ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.1—XXXX
代替 GB/T 17903.1-2008

信息技术 安全技术 抗抵赖
第1部分：概述

Information technology—Security techniques—Non-reputation—

Part 1: General

(ISO/IEC 13888-1:2020,MOD)

（征求意见稿）

（本稿完成日期：2022年2月）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 5
1　范围 6
2　规范性引用文件 6
3　术语和定义 6
4　符号和缩略语 13
4.1　符号 13
4.2　缩略语 14
5　本文件各章的主要内容 14
6　要求 14
7　通用抗抵赖服务 15
7.1　抗抵赖服务概述 15
7.2　证据提供与验证过程中涉及的实体 15
8　可信第三方 15
8.1　概述 15
8.2　证据生成阶段 16
8.3　证据传输、存储和检索阶段 16
8.4　证据验证阶段 16
9　证据生成与验证机制 17
9.1　概述 17
9.2　安全信封 17
9.3　数字签名 17
9.4　证据验证机制 18
10　抗抵赖令牌 18
10.1　概述 18
10.2　通用抗抵赖令牌 18
10.3　时间戳令牌 19
10.4　公证令牌 19
11　特定的抗抵赖服务 20
11.1　概述 20
11.2　原发抗抵赖 20
11.3　交付抗抵赖 20
11.4　提交抗抵赖 20
11.5　传输抗抵赖 20

12　消息传输环境中特定抗抵赖令牌的使用 21
参考文献 23

前　　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 17903《信息技术 安全技术 抗抵赖》的第1部分。GB/T 17903已经发布了以下部分：

——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。

本文件代替GB/T 17903.1-2008《信息技术 安全技术 抗抵赖 第1部分：概述》。GB/T 17903.1-2008相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 在 6 中增加了对于杂凑函数的要求，为使这些要求符合密码相关国家标准和行业标准，将原有标准的等同采用方式调整为修改采用。

b) 将原有标准中未被引用的规范性引用文件调整至参考文献；

c) 将原 3.1 至 3.9 合并为 3，不再区分术语来源；

d) 删除了原 6.1 至 6.7 节，改为列项；

e) 将原 7.2 和 7.1 的顺序进行了调整，对 7.1 的抗抵赖服务概述进行了修改；

f) 增加了 9.1、10.1 和 11.1，以消除悬置段。

本文件修改采用 ISO/IEC 13888-1:2020《信息技术 安全技术 抗抵赖 第 1 部分：概述》。

本文件与国际标准 ISO/IEC 13888-1:2020 的技术差异及其原因如下：

a) 使用 GB/T 20520 替代了规范性引用文件中的 ISO/IEC 18014，GB/T 20520 规定了时间戳的格式；

b) 删除了部分 GB/T 25069 中已规定的通用术语，增加了规范性引用文件 GB/T 25069；

c) 在 6 中明确抗碰撞杂凑函数应使用符合相关国家标准和行业标准要求的抗碰撞杂凑函数。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国科学院软件研究所、长春吉大正元信息技术股份有限公司、成都卫士通信息产业股份有限公司、中国科学院大学、奇安信科技集团股份有限公司、国民认证科技（北京）有限公司、格尔软件股份有限公司、北京信安世纪科技有限公司、西安西电捷通无线网络通信股份有限公司。

本文件主要起草人：张立武、张严、张振峰、冯登国、王蕊、张妍、张立廷、刘丽敏、张宝欣、黄亮、汪宗斌、李汝鑫、李俊、郑强、杜志强。

本文件及其所代替文件的历次版本发布情况为：

——2008 年首次发布为 GB/T 17903.1-2008；

——本次为第一次修订。

信息技术 安全技术 抗抵赖 第1部分：概述

1 范围

本文件规定了抗抵赖机制的一般模型，可作为本系列标准其它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。

本文件适用于信息系统中实现消息抗抵赖相关应用的设计、实现与测试。争议仲裁不在本文件的范围之内。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069中界定的以及下列术语和定义适用于本文件。

