

ICS 03.060
CCS A 11



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

GB/T 27911-2011

**Banking -- Security and other financial services -- Framework
for security in financial systems**

银行业 安全和其他金融服务 金融系统的安全框架

(English Translation)

Issued on: December 30, 2011

Implemented on: February 1, 2012

Issued by: Standardization Administration of China

Table of Contents

Introduction
1 Scope
2 Standardized field
2.1 Overview
2.2 Identification and authentication
2.3 Data Integrity
2.4 Privacy and confidentiality
2.5 Non-repudiation
Service availability 2.6
2.7 Traceability and Audit
2.8 Interoperability
2.9 Security Management
2.10 Encryption Algorithm
3 ISO standardization blank
Appendix A (informative) Supplementary Information
Reference

Foreword

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

This standard uses redrafted law revision using ISO/T R17944.2002 "Banking and other financial services secure financial system Security framework. " Taking into account China's national conditions, and taking into account released some new information related to safety class international financial standards since 2002, Using ISO/T R17944.2002 doing the following modifications.

--- 2.2 in Table 1, in the "biometric identification technology," adding a number of new international standards in recent years published;

--- 2.3 Table 2, in the "message authentication" added the ISO/IEC 19772:2009;

--- 2.6 in Table 5, in the "Disaster Recovery" added the ISO/IEC 24762:2008;

--- 2.7 Table 6, in the "evaluation criteria" to add the ISO/IEC 18045:2008, ISO/IEC TR19791:2006, ISO/IEC 21827:2008;

--- 2.9 in Table 8, in the "Certificate management", added ISO 21188;

--- 2.9 in Table 8, "Security Management" to add ISO/IEC TR18044, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 18043:2006, ISO/IEC 27000:2009, ISO/IEC 27005:2008, ISO/IEC 27006:2007, ISO/IEC 27011:2008;

--- 2.10 in Table 9, in the "general" added the ISO/IEC 18031:2005, ISO/IEC 18032:2005, ISO/IEC 18033-1:2005, ISO/IEC 18033-2:2006, ISO/IEC 18033-3:2005, ISO/IEC 18033-4:2005, ISO/IEC 19790:2006;

--- 2.10 Table 9 in the "symmetrical" added the ISO 19038;

Chapter 3 10 --- table delete biometrics, two-line disaster recovery, because in the text added to the ISO standard in both areas, Also added three lines. "Privacy and confidentiality", "business entity identifier identities", "token";

--- Each table, the referenced standard's number, if the updated version, replace it with the latest standard's number;

--- The tables, delete defunct international standards.

For ease of use, this standard also made the following editorial changes.

--- Delete ISO foreword and introduction;

--- For the standard has been released, remove the original table in note "forthcoming." the standard proposed by the People's Bank of China.

This standard by the National Standardization Technical Committee on Finance (SAC/TC180) centralized.

1 Scope

This standard provides a standard framework for the financial sector necessary for security.

This standard summarizes some of the key security problems in the financial sector have emerged, as well as the relevant existing standards for each question.

This standard applies to financial institutions in the implementation of standard security policies by reference.

2.1 Overview

The financial sector, IT security requirements embodied in a token device, encryption, key management, application program interface (API) and Standard applications protocols, etc. These different areas can be grouped according to the following basic business needs of these basic areas.

Most areas have a wide variety of available standard, while in other areas, standards or are developing or have a (new) standard requirements.

Chapter 2 of the financial institutions mentioned in the main areas of information security standardization, which in Table 1 to Table 9 includes those available in the art (sometimes Required) standards. Table top surface with international standards from the International Organization for Standardization, followed in subsequent relevant standards from other standards Organization 1). Based on these tables lack of standards, Chapter 3 provides an overview of ISO standardization in the field blank.

1) The Central African Standard ISO standard reference for information purposes only; they should be a consensus and should be published or accepted available. Non-ISO ISO standard reference does not indicate an endorsement of these non-ISO standards.

Note: For more detailed information on the mentioned criteria, you can contact the reference standards organizations (see Appendix A).

2.2 Identification and authentication

The identity of all entities involved in financial transactions should be OK. Identification ensure the identity of the identity of an entity is its declaration. financial Agencies shall ensure that. only authorized users can access their information technology systems.

Identification and authentication mechanisms in use for establishing identity, token, password phrases, personal identification number (PIN), biometric Do technology, digital signatures and certificates on the basis of the relevant criteria in Table 1.

Table 1 identification and authentication

Demand available standard title/description Identification and authentication ISO/IEC 9798-1 Identification Information technology - Security techniques - Entity Part 1. Overview ISO/IEC 9798-2 Information technology - Security techniques - Entity Identification - Part 2. Symmetric plus Mechanism secret algorithm ISO/IEC 9798-3 Information technology - Security techniques - Entity Identification - Part 3. Digital Signature Mechanism of technicians ISO/IEC 9798-4 Information technology - Security techniques - Entity Identification Part 4. The password school Mechanisms function test ISO/IEC 9798-5 Information technology - Security techniques - Entity Identification Part 5. Using zero-knowledge Mechanism of Technology ISO/IEC 9594-8 Information technology - OSI Directory - Part 8. a public key and attribute Certificate frameworks