中国标准出版社第四编辑室　编

信息安全标准汇编

技术与机制卷

授权与访问控制分册

中国标准出版社

信息安全标准汇编

技术与机制卷

授权与访问控制分册

中国标准出版社第四编辑室　编

中国标准出版社
北京

图书在版编目（CIP）数据

信息安全标准汇编．技术与机制卷．授权与访问控制分册/中国标准出版社第四编辑室编．—北京：中国标准出版社，2009

ISBN 978-7-5066-5110-3

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统-安全管理-国家标准-汇编-中国 Ⅳ.TP309-65

中国版本图书馆 CIP 数据核字（2008）第 199545 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045

网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 23 字数 700 千字
2009 年 1 月第一版 2009 年 1 月第一次印刷

*

定价 120.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中基础卷、信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本册为技术与机制卷的授权与访问控制分册，共收入截至2008年11月发布的相关标准11项。

编　　者

2008年11月

目　　录

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

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。

3.1.2

数据完整性 data integrity

这一性质表明数据没有遭到非授权的篡改或破坏。

3.1.3

数据源鉴别 data origin authentication

确认接收到的数据的来源与其声明的一致。

3.1.4

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用于确认数据单元的来源和完整性，并保护数据防止被人(例如接收者)伪造。

3.1.5

安全策略 security policy

为提供安全服务而制定的一套准则。

3.2 **ISO/IEC 9594-8:2001 中的定义**

3.2.1

认证机构 certification authority

受一个或多个用户信任的职能机构，负责创建和分发证书。认证机构也可创建用户密钥。

3.3 **ISO/IEC 9797 中的定义**

3.3.1

消息鉴别码(MAC) message authentication code

MAC 算法输出的比特串。

注：MAC 有时也称作密码校验值(比如 GB/T 9387.2)。

3.4 **GB/T 18238 中的定义**

3.4.1

散列码 hash-code

散列函数输出的比特串。

3.4.2

散列函数 hash-function

将比特串映射成固定长度比特串的函数，它具有以下两个性质：

a) 对一个给定的输出，要找到可映射到该输出的一个输入，在计算上不可行；

b) 对一个给定的输入，要找到可映射到其输出的第二个输入，在计算上不可行。

3.5 **GB/T 18794.1—2002 中的定义**

3.5.1

安全机构 security authority

负责定义或者执行安全策略的实体。

3.5.2

安全证书 security certificate

由某一安全机构或可信第三方颁发的，其中带有用于提供完整性和数据源鉴别的安全信息数据集。

3.5.3

安全权标 security token

一种与安全有关的数据集合，受到完整性和数据源鉴别的保护，以防其来源于非安全机构。

3.5.4

信任 trust

两个元素之间的一种关系，在一组活动和一个安全策略中，元素 x 信任元素 y 当且仅当元素 x 确信

元素 y 会以不违背安全策略的既定方式(相对于该活动)进行运行。

3.6 GB/T 18794.4—2003 中的定义

3.6.1

证据生成者 evidence generator

生成抗抵赖证据的实体。

3.6.2

证据用户 evidence user

使用抗抵赖证据的实体。

3.6.3

证据验证者 evidence verifier

验证抗抵赖证据的实体。

3.6.4

抗抵赖服务请求者 non-repudiation service requester

要求为某特定事件或动作生成抗抵赖证据的实体。

3.7 ISO/IEC 11770-3:1999 中的定义

3.7.1

密钥 key

用于控制密码变换操作(例如加密、解密、密码校验函数计算、签名生成或签名验证)的符号序列。

3.7.2

私有密钥/私钥 private key

在实体的非对称密钥对中,只应由该实体使用的密钥。

注:在非对称签名机制中,私钥定义签名变换。在非对称加密体制中,私钥定义解密变换。

3.7.3

公开密钥/公钥 public key

在实体的非对称密钥对中,可以公开的密钥。

注:在非对称签名机制中,公开密钥定义了验证变换。在非对称加密系统中,公开密钥定义了加密变换。一个可以"公开获知"的密钥并非任何人都可获得,可能只有事先指定的群体中的所有成员可以得到公开密钥。