3.1

仲裁方 adjudicator

在当事人之间进行仲裁的实体。

3.2

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。

3.3

证书机构 certification authority

CA

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。

3.4

抗碰撞杂凑函数 collision-resistant hash-function

满足以下特性的杂凑函数(3.18)：找到两个输入比特串，使其映射为同一输出，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

3.5

密码校验函数 cryptographic check function

CHK

消息校验码或数字签名。

3.6

密码校验值 cryptographic check value

密码校验函数的输出值。

3.7

数据存储 data storage

存储数据的方式或介质，数据可以由此提交递送，交付机构也可以向其中放置数据。

3.8

交付机构 delivery authority

DA

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

数字签名 digital signature

SIG

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。

3.10

可区分标识符 distiguishing identifier

可无歧义地区分抗抵赖处理中某个实体的信息。

3.11

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。

3.12

证据生成者 evidence generator

产生抗抵赖证据的实体。

3.13

证据使用者 evidence user

使用抗抵赖证据的实体。

3.14

证据验证者 evidence verifier

验证抗抵赖证据的实体。

3.15

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。

3.16

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。

3.17

杂凑码 hash-code

杂凑函数的输出值。

3.18

杂凑函数 hash-function

将任意长比特串映射为定度比特串的函数，满足如下属性：

——对于一个输出比特串，寻找一个输入比特串来产生这个输出比特串，在计算上是不可行的；

——给定一个输入比特串，寻找另一个不同的输入比特串来产生相同的输出比特串，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

