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。

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

参与，用于生成和验证安全信封(SENV)。有效的抗抵赖策略可要求部分或者全部证据由可信第三方生成。

有效的抗抵赖策略还可能要求：

a) 由可信时间戳机构提供的可信时间戳；

b) 公证机构(公证人)，以证实所涉及到的实体以及存储或传输数据的性质，或者将现有权标的生命期延长到期满和撤消之后；

c) 监控机构，提供有关涉及到的实体的性质和存储或传输数据的性质的证据。

可信第三方可以不同程度地参与到抗抵赖过程中。当交换证据时，双方必须知道、被通知到，或者同意适用于证据的抗抵赖策略。

根据抗抵赖策略的要求，可以有多个可信第三方参与并担当不同的角色，如公证、时间戳、监控、密钥证明、签名生成、签名验证、安全信封生成、安全信封验证、权标生成或交付等角色。一个可信第三方可能担当一个或多个上述角色。

8.1 证据生成过程

证据是用于解决争议的信息，由证据生成者代表证据主体、可信第三方生成，或者应证据请求者的请求而生成。在证据生成阶段，TTP 可以下述方式参与(关于在线、联线、离线机构的定义，参见 ISO TR 14516)：

a) 当作为在线机构参与每个抗抵赖服务实例时，可信第三方代表证据主体独立生成证据。当使用对称密码技术来提供证据时，可能要求在线产生密码校验值和抗抵赖权标，如生成 GB/T 17903 中定义的安全信封；

b) 当作为联线的证据生成机构时，可信第三方可以自己生成证据(如作为交付机构)；

c) 当作为离线机构时，可信第三方不参与每一个抗抵赖服务实例，而使用签名为生成证据的实体提供离线的公开密钥证书；

d) 如果担任权标生成机构，可信第三方可构造任何类型的抗抵赖权标，该权标由证据主体、一个或多个可信机构提供的一个或多个抗抵赖权标组成；

e) 如果担任数字签名生成机构，可信第三方代表证据主体或者应证据请求者的请求而生成数字签名；

f) 如果担任时间戳机构(见 ISO/IEC 18014)，可信第三方可信赖地提供包括时间戳权标生成的时间的证据；

g) 如果担任公证机构(公证人)，可信第三方可信赖地提供有关实体以及存储的或实体间通信数据的性质的证据，在现有权标期满或者撤销时公证人可信赖地延长其生命期；

h) 如果担任监控机构，可信第三方监控动作和事件，并且可信赖地提供其监控内容的证据。

8.2 证据传输、存储和检索过程

在这一过程中，证据在各参与方间传输，或者在数据存储区之间传输。根据有效的抗抵赖策略，这一阶段的活动未必在抗抵赖服务的所有情况中都进行。本阶段的活动可由可信第三方执行。

a) 作为交付机构时，可信第三方处于联线状态，完成提交抗抵赖和传输抗抵赖；

b) 作为证据记录保管机构时，可信第三方记录证据，可供证据用户或仲裁者之后进行检索。

8.3 证据验证过程

作为证据的验证机构，可信第三方是受证据用户信任的在线机构，用于验证抗抵赖权标提供的每一种抗抵赖信息。当使用对称密码技术生成证据时，证据只能由可信第三方验证；否则，可信第三方的参与是可选的。

抗抵赖权标的验证取决于所使用的技术：

a) 安全信封只能由可信第三方验证；

b) 数字签名可以使用一个或多个公开密钥证书和证书撤消列表验证(在证据生成时所有这些公

钥证书及撤销列表都是有效的)；

c) 公开密钥证书在证据生成时是有效的，这一点必须在出示证据时进行验证。有时可能在几年以后进行验证；

d) 公开密钥证书撤销列表在证据生成时是有效的，这一点必须在出示证据时进行验证，有时可能在几年以后进行验证；

e) 如果抗抵赖服务需要使用时间戳机构提供证据，应以下列方式进行：该证据(如时间戳权标)提供的时间必须与证据生成者、可信第三方或证据请求者产生的证据中所附时间进行比较。在验证这些时间充分接近(按安全策略)之后，证据生成实体、可信第三方或者证据请求者产生的证据才可以接受；

f) 附加的抗抵赖权标(如公证权标)按照其生成时所使用的技术进行验证。

9 证据生成与验证机制

在本阶段，证据由安全信封(SENV)或者数字签名(SIG)组成的抗抵赖权标表示，两者分别是基于对称密码与非对称密码技术生成的密码校验值(CHK)。对于基于证书的签名，抗抵赖权标基本上由已签名的消息(包括消息及签名)及其公开密钥证书组成。如果公开密钥没有与数字签名一起提供，那么相关实体必须可以得到它。对于基于身份的签名，抗抵赖权标由已签名的消息、签名实体的标识数据和为签名者提供密钥的机构的身份(即可区分标识符)组成。