3.7.4

公钥证书 public key certificate

实体的公开密钥信息,由证书权威机构签发从而确保是不可伪造的。

3.7.5

秘密密钥 secret key

一种密钥,用于对称密码技术,只能由一组规定的实体使用。

3.8 ISO/IEC 18014 中的定义

3.8.1

时间戳 time-stamp

时间变量参数,表示与通用时间参考相关的一个时间点。

3.8.2

时间戳机构 time stamping authority

能够可信地提供时间戳服务的可信第三方。

3.9 本标准中有关抗抵赖的专用定义

下列定义适用于本标准。

3.9.1

证书 certificate

关于实体的一种数据，由认证机构的私有密钥或秘密密钥签发，确保其不可伪造性。

3.9.2

交付机构 delivery authority

发送者所信任的机构，把发送者的数据交付给接收者，并且根据发送者的要求向发送者提供提交和传输数据的证据。

3.9.3

数据存储区 data storage

存储数据的一种方式，数据可以由此提交递送，交付机构也可以往该区域放置数据。

3.9.4

可区分标识符 distinguishing identifier

在抗抵赖过程中可以无歧义地识别一个实体的信息。

3.9.5

证据 evidence

用来证明一个事件或动作的信息，可单独使用或与其他信息一起使用。

注：证据本身未必证明了某事件的真实性或存在性，但它可用于提供证明。

3.9.6

证据请求者 evidence requester

请求另一个实体或可信第三方生成证据的实体。

3.9.7

证据主体 evidence subject

对某个动作负责或者与某事件相关的实体，证据即是针对该动作或事件而产生的。

3.9.8

印迹 imprint

一种比特串，或者是数据串的散列码，或者是该数据串本身。

3.9.9

监控者(监控机构) monitor (monitor authority)

对动作或事件进行监控，并可信赖地对其所监控内容提供证据的可信第三方。

3.9.10

抗抵赖策略 non-repudiation policy

一组提供抗抵赖服务的准则，确切的说，用于生成和验证证据以及用于仲裁的一组规则。

3.9.11

抗抵赖信息 non-repudiation information

一组信息，包括证据的生成和验证所涉及的事件或动作的信息、证据本身以及有效的抗抵赖策略。

3.9.12

抗抵赖交换 non-repudiation exchange

以抗抵赖为目的、一次或多次传送抗抵赖信息(NRI)所组成序列。

3.9.13

创建抗抵赖 non-repudiation of creation

防止一个实体否认其已经创建的消息(即对消息内容负责)的服务。

3.9.14

交付抗抵赖 non-repudiation of delivery

防止接收者否认已经接收过消息并且认可消息内容的服务。

3.9.15

认知抗抵赖 non-repudiation of knowledge

防止接收者否认其已经注意到所接收消息的内容的服务。

3.9.16

原发抗抵赖 non-repudiation of origin

防止消息的原发者否认其创建了消息的内容并且已经发送了该消息的服务。

3.9.17

接收抗抵赖 non-repudiation of receipt

防止接收者否认其已经接收了消息的服务。

3.9.18

发送抗抵赖 non-repudiation of sending

防止发送者否认其已经发送了消息的服务。

3.9.19

提交抗抵赖 non-repudiation of submission

这一服务旨在提供证据以表明交付机构已经接收到了用于传送的消息。

3.9.20

传输抗抵赖 non-repudiation of transport

这一服务旨在向消息的原发者提供证据,以表明交付机构已经把消息递送给了指定的接收者。

3.9.21

抗抵赖权标 non-repudiation token

GB/T 18794.1—2002 中定义的一种特殊类型的安全权标,由证据和可选的附加数据组成。

3.9.22

公证 notarization

公证人提供的、关于一个活动或者事件所涉及实体以及存储或通信数据的性质的证据。

3.9.23

公证人(公证机构) notary (notary authority)