3.19

印记 imprint

一种比特串，或者是数据串的杂凑码，或者是该数据串本身。

3.20

密钥 key

一种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。

3.21

监控机构 monitoring 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。

3.22

消息鉴别码 message authentication code

MAC
消息鉴别码算法的输出的比特串。

3.23

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。

3.24

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。

3.25

交付抗抵赖令牌 non-repudiation of delivery token

NRDT
允许发送者为消息建立交付抗抵赖的数据项。

3.26

抗抵赖交换 non-repudiation exchange

为建立抗抵赖而传输的抗抵赖信息的序列。

3.27

抗抵赖信息 non-repudiation information

NRI
与一个事件或动作有关的信息的集合，包括：可用来生成、验证证据的信息、证据本身和有效的抗抵赖策略。

3.28

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。

3.29

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。

3.30

原发抗抵赖令牌 non-repudiation of origin token

NROT

允许接收者为消息建立原发抗抵赖的数据项。

3.31

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。

3.32

抗抵赖处理 non-repudiation process

一系列相关/交互行为的集合，用于提供一个或多个抗抵赖服务。

3.33

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。

3.34

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。

3.35

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。

3.36

提交抗抵赖令牌 non-repudiation of submission token

NRST

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。

3.37

抗抵赖令牌 non-repudiation token

NRT

一种特殊类型的安全令牌，由证据和可选的附加数据组成。

注：在GB/T 25069等文件中，令牌也称作权标。

3.38

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。

3.39

传输抗抵赖令牌 non-repudiation of transport token

NRTT

允许原发者或交付机构为消息建立传输抗抵赖的数据项。

3.40

公证机构 notary authority

NA

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，或者将现有令牌的生命期延长到期满和撤消之后。

3.41

公证 notarization

公证机构为涉及到的实体以及存储或通信数据的性质提供证据的行为。

3.42

公证令牌 notarization token

NT

由公证机构生成的抗抵赖令牌。

3.43

原发者/ oringinator

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。

3.44

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。

3.45

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。

3.46

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。

3.47

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。

3.48

秘密密钥 secret key

用于对称密码技术中的一种密钥，并仅有一组规定实体所使用。

3.49

安全信封 secure envelope

SENV

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TTP使用仅为 TTP所知的秘密密钥来构造和验证。

3.50

安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。

3.51

安全令牌 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。

3.52

签名者 signer

生成数字签名的实体。

3.53

时间戳 time-stamp

对时间和其它待签名数据进行签名得到的数据，用于表明数据的时间属性。

3.54

时间戳机构 time-stamp authority

TSA

用来产生和管理时间戳的可信服务机构。

3.55

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。

3.56

可信时间戳 trusted time-stamp

由时间戳机构担保的时间戳。

3.57

验证密钥 verification key

验证密码校验值时所需要的数值。

3.58

验证者 verifier

验证证据的实体。

4 符号和缩略语

4.1 符号

下列符号适用于本文件。

A, B, C, D, E	（实体的）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	标明有效的抗抵赖服务类型的数据项（标记）
$GNRT$	通用抗抵赖令牌的可区分标识符
$Imp(y)$	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 本身
$MAC_X(y)$	使用实体 X 的密钥对数据 y 计算而得到的消息鉴别码
m	生成证据的消息
n	交付机构链中包含的子交付机构的数量
NA	公证机构的可区分标识符
$NRDT$	交付抗抵赖令牌的可区分标识符
NRI	抗抵赖信息的可区分标识符
$NROT$	原发抗抵赖令牌的可区分标识符
$NRST$	提交抗抵赖令牌的可区分标识符
$NRTT$	传输抗抵赖令牌的可区分标识符
NT	公证令牌的可区分标识符
Pol	适用于证据的抗抵赖策略的可区分标识符
Q	需要进行原发性/完整性保护的可选数据
$SENV_X(y)$	使用实体 X 的密钥对数据 y 计算而得到的安全信封
$SIG_X(y)$	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
$text$	可以构成令牌一部分的数据项，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
TSA	时间戳权威的可区分标识符
TTP	可信第三方实体的可区分标识符
$V_X(y)$	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
w, y, z	（不同的）数据
(y, z)	y 与 z 按顺序的连接

4.2 缩略语

下列缩略语适用于本文件。

GNRT：通用抗抵赖令牌(Generic Non-Repudiation Token)

TA：可信机构(Trusted Authority)

TST：时间戳令牌(Time-Stamp Token)

TTP：可信第三方(Trusted Third Party)

5 本文件各章的主要内容

本文件的第 6 章给出了抗抵赖服务的模型并规定了抗抵赖服务的基本要求；第 7 章描述了证据提供和验证所涉及实体的角色；第 8 章描述了可信第三方在抗抵赖各阶段，特别是证据提供和验证阶段的参与情况；第 9 章描述了证据的生成和验证机制，包括采用对称密码技术的安全信封机制和采用非对称密码技术的数字签名机制，同时为了更好地表示抗抵赖令牌，还给出了两种基本机制中通用的密码校验函数。

本文件的第 10 章定义了如下三种令牌：

1）适用于多种抗抵赖服务的通用抗抵赖令牌；

2）由可信时间戳机构生成的时间戳令牌；

3）公证机构生成的公证令牌，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。

本文件的第11章描述了特定的抗抵赖服务和抗抵赖令牌；第12章给出了消息发送环境中特定抗抵赖令牌的应用实例。

6 要求

下列要求适用于抗抵赖交换所涉及的实体：

——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在线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。

——在证据生成之前，证据生成者应明确知晓以下三方面的情况：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抗抵赖机制的集合；

——特定抗抵赖交换中的实体应可以获得用于生成或验证证据的机制；或者应存在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；

——适用于上述机制的密钥（例如：非对称技术中的私有密钥，对称技术中的秘密密钥）应只由相关的实体拥有（必要时可共享）；

——证据的使用者和仲裁者应能够验证证据；

——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应能够访问时间戳机构；

——如果使用杂凑函数，应使用符合相关国家标准和行业标准的抗碰撞杂凑函数。

7 通用抗抵赖服务

7.1 抗抵赖服务概述

抗抵赖涉及抗抵赖证据的生成，用于证明一个事件或动作已经发生。抗抵赖证据以描述动作或事件的可验证数据的形式生成。此外，抗抵赖过程还涉及抗抵赖交换中数据和证据的存储和通信。抗抵赖交换在参与方间进行，包括以抗抵赖令牌形式对证据进行传递。

