

ICS 35.100.01
CCS L 79



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

GB/T 18794.4-2003

**Information technology -- Open Systems Interconnection --
Security frameworks for open systems -- Part 4:
Non-repudiation framework**

信息技术 开放系统互连 开放系统安全框架 第4部分：抗抵赖框架
(English Translation)

Issued on: November 24, 2003

Implemented on: August 1, 2004

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People Republic of China**

Table of Contents

What this standard covers	1
Document data	2

What this standard covers

This standard discusses in an open system environment security service application, where the term "open system " includes such as databases, distributed applications, Open Distributed Processing and OSI so some areas. Security Framework relates define objects within the system and the system to provide protection methods, and interaction between systems. The security framework or mechanism does not involve building systems methodology. Data elements and security framework discusses the sequence of operations (rather than the protocol elements), both of which can be used to obtain specific security services. These security services can be applied to the system is communicating entities, the data exchanged between systems, and system management data. This standard: Defining the basic concepts of non-repudiation, defines general repudiation services, provide non-repudiation services to determine possible mechanisms, repudiation services and mechanisms to determine a common management needs. And other security services, non-repudiation services can only be provided for specific applications provided within the security policy. Definition of security policy is not within the scope of this standard. This standard does not include realized repudiation protocol exchanges need to complete the details of instructions. This standard does not describe in detail the text can be used to support specific mechanisms Hang -repudiation services, nor are given in support of security management services and details of the agreement. In this framework, certain procedures described in technology through the application password security. While some types of non-repudiation mechanism may be related to specific properties of the algorithm, but the frame does not depend on a specific cryptographic algorithm, or other algorithms are used, does not depend on specific (such as a symmetric or asymmetric) encryption technology.

Document data

International classification (ICS): 35.100.01.

Chinese classification (CCS): L79.

Estimated length of the Chinese original: 22,225 words.

Adopted international standard: ISO/IEC 10184-4-1997, IDT.