

ICS 35.240.01
CCS A16

SF

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

SF/T 0036-2019

**Notary information security technical specifications
(English Translation)**

Issued on: January 1, 2019

Implemented on: May 20, 2019

Issued by: Ministry of Justice of the People's Republic of China

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms, definitions and abbreviations	
3.1 Terms and definitions	
3.2 Abbreviations	
4 Notarized information security objects and content	
4.1 Information Security Object	
4.2 Information security content	
5 Notarization information security construction	
5.1 Basic requirements for information security construction	
5.2 Implementation methods of information security construction	
5.3 Information security protection level	
6 Physical security	
6.1 Basic requirements for physical security	
6.2 Environmental safety	
6.3 Equipment safety	
7 Cybersecurity	
7.1 Basic requirements for network security	
7.2 Network access control	
7.3 Network transmission security	
7.4 Network security audit and monitoring	
7.5 Security Management of Network Equipment	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

1 Scope

This standard specifies notarized information security objects and content, information security construction, physical security, network security, system security, application security Complete, data security and backup recovery and notarization PKI system security protection requirements.

This standard applies to the planning, design, and construction of notarization information security by judicial administrative notarization management departments, notary associations and various notary institutions and management.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated reference documents, the latest version (including all amendments) is applicable to this document.

GB/T 17859 Computer Information System Security Protection Classification Criteria GB/T 19713 Information Technology Security Technology Public Key Infrastructure Online Certificate Status Protocol GB/T 20269 Information Security Technology Information System Security Management Requirements GB/T 20271-2006 Information Security Technology Information System General Security Technical Requirements GB/T 20518 Information Security Technology Public Key Infrastructure Digital Certificate Format GB/T 22239-2008 Information Security Technology Information System Security Level Protection Basic Requirements GB/T 22240-2008 Information Security Technology Information System Security Level Protection Rating Guidelines GB/T 50052 Code for Design of Power Supply and Distribution System SF/T 0034-2019 Notarized data requirements and specifications

3.1 Terms and definitions

The following terms and definitions apply to this document.

3.1.1

Notarization

According to the application of a natural person, legal person or other organization, a notary institution shall, in accordance with legal procedures, deal with civil legal acts and matters of legal significance.

Activities that prove the authenticity and legality of documents and documents.

3.1.2

Notarial institutions A certification agency established in accordance with the law, not for profit, independently performing notarization functions in accordance with the law, and assuming civil liabilities.

3.1.3

Notarized matters

According to the provisions of Article 11 of the "Notarization Law of the People's Republic of China", the notary institution shall conduct the notarization business in accordance with the notarization certification object the detailed classification.

3.1.4

Notarial affairs

According to the provisions of Article 12 of the "Notarization Law of the People's Republic of China", non-certification business handled by a notary institution.

3.1.5

Notarization information security the security of notarized data and information facilities.

3.1.6

Data confidentiality Unauthorized users, entities, or processes have no access rights to the information, thereby ensuring that confidential information is not stolen or used.

3.1.7

Message-digest algorithm an encryption process does not require a key, and the encrypted data cannot be decrypted. Only the same plaintext data is entered after the same the algorithm can get the same ciphertext algorithm.

3.1.8

Block chain

In a peer-to-peer network environment, through transparent and trustworthy rules, a block chain data structure that cannot be forged, tampered and traceable is constructed Structuring, implementing and managing the transaction processing model.

Note: Transaction processing includes but is not limited to the generation, access and use of trusted data.

[GB/T 37043-2018, definition 2.5.8] 3.1.9 Digital signature Some data attached to the data unit, or the cryptographic exchange of the data unit (see "cryptography"), this data may change the change allows the recipient of the data unit to confirm the source of the data unit and the integrity of the data unit, and to protect the data to prevent others (such as receiving Recipient) forgery.

[GB/T 9387.2-1995, definition 3.3.26] 3.1.10 Asymmetric cryptographic technique Two cryptographic techniques with related transformations are used.

Note: One is the public transformation defined by the public key, and the other is the private transformation defined by the private key.

3.2 Abbreviations

The following abbreviations apply to this document.

CA certificate certification authority (Certificate Authority) CRL certificate revocation list (Certificate Revocation List) IDS Intrusion Detection Systems (Intrusion Detection Systems) IPSec Internet Protocol Security (Internet Protocol Security) OCSP Online Certificate Status Protocol (Online Certificate Status Protocol) PKI Public Key Infrastructure (Public Key Infrastructure) RA Certificate Registration Authority (Registration Authority) SSL Secure Sockets Layer (Secure Sockets Layer)

4.1 Information Security Object

Information security objects include notarization matters, notarization affairs, notarization data and notarization information facilities.

4.2 Information security content

Information security includes technical security and management security. among them.

a) Technical security includes physical security, network security, system security, application security, data security, PKI security, etc.

as follows.

1) Physical security. Notarization data centers and electronic notarization information facilities, including computer rooms, servers, network equipment, storage devices Protect equipment, PCs, mobile devices, etc. from illegal physical access, natural disasters and environmental disasters;

2) Network security. identity authentication, confidentiality, integrity, availability, controllability, authenticity and availability of data in the communication process Examination guarantee, etc.;

3) System security. operating system, database, middleware, etc.;

4) Application security. Notarization information related systems, platforms, tools and applications, such as notarization business certification system, notarization business Management system, notarized electronic file management system, notarized online acceptance system, notarized electronic data storage tool, screen record Like tools, etc.;

5) Data security. Notarized data storage security, communication security, and authority security (see SF/T 0034-2019 for details), and the staff data, user data and other data stored in the electronic notarization;

6) PKI security. PKI system security and security management in the notarization industry.

b) Management security should follow the content of GB/T 20269, the specific content is as