某些抗抵赖服务可以由多个服务组合而成。例如：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。

7.2 证据提供与验证过程中涉及的实体

在提供抗抵赖服务时，证据生成过程涉及以下三个实体：

——想要得到证据的证据请求者；

——执行某动作的或者某事件中涉及到的证据主体；

——生成证据的证据生成者。

证据验证过程涉及以下两个实体：

——（能够或者不能够直接验证证据的）证据使用者；

——应证据使用者的要求，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。证据可以是应证据请求者的请求而提供，也可以是应证据主体自己的请求而提供。

在某些场景中，如果证据主体和证据请求者都不能直接提供证据，证据生成需要第三方的参与。在这种情况下，证据将在证据产生后返回给证据请求者或通过其它方式使证据请求者能够获取，之后，证据可能还会传递或共享给其它实体。

在证据验证阶段中，证据使用者希望验证证据的正确性。如果证据使用者不能直接验证证据的正确性，则证据由证据验证者应证据使用者的请求进行验证。

8 可信第三方

8.1 概述

根据所使用的抗抵赖机制和有效的抗抵赖策略，抗抵赖服务可能需要可信第三方的参与。在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，密钥的真实性保证可通过认证机构签发的数字证书来实现。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。此外，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。

注：有效的抗抵赖策略指正在生效中的抗抵赖策略。

有效的抗抵赖策略还可能要求以下信息：

——由可信时间戳机构提供的可信时间戳；

——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，或者将现有令牌的生命期延长到期满和撤消之后；

——监控机构，提供有关涉及到的实体性质以及存储或传输数据性质的证据。

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，双方应知道、被通知，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，可有多个可信第三方参与并担当不同的角色，这些角色包括：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、令牌生成或交付等。同一个可信第三方可能担当上述角色中的一个或多个。

8.2 证据生成阶段

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/IEC TR 14516)：

——直接参与：

- 当作为在线机构参与每个抗抵赖服务实例时，TTP 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，通常要求在线产生密码校验值和抗抵赖令牌，如生成 GB/T 17903.2 中定义的安全信封；
- 当作为联线的证据生成机构时，TTP 可以自己生成证据（如作为交付机构）。

——间接参与：

- 当作为离线机构时，TTP 不直接参与每一个抗抵赖服务实例，而是使用签名技术为生成证据的实体提供离线的公开密钥证书；
- 如果担任令牌生成机构，TTP 可构造任何类型的抗抵赖令牌，该令牌由证据主体、一个或多个可信机构提供的一个或多个抗抵赖令牌组成；
- 如果担任数字签名生成机构，TTP 代表证据主体或者应证据请求者的请求而生成数字签名；
- 如果担任时间戳机构（参见 GB/T 20520），TTP 可信赖地提供包含 TST 生成时间的证据；
- 如果担任公证机构（公证人），TTP 可信赖地提供有关实体以及存储的或实体间通信数据性质的证据，在现有令牌期满或被撤销时公证人可信赖地延长其生命期；
- 如果担任监控机构，TTP 监控动作和事件，并且可信赖地提供其监控内容的证据。

8.3 证据传输、存储和检索阶段

在这一过程中，证据在各参与方间传输，或者在数据存储之间传输。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发生。本阶段的活动可由可信第三方执行。

——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；

——作为证据记录保管机构时，可信第三方记录证据，可供证据使用者或仲裁者之后进行检索。

8.4 证据验证阶段

作为证据的验证机构，可信第三方是受证据使用者信任的在线机构，用于验证抗抵赖令牌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，证据应由可信第三方验证；否则，可信第三方的参与是可选的。