9.1 安全信封

安全信封(SENV)要成为证据的一部分，就必须由可信第三方使用仅为可信第三方所知的秘密密钥来生成。

注：SENV 也可用于抗抵赖交换的实体与 TTP 之间的原发性或完整性通信保护。此时，SENV 由实体与 TTP 共知的密钥来生成与验证。

创建安全信封的方法是：利用实体 X 的秘密密钥，通过对称完整性技术作用对数据 y 进行计算而生成校验值 $CHK_X(y)$，并把它附在数据 y 的后面：

$SENV_X(y)=y \parallel CHK_X(y)$

函数 $CHK_X(y)$ 可由不同的数据完整性机制表示，例如 MAC。

注：MAC 是 ISO/IEC 9797 规定的消息鉴别码。

其他机制将在 GB/T 17903 的其他部分进行规定。

9.2 数字签名

某实体 X 可以使用其私有密钥和数字签名操作对消息 y 做变换从而进行签名，结果表示为 $SIG_X(y)$。只要持有实体 X 的公开密钥的可信拷贝，任何人都可以验证已签名的消息 $SIG_X(y)$ 的有效性。

如果数字签名操作不具有消息恢复功能，已签名的消息由消息 y 附加上签名 $S_X(y)$ 组成。

$SIG_X(y)=y \parallel S_X(y)$

如果数字签名操作具有消息恢复功能，消息 y 的一部分或者全部可以从 $S_X(y)$ 中恢复，那么已签名的消息 $SIG_X(y)$ 就由 y 中不能由签名 $S_X(y)$ 恢复的那一部分消息附加上 $S_X(y)$ 组成。

注 1：带消息恢复的数字签名在标准 GB 15851—1999 和 ISO/IEC 15946-4 中规定；

注 2：带附录的数字签名在标准 GB/T 17902 和 ISO/IEC 15946-2 中规定。

9.3 证据验证机制

使用证据生成实体 X 的验证密钥，利用验证操作 $V_X(SENV)$ 和 $V_X(SIG)$，可以分别对安全信封(SENV)和数字签名(SIG)进行验证。验证结果为肯定或否定。

安全信封只能由持有用于生成安全信封的秘密密钥的可信第三方进行验证。

注：如果 SENV 用于原发性或完整性通信保护，那么它可由任何持有对应的秘密密钥的实体验证。

持有签名者的公开密钥的任何实体都可以验证数字签名。向验证者提供公开密钥证书的方式依赖

于生成数字签名的签名方案的类型。

a) 基于证书的签名使用签名者的公开密钥进行验证，该公开密钥可以从认证机构(CA)颁发的公开密钥证书中得到；

b) 对于基于身份的签名，持有签名实体的标识数据和可信机构(TA)的公开系统参数的任何实体都可以进行验证。这里，签名者的基于身份的私有密钥是由 TA 来提供的。

对于数字签名来说，必须对一个公开密钥证书链或身份标识符链顺序进行验证才可得到必要的保证。

10 抗抵赖权标

抗抵赖服务以抗抵赖信息为媒介。抗抵赖信息由一个或多个抗抵赖权标组成。证据生成者必须提供至少一个由通用抗抵赖权标(GNRT)导出的抗抵赖权标。验证证据时通常需要附加的权标。附加权标可以提供给验证者，也可以不提供给验证者。当不提供附加权标时，验证者必须可以得到它们(例如公开密钥证书和(或)证书撤消列表)或者请求它们(例如来自时间戳机构的时间戳)。本标准讨论三种通用权标：通用抗抵赖权标(GNRT)、时间戳权标(TST)和公证权标(NT)。根据 GNRT 导出的权标由证据生成者生成，而其他权标由可信第三方生成：时间戳权标由时间戳机构(TSA)生成，公正权标由公证机构(NA)生成。