可信第三方,为涉及到的实体以及存储或通信数据的性质提供证据,或者将现有权标的生命期延长到期满和撤消之后。

3.9.24

公证权标 notarization token

由公证人生成的抗抵赖权标。

3.9.25

NRD 权标 NRD token

交付抗抵赖权标。允许发送者为消息建立交付抗抵赖的数据项。

3.9.26

NRO 权标 NRO token

原发抗抵赖权标。允许接收者为消息建立原发抗抵赖的数据项。

3.9.27

NRS 权标 NRS token

提交抗抵赖权标。允许原发者(发送者)或交付机构为已提交的、待传输的消息建立提交抗抵赖的数据项。

3.9.28

NRT 权标 NRT token

传输抗抵赖权标。允许原发者或交付机构为消息建立传输抗抵赖的数据项。

3.9.29

原发者 originator

向接收者发送消息的实体，或者产生有待于对其提供抗抵赖服务的消息的实体。

3.9.30

证明 proof

按照有效的抗抵赖策略，能够证实证据的合法性的数据。

注：证明是用于证明某件事情真实性或者存在性的证据。

3.9.31

接收者 recipient

获得（收到或取得）消息的实体，抗抵赖服务针对该消息提供。

3.9.32

冗余 redundancy

已知并可以检验的任何消息。

3.9.33

安全信封（SENV） secure envelope

由某实体构造的一组数据项，其构造方式应使得任何持有秘密密钥的实体能够验证这些数据项的完整性和来源。为了生成证据，SENV 由可信第三方（TTP）使用仅为 TTP 所知的秘密密钥来构造和验证。

注：其他国际标准也常使用信封这一术语来表示加密的对象。在本标准中，安全信封一般不需要加密。

3.9.34

签名者 signer

生成数字签名的实体。

3.9.35

可信第三方 trusted third party(TTP)

在安全活动方面为其他实体所信任的安全机构或其代理（见 GB/T 18794.1—2002）。

注：在本标准中，为了实现抗抵赖的目的，可信第三方为原发者、接收者和（或）交付机构所信任，也可以为其他参与方（如仲裁者）信任。

3.9.36

可信时间戳 trusted time stamp

由时间戳机构担保的时间戳。

3.9.37

验证密钥 verification key

验证密码校验值时所需要的数值。

3.9.38

验证者 verifier

验证证据的实体。

4 符号和缩略语

4.1 符号

A	实体 A 的可区分标识符
B	实体 B 的可区分标识符
$CHK_X(y)$	使用实体 X 的密钥对数据 y 计算而得到的密码校验值
DA	交付机构的可区分标识符

f_i	标明有效的抗抵赖服务类型的数据项(标记)
$H(y)$	数据串 y 的散列码
$Imp(y)$	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
m	待生成证据的消息
MAC	消息鉴别码
Pol	适用于证据的抗抵赖策略的可区分标识符
$SENV$	安全信封
$SENV_X(y)$	使用实体 X 的私有密钥对数据 y 计算而得到的安全信封
SIG	已签名消息
$SIG_X(y)$	实体 X 使用其私有密钥对数据 y 生成的已签名消息
$S_X(y)$	使用签名算法和实体 X 的私有密钥对数据 y 计算的签名
$text$	可以构成权标一部分的数据项,包括密钥标识符和(或)消息标识符等附加信息
T_g	证据生成的日期和时间
T_i	事件或动作发生的日期和时间
$V_X(y)$	使用验证算法和实体 X 的验证密钥对数据 y(安全信封或者数字签名)进行的验证操作
$y \parallel z$	y 和 z 按顺序的连接

4.2 缩略语

CA	Certification Authority 认证机构
GNRT	Generic Non-Repudiation Token 通用抗抵赖权标
NA	Notary Authority 公证机构
NRDT	Non-Repudiation of Delivery Token 交付抗抵赖权标
NRI	Non-Repudiation Information 抗抵赖信息
NROT	Non-Repudiation of Origin Token 原发抗抵赖权标
NRST	Non-Repudiation of Submission Token 提交抗抵赖权标
NRTT	Non-Repudiation of Transport Token 传输抗抵赖权标
NT	Notarization Token 公证权标
OSI	Open Systems Interconnection 开放系统互连
TSA	Time-Stamping Authority 时间戳机构
TST	Time-Stamping Token 时间戳权标
TTP	Trusted Third Party 可信第三方