抗抵赖令牌的验证取决于所使用的技术：

——安全信封应由可信第三方验证；

——数字签名可使用一个或多个公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）；

——在出示证据时应验证公钥证书在证据生成时是有效的。要注意的是，在实际应用中，证据生成和证据出示可能存在较长时间（例如：几年）的间隔；

——在出示证据时应验证公钥证书撤销列表在证据生成时是有效的。在实际应用中，证据生成和证据出示可能存在较长时间的（例如：几年）的间隔；

——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：将该证据（如时间戳令牌）提供的时间与证据生成者、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；

——附加的抗抵赖令牌（如公证令牌）应根据其生成时所使用的技术进行验证。

9 证据生成与验证机制

9.1 概述

在证据生成和验证阶段，证据由安全信封或者数字签名组成的抗抵赖令牌表示，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。对于基于证书的签名，抗抵赖令牌通常由已签名的消息（包括消息及签名）及其公钥证书组成。如果公钥没有与数字签名一起提供，那么相关实体应能获取它。对于基于标识的签名，抗抵赖令牌由已签名的消息、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。

9.2 安全信封

如果安全信封要成为证据的一部分，应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。

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 进行计算而生成消息鉴别码 $MAC_X(y)$，并把它附在数据 y 的后面，即：

$$SENV(y) = (y,\ MAC_X(y))$$

注：MAC为消息鉴别码，本文件规定的安全信封的强度依赖于所使用的密码学机制和参数的安全级别和强度，抗抵赖机制的使用者可根据实际业务的安全需求来选择适当的机制，GB/T 15852（所有部分）中给出了各种消息鉴别码机制安全性的说明。计算上的可行性取决于特定安全要求和环境。

对于安全信封进一步描述将在 GB/T 17903 的其他部分进行规定。

9.3 数字签名

某实体 X 使用其私有密钥和数字签名操作对消息 y 做变换进行签名，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，任何实体都可以验证已签名的消息 $SIG_X(y)$ 的有效性。

如果数字签名机制的签名操作不具有消息恢复功能（即：带附录的数字签名机制），已签名的消息由消息 y 附加上签名 $S_X(y)$ 组成，即。

$$SIG_X(y) = (y, S_X(y))$$

如果数字签名机制的签名操作具有消息恢复功能（即：带消息恢复的数字签名机制），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：带消息恢复的数字签名在标准GB/T 15851中规定；带附录的数字签名在标准GB/T 17902和ISO/IEC 29192-4（轻量级数字签名）中规定。

9.4 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 $V_X(y)$、消息 y 和 $SENV$ 或 SIG，可以分别对安全信封和数字签名进行验证。验证结果为接受或拒绝。

安全信封应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/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：

——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。

——对于基于标识的签名，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签名验证。这里，签名者的基于标识的私有密钥是由 TA 来提供的。

当使用数字签名技术时，在某些应用场景下需要对一个公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 抗抵赖令牌

10.1 概述

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令牌组成。证据生成者应提供至少一个由通用抗抵赖令牌导出的抗抵赖令牌。验证证据时通常还需要附加的令牌（例如：公开密钥证书、证书撤消列表、可信时间戳等等）。附加令牌可以直接提供给验证者，当不直接提供附加令牌时，验证者应可以获取它们（例如：公开密钥证书和/或证书撤消列表）或者请求它们（例如：向 TSA 请求时间戳）。

本章描述了三种通用令牌：通用抗抵赖令牌、时间戳令牌和公证令牌。根据 GNRT 导出的抗抵赖令牌（例如：NROT、NRST、NRTT 和 NRDT）由证据生成者生成，其它令牌由可信第三方生成，其中：时间戳令牌由时间戳机构生成，公证令牌由公证机构生成。

抗抵赖服务应只在既定的时间周期内提供。当令牌颁发后，可对其生命周期进行改变，例如：如果新发现了对一个特定的签名机制的攻击，那么使用该签名机制的令牌的生命周期就需要缩短。另一方面，如果一个抗抵赖令牌在其过期之后仍然被看作是（密码意义下）安全的，那么抗抵赖策略可允许延长其生命周期。