10.1 通用抗抵赖权标

通用抗抵赖权标(GNRT)定义如下：

GNRT=$text \| z \| CHK_X(z)$，其中

$z=Pol \| f \| A \| B \| C \| D \| E \| Tg \| Ti \| Q \| Imp(m)$。

数据字段 z 包括以下数据项：

Pol	适用于证据的抗抵赖策略的可区分标识符
f	所提供的抗抵赖服务类型
A	证据主体的可区分标识符
B	证据生成者的可区分标识符，如果证据生成者与证据主体不同
C	与证据主体(包括消息发送者、消息的预定接收者或交付机构)进行交互的实体的可区分标识符
D	证据请求者的可区分标识符，如果证据请求者与证据主体不同
E	动作中涉及到的其他实体(如消息的预定接收者)的可区分标识符
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
Q	需要原发性或完整性保护的可选数据
$Imp(m)$	与事件或动作有关的消息的印迹

注：根据有效的抗抵赖策略，有些数据项是可选的。

可区分标识符 A 是必不可少的，其他的可区分标识符 B,C,D,E 不一定出现。如果证据是由某机构代表证据主体产生的，证据生成者的可区分标识符 B 是必要的。在传输消息时，可区分标识符 C 是必要的。当证据请求者与证据主体不同时，证据请求者的可区分标识符 D 必须出现。对于提交给交付机构的抗抵赖情形和交付机构传输的抗抵赖情形，涉及的其他实体的可区分标识符 E 必须出现。

字段"*text*"包括一些不需要密码保护的附加数据，这些信息与所使用的技术有关：

a) 对于基于证书的签名，"*text*"字段包括一个或多个公开密钥证书，或者仅仅包括认证机构的可区分标识符和分配给公开密钥证书的证书序列号。

b) 对于基于身份的签名，"*text*"字段包含为签名者提供密钥的机构的可区分标识符。

10.2 时间戳权标

如果需要可信的时间，或者抗抵赖权标生成者所提供的时钟不可信，就需要依赖一个可信第三方，即时间戳机构(TSA)。TSA 的职责是建立另外的证据以证明权标生成的时间。

数据 y 由请求时间戳服务的实体提供。

时间戳权标(TST)定义如下：

TST=$text \parallel w \parallel CHK_{TSA}(w)$，其中

$w=Pol \parallel f \parallel TSA \parallel T_g \parallel Q \parallel Imp(y)$

数据元 w 包括以下数据项：

Pol	适用于证据的抗抵赖策略的可区分标识符
f	所提供的抗抵赖服务类型
TSA	时间戳机构的可区分标识符
T_g	时间戳操作执行的日期和时间
Q	需要原发性或完整性保护的可选数据
$Imp(y)$	待提供可信时间戳的数据 y 的印迹

10.3 公证权标

由公证机构(NA)提供的公证服务用于证实所涉及实体以及存储或通信数据的性质，或用于在现有抗抵赖权标期满或撤消时延长其生命期。

数据 y 由服务请求实体提供。

注：数据 y 可以是消息、抗抵赖权标、消息的散列码、权标的散列码，或者服务请求者希望得到公证人证实的任何数据。

公正权标(NT)定义如下：

NT=$text \parallel w \parallel CHK_{NA}(w)$，其中

w=$Pol \parallel f \parallel X \parallel NA \parallel T_g \parallel Q \parallel Imp(y)$

数据元 w 包括以下数据项：

Pol	适用于证据的抗抵赖策略的可区分标识符
f	标明公证服务的标记
X	请求公证服务的实体 X 的可区分标识符
NA	公证机构的可区分标识符
T_g	公证执行的日期和时间
Q	需要原发或完整性保护的可选数据
$Imp(y)$	待提供公证服务的数据 y 的印迹

监控机构可使用类似的权标来对证据主体提供的、或者监控机构自己生成的数据 y 生成证据。

11 特定的抗抵赖服务

抗抵赖生成的证据用于证明某事件或动作已经发生。证据是针对描述事实或事件的数据而生成的。数据和证据或者予以存储(在非 OSI 环境中)或者在抗抵赖交换的有关实体之间进行传递。证据作为抗抵赖协议的一部分在抗抵赖权标中传输。

下面讨论一组特定的活动，它们全部与实体 A 和实体 B 之间的数据传输有关。中介方(如交付机构)也在讨论之列。

实体 A 创建一条消息 m，按照自己的意愿、或者根据有效的抗抵赖策略的要求、或者应其他实体(如接收者)的请求，建立原发抗抵赖。原发抗抵赖由证据生成者(或者是证据生成者自己，或者是可信第三方)提供。

