ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17903.1—2008/ISO/IEC 13888-1:2004
代替 GB/T 17903.1—1999

信息技术　安全技术　抗抵赖
第1部分:概述

Information technology—Security techniques—Non-repudiation—Part 1:General

(ISO/IEC 13888-1:2004,IDT)

2008-06-26 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 17903 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：采用对称技术的机制；

——第 3 部分：采用非对称技术的机制。

本部分是 GB/T 17903 的第 1 部分，等同采用 ISO/IEC 13888-1:2004《信息技术　安全技术　抗抵赖　第 1 部分：概述》，仅有编辑性修改。

本部分代替 GB/T 17903.1—1999《信息技术　安全技术　抗抵赖　第 1 部分：概述》。本部分与 GB 17903.1—1999 相比，主要差别如下：

——本部分修订了第 3 章中的部分术语和定义。

——本部分对部分叙述进行了文字修订，并把第 11 章中的“NRDT”修正为“NROT”。

——本部分对第 5 章和第 6 章的顺序进行了调整。

——本部分删除了原附录 A。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分主要起草单位：中国科学院软件研究所 信息安全国家重点实验室。

本部分主要起草人：张振峰、冯登国。

本部分所代替标准的历次版本发布情况为：

——GB/T 17903.1—1999。

引　言

本部分对应的国际标准 ISO/IEC 13888-1:2004 是由联合技术委员会 ISO/IEC JTC1(信息技术)分技术委员会 SC 27(IT 安全技术)提出的。

第二版(ISO/IEC 13888-1:2004)撤销并替代了第一版(ISO/IEC 13888-1:1997),并在技术上进行了修改。

抗抵赖服务旨在生成、收集、维护、利用和验证有关已声称的事件或动作的证据,以解决关于此事件或动作的已发生或未发生的争议。本部分描述了抗抵赖机制的一种模型,所提供的证据是基于由对称密码或非对称密码技术而生成的密码校验值。首先描述各种抗抵赖服务通用的抗抵赖机制,然后将这一抗抵赖机制应用于一系列特定的抗抵赖服务,诸如:

——原发抗抵赖;

——交付抗抵赖;

——提交抗抵赖;

——传输抗抵赖。

抗抵赖服务生成证据,证据则用于确定某事件或动作的责任。就产生证据所针对的动作或事件而言,对该动作负责或与该事件相关的实体,称为证据主体。主要有两类证据,从本质上讲他们依赖于所使用的密码技术:

——安全信封,由证据生成机构使用对称密码技术生成;

——数字签名,由证据生成者或证据生成机构使用非对称密码技术生成。

抗抵赖机制提供的协议用于交换各种抗抵赖服务所规定的抗抵赖权标。抗抵赖权标由安全信封和(或)数字签名以及可选的附加数据组成。抗抵赖权标可作为抗抵赖信息予以存储,这些信息以后可以由争议双方或者仲裁者在仲裁争议时使用。

依据特定应用下所使用的抗抵赖策略以及该应用操作所处的法律环境,抗抵赖信息可能需要包括以下附加信息:

——包括时间戳机构提供的可信时间戳在内的证据;

——公证人提供的证据,以确保数据、行为或事件是由一个或多个实体所生成、执行或参与的。

抗抵赖只能在特定应用及其法律环境下、有明确定义的安全策略的范围内才可生效。

信息技术　安全技术　抗抵赖
第1部分:概述

1　范围

本部分可作为其他几部分中规定的使用密码技术的抗抵赖机制的一般模型。GB/T 17903提供的抗抵赖机制可用于如下阶段的抗抵赖:

a)　证据生成;

b)　证据传输、存储和检索;

c)　证据验证。

争议仲裁不在本标准的范围之内。

2　规范性引用文件

下列文件中的条款通过GB/T 17903的本部分的引用而成为本部分的条款。凡是注明日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB 15851—1995　信息技术　安全技术　带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

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/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 17902(所有部分)　信息技术　安全技术　带附录的数字签名(idt ISO/IEC 14888)

GB/T 18238(所有部分)　信息技术　安全技术　散列函数(idt ISO/IEC 10118)

GB/T 18794.1—2002　信息技术　开放系统互连　开放系统安全框架　第1部分:概述(idt ISO/IEC 10181-1:1996)

GB/T 18794.4—2003　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(ISO/IEC 10181-4:1997,IDT)

GB/T 17903.2—2008　信息技术　安全技术　抗抵赖　第2部分:采用对称技术的机制(ISO/IEC 13888-2:1998,IDT)

GB/T 17903.3—2008　信息技术　安全技术　抗抵赖　第3部分:采用非对称技术的机制(ISO/IEC 13888-3:1997,IDT)

ISO/IEC 9594-8:2001　信息处理系统　开放系统互连　目录　第8部分:鉴别框架

ISO/IEC 9797(所有部分)　信息技术　安全技术　消息鉴别码

ISO/IEC 11770-3:1999　信息技术　安全技术　密钥管理　第3部分:使用非对称技术的机制

ISO/IEC 18014　信息技术　安全技术　时间戳服务

3　术语和定义

3.1　GB/T 9387.2—1995中的定义

3.1.1

可核查性　accountability

确保一个实体的行为可唯一地追踪到该实体的性质。