ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.1—2024
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-repudiation—Part 1：General

（ISO/IEC 13888-1：2020，Information security—Non-repudiation—Part 1：General，MOD）

2024-03-15 发布　　2024-10-01 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

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》。与GB/T 17903.1—2008相比，除编辑性改动外，主要技术变化如下：

a) 增加了对于杂凑函数的要求(见第6章，2008版的第6章)

b) 更改了对抗抵赖服务的表述(见7.1、7.2，2008版的7.1、7.2)。

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

本文件与ISO/IEC 13888-1:2020的技术差异及其原因如下：

a) 用规范性引用的GB/T 20520替换了ISO/IEC 18014(所有部分)(见10.3)，以适应我国的技术条件；

b) 增加了规范性引用的GB/T 25069，并使用GB/T 25069中的术语定义替代了部分原有术语的定义(见第3章)，以适应我国的技术条件；

c) 删除了ISO/IEC 13888-1:2020中第4章的缩略语“TA”，此缩略语在正文未引用；

d) 删除了ISO/IEC 13888-1:2020中第5章的“文档结构”，增加了“概述”，以使本文件符合国家标准的结构惯例；

e) 修改了对抗碰撞杂凑函数的要求(见第6章)，以适应我国的技术条件。

本文件做了下列编辑性改动：

a) 为了与现有标准协调一致，将标准名称更改为《信息技术　安全技术　抗抵赖　第1部分：概述》；

b) 调整了术语的排列顺序，将按英语字母顺序排列更改为按术语间关系排列(见第3章)；

c) 用资料性引用的GB/T 17903(所有部分)替换了ISO/IEC 13888(所有部分)(见第6章)；

d) 删除了ISO/IEC 13888-1:2020中9.1资料性引用的ISO/IEC 14888(所有部分)；

e) 用资料性引用的GB/T 15852(所有部分)替换了ISO/IEC 9797(所有部分)(见9.2)；

f) 用资料性引用的GB/T 15851替换了ISO/IEC 9796(见9.3)；

g) 用资料性引用的GB/T 17902替换了ISO/IEC 14880(见9.3)。

h) 增加了有关消息鉴别码安全性的提示(见9.2的注)。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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、北京中关村实验室、中国科学院大学、中电科网络安全科技股份有限公司、中国电子技术标准化研究院、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、殷其雷、刘丽敏、张宝欣、

林阳荟晨、黄亮、汪宗斌、李汝鑫、李俊、郑强、杜志强、杨领波、钱维、王现方。

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。

引　言

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。GB/T 17903 旨在描述抗抵赖机制的模型及采用对称密码技术和非对称密码技术的具体抗抵赖机制。拟由三个部分构成。

——第 1 部分：概述。目的在于给出抗抵赖机制的一般模型，作为 GB/T 17903 的其他部分中规定的使用密码技术的抗抵赖机制的一般模型。

——第 2 部分：采用对称技术的机制。目的在于给出采用对称密码技术的具体抗抵赖机制。

——第 3 部分：采用非对称技术的机制。目的在于给出采用非对称密码技术的具体抗抵赖机制。

信息技术　安全技术　抗抵赖
第1部分:概述

1　范围

本文件给出了抗抵赖机制的一般模型,作为GB/T 17903的其他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。争议仲裁不适用于本文件。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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界定的以及下列术语和定义适用于本文件。

3.1

抗抵赖策略　non-repudiation policy

一组提供抗抵赖服务的准则。

注:具体而言,用于生成和验证证据以及裁决的一组规则。

3.2

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。

3.3

抗抵赖信息　non-repudiation information;NRI

与一个事件或动作有关,包括可用来生成、验证证据的信息、证据本身和生效中的抗抵赖策略的信息的集合。

3.4

抗抵赖交换　non-repudiation exchange

以抗抵赖为目的,抗抵赖信息(NRI)的一次或多次传送所组成的序列。

3.5

安全令牌　security token

一种与安全有关的数据集合。

注：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。

3.6

抗抵赖令牌　non-repudiation token；NRT

由证据和可选的附加数据组成的一种特殊类型的安全令牌(3.5)。

3.7

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。

3.8

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

可信第三方　trusted third party；TTP

在安全活动方面，被其他实体信任的安全机构或其代理。

[来源：GB/T 25069—2022，3.334]

