ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17903.2—1999
idt ISO/IEC 13888-2:1998

信息技术　安全技术　抗抵赖
第2部分:使用对称技术的机制

Information technology—Security techniques—Non-repudiation—Part 2:Mechanisms using symmetric techniques

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局 发布

前　　言

本标准等同采用国际标准 ISO/IEC 13888-2:1998《信息技术　安全技术　抗抵赖　第 2 部分:使用对称技术的机制》。

GB/T 17903 在总标题《信息技术　安全技术　抗抵赖》下,目前由以下几部分组成:

——第 1 部分:概述

——第 2 部分:使用对称技术的机制

——第 3 部分:使用非对称技术的机制

本标准的附录 A 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。

本标准由航天工业总公司二院 706 所负责起草。

本标准主要起草人:王轶昆、谢小权。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方的或非官方的国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决,发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 13888-1 由联合技术委员会 ISO/IEC JTC1(信息技术)分技术委员会 SC27(IT 安全技术)提出。

ISO/IEC 13888 在总标题《信息技术　安全技术　抗抵赖》下由以下几部分组成:

——第 1 部分:概述

——第 2 部分:使用对称技术的机制

——第 3 部分:使用非对称技术的机制

本标准的附录 A 是提示的附录。

中华人民共和国国家标准

信息技术　安全技术　抗抵赖　第2部分：使用对称技术的机制

GB/T 17903.2—1999
idt ISO/IEC 13888-2:1998

Information technology—Security techniques—Non-repudiation—Part 2:Mechanisms using symmetric techniques

1　范围

抗抵赖服务旨在生成、收集、维护已声明的事件或动作的证据，并使该证据可得并且确认该证据，以此来解决关于某事件或动作发生或未发生而引起的争议。本标准描述了可用于抗抵赖服务的通用结构，以及能用来提供原发抗抵赖(NRO)、交付抗抵赖(NRD)、提交抗抵赖(NRS)和传输抗抵赖(NRT)等有关的特殊通信机制。其他抗抵赖服务可用第8章所描述的通用结构组成，以满足安全策略的要求。

本标准利用可信第三方防止抵赖的发生。一般需要在线的可信第三方。

抗抵赖机制提供专用于每一个抗抵赖服务的抗抵赖权标的交换协议。抗抵赖权标由安全信封和附加数据组成。抗抵赖权标应作为抗抵赖信息予以存储，以后发生争议时使用。

按照特殊应用下所使用抗抵赖策略以及该应用所处的合法环境，抗抵赖信息可能包括以下附加信息：

a) 包括一个由时间标记机构所生成的可信时间标记的证据；

b) 公证人提供的证据，为一个或多个实体执行的动作或事件提供保证。

抗抵赖一词只能在特定的应用及其合法环境所清晰定义的安全策略中才可以有效。

2　引用标准

下列标准所包括的条文，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 15852—1995　信息技术　安全技术　用块密码算法作密码校验函数的数据完整性机制(idt ISO/IEC 9797:1994)

GB/T 15843.1—1999　信息技术　安全技术　实体鉴别　第1部分：概述(idt ISO/IEC 9798-1:1997)

GB/T 17903—1999　信息技术　安全技术　抗抵赖　第1部分：概述(idt ISO/IEC 13888-1:1997)

ISO/IEC 10118-1:1994　信息技术　安全技术　散列函数　第1部分：概述

ISO/IEC 10181-4:1996　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

3　定义

GB/T 17903.1中的定义适用于本标准。

国家质量技术监督局1999-11-11批准　　2000-05-01实施