CCS A 11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 27913-2022

Public key infrastructure for financial services - Practices and policy framework

Issued on: April 15, 2022 **Implemented on: April 15, 2022**

Issued by: State Administration for Market Regulation, China National Standardization Administration

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 of Standardization Documents"

drafted.

This document replaces GB/T 27913-2011 "Public Key Infrastructure Implementation and Policy Framework for Financial Services", and GB/T 27913-

Compared with.2011, in addition to editorial changes, the main technical changes are as follows.

--- Deleted "Business continuity considerations comply with Annex J of ISO 15782-1.2003" (see D.4 of the.2011 edition);

--- Modify "should be performed by the authorized person" to "executed by the process initiated by the authorized person" (see 7.4.1, 8.4.1 of the.2011 edition);

--- Added about "two or more CAs can join a common scheme for mutual identification" (see 5.4);

--- Added information about "the responsible management of the CA should be able to demonstrate that the information security policy is implemented and followed" and "should exist and be enforced.

Procedures for conducting risk assessments that consider business and technical factors to identify, analyze, and evaluate trusted service risks. Conclusion of the risk assessment

The results shall be communicated to the management group or committee responsible for information security and risk management" section (see 7.2.2).

This document is modified to adopt ISO 21188.2018 "Public Key Infrastructure Implementation and Policy Framework for Financial Services".

The technical differences between this document and ISO 21188.2018 and their reasons are as follows.

--- Deleted the relevant terms of FIPS (US Federal Information Processing Standard) and references related to FIPS140-2 in the full text, choose to use

Use ISO 19790 to meet the requirements of my country's password management.

--- Added Chapter 2 for GB/T 16649.1~GB/T 16649.12, GB/T 16649.15, GB/T 18336.1-2015,

References to GB/T 18336.2-2015 and GB/T 18336.3-2015.

did not appear.

--- Added SAN (Subject Alternative Name) and EV (Extended Validation) in Chapter 4, these terms appear in this document.

--- Changed "as shown in 5.7.3 and 5.7.6" mentioned in 5.7.1 to "as shown in 5.7.2 and 5.7.6", in ISO 21188.2018

Citation error.

--- Delete the "(see 0)" appearing in D.3 of Appendix D, the citation error in ISO 21188.2018.

The following editorial changes have been made to this document.

--- Deleted the relevant examples involving DOD (United States Department of Defense) in 5.10.

Introduction

With the continuous expansion of the application of Internet technology in the financial services industry, the financial industry has become increasingly concerned about providing secure, confidential and trustworthy financial transactions.

The growing demand for easy and processing systems has led to the combination of advanced security techniques and public key cryptography. public key cryptography needs

Business-optimized technical, management and policy infrastructure (defined in this document as public key infrastructure or PKI) to meet the needs of financial application systems

Requirements for electronic identification, authentication, message integrity protection and authorization. The application of electronic identification, authentication and authorization standards in PKI further ensures that

It improves the consistency, predictability and trustworthiness of electronic transactions in system security.

In my country, digital signature and PKI technology can be used to develop applications in the financial service industry. The safety and efficacy of these applications depend in part

on

Rely on practices that ensure the overall integrity of the infrastructure. For bases that associate personal identities with other entities and key elements such as keys

For authorized systems, its users can benefit from a standard risk management system and the auditable business basis defined in this document.

This document establishes a framework for managing PKI through certificate policies, authentication service descriptions, control objectives and control procedures. to these marks

For standard implementers, entities in my country's financial transactions can rely on the extent to which this document is implemented and the inter-PKI relationship achieved by using this document.

The degree of interoperability will depend on the policy and implementation-related factors defined in this document.

Public Key Infrastructure for Financial Services

Implementation and Policy Framework

1 Scope

This document specifies the management of PKI through certificate policies and authentication business specifications, and the use of public key certificates in the financial services industry

requirements framework. It also defines the control objectives and control procedures for risk management. Although this document may be used to process digital signatures or encryption

generation of public key certificates for key establishment, but it will not be used to handle authentication methods, non-repudiation requirements, or key management protocols.

This document applies to distinguish between PKI systems in open, closed and contractual environments, and is based on the financial services industry information system

Control objectives further define the business that is run. The purpose of this document is to help implementers define PKI services that support multi-certificate policies,

Includes the use of digital signatures, remote authentication, key exchange, and data encryption.

This document makes it easier to implement the operability of PKI-controlled businesses that meet the requirements of the financial services industry in a contractual environment.

Although this document is primarily aimed at the contract environment, it does not preclude

the application of the document to other environments. The term "certificate" in this document refers to a public key certificate.

Attribute certificates are outside the scope of this document.

This document is aimed at a variety of users with different needs, so each type of user will focus on different content.

Business managers and analysts are those who need to use PKI technology in the conduct of business (e.g. e-commerce), see Section 1

Chapter ~ Chapter 6.

Technical designers and implementers are those who write the certificate policy and authentication business descriptions, see Chapters 6 to 7, and Appendix A to Appendix A.

record G.

Operational managers and auditors are those who are responsible for the day-to-day operation of the PKI system and perform consistency checks according to this document, see Chapters 6-

Chapter 7.

2 Normative references

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, dated citations

documents, only the version corresponding to that date applies to this document; for undated references, the latest edition (including all amendments) applies to

this document.

GB/T 14916-2006 Physical Characteristics of Identification Cards (ISO /IEC 7810.2003, IDT)

GB/T 16649.1 Integrated circuit cards with contacts for identification cards - Part 1.Physical characteristics

GB/T 16649.2 Identification card for integrated circuit cards with contacts - Part 2.Dimensions and locations of contacts

GB/T 16649.3 Identification Cards Integrated Circuit Cards with Contacts Part 3.Electrical Signals and Transmission Protocols

GB/T 16649.4 Identification Card Integrated Circuit Card Part 4.Structure, Security and Command for Switching

GB/T 16649.5 Integrated circuit cards with contacts for identification cards - Part 5.National