3.10

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。

3.11

时间戳　time-stamp；TS

对时间和其他待签名数据进行签名得到，用于表明数据时间属性的数据。

[来源：GB/T 25069—2022，3.541]

3.12

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。

[来源：GB/T 25069—2022，3.544]

3.13

可信时间戳　trusted time-stamp

由时间戳机构担保的时间戳。

3.14

安全策略　security policy

用于治理组织及其系统内，特别是那些对系统安全及相关元素具有影响的资产，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。

3.15

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。

3.16

公证机构　notary authority；NA

就所涉及的实体以及所存储或通信的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或被撤销以后的可信第三方。

3.17

公证　notarization

公证机构为涉及的实体以及存储或通信数据的性质提供证据的行为。

3.18

公证令牌　notarization token;NT

由公证机构生成的抗抵赖令牌。

3.19

仲裁方　adjudicator

在当事人之间进行仲裁的实体。

3.20

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。

3.21

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。

3.22

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。

3.23

证据生成者　evidence generator

产生抗抵赖证据的实体。

3.24

证据使用者　evidence user

使用抗抵赖证据的实体。

3.25

证据验证者　evidence verifier

验证抗抵赖证据的实体。

3.26

验证者　verifier

验证证据的实体。

3.27

原发抗抵赖　non-repudiation of origin

防止原发者不实否认其已创建了消息内容并已发送消息的服务。

3.28

交付抗抵赖　non-repudiation of delivery

防止接收者不实否认已经收到消息并认可其内容的服务。

3.29

提交抗抵赖　non-repudiation of submission

为交付机构已收下所传输消息提供证据的服务。

3.30

传输抗抵赖　non-repudiation of transport

旨在向消息原发者提供证据,证明交付机构已将消息递送给了预期接收者的服务。

3.31

创建抗抵赖　non-repudiation of creation

旨在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。

3.32

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。

3.33

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

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。

3.35

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

允许接收者为某一消息建立原发抗抵赖的数据项。

3.36

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。

3.37

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。

3.38

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

允许原发者或交付机构为某一消息建立传输抗抵赖的数据项。

3.39

消息鉴别码　message authentication code;MAC

消息鉴别码算法输出的位串。

[来源:GB/T 25069—2022,3.660]

3.40

数字签名　digital signature;SIG

附加在数据单元上的一些数据,或是对数据单元做密码变换,这种附加数据或密码变换允许数据单元的接收者用以确认数据单元的来源和完整性,达到保护数据,防止被人(例如接收者)伪造的目的。

[来源:GB/T 25069—2022,3.576,有修改]

3.41

签名者　signer

生成数字签名的实体。

[来源:GB/T 25069—2022,3.465]

3.42

密码校验函数　cryptographic check function;CHK

消息鉴别码或数字签名。

注:即以消息和一个秘密或私有密钥作为输入,输出可用来校验消息来源和完整性的比特串的函数。

3.43

密码校验值　cryptographic check value

密码校验函数的输出值。

3.44

密钥　key

控制密码变换操作的符号序列。

[来源:GB/T 25069—2022,3.389]

3.45

验证密钥　verification key

验证密码校验值时所需要的密钥。

3.46

秘密密钥　secret key

用于对称密码技术,只能由一组指定实体使用的密钥。

[来源:GB/T 25069—2022,3.374]

3.47

私钥　private key

私有密钥

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源:GB/T 25069—2022,3.580,有修改]

3.48

公钥　public key

公开密钥

非对称密码算法中可公开的密钥。

[来源:GB/T 25069—2022,3.211,有修改]

3.49

证书　certificate

关于实体的一种数据,该数据由认证机构的私有密钥或秘密密钥签发,并无法伪造。

[来源:GB/T 25069—2022,3.779]

3.50

公钥证书　public key certificate

由证书认证机构对一个实体签发并不可伪造的、有关其公钥信息的数据结构。

[来源:GB/T 25069—2022,3.214]

3.51

证书认证机构　certification authority;CA

对证书进行全生存周期管理的实体。

[来源:GB/T 25069—2022,3.785,有修改]