5 本部分各章的组织

首先在第 6 章规定抗抵赖服务的基本需求,在第 7 章描述证据的提供与验证所涉及实体的角色。第 8 章描述可信第三方在抗抵赖各阶段的参与情况,尤其是证据的提供和验证阶段。第 9 章描述了证据的生成和验证机制,包括基于对称密码技术的安全信封和基于非对称密码技术的数字签名。为了更好地表示抗抵赖权标,导出了两种基本机制中通用的密码校验函数。第 10 章定义了三种权标:第一种是适用于多种抗抵赖服务的通用抗抵赖权标;第二种是由可信时间戳机构生成的时间戳权标;第三种是公证机构生成的公证权标,可以提供有关涉及到的实体以及存储或通信数据的性质的证据。第 11 章描述了特定的抗抵赖服务和抗抵赖权标。第 12 章给出了消息发送环境中特定抗抵赖权标的应用实例。

6 要求

下列要求适用于抗抵赖交换所涉及的实体,这些要求与用于生成安全信封和数字签名的密码校验

值的导出方式有关，与抗抵赖机制所支持的抗抵赖服务无关。

6.1 抗抵赖交换的实体应信任一个可信第三方。

注：使用对称密码算法时总是需要 TTP；使用非对称密码算法时，或者需要离线 TTP 来生成公钥证书，或者需要 TTP 来创建用作证据的数字签名。

6.2 在证据生成之前，证据生成者必须清楚以下三件事情：验证者可以接受的抗抵赖策略、所要求的证据类型、以及验证者可以接受的机制集合。

6.3 特定抗抵赖交换中的实体必须可以得到用于生成或验证证据的机制；或者必须有一个可信机构来提供这些机制，并且代表证据请求者来执行必要的功能。

6.4 适用于这些机制的密钥（如非对称技术中的私有密钥，对称技术中的秘密密钥）只能由相关的实体拥有（必要时可以共享）。

6.5 证据的使用者和仲裁者必须能够验证证据。

6.6 证据中要求的时间信息包括事件发生的时间和证据生成的时间。

6.7 如果需要可信时间戳，或者证据生成者所提供的时钟不可信，那么证据生成者或证据验证者必须可以访问时间戳机构。

7 通用抗抵赖服务

7.1 证据提供与验证过程中涉及的实体

在提供抗抵赖服务时，要涉及到几个不同的实体。

证据生成过程涉及到三个实体：

a) 想要得到证据的证据请求者；

b) 执行某动作的或者某事件中涉及到的证据主体；

c) 生成证据的证据生成者。

证据验证过程涉及到两个实体：

a) 能够或者不能够直接验证证据的证据用户；

b) 应证据用户的要求，能够验证证据的证据验证者。

在证据生成过程中，事件或动作与证据主体相关。证据可以应证据请求者的请求而提供，也可以应证据主体自己的要求而提供。

如果证据主体和证据请求者都不能直接提供证据，那么证据由证据生成者产生。然后证据将返回给证据请求者，或者可以供其使用。证据可以传送给其他实体，或者可供其使用。

在证据验证阶段中，证据用户希望验证证据的正确性。如果证据用户不能直接验证证据的正确性，则证据由证据验证者应证据用户的请求而进行验证。

7.2 抗抵赖服务

通用模型适用于以下六种基本的抗抵赖服务：创建抗抵赖、发送抗抵赖、接收抗抵赖、认知抗抵赖、提交抗抵赖和传输抗抵赖。其他抗抵赖服务可由这些基本服务组合而成。结合创建抗抵赖和发送抗抵赖可以提供原发抗抵赖；结合接收抗抵赖和认知抗抵赖可以提供交付抗抵赖。抗抵赖服务只能在既定的时间周期内提供。有时可能需要在权标颁发之后修改其生命周期，比如，如果一个特定的签名方案发现了攻击，那么其生命周期就需要缩短。另一方面，如果一个抗抵赖权标在其过期之后仍然被看作是（密码意义下）安全的，那么抗抵赖策略就允许延长其生命周期。

8 可信第三方

抗抵赖服务可能需要可信第三方的参与，这依赖于所使用的抗抵赖机制和有效的抗抵赖策略。使用非对称密码技术时需要一个离线的可信第三方来保证密钥的真实性，可信第三方可以是 TTP 链中的一部分，只要他们同意在抗抵赖服务中履行义务。使用对称密码技术时，需要一个在线的可信第三方的