ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.4—2003/ISO/IEC 10181-4:1997

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

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 4:Non-repudiation framework

(ISO/IEC 10181-4:1997,Information technology—Open Systems Interconnection—Security frameworks for open systems:Non-repudiation framework,IDT)

2003-11-24 发布　　2004-08-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

GB/T 18794《信息技术　开放系统互连　开放系统安全框架》目前包括以下几个部分：

——第 1 部分(即 GB/T 18794.1)：概述

——第 2 部分(即 GB/T 18794.2)：鉴别框架

——第 3 部分(即 GB/T 18794.3)：访问控制框架

——第 4 部分(即 GB/T 18794.4)：抗抵赖框架

——第 5 部分(即 GB/T 18794.5)：机密性框架

——第 6 部分(即 GB/T 18794.6)：完整性框架

——第 7 部分(即 GB/T 18794.7)：安全审计和报警框架

本部分为 GB/T 18794 的第 4 部分，等同采用国际标准 ISO/IEC 10181-4:1997《信息技术 开放系统互连 开放系统安全框架：抗抵赖框架》(英文版)。

按照 GB/T 1.1—2000 的规定，对 ISO/IEC 10181-4 作了下列编辑性修改：

a) 增加了我国的“前言”；

b) “本标准”一词改为“GB/T 18794 的本部分”或“本部分”；

c) 对“规范性引用文件”一章的导语按 GB/T 1.1—2000 的要求进行了修改；

d) 在引用的标准中，凡已制定了我国标准的各项标准，均用我国的相应标准编号代替。对“规范性引用文件”一章中的标准，按照 GB/T 1.1—2000 的规定重新进行了排序。

本部分的附录 A 至附录 F 都是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所归口。

本部分起草单位：四川大学信息安全研究所。

本部分主要起草人：方勇、罗万伯、罗建中、周安民、龚海澎、戴宗坤、欧晓聪、李焕洲。

引　言

抗抵赖服务的目标是为解决有关事件或动作发生与否的纠纷而收集、维护、提供和证实被声称事件或动作的不可反驳的证据。抗抵赖服务能应用于很多不同的上下文和情况。此服务能用于数据生成、数据存储或数据传输。抗抵赖包括生成能用来证明某类事件或动作已发生的证据，以便日后这个事件或动作不能被抵赖。

在OSI环境下(见GB/T 9387.2)，抗抵赖服务有两种形式：

——具有源证明的抗抵赖，用于对付发送方虚假地否认已发送过数据或其内容。

——具有递交证明的抗抵赖，用于对付接受者虚假地否认已接收过数据或其内容(即数据所代表的信息)。

使用OSI协议的应用可能需要其他针对特定应用类别的抗抵赖服务。例如，MHS(GB/T 16284.2)定义提交服务的抗抵赖，而EDI消息处理系统(见GB/T 16651)定义检索的抗抵赖和传送服务的抗抵赖。

本框架中的概念不局限于OSI通信，而可更广泛地解释为包括今后使用的数据创建和存储之类。

本部分为提供抗抵赖服务定义通用性框架。

本框架：

——扩展GB/T 9387.2中描述的抗抵赖服务的概念，以及描述可以怎样将它们应用于开放系统；

——描述提供这些服务的可选择的方法；

——阐明这些服务与其他安全服务的关系。

抗抵赖服务可能需要：

——判决者，他将对由于抵赖事件或动作而可能出现的纠纷做出裁决；

——可信第三方，他将确保用于证据验证的数据的真实性和完整性。

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

1　范围

本开放系统安全框架的标准论述在开放系统环境中安全服务的应用,此处术语"开放系统"包括诸如数据库、分布式应用、开放分布式处理和开放系统互连这样一些领域。安全框架涉及定义对系统和系统内的对象提供保护的方法,以及系统间的交互。本安全框架不涉及构建系统或机制的方法学。

安全框架论述数据元素和操作的序列(而不是协议元素),这两者可被用来获得特定的安全服务。这些安全服务可应用于系统正在通信的实体,系统间交换的数据,以及系统管理的数据。

本部分:

——定义抗抵赖的基本概念;

——定义通用的抗抵赖服务;

——确定提供抗抵赖服务的可能的机制;

——确定抗抵赖服务和机制的通用管理需求。

和其他安全服务一样,抗抵赖服务只能在为特定应用而规定的安全策略范围内提供。安全策略的定义则不在本部分范围内。

本部分不包括实现抗抵赖所需要完成的协议交换的细节说明。

本部分不详细描述可用于支持抗抵赖服务的特定机制,也不给出所支持的安全管理服务和协议的细节。

在本框架中描述的某些规程通过应用密码技术实现安全。尽管某些种类的抗抵赖机制可能与特定的算法特性有关,但本框架不依赖于特定密码算法或其他算法的使用,也不依赖于特定的(如对称或非对称)密码技术。实际上,的确可能会要使用大量不同的算法。两个希望使用密码保护数据的实体必须支持同一种密码算法。

注:密码算法及其登记规程应符合我国有关规定。

很多不同类型的标准能使用此框架,包括:

1)　体现抗抵赖概念的标准;

2)　规定抽象服务、而这些服务含有抗抵赖的标准;

3)　规定使用抗抵赖服务的标准;

4)　规定在开放系统体系结构内提供抗抵赖方法的标准;

5)　规定抗抵赖机制的标准。

这些标准可按下述方式使用本框架:

——标准类型1)、2)、3)、4)或5)能使用本框架的术语;

——标准类型2)、3)、4)或5)能使用第7章定义的设施;

——标准类型5)能基于第8章定义的机制类。

2　规范性引用文件

下述文件中的条款通过GB/T 18794的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修改版均不适用于本部分,然而,鼓励根据本部分达成