实体 A 将消息 m 和包含原发抗抵赖权标(NROT)的证据一起发送给接收者——实体 B(如图 1 所示)。

在某些情况下，存在一个或多个可信第三方来履行交付机构的职责。如果存在交付机构，本条款中

描述的所有抗抵赖服务都可以提供。

根据特定应用和有效的抗抵赖策略，交付系统可信赖地生成证据以表明其：

a) 接收到来自实体 A 待传送给实体 B 的消息 m 以及抗抵赖权标 NROT(若存在)——通过生成提交抗抵赖权标(NRST)；

b) 交付了消息 m 以及抗抵赖权标 NROT(若存在)给预定的接收者(实体 B)的数据存储区——通过生成传输抗抵赖权标(NRTT)。

根据有效的抗抵赖策略，可能需要时间戳权标(TST)或者公证权标(NT)为现有的抗抵赖权标提供(附加的)证据。

注：发送者或接收者否认发送或接收消息的情况可能是对发送或接收消息的时间有异议，而不是否认发送过或接收到了消息。

11.1 原发抗抵赖

原发抗抵赖服务包括如下情况：消息的发送者已经创建消息并且发送了该消息。

该服务旨在防止发送者否认自己是消息的创建者(消息的作者)以及该消息的发送者。

该服务可以由发送者自己提供，或者由一个代表发送者的机构来提供。

11.2 交付抗抵赖

交付抗抵赖服务是指：接收者承认已收到消息并且已经了解了消息的内容。

11.3 提交抗抵赖

该服务要求在发送者与一个或多个接收者之间的消息传输过程中存在交付机构。发送者信任交付机构接收自己的消息并尽力递送该消息。接收消息之后，交付机构提供有关发送者已提交该消息的证据。交付机构只承认消息已经提交这一事实，但并不关心消息的内容。

11.4 传输抗抵赖

该服务要求在发送者和接收者之间的消息传输过程中存在交付机构。发送者信任交付机构把消息递送到接收者可以得到的地方。在交付消息时，交付机构提供有关其把消息存放在接收者的数据存储区中的证据，交付机构承认消息已经存放的事实，但并不关心该消息的内容。交付机构不能保证消息被接收者按时接收。

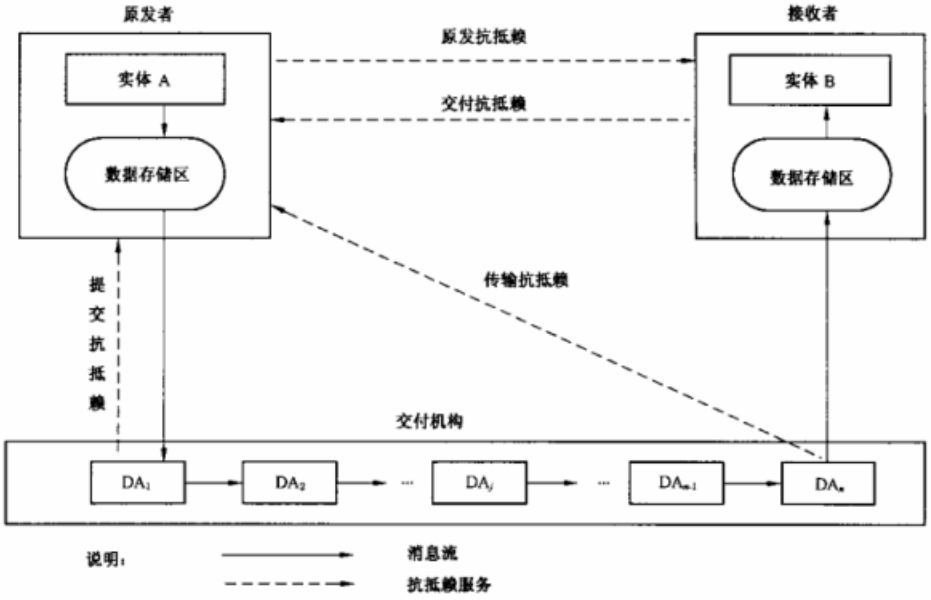

图 1 特定的抗抵赖服务

12 消息传输环境中特定抗抵赖权标的使用

在本标准的其他部分，对前面章条讨论的特定抗抵赖服务的抗抵赖权标(NROT，NRST，NRTT 和 NRDT)，使用 10.1 中给出的通用抗抵赖权标 GNRT 进行定义。特别是，如果交付机构系统由一串子交付机构 DA_i($i=1,2,\cdots\cdots,n$)组成，这四种权标可以按照下列方式使用。

