ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 19714-2025

Replacing GB/T 19714-2005

Cybersecurity technology - Public key infrastructure - Certificate management protocol

网络安全技术 公钥基础设施 证书管理协议

Issued on: August 1, 2025 **Implemented on: February 1, 2026**

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.

This document replaces GB/T 19714-2005 "Information Technology Security Technology Public Key Infrastructure Certificate Management Protocol".

Compared with GB/T 19714-2005, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) The scope of the standard has been changed (see Chapter 1, Chapter 1 of the 2005 edition);

b) Deleted the PKI management overview (see Chapter 5 of the 2005 edition);

c) Deleted the content related to proof of possession of encryption key and private key (see 6.3.2 and 7.2.8 of the 2005 edition) and proof of possession of negotiation key and private key.

Content (see 6.3.3 of the 2005 edition);

d) Deleted the content related to root CA updates (see 6.4 and 8.2 of the 2005 edition);

e) Deleted the prerequisites and restrictions related to terminal entity initialization and initial registration/authentication (see Chapter 6 of the 2005 edition);

f) Added "Process and Message Structure" to describe the process and message structure of certificate management between PKI components (see Chapter 6);

g) Added national standard algorithms and algorithm OIDs supported by the protocol (see Table A.1 in Appendix A);

h) Added the description of "transactionID" (see C.1.2.1 of Appendix C);

i) Added the setting of the protocol version field value (see C.1.2.1);

j) Added the "implicit confirmation" data structure (see C.1.2.2) and the "confirmation waiting time" data structure (see C.1.2.3);

k) Added support for the certificate template identifier "certTemplateID" field in the generalInfo extension of PKIHead (see C.1.2.4);

l) Added descriptions on "multiple protection" (see C.1.4);

m) The encrypted value data structure has been changed to "SM2EnvelopedKey" (see C.2.2, 7.2.2 of the 2005 edition), and the protocol has been added Encrypted data is uniformly changed to use "SM2EnvelopedKey" (see C.3.2, 6.2.2, 7.3.2, Appendix E of the 2005 edition);

n) Added content related to certificate confirmation (see C.1.3, C.3.15);

o) Added "Polling Request and Response" data structures (see C.3.19);

p) Added content related to certificate freeze and certificate thawing requests and responses (see C.1.3, C.3.20, and C.3.21);

q) added more information on failure conditions (see C.2.3);

r) Added support for applying for multiple certificates using CertReqMessages and for requesting multiple certificates using CertRepMessage There are multiple implementation options for response, clarifying that there are multiple options for implementation (see C.3.1 and C.3.2), clarifying a Common implementation methods (see A.5);

s) Deleted the content related to cross-certification (see 7.3.11, 7.3.12, and 8.6 of the 2005 edition);

t) Deleted the PKI management functions related to CA initialization and terminal entity initialization (see Chapter 8 of the 2005 edition);

u) Deleted the transmission-related content of the CMP protocol (see Chapter 9 and Appendix G of the 2005 edition);

v) Deleted "Request Message Behavior Description" (see Appendix D of the 2005 edition) and incorporated its main content into Appendix C (see C.2.8, C.3.1);

w) The certificate management protocol OID has been changed (see Appendix F of the 2005 edition).

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 is proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: Beijing Digital Certification Co., Ltd., China Electronics Technology Standardization Institute, Xi'an Xidian Jietong Wireless Network Network Communications Co., Ltd., Boya Zhongke (Beijing) Information Technology Co., Ltd., Changchun Jida Zhengyuan Information Technology Co., Ltd., Shanghai Municipal Digital

Certificate Certification Center Co., Ltd., Huawei Technologies Co., Ltd., Wuhan University, the First Research Institute of the Ministry of Public Security, and Asiasoft Information Technology (Shanghai) Co., Ltd., Changyang Technology (Beijing) Co., Ltd., Shenzhen E-Commerce Security Certificate Management Co., Ltd., Shaanxi Provincial Information Engineering Research Institute, Jiangnan Xinan (Beijing) Technology Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Tsinghua University, Geer Software Co., Ltd.

Co., Ltd., Guangdong Electronic Commerce Certification Co., Ltd., Tongzhi Weiye Software Co., Ltd., Beijing Times Newway Information Technology Co., Ltd.

Beijing Zhongguancun Laboratory, Zhejiang Dahua Technology Co., Ltd., and the Cybersecurity Industry Development Center of the Ministry of Industry and Information Technology (MIIT).

Information Center of the Ministry of Information Technology), Gongxintong (Beijing) Information Technology Co., Ltd., the Sixth Research Institute of China Electronics Information Industry Group Co., Ltd., State Grid Blockchain Technology (Beijing) Co., Ltd., China Science and Technology Information Security Common Technology National Engineering Research Center Co., Ltd., Digital Security Times Technology Co., Ltd.

Co., Ltd., Qi'anxin Wangshen Information Technology (Beijing) Co., Ltd., and China Electronics Technology Group Corporation Network Security Technology Co., Ltd.

The main drafters of this document are: Gao Wenhua, Gao Wenju, Li Yanfeng, Li Qin, Wang Bingxin, Ding Zhaowei, Wang Yulin, Zeng Guang, He Debiao, Hu Guangjun, Lin Xueyan, Xia Luning, Xia Bingbing, Li Xiangfeng, Fu Dapeng, Liu Zhong, Wang Yuehui, Zhang Guoqiang, Li Zhiyong, Tian Yucun, Li Liang, Guo Yanfei, Ding Beijing, Deng Chen, Liu Bin, Zhao Jing, Zhang Ziwei, Wei Yicai, Zhao Hua, Shen Zhichun, Zhang Xin, Su Jinyan, Wang Zhihui, Zheng Huitao, Zhao Xiaorong, Xu Jiannan, Wang Tong, Wang Haiyang, Liu Weihua, Jia Keting, Zheng Qiang, Chen Shule, Jiao Zhengkun, Yu Zhengchen, Zhu Weiru, Zhao Boxin, Zhang Jianqing, Chen Zixiong, Wang Jin, Wang Bin, Wang Long, Yang Ke, Gao Zhenpeng, Du Zhiqiang, An Jincheng, and Kou Jianbo.

The previous versions of this document and the documents it replaces are as follows.

- First published in 2005 as GB/T 19714-2005;

- This is the first revision.

Cybersecurity Technology Public Key Infrastructure Certificate Management Protocol

1 Scope

This document provides the structure and content of the certificate management protocol in the public key infrastructure (PKI), and specifies the requirements for certificate generation and management. The protocol message format.