ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 17901.1-2020

Replacing GB/T 17901.1-1999

Information technology - Security techniques - Key management - Part 1: Framework

Issued on: March 6, 2020 **Implemented on: October 1, 2020**

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

Table of Contents

Foreword

GB/T 17901 "Information Technology Security Technology Key Management" is planned to be divided into 6 parts.

---Part 1.Framework;

---Part 2.Mechanisms using symmetric technology;

---Part 3.The mechanism of adopting asymmetric technology;

---Part 4.Mechanism based on weak secrets;

---Part 5.Group key management;

---Part 6.Key Derivation.

This part is Part 1 of GB/T 17901.

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

This part replaces GB/T 17901.1-1999 "Information Technology Security Technology Key Management Part 1.Framework", and

Compared with GB/T 17901.1-1999, the main technical changes are as follows.

---New reference documents have been added to the normative reference documents (see Chapter 2);

--- Deleted "decryption, encryption, key confirmation, key control, key distribution center (KDC), key material, key management, key transfer

The terms and definitions of KTC, public key information, random numbers, sequence numbers, and "hash function, key derivation letter" have been added

The terms and definitions of "number, key establishment, key token, message authentication code, signature system" (see Chapter 3, Chapter 3 of the.1999 edition);

--- Added Chapter 4 "Symbols and Abbreviations" (see Chapter 4);

---Chapter 4 "Summary of Key Management" of the.1999 edition was revised to Chapter 5 "General Model of Key Management", and.1999 was deleted

Version 4.1.2, adding 5.1, 5.3.1, and modifying part of the content (see Chapter 5, Chapter 4 of the.1999 edition);

---Chapter 6 "Conceptual Model of Key Distribution" of the.1999 edition was revised to Chapter 7 "Conceptual Model of Key Distribution between Two Entities", adding

7.1 has been added and part of the content has been modified (see Chapter 7, Chapter 6 of the.1999 edition);

--- Deleted Appendix D of the.1999 edition, and the relevant content is consistent with the existing national standards and cryptographic industry standards.

This section uses the redrafting law to modify and adopt ISO /IEC 11770-1.2010 "Information Technology Security Technology Key Management Part 1.Framework".

Compared with ISO /IEC 11770-1.2010, the structure of this part has been adjusted. Chapter 2 has been added. Subsequent clause numbers have been sequentially changed and adjusted.

4.2.3~4.2.5 are 5.2.2, 5.2.3.1 and 5.2.3.2, adjust Appendix B to Appendix C, and Appendix C to Appendix B.

The technical differences between this part and ISO /IEC 11770-1.2010 and the reasons are as follows.

---Chapter 2 normative references have been added (see Chapter 2);

--- Deleted some terms and definitions (see Chapter 2 of ISO /IEC 11770-1.2010);

--- The symbols of "CA" and "RA" are deleted (see 3.1 of ISO /IEC 11770-1.2010);

---Chapter 5 clarifies that "cryptographic algorithms recognized by the national cryptographic management department should be used", and ISO /IEC 11770-1.2010

The referenced cryptographic algorithm standards are modified to quote the corresponding cryptographic algorithm standards of our country for ease of use (see Chapter 5).

This section also made the following editorial changes.

---Delete the informative appendix D of ISO /IEC 11770-1.2010, and the relevant content is consistent with the existing national standards and cryptographic industry standards.

Please note that certain contents of this document may involve patents. The issuing agency of this document is not responsible for identifying these patents.

This part is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260).

Drafting organizations of this section. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd., National Engineering Laboratory of Wireless Network Security Technology,

Zhongguancun Wireless Network Security Industry Alliance, Commercial Password Testing Center of National Cryptography Administration, Peking University Shenzhen Graduate School, China Electronics

The 30th Research Institute of Science and Technology Group Corporation, National Radio Monitoring Center Testing Center, China Electronic Technology Standardization Institute, China General Technology

Technology Research Institute, China Network Security Review Technology and Certification Center, Tianjin Radio Monitoring Station, Beijing Institute of Computer Technology and Application,

Tianjin Electronic and Mechanical Products Testing Center, Chongqing University of Posts and Telecommunications.

Introduction

In information technology, the need to use password mechanisms to protect data from illegal theft or tampering, to achieve entity identification and non-repudiation is increasing.

increase. The security and reliability of these mechanisms directly depend on the management and protection of keys. If there are weak links in key management, then

It invalidates all the cryptographic functions it claims, so safe management of keys is essential for integrating cryptographic functions into the system. Key management

The purpose is to provide key processing procedures used in symmetric or asymmetric cryptographic mechanisms.

This part of the revision adopts ISO /IEC 11770-1.2010 "Information Technology Security Technology Key Management Part 1.Framework", suitable

Used for the management of communication keys. ISO /IEC 11770 defines a general model of key management, which does not depend on the specific cryptographic algorithm used.

But some key distribution mechanisms depend on the characteristics of specific algorithms, such as asymmetric algorithm characteristics.

If the non-repudiation function is needed in key management, see GB/T 17903.

This section describes both automatic and manual key management methods, including the data element framework and the operations used to obtain key management services.

Work process, but does not elaborate on the details required for protocol exchange.

Like other security services, key management only provides key management services in the defined security policy, but the definition of security policy exceeds

Out of the scope of this section.

The fundamental problem of key management is to confirm the key material by all parties involved, and ensure its source, integrity, and immediacy to direct and indirect users

And (in the case of secret keys) confidentiality. Key management includes generating, storing, distributing, deleting and archiving keys according to a certain security policy

(GB/T 9387.2-1995) and other functions.

Information technology security technology key management

Part 1.Frame

1 Scope

This part of GB/T 17901 contains the following.

a) Establish a general model of key management mechanism;