ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17901.1—1999
idt ISO/IEC 11770-1:1996

信息技术　安全技术　密钥管理
第1部分:框架

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

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局　发布

目　　次

前　　言

本标准等同采用国际标准 ISO/IEC 11770-1:1996《信息技术　安全技术　密钥管理　第 1 部分:框架》。

本系列标准规定了密钥管理框架,适合于我国使用。

GB/T 17901 在总标题《信息技术　安全技术　密钥管理》下,包含以下几个部分:

——第 1 部分:框架

——第 2 部分:采用对称技术的机制

——第 3 部分:采用非对称技术的机制

本标准的附录 A、附录 B、附录 C、附录 D 和附录 E 都是提示的附录。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位:电子工业部第三十研究所。

本标准主要起草人:雷利民、龚奇敏、方姝妹、鲍振东、吴娅若、杜明钰。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了世界范围内的标准化专门体系。ISO或IEC的成员国,通过由处理特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准的开发。ISO和IEC的技术委员会在共同感兴趣的领域内合作,其他与ISO和IEC有联络的官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO和IEC已建立了一个联合技术委员会ISO/IEC JTC1。被联合技术委员会接受的国际标准草案送给各成员国表决。一个国际标准的发布,需要至少75%的成员国投赞成票。

国际标准ISO/IEC 11770-1是由信息技术联合技术委员会ISO/IEC JTC1的IT安全技术SC 27分委员会制定的。

ISO/IEC 11770的总标题《信息技术　安全技术　密钥管理》下,包含以下部分:

——第1部分:框架

——第2部分:采用对称技术的机制

——第3部分:采用非对称技术的机制

可能有后续部分。

附录A、附录B、附录C、附录D和附录E只作为参考。

引　　言

在信息技术中，采用密码机制保护数据不被非授权地泄露或窜改、实现实体鉴别和抗抵赖功能的需求与日俱增。这些机制的安全性和可靠性直接取决于对密钥这一安全参数的管理和保护。如果密钥管理有薄弱环节，那么即使是最完善的安全概念都将不起作用，因此安全地管理这些密钥对于将密码功能集成到系统中去是至关重要的。密钥管理的目的是提供对用于对称或非对称密码机制中的密码密钥材料的处理程序。

根本问题是要确定密钥材料，向直接和间接用户保证其来源、完整性、即时性和(秘密密钥情形下的)保密性。密钥管理包括根据某一安全策略产生、存储、分发、删除和归档密钥材料(GB/T 9387.2—1995)等功能。

本标准与开放系统安全框架(ISO/IEC 10181)有着特殊的关系。所有这些框架，包括本框架，确定涵盖安全各个方面的机制的基本概念和特性。本标准介绍作为对称和非对称密码机制基础的密钥管理的一般模型。

中华人民共和国国家标准

信息技术　安全技术　密钥管理
第1部分:框架

GB/T 17901.1—1999
idt ISO/IEC 11770-1:1996

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

1　范围

本标准:

1）确定密钥管理的目标;

2）描述作为密钥管理机制基础的一般模型;

3）定义对GB/T 17901所有部分通用的密钥管理基本概念;

4）定义密钥管理服务;

5）确定密钥管理机制的特性;

6）规定对密钥材料在其生存期内进行管理的需求;

7）描述对密钥材料在其生存期内进行管理的框架。

本框架定义了与任何特定密码算法的使用无关的密钥管理一般模型,但是某些密钥分发机制可能与特定的算法特性(如非对称算法的特性)有关。

具体的密钥管理机制在本系列标准的其他部分阐述。其中,第2部分阐述对称体制,第3部分阐述非对称体制。本标准的内容是理解第2和第3部分的基础。ISO 8732和ISO 11166中有使用密钥管理机制的范例。如果密钥管理需要抗抵赖功能,应采用GB/T 17903。

本标准对密钥的自动与人工管理都进行了阐述,包括用来获得密钥管理服务的数据元素和操作顺序的概貌,但对可能需要的协议交换的细节未作规定。

和其他安全服务一样,只有在已定义的安全策略中才能提供密钥管理服务。安全策略的定义超出了GB/T 17901的范围。

2　引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB 15843.1—1995　信息技术　安全技术　实体鉴别机制　第1部分:一般模型(idt ISO/IEC 9798-1:1991)

ISO/IEC 10181-1:1996　信息技术　开放系统互连　开放系统的安全框架:概述

国家质量技术监督局1999-11-11批准　　2000-05-01实施