当接收到提交实体或者前一个交付机构的消息时，每一个子交付机构生成一个提交抗抵赖权标 $NRST_i$。这样就建立了一串的中间 $NRST_i$ 权标，各个接收者分别存储这些权标以作为证据。第一个 NRS 权标 $NRST_1$ 发送给原发者以作为提交抗抵赖权标。只有最后一个子交付机构 DA_n 在将消息存入预定接收者的数据存储区之后，才会生成传输抗抵赖权标 NRTT(见图 2)。

根据有效的抗抵赖策略的要求，或者应原发者的要求，实体 B 建立交付抗抵赖：在收到消息 m 后生成证据，并把交付抗抵赖权标 NRDT 发送给原发者 A，A 存储 NRDT 以作为发生争议时的证据。

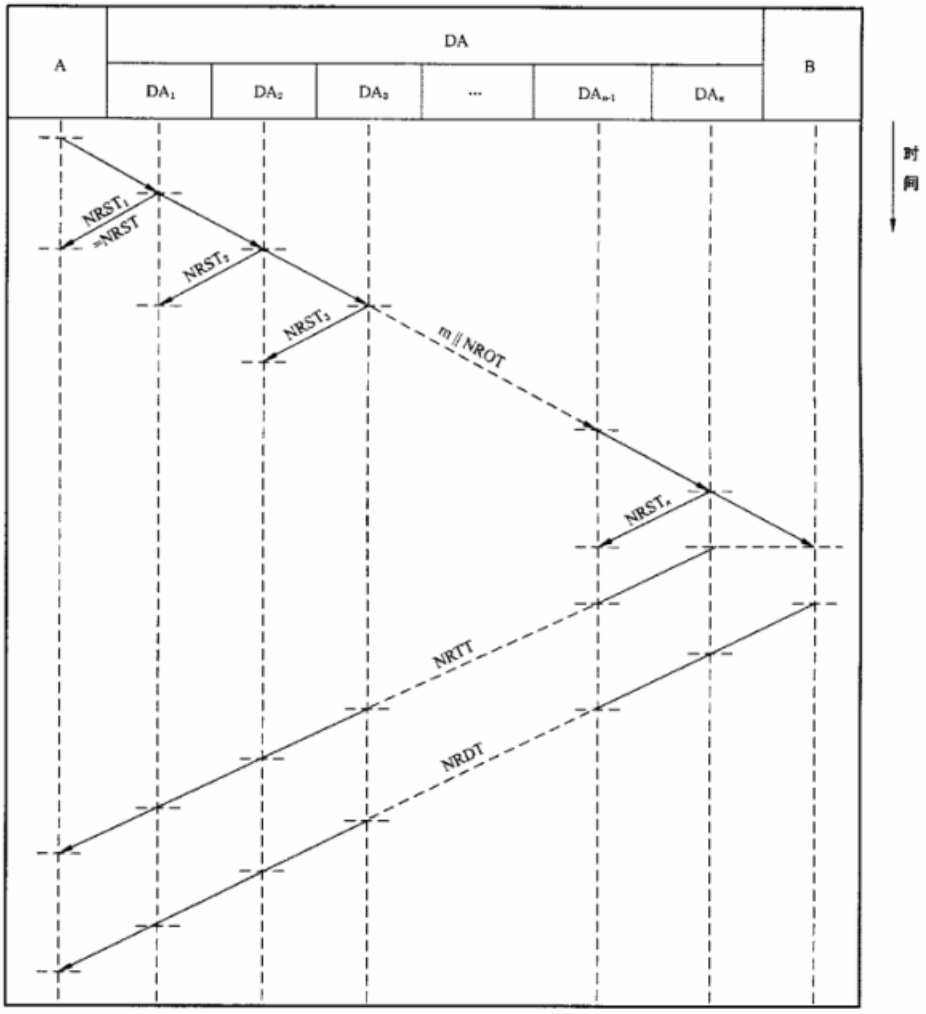

图 2 抗抵赖服务协议(例)