ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17903.2—2008/ISO/IEC 13888-2:1998
代替 GB/T 17903.2—1999

信息技术　安全技术　抗抵赖
第2部分:采用对称技术的机制

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

(ISO/IEC 13888-2:1998,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 2 部分，等同采用 ISO/IEC 13888-2:1998《信息技术　安全技术　抗抵赖　第 2 部分：采用对称技术的机制》，仅有编辑性修改。ISO/IEC 13888-2:1998 是由联合技术委员会 ISO/IEC JTC 1(信息技术)分技术委员会 SC 27(IT 安全技术)提出的。

本部分代替 GB/T 17903.2—1999《信息技术　安全技术　抗抵赖　第 2 部分：采用对称技术的机制》。本部分与 GB/T 17903.2—1999 相比，主要差异如下：

——本部分根据第 1 部分的修订，更改部分术语。

——本部分对部分叙述进行了文字修订，并修正了第 10 章中的“NORT”。

本部分的附录 A 是资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分主要起草人：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 17903.2—1999。

信息技术　安全技术　抗抵赖
第2部分:采用对称技术的机制

1　范围

抗抵赖服务旨在生成、收集、维护、利用和验证有关已声称事件或动作的证据,以解决有关该事件或动作已发生或未发生的争议。本部分描述了用于抗抵赖服务的通用结构,以及一些特定的、与通信有关的机制,用于提供原发抗抵赖(NRO)、交付抗抵赖(NRD)、提交抗抵赖(NRS)和传输抗抵赖(NRT)等。其他抗抵赖服务可用第8章描述的通用结构来构建,以满足安全策略的要求。

本部分依赖于可信第三方来防止欺诈性的抵赖。一般需要在线的可信第三方。

抗抵赖机制提供的协议用于交换各种抗抵赖服务规定的抗抵赖权标。本部分中使用的抗抵赖权标由安全信封和附加数据组成。抗抵赖权标作为抗抵赖信息予以存储,以备之后发生争议时使用。

依据特定应用的有效抗抵赖策略以及该应用操作所处的法律环境,抗抵赖信息可能包括以下附加信息:

a)　包括时间戳机构提供的可信时间戳在内的证据;

b)　公证人提供的证据,以确保动作或事件是由一个或多个实体执行或参与的。

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。

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 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 15843.4—1999　信息技术　安全技术　实体鉴别　第4部分:采用密码校验函数的机制(idt ISO/IEC 9798-4:1997)

GB/T 18238.1—2000　信息技术　安全技术　散列函数　第1部分:概述(idt ISO/IEC 10118-1:1994)

GB/T 17903.1—2008　信息技术　安全技术　抗抵赖　第1部分:概述(ISO/IEC 13888-1:2004,IDT)

3　术语和定义

GB/T 17903.1—2008中的术语和定义适用于本部分。

4　记法和缩略语

4.1　记法

4.1.1　GB/T 17903.1—2008中的记法

$Imp(y)$	数据串y的印迹,或者是数据串y的散列码,或者是数据串y
$SENV_X$	使用实体X的秘密密钥x生成的安全信封