在本章描述的通用抗抵赖令牌中，$CHK_X(z)$ 表示由使用实体 X 的秘密MAC密钥对数据计算得到的消息鉴别码或使用签名算法和实体 X 的私有密钥对数据计算的签名。在前一种情况下，通用令牌中将包含一个安全信封。

10.2 通用抗抵赖令牌

通用抗抵赖令牌定义如下：

$GNRT = (text, z, CHK_X(z))$，其中

$z = (Pol, f, A, B, C, D, E, T_g, T_i, Q, Imp(m))$

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/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，某些数据项是可选的。

生成令牌时，数据字段 z 应经过编码以确保可以唯一、无歧义地从 z 中获取其所有的组成元素，且对于对令牌进行处理的各实体来说，各元素的含义应是明确、无歧义的。

可区分标识符 A 应存在。其他的可区分标识符 B、C、D、E 是可选的。如果证据是由某机构代表证据主体产生的，则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 应存在。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 应存在。

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：

——对于基于证书的签名，“$text$”字段可包括一个或多个公开密钥证书，或者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；

——对于基于标识的签名，“$text$”字段可包含为签名者提供密钥的机构的可区分标识符。

10.3 时间戳令牌

如果需要可信的时间，或者抗抵赖令牌生成者所提供的时钟不可信，抗抵赖机制需要依赖一个可信第三方，即时间戳机构。TSA 的职责是建立另外的证据以证明令牌生成的时间。

由可信第三方TSA提供的时间戳令牌TST应符合GB/T 20520等相关国家和行业标准中的规定。

10.4 公证令牌

由公证机构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令牌期满及被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、抗抵赖令牌、消息的杂凑码、令牌的杂凑码，或者服务请求者希望得到公证人证实的任何数据。

公证令牌 NT 定义如下：

$NT = (text, w, CHK_{NA}(w))$，其中

$w = (Pol,\ f,\ A,\ NA,\ T_g,\ Q,\ Imp(y))$

数据元素 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

A 请求公证服务的实体的可区分标识符

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 需要原发性/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

生成令牌时，数据字段 w 应经过编码以确保可以唯一、无歧义地从 z 中获取其所有地组成元素，且对于对令牌进行处理的各实体来说，各元素的含义应是明确、无歧义的。

监控机构可使用与公证令牌具有类似结构的令牌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

11.1 概述

本章规定了实体A和实体B之间进行的数据传输相关的一系列特定活动集合，用于实现抗抵赖服务。此外，这些动作还可能涉及消息传递的中介方，例如：交付机构等。

实体A（原发者）创建一条消息m，然后按照自己的意愿、或根据有效的抗抵赖策略的要求、或应其他实体（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（原发者自己或是可信第三方）提供。

实体A将消息m和包含原发抗抵赖令牌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，可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，则本章中描述的所有类型的抗抵赖服务都可以提供。如果不存在交付机构，则只能提供原发抗抵赖和交付抗抵赖这两类抗抵赖服务。

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：

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

——根据有效的抗抵赖策略，可能需要时间戳令牌或者公证令牌为现有的抗抵赖令牌提供（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。

11.2 原发抗抵赖

原发抗抵赖是指：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。

该服务可由发送者自己提供，也可由一个代表发送者的机构来提供。

11.3 交付抗抵赖

交付抗抵赖是指：接收者承认已收到消息并且已经了解了消息的内容。

11.4 提交抗抵赖

提交抗抵赖要求在发送者和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。

11.5 传输抗抵赖

传输抗抵赖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获取的地方。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。

