

中华人民共和国国家标准

GB/T 17903.3—2024

代替 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

Information technology—Security techniques—Non-repudiation—
Part 3: Mechanisms using asymmetric techniques

(ISO/IEC 13888-3:2020, Information security—Non-repudiation—
Part 3: Mechanisms using asymmetric techniques, MOD)

2024-03-15 发布

2024-10-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目次

前言 I

引言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号 1

5 要求 2

6 可信第三方的参与 2

7 数字签名 3

8 抗抵赖令牌 3

9 由终端实体生成证据的机制 4

 9.1 一般规则 4

 9.2 原发抗抵赖机制 4

 9.3 交付抗抵赖机制 5

10 由交付机构生成证据的机制 6

 10.1 一般规则 6

 10.2 提交抗抵赖机制..... 6

 10.3 传输抗抵赖机制 7

11 时间保证机制 8

 11.1 一般规则 8

 11.2 采用时间戳的机制..... 9

 11.3 采用时间公证服务的机制 9

参考文献 10

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3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 17903.3—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》。与 GB/T 17903.3—2008 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加了关于数字签名的安全性要求(见第5章)；
- b) 增加了时间保证机制(见第11章)。

本文件修改采用 ISO/IEC 13888-3:2020《信息安全 抗抵赖 第3部分：采用非对称技术的机制》。

本文件与 ISO/IEC 13888-3:2020 的技术差异及其原因如下：

- a) 增加了规范性引用的 GB/T 20520(见第3章)，引用了此标准的术语；
- b) 删除了 ISO/IEC 13888-3:2020 的第3章定义“3.2 时间戳服务”，此术语已在规范性引用的 GB/T 20520 中给出了定义；
- c) 用规范性引用的 GB/T 17903.1 替换了 ISO/IEC 13888-1(见第3章、第4章)，以适应我国的技术条件；
- d) 修改了對抗碰撞杂凑函数的要求，以适应我国的技术条件(见第5章)；
- e) 用规范性引用的 GB/T 15851 (所有部分) 替换了 ISO/IEC 9796(所有部分)，以及用规范性引用的 GB/T 17902 (所有部分) 替换了 ISO/IEC 14888 (所有部分)(见第7章)，以适应我国的技术条件；
- f) 用规范性引用的 GB/T 20520 替换了 ISO/IEC 18014 (所有部分)(见11.2)，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3部分：采用非对称技术的机制》；
- b) 删除了 ISO/IEC 13888-3:2020 中资料性引用的 ISO/IEC 10118(所有部分)；
- c) 用资料性引用的 GB/T 16264.8—2005 替换了 ISO/IEC 9594-8(见第6章)。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)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、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：张严、张立武、张振峰、冯登国、张妍、王蕊、刘丽敏、殷其雷、张立廷、林阳荟晨、张宝欣、黄亮、汪宗斌、郑强、李俊、李汝鑫、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：

- 1999年首次发布为 GB/T 17903.3—1999；
- 2008年第一次修订；
- 本次为第二次修订。

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/T17903 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/T17903 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3部分：采用非对称技术的机制

1 范围

本文件确立了若干特定的抗抵赖机制，用于提供原发抗抵赖、交付抗抵赖、传输抗抵赖和提交抗抵赖。

本文件适用于采用非对称技术实现的消息抗抵赖相关应用的设计、实现与测试。

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/T15851 (所有部分) 信息技术 安全技术 带消息恢复的数字签名方案[ISO/IEC 9796 (所有部分)]

注1:GB/T15851.3—2018 信息技术 安全技术 带消息恢复的数字签名方案 第3部分：基于离散对数的机制 (ISO/IEC 9796-3:2006,MOD)

GB/T17902 (所有部分) 信息技术 安全技术 带附录的数字签名[ISO/IEC14888 (所有部分)]

注2:GB/T17902.1—2023 信息技术 安全技术 带附录的数字签名 第1部分：概述(ISO/IEC 14888-1:2008, IDT)

GB/T 17902.2—2023 信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制(ISO/IEC 14888-2:1999, IDT)

GB/T17902.3—2023 信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制(ISO/IEC 14888-3:1998, IDT)

GB/T 17903.1 信息技术 安全技术 抗抵赖 第1部分：概述 (GB/T 17903.1—2024, ISO/IEC 13888-1:2020, MOD)

GB/T 20520 网络安全技术 公钥基础设施 时间戳规范

ISO/IEC 29192-4 信息技术 安全技术 轻量级密码学 第4部分：使用非对称技术的机制 (Information technology—Security techniques—Lightweight cryptography—Part 4:Mechanisms using asymmetric techniques)