3.52

杂凑函数　hash-function

将任意长位串映射为定度位串的函数,并满足下列性质:

——对于一个输出位串,寻找一个输入位串来产生该输出位串,在计算上不可行;

——给定一个输入位串,寻找另一个不同的输入位串来产生相同的输出位串,在计算上不可行。

[来源:GB/T 25069—2022,3.505,有修改]

3.53

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

满足如下性质的杂凑函数(3.52):找出映射到同一输出的任何两个不同输入在计算上是不可行的。

注:计算可行性依赖于特定安全要求和环境。

[来源:GB/T 25069—2022,3.322]

3.54

杂凑码　hash-code

杂凑函数的输出值。

3.55

印记　imprint

一种位串,或者是数据串的杂凑码,或者是该数据串本身。

3.56

安全信封　secure envelope;SENV

由某实体构造,使得任何持有秘密密钥的实体能够验证其完整性和来源的一组数据项。

注 1:为了生成证据,安全信封由可信第三方使用仅为其所知的秘密密钥来构造和验证。

注 2:安全信封使用密码校验函数生成。

3.57

区分性标识符　distiguishing identifier

无歧义地区分出抗抵赖处理中某一实体或数据项类型的一组字符。

[来源:GB/T 25069—2022,3.474,有修改。]

3.58

数据存储　data storage

用于数据提交递送或交付机构放置数据的信息存储部件或介质。

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)区分性标识符
$CHK_X(y)$	使用实体 X 的密钥对数据 y 计算而得到的密码校验值
DA	交付机构的区分性标识符
f	标明有效的抗抵赖服务类型的数据项(标记)
$GNRT$	通用抗抵赖令牌的区分性标识符
$Imp(y)$	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	公证机构的区分性标识符
$NRDT$	交付抗抵赖令牌的区分性标识符
NRI	抗抵赖信息的区分性标识符
$NROT$	原发抗抵赖令牌的区分性标识符
$NRST$	提交抗抵赖令牌的区分性标识符

$NRTT$	传输抗抵赖令牌的区分性标识符
NT	公证令牌的区分性标识符
Pol	适用于证据的抗抵赖策略的区分性标识符
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	时间戳权威的区分性标识符
TTP	可信第三方实体的区分性标识符
$V_X(y)$	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)

TST：时间戳令牌(Time-Stamp Token)

5 概述

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。本文件描述了抗抵赖机制的模型，所提供的证据基于由对称密码或非对称密码技术而生成的密码校验值。

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。

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令牌。抗抵赖令牌由安全信封和/或数字签名，以及可选的附加数据组成，其中：

——安全信封由生成证据的机构使用对称密码技术生成；

——数字签名由证据生成者或生成证据的机构使用非对称密码技术生成。

抗抵赖令牌可作为抗抵赖信息存储，该信息可在之后的争议仲裁中被争议方和仲裁方使用。

根据生效中的抗抵赖策略，以及应用运行的环境规则，完成抗抵赖信息可能还需要其他信息，例如：

——包含由时间戳权威提供的可信时间戳的证据；

——由公证方提供的，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。ISO/IEC 10181-4描述了抗抵赖策略。

本文件首先描述通用的抗抵赖机制，然后将这一抗抵赖机制应用于以下类型的特定抗抵赖服务：

——原发抗抵赖；

——交付抗抵赖；

——提交抗抵赖；

——传输抗抵赖。

此外，本文件还涉及以下类型的抗抵赖服务：

——创建抗抵赖；

——接收抗抵赖；

——认知抗抵赖；

——发送抗抵赖。

6 要求

根据用于生成SENV和SIG的CHK的性质，以及抗抵赖机制所支持的抗抵赖服务的类型，下列要求中的部分或全部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参与交换的所有可信第三方；

注：使用对称密码算法时，TTP是必需的；使用非对称密码算法时，需要TTP来生成公钥证书，或是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接受的抗抵赖机制的集合；

——特定抗抵赖交换中的实体应能够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，并代表证据请求者来执行必要的功能；