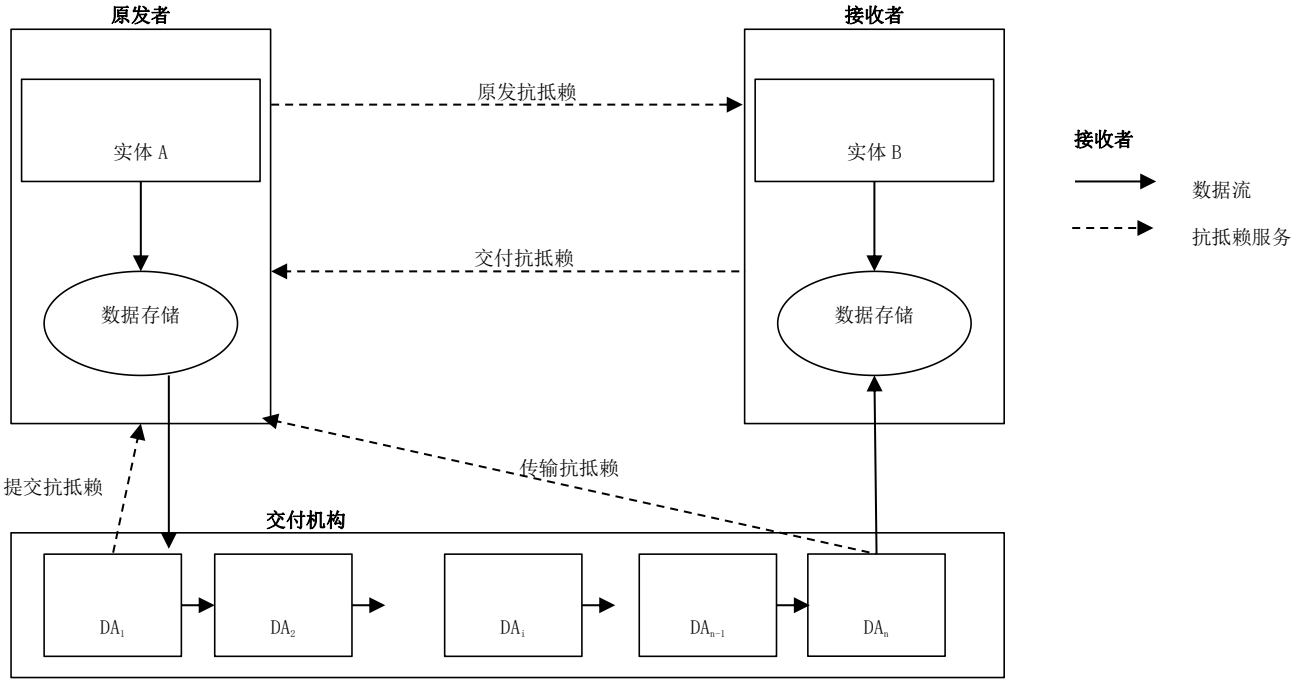

图 1　特定抗抵赖服务

12　消息传输环境中特定抗抵赖令牌的使用

如果交付机构系统由一串子交付机构 DA_i（i=1,2,…,n）组成，则在此场景下，11 章规定的四种特定抗抵赖服务的抗抵赖令牌（NROT、NRST、NRTT 和 NRDT）可以按照如下方式使用：

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 DA_i 生成一个提交抗抵赖令牌 $NRST_i$。这样就建立了一串的中间令牌 $NRST_i$，各个接收者分别存储这些令牌以作为证据。第一个提交抗抵赖令牌 $NRST_1$ 发送给原发者以作为 NRST。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之后，才会生成传输抗抵赖令牌 *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，并把交付抗抵赖令牌*NRDT*发送给原发者*A*，*A*存储*NRDT*以作为发生争议时的证据。

