ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17903.1—1999
idt ISO/IEC 13888-1:1997

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

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 13888-1:1997《信息技术　安全技术　抗抵赖　第 1 部分:概述》。

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第二研究院 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订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订工作。

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1部分：概述

GB/T 17903.1—1999
idt ISO/IEC 13888-1:1997

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

1　范围

抗抵赖服务旨在生成、收集、维护有关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，以此来解决关于此事件或动作发生或未发生而引起的争议。本标准描述了基于密码技术提供证据的抗抵赖机制的一种模型，并且描述了如何使用对称或非对称密码技术生成密码校验值并以此形成证据。首先描述的是通用于不同抗抵赖服务的抗抵赖机制，然后将这些抗抵赖机制应用于一系列的特殊抗抵赖服务，诸如：

a）原发抗抵赖；

b）交付抗抵赖；

c）提交抗抵赖；

d）传输抗抵赖。

抗抵赖服务生成证据，证据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，从本质上讲他们都依赖于所使用的密码技术：

a）安全信封(SENV)，由证据生成机构使用对称密码技术形成；

b）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形成。

抗抵赖机制提供交换专用于每一个抗抵赖服务的抗抵赖权标的协议。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评判者在仲裁争议时使用。

按照特殊应用下所使用的抗抵赖策略以及该应用所处的合法的应用环境，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提供的可信时间标记的证据；

b）公证人提供的证据，该证据可以为一个或多个实体所生成的数据。动作或事件提供可确认性。

抗抵赖只能在某特殊应用及其合法环境所清晰定义的安全策略范围内提供。

本标准可作为其他几部分中，规定使用密码技术的抗抵赖机制时的一般模型。GB/T 17903 为以下抗抵赖阶段提供抗抵赖机制：

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 GB/T 17903 范围。

国家质量技术监督局 1999-11-11 批准　　2000-05-01 实施