——相关的实体应持有（必要时可共享）上述机制中需要使用的密钥（例如：非对称技术中的私有密钥，对称技术中的秘密密钥）；

——证据使用者和仲裁者应是证据验证者，或信任提供证据验证服务的实体；

——如果需要可信时间戳，或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；

——在GB/T 17903（所有部分）中如果使用杂凑函数，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能提供原发抗抵赖；结合接收抗抵赖和认知抗抵赖能提供交付抗抵赖。

7.2 证据生成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。证据可应证据请求者的请求而提供，也可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，则证据生成需要第三方的参与。在这种情况下，证据将在产生后返回给证据请求者或通过其他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他实体。

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生效中的抗抵赖策略，不同的抗抵赖服务需要不同类型的可信第三方的参与。在使用非对称密码技术时所需的真实性密钥可能通过可信第三方（即认证机构）所签发的数字证书来实现。在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，生效中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。

生效中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），以证实所涉及的实体以及存储或传输数据的性质，并将对该数据计算生成的数字签名返回给相关实体；

——监控机构，提供有关涉及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 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（见 GB/T 20520），TTP 被信任用于提供包含 TST 生成时间的证据；

- 如果担任公证机构(公证人),TTP 被信任用于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延长其生命期;
- 如果担任监控机构,TTP 监控动作和事件,并且被信任用于提供其监控内容的证据。

8.3 证据传输、存储和检索阶段

在证据传输、存储和检索阶段中,证据在各参与方之间传输,或者在数据存储之间传输。根据生效中的抗抵赖策略,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 TTP 执行。

——作为交付机构时,TTP 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,TTP 记录证据,可供证据使用者或仲裁方之后进行检索。

8.4 证据验证阶段

作为证据的验证机构,TTP 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 TTP 验证;否则,TTP 的参与是可选的。

抗抵赖令牌的验证取决于所使用的技术,具体验证方式如下。

——安全信封只能由 TTP 验证。

——数字签名可使用一个或多个公钥证书和证书撤销列表验证(这些公钥证书及撤销列表在证据生成的时间是有效的)。

——在出示证据时应验证公钥证书在证据生成时是有效的。如果公钥证书在出示证据时已到期或被撤销,根据生效中的抗抵赖策略,可通过证据中时间戳令牌或公证令牌所确认的证据生成时间,并验证该证书在该时间的有效性。

——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。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的(例如:几年)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、TTP 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、TTP 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)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 规则

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(即区分性标识符)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

$$SENV_X(y)=(y,MAC_X(y))$$

注：本文件规定的安全信封的强度依赖于所使用的消息鉴别码等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。

对于安全信封的进一步描述将在 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 1：带消息恢复的数字签名在 GB/T 15851 中规定。

注 2：带附录的数字签名在 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，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/完整性通信保护，那么它能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能够验证数字签名。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，该公开密钥可能从认证机构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的公开系统参数的任何实体都进行签名验证。其中签名者的基于标识的私有密钥是由可信机构来提供的。

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 通用要求

抗抵赖服务涉及对抗抵赖信息的生成和验证。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、证书撤销列表、可信时间戳等等)。附加令牌可直接提供给验证者，当不直接提供附加令牌时，验证者应获取它们(例如：公开密钥证书和/或证书撤销列表)或者请求它们(例如：向 TSA 请求时间戳)。本文件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，其他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 MAC 算法和实体 X 的秘密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区分性标识符；

f 所提供的抗抵赖服务类型；

A 证据主体的区分性标识符；

B 证据生成者的区分性标识符，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)进行交互的实体的区分性标识符；

D 证据请求者的区分性标识符，如果证据请求者与证据主体不同；

E 动作中涉及的其他实体(如消息的预定接收者)的区分性标识符；

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：根据生效中的抗抵赖策略，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。

区分性标识符 A 应存在。其他的区分性标识符 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，则证据生成者的区分性标识符 B 是必要的。在传输消息时，区分性标识符 C 是必要的。当证据请求者与证据主体不同时，证据请求者的区分性标识符 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，涉及的其他实体的区分性标识符 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区分性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区分性标识符。

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 TSA 提供的 TST 应符合 GB/T 20520 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销时延长其生命期。

