ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21054-2023

Information security techniques - Public key infrastructure - Security testing assessment approaches for PKI system

信息安全技术 公钥基础设施 PKI系统安全测评方法

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 1
2 Normative references 1
3 Terms and Definitions 1
4 Abbreviations 1
5 Overview 1
6 Safety function evaluation method 1
6.1 Key management general requirements evaluation method 1
6.2 System Key Management 2
6.3 Subscriber Key Management 6
6.4 Template Management 10
6.5 Certificate Management 11
6.6 Identification 13
6.7 Access Control 15
6.8 Security Audit 16
6.9 Origin non-repudiation 17
6.10 Backup and restore 18
6.11 Startup and running test 18
6.12 Inter-component communication security 19
7 Safety Assurance Requirement Evaluation Method 19
7.1 Development 19
7.2 Guidance documents 20
7.3 Life cycle support 21
7.4 Developer testing 23
24 Reference 25

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 21054-2007 "Information Security Technology Public Key Infrastructure PKI System Security Level Protection Assessment Criteria" but". Compared with GB/T

21054-2007, except for structural adjustment and editorial changes, the main technical changes are as follows:

a) Change the name to "Information Security Technology Public Key Infrastructure PKI System Security Evaluation Method";

b) The content of the scope has been revised (see Chapter 1, Chapter 1 of the.2007 edition);

c) Adjusted and modified the normative references (see Chapter 2, Chapter 2 of the.2007 edition);

d) The chapter "Overview" has been added to describe the general evaluation methods of PKI systems (see Chapter 5);

e) Adjust the evaluation content of Chapter 5 in the.2007 edition to the newly added Chapter

1 Scope

GB/T 21054-2023 specifies how a PKI system is tested against its security requirements. Public key infrastructure is the foundation the rest of digital trust rests on: if a certification authority can be induced to issue a certificate to the wrong party, or if its signing key can be extracted, then every signature and every encrypted session that relied on it becomes worthless retrospectively, and the compromise may not be discovered for a long time. That makes assessment of a CA unusually consequential, and it makes the assurance side - how the system was built, how its keys are generated and stored, how registration is controlled, how the audit trail is kept - as important as its functional behaviour. This document specifies the security evaluation methods for PKI systems on the basis of GB/T 21053-2023, covering both the security function evaluation methods and the security assurance requirement assessment methods. It applies to the security testing and evaluation of PKI systems. Under ICS 35.030 and CCS L80, it is written for the evaluation bodies assessing certification authorities, for the operators of PKI systems, and for the regulators who accredit them.

This document specifies the security evaluation method of the PKI system based on GB/T 21053-2023, including the security function evaluation method and security Assurance requirements assessment methods. This document is applicable to the security evaluation of PKI system.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for

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

GB/T 20518-2018 Information Security Technology Public Key Infrastructure Digital Certificate Format

GB/T 21053-2023 Information Security Technology Public Key Infrastructure PKI System Security Technical Requirements

GB/T 25069 Information Security Technical Terms GM/T 0014-2012 Cryptography protocol specification for digital certificate authentication system

3 Terms and Definitions

The terms and definitions defined in GB/T 21053-2023 and GB/T 25069 apply to this document.

4 Abbreviations

The abbreviations defined in GB/T 21053-2023 apply to this document.

5 Overview

This document is based on the security level of the PKI system specified in GB/T 21053-2023 and the security technical requirements of the corresponding level, and gives the Appropriate security assessment methods. For the typical framework, security functions and security level division of the PKI system, see Chapter 5 of GB/T 21053-2023.for basic level The PKI system shall be evaluated according to the evaluation methods corresponding to the basic level security requirements in Chapters 6 and 7 of this document; for the enhanced level The PKI system shall be evaluated according to the evaluation methods corresponding to the enhanced security requirements in Chapters 6 and 7 of this document. Complete all security requirements After the basic evaluation, all the evaluation conclusions are "conforming", and the evaluation conclusion that the evaluated PKI system "conforms to the corresponding security level" can be given. other things In other cases, the evaluation conclusion should be recorded as "does not meet the corresponding safety level". Appropriate assessment methods.

6 Safety function evaluation method

6.1 Evaluation method for general requirements of key management The test methods, expected results and result judgments of the general requirements for key management are as follows: