ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21053-2023

Replacing GB/T 21053-2007

Information security techniques - Public key infrastructure - Security technology requirement for PKI system

信息安全技术 公钥基础设施 PKI系统安全技术要求

Issued on: March 17, 2023 **Implemented on: October 1, 2023**

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

Table of Contents

1 Scope

The document divides the security levels of a PKI system into a basic level and an

enhanced level, and lays down the security function requirements and the security assurance requirements that belong to each of those levels.

The document applies to the research and development of PKI systems, and is used as a reference for the evaluation and the procurement of PKI system products.

2 Normative references

The content of the following documents becomes, through normative reference in the text, an indispensable part of the document. For a dated reference only the edition bearing that date applies; for an undated reference the latest edition, including all amendments, applies.

GB/T 20518-2018, Information security technology - Public key infrastructure - Digital certificate format.

GB/T 25056-2018, Information security technology - Specification for the cryptography of certificate authentication systems and the related security technology.

GB/T 25069, Information security technology - Terminology.

GM/T 0014-2012, Specification for the cryptographic protocol of digital certificate authentication systems.

3 Terms and definitions

The terms and definitions delimited in GB/T 25069, together with those below, apply to the document.

3.1 PKI system: within a public key infrastructure, an information system that carries out functions such as the issuing, the revocation and the management of digital certificates on the basis of a public key cryptosystem, and that provides the corresponding services to subscribers (3.4).

3.2 split knowledge: the process of splitting a cryptographic key into several key components in such a way that no single component shares knowledge of the original key, while separable entities can afterwards input them into or output them from a cryptographic module and recombine them to recreate the original cryptographic key. Note: the combination can be completed by requesting all of the components or a subset of them. Source: GB/T 25069-2022, 3.120.

3.3 system user: in a PKI system, a user who performs particular operations through the system operating interface so as to control particular functions of the system. Example: the administrator, the auditor and the operator of the PKI system. Source: GB/T 25069-2022, 3.652, modified.

3.4 subscriber: a user who obtains a digital certificate through the services provided by the PKI system.

3.5 system user key: the key used by a system user. Example: the key used to authenticate the identity of a user of the PKI system.

3.6 system component key: the key used by each component in the PKI system. Example: the CA signing key.

3.7 system key: the collective name for the system component keys and the system user keys of a PKI system.

3.8 subscriber key: the key used by a subscriber. Example: the certificate subject key of a user certificate issued by the PKI system.

4 Abbreviations

The following abbreviations apply to the document.

CA: certification authority. CRL: certificate revocation list. OCSP: online certificate status protocol. PKI: public key infrastructure. RA: registration authority.

5 PKI system framework and security levels

5.1 Typical framework. The typical framework of a PKI system is shown in Figure 1 and takes in the CA, the RA, the certificate repository, key management and the OCSP service. The RA interacts with the subscriber, receives the certificate request and forwards it to the CA; once the CA has signed the certificate, the RA sends the issued subscriber certificate back to the subscriber. The CA issues the corresponding certificate against the certificate request, publishes a CRL for revoked certificates, and then stores certificates and CRLs in the certificate repository. The certificate repository component provides storage and query services for certificates and CRLs. The key management component provides the management functions of generation, storage, distribution, import and export, use, backup, recovery, archiving and destruction for the various kinds of key in the PKI system. The OCSP service component is optional: where the PKI system supports the OCSP function, that component carries out the reception of OCSP requests and the response to them. A note refers the reader to Clause 5 of GB/T 19771-2005 for a detailed description of the functions and transactions of the components of a PKI system.

5.2 Security functions. The security function requirements that a PKI system is required to satisfy cover key management, template management, certificate management and the functions bearing on the security of the PKI system itself. Key management is the function needed to support certificate security and cryptographic application security; template management and certificate management are the main security functions the PKI system offers; identity authentication, access control, security audit, non-repudiation of origin, backup and recovery, start-up and operation monitoring and communication security between components are the functions needed to secure the PKI system itself.

5.2 Security functions, continued. Key management, at 6.1 to 6.3, realises the several key management functions through the key management component, managing the generation, storage, distribution, import and export, use, backup, recovery, archiving and destruction of the subscriber keys of the PKI system and of the system keys used in the components. Template management, at 6.4, is realised through the CA and the RA, predefining the fields of certificates, CRLs and OCSP responses and the values the extensions can take. Certificate management, at 6.5, realises the management functions for certificates and CRLs through the CA and the RA. Identity authentication, at 6.6, and access control, at 6.7, authenticate and control the login to and the operations on each component, so as to prevent unauthorised users and unauthorised operations. Security audit, at 6.8, generates audit records for the key security events of each component and gives log support for accountability and its determination. Non-repudiation of origin, at 6.9, produces non-repudiation evidence for security-related information through the generation and verification of that evidence, and provides evidence of non-repudiation when a dispute arises. Backup and recovery, at 6.10, restores the normal operation of the components from backup data by calling the recovery function when a system failure or another serious error occurs. The list of security functions continues beyond the pages available.