数据 y 由服务请求实体提供。

注：数据 y 可能是消息、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区分性标识符；

f 标明公证服务的标记；

A 请求公证服务的实体的区分性标识符；

NA 公证机构的区分性标识符；

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 应经过编码以确保能够唯一、无歧义地从 w 中获取其所有的组成元素，且对于处理令牌的各实体，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。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、或根据生效中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（见图 1）。

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。

根据特定应用和生效中的抗抵赖策略，交付系统被信任用于生成证据以表明其：

——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 $NRST$；

——将消息 m 以及抗抵赖令牌 $NROT$（若存在）提交至实体 B 的数据存储——通过生成传输抗抵赖令牌 $NRTT$；

——根据生效中的抗抵赖策略，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。

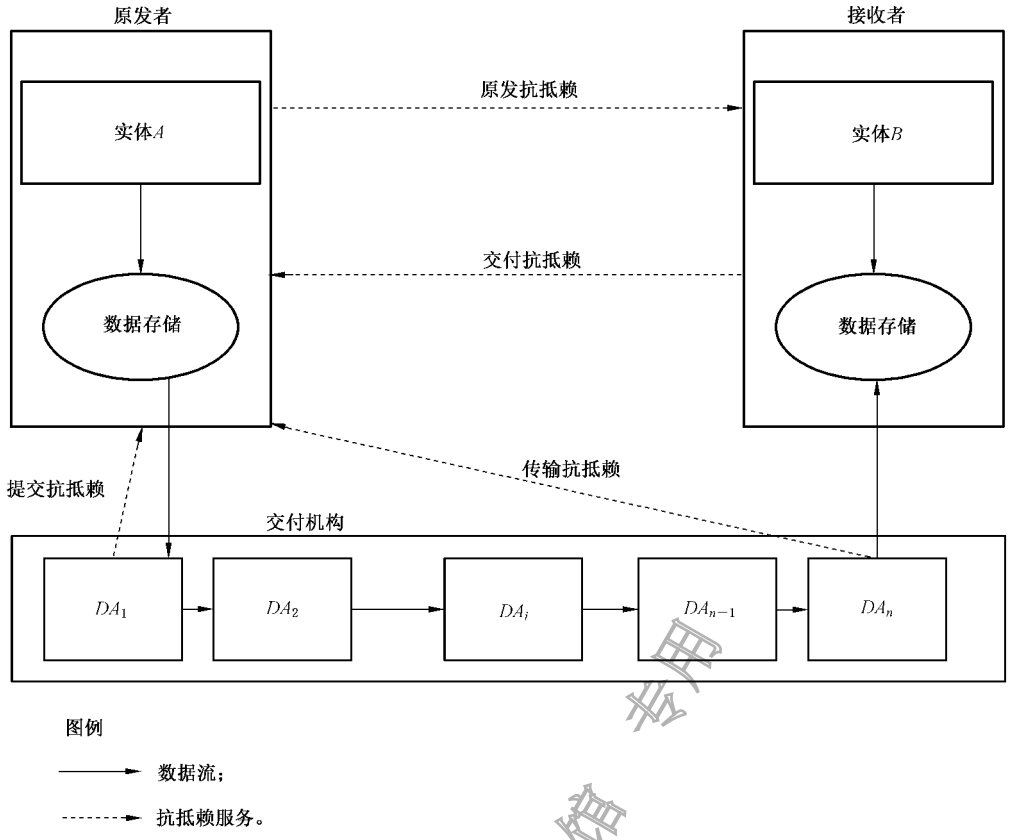

图 1　特定抗抵赖服务

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。

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($i=1,2,\cdots,n$)组成,则在此场景下,第 11 章描述的(具体定义见 GB/T 17902.2 和 GB/T 17902.3)特定抗抵赖服务的抗抵赖令牌可能按照如下方式使用:

