicable to the development of certificate application middleware and certificate application system under the public key cryptography infrastructure application technology system, as well as the development of certificate application middleware and certificate application system under the public key cryptography infrastructure application technology system: Development and testing of code application support platform:

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 20518 Information security technology Public key infrastructure Digital certificate format

GB/T 25061 Information security technology XML digital signature syntax and processing specification

GB/T 25069 Information security technical terms

GB/T 33560 Information security technology cryptographic application identification specification

GB/T 35275 Information security technology SM2 cryptographic algorithm encryption

signature message syntax specification

GB/T 35276 Information security technology SM2 cryptographic algorithm usage specification

GB/T 35291 Information security technology Intelligent password key application interface specification

GB/T 36322 Information security technology cryptographic equipment application interface specification

GB/T 43578 Information security technology general cryptographic service interface specification GM/T 0094-2020 Public Key Cryptography Application Technology System Framework Specification GM/Z4001 Cryptographic Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 25069, GM/Z4001 and the following apply to this document: 3:1 digital certificatedigitalcertificate A data signed by a CA that contains information about the public key owner, public key, issuer, validity period, and extended information: structure:

Note: Digital certificates are also called public key certificates: They are divided into personal certificates, institutional certificates, and device certificates by category, and into signature certificates and encryption certificates by purpose: [Source: GM/Z4001-2013, 2:115] 3:

2 User key userkey An asymmetric key pair stored inside the device and used for application cryptographic operations:

Note: User keys include a signature key pair and an encryption key pair: 3:3 keycontainer A unique storage space in a cryptographic device used to store user keys: