ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43578-2023

Information security technology-Universal cryptography service interface specification

信息安全技术 通用密码服务接口规范

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

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

Table of Contents

Preface

1 Scope

2 Normative references

3 Terms and Definitions

4 Abbreviations

5 General cryptographic service interface description

5:1 The position of the general cryptographic service interface in the public key cryptography application technology system framework

5:2 General password service interface composition and function description

6 General cryptographic service interface function definition

6:1 Algorithm identification and data structure

6:2 Environment class functions

6:3 Certificate class functions

6:4 Cryptographic operation functions

6:5 Message functions

7 Verification methods

7:1 Verification environment

7:2 Operation verification of cryptographic service environment

7:3 Certificate class function function verification

7:4 Signature verification and verification

7:5 Digest calculation verification

7:6 Asymmetric encryption and decryption verification

7:7 Symmetric encryption and decryption verification

7:8 Generate key pair verification

7:9 PKCS

Foreword

This document complies with the provisions of GB/T 1:1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

Please note that some content in this document may be subject to patents: The publisher of this document assumes no responsibility for identifying patents:

This document is proposed and coordinated by the National Information Security Standardization Technical Committee (SAC/TC260):

This document was drafted by: Beijing Digital Certification Co:, Ltd:, Wuxi Jiangnan Information Security Engineering Technology Center, China Electric Power Research Institute Research Institute, China Electronics Technology Standardization Institute, Boya Zhongke (Beijing) Information Technology Co:, Ltd:, Shandong De'an Information Technology Co:, Ltd:, Shanghai Haishi Digital Certificate Certification Center Co:, Ltd:, Beijing Xin'an Century Technology Co:, Ltd:, Zhixun Password (Shanghai) Detection Technology Co:, Ltd:

Company, Geer Software Co:, Ltd:, Zhongke Information Security Common Technology National Engineering Research Center Co:, Ltd:, DataAn Times Technology Co:, Ltd:

Co:, Ltd:, Alibaba Cloud Computing Co:, Ltd:, Zhengzhou Xinda Jiian Information Technology Co:, Ltd:, China Electronics Network Security Technology Co:, Ltd:

Company, China Mobile (Hangzhou) Information Technology Co:, Ltd:, Zhejiang Jiuzhou Quantum Information Technology Co:, Ltd:, Aerospace Information Co:, Ltd:, OP- PO Guangdong Mobile Communications Co:, Ltd:, Shenzhen Real Estate Registration Center:

The main drafters of this document: Zhao Song, Wang Yinping, Cheng Lei, Xia Luning, Hou Pengliang, Li Shusheng, Liu Ping, Li Zhihu, Huang Jingjing, Cheng Kewei, Pu Yusan, Ma Hongfu, Yuan Zhonglin, Xu Tao, Wang Yulin, Jiao Jingwei, Han Wei, Tan Wuzheng, Gao Zhenpeng, Du Zhiqiang, Xiao Shuting, Liang Songtao, Liu Weihua, Wang Zhongwu, Wang Chenguang, Zhang Wenke, Dong Liangliang, Li Gen, Lu Xiaoming, Yang Qianmei, Yan Hailong:

Information security technology general cryptographic service interface specification

1 Scope

This document specifies the data structure, interface description, and function definition requirements of the universal cryptographic service interface, and describes the corresponding verification methods:

This document is applicable to the development of cryptographic application services under the public key application technology system, the development and testing of cryptographic application support platforms, and the development and testing of cryptographic application support platforms:

Development of application systems for code equipment:

2 Normative reference documents

GB/T 20518

GB/T 25069

GB/T 32918

GB/T 33560

GB/T 35275

GB/T 35276

GB/T 35291

GB/T 36322

GB/T 41389

4 Abbreviations

The following abbreviations apply to this document: CA: Certificate Authority CRL: Certificate Revocation List