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)。

根据生效中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。

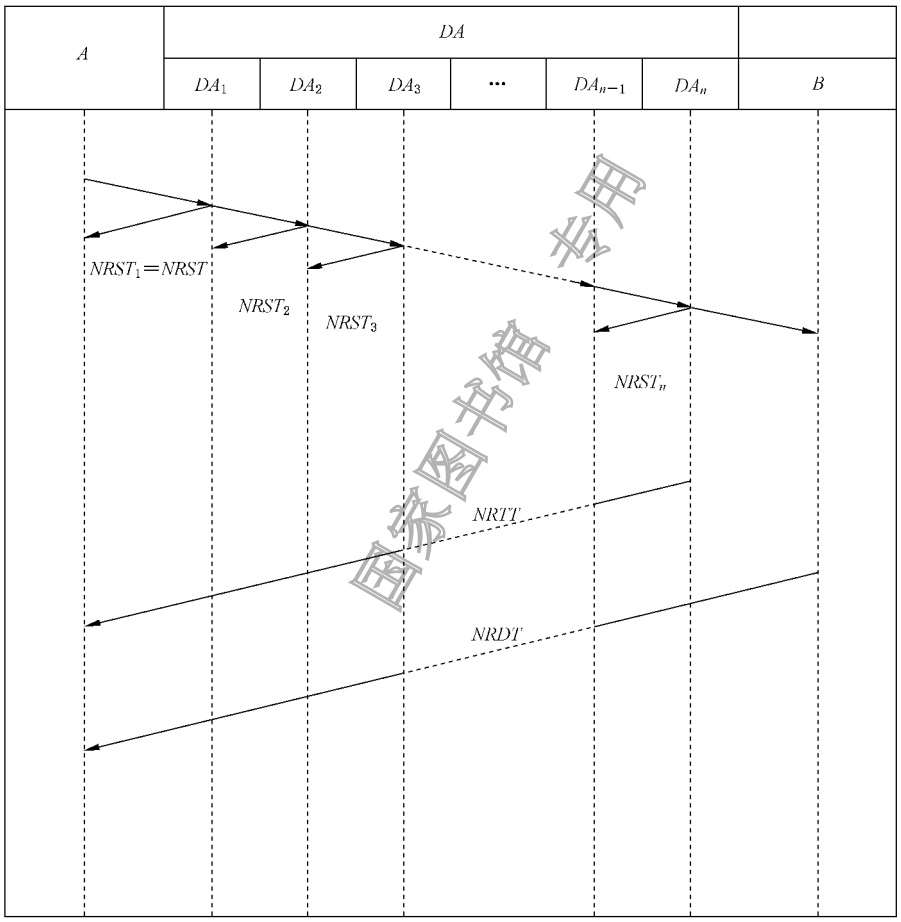

图 2 抗抵赖服务协议(示例)

参 考 文 献

[1] GB/T 15851(所有部分) 信息技术 安全技术 带消息恢复的数字签名

[2] GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码

[3] GB/T 17902(所有部分) 信息技术 安全技术 带附录的数字签名

[4] GB/T 17903.2—2021 信息技术 安全技术 抗抵赖 第2部分:采用对称技术的机制

[5] ISO 7498-2:1989 Information processing systems—Open systems interconnection—Basic reference model—Part 2:Security architecture

[6] ISO 8601(所有部分) Date and time—Representations for information interchange

[7] ISO/IEC 9594-8:2017 Information technology—Open systems interconnection—Part 8:The Directory:Public-key and attribute certificate frameworks

[8] ISO/IEC 9798-1:2010 Information technology—Security techniques—Entity authentication—Part 1:General

[9] ISO/IEC 10118-1:2016 Information technology—Security techniques—Hash-functions—Part 1:General

[10] ISO/IEC 10181-4 Information technology—Open systems interconnection—Security frameworks for open systems:Non-repudiation framework—Part 4:Non-repudiation framework

[11] ISO/IEC 11770-1:2010 Information technology—Security techniques—Key management—Part 1:Framework

[12] ISO/IEC 11770-3:2021 Information technology—Key management—Part 3:Mechanisms using asymmetric 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 15946(所有部分) Information technology—Security techniques—Cryptographic techniques based on elliptic curves

[16] ISO/IEC 29192-4 Information technology—Security techniques—Lightweight cryptography—Part 4:Mechanisms using asymmetric techniques

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—2024
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.net.cn
服务热线:400-168-0010
2024 年 3 月第一版
*
书号:155066·1-75199

GB/T 17903.1-2024