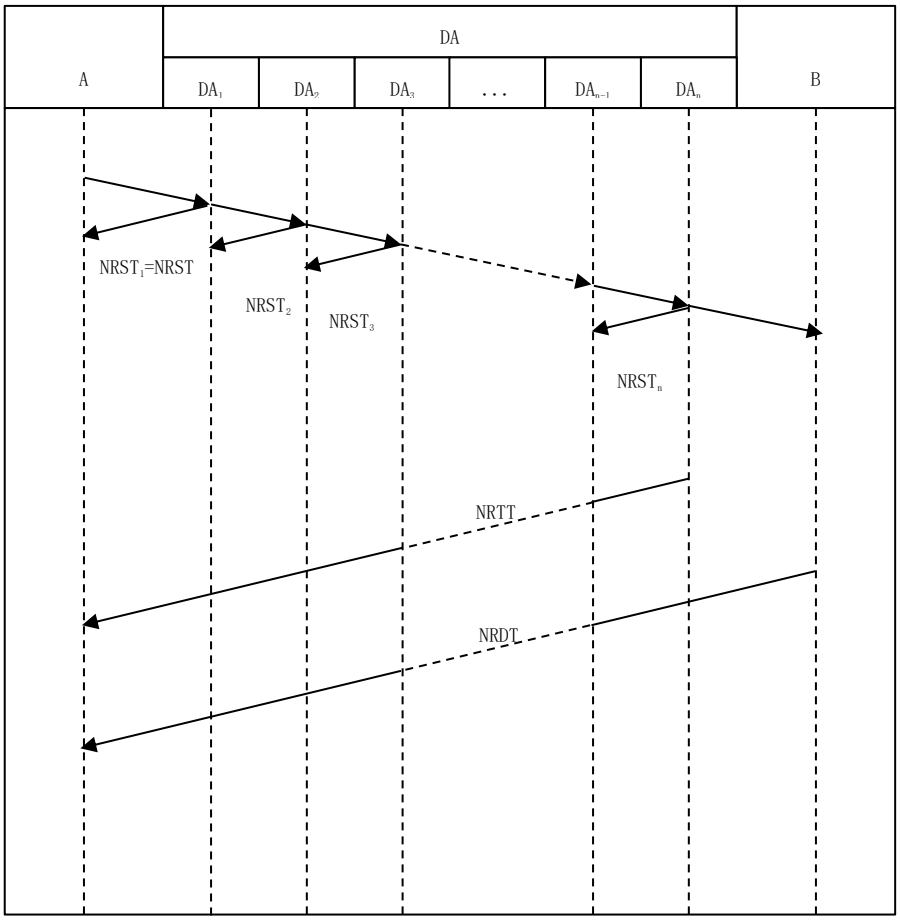

图 2　抗抵赖服务协议（示例）

参 考 文 献

[1] ISO 7498-2:1989 Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture
[2] ISO 8601（所有部分）Date and time — Representations for information interchange
[3] ISO/IEC 9594-8:2017 Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks
[4] ISO/IEC 9796（所有部分）Information technology — Security techniques — Digital signature schemes giving message recovery
[5] ISO/IEC 9797（所有部分）Information technology — Security techniques — Message Authentication Codes (MACs)
[6] ISO/IEC 9798-1:2010 Information technology — Security techniques — Entity authentication — Part 1: General
[7] ISO/IEC 10118-1:2016 Information technology — Security techniques — Hash-functions — Part 1: General — Amendment 1: Padding methods for sponge functions
[8] ISO/IEC 10181-1:1996 Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview
[9] ISO/IEC 10181-4:1997 Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework — Part 4:
[10] ISO/IEC 11770-1:2010 Information technology — Security techniques — Key management — Part 1: Framework
[11] ISO/IEC 11770-3:2015 Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques
[12] ISO/IEC 13888-2:2010 Information technology — Security techniques — Non-repudiation — Part 2: Mechanisms using symmetric techniques
[13] ISO/IEC TR 14516 Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[14] ISO 14641 Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications
[15] ISO/IEC 14888（所有部分）Information technology — Security techniques — Digital signatures with appendix
[16] ISO/IEC 15946（所有部分）Information technology — Security techniques — Cryptographic techniques based on elliptic curves