3 术语和定义

GB/T17903.1 及 GB/T 20520 界定的以及下列术语和定义适用于本文件。

3.1

时间公证服务 time-marking service

提供用于证明某条记录发生早于特定时间点的证据的服务。

注：该证据包含一个杂凑码以及所使用的杂凑函数的标识符。

4 符号

- GB/T17903.1 界定的以及下列符号适用于本文件。
- A 消息原发者
 - B 消息接收者或期待的消息接收者 B
 - C 可信第三方
 - D_i 第 i 个交付机构，交付机构属于可信第三方，其中 $1 \leq i \leq n$ 表示系统中交付机构的顺序编号
 - f_i 标明抗抵赖服务类型的数据项(标记)($i \in \{ \text{原发, 交付, 提交, 传输} \}$)
 - ID₄, ID, IDc, IDp; 实体A、B、C、D_i 的区分性标识符
 - Imp(y) 数据串y 的印迹，或者是数据串y 的杂凑码(及使用的杂凑函数的标识符)，或者是数据串y 本身
 - m 实体 A 发送给实体B 的消息，抗抵赖服务针对该消息提供
 - NRDT 交付抗抵赖令牌
 - NROT 原发抗抵赖令牌
 - NRST 提交抗抵赖令牌
 - NRTT 传输抗抵赖令牌
 - Pol 适用于证据的抗抵赖策略的区分性标识符
 - Q 包含附加信息的可选数据项，例如：消息m、签名机制或杂凑函数的区分性标识符
 - 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
 - T. 证据生成的日期和时间
 - T_i 第 i 类事件或动作发生的日期和时间(i 为抗抵赖类型， $i \in \{1, 2, 3, 4\}$)
 - text_i 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($i \in \{1, 2, 3, 4, 5, 6\}$)
 - X, Y 指代实体名称的变量
 - (y, z) y 与x 的串接

5 要求

- 下列要求适用于本文件中抗抵赖交换所涉及的实体。
- 抗抵赖交换中的实体应信任同一个可信第三方。
 - 实体的签名密钥应由该实体秘密持有。
 - 所有实体应就数据印迹的生成方式达成一致。包括：使用全等映射函数或符合密码相关国家和行业标准要求的抗碰撞杂凑函数等。
 - 所用数字签名机制应满足策略所规定的安全要求。
 - 在证据生成之前，证据生成者应了解以下三件事情：验证者接受的抗抵赖策略、所要求的证据类型以及验证者接受的机制集合。
 - 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。
 - 证据生成者和证据验证者之一应使用可信时间戳或时间公证服务。
 - 本文件规定的机制中使用的数字签名应为基于证书的数字签名，不应使用基于标识的数字签名。

6 可信第三方的参与

根据所使用的机制和有效的抗抵赖策略，抗抵赖服务的提供可能需要可信第三方的参与。一个可信第三方可能会担当下列角色中的一个或多个。

- 交付机构，被信任用于将消息交付给预定的接收者，并提供提交抗抵赖令牌或者传输抗抵赖令牌。
- 使用非对称密码技术时至少需要一个可信第三方的参与，以确保公开验证密钥的真实性，参见 GB/T 16264.8—2005。
- 有效的抗抵赖策略可能要求部分或全部证据由可信第三方生成。
- 时间戳机构，用于提供可信时间戳。TSA 也可用于保证抗抵赖令牌在签署该令牌的密钥泄漏或者撤消之后仍然是有效的。
- 时间公证服务，用于证实令牌中的签名生成于特定事件之前。
- 证据记录机构，用于记录证据，供将来解决争议时进行证据提取。

可信第三方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。

7 数字签名

本文件规定的抗抵赖机制使用数字签名来创建抗抵赖令牌。当使用数字签名机制时，应遵循密码相关国家和行业标准。对于带消息恢复的数字签名、带附录的数字签名和轻量级数字签名机制，还应分别遵循GB/T15851（所有部分）、GB/T17902（所有部分）和ISO/IEC 29192-4 中的要求。

用于校验签名的公钥应包含于一个公钥数字证书中，该数字证书应包含有效期。

即使抗抵赖令牌中的签名对应的验证密钥的证书过期，抗抵赖机制也应确保签名验证能够有效进行，为了实现这一性质，应使用时间戳服务或时间公证服务，见第11章。第11章中描述的机制应用于保证当用于验证抗抵赖令牌签名的证书过期，或如果该证书被撤销时，抗抵赖令牌仍然有效。

8 抗抵赖令牌

在无第三方交付机构参与时，各种抗抵赖令牌的使用方法见图1。与图1中模型相关的各类型的抗抵赖令牌的详细定义见第9章。其中用于生成 NROT 和NRDT 的可信第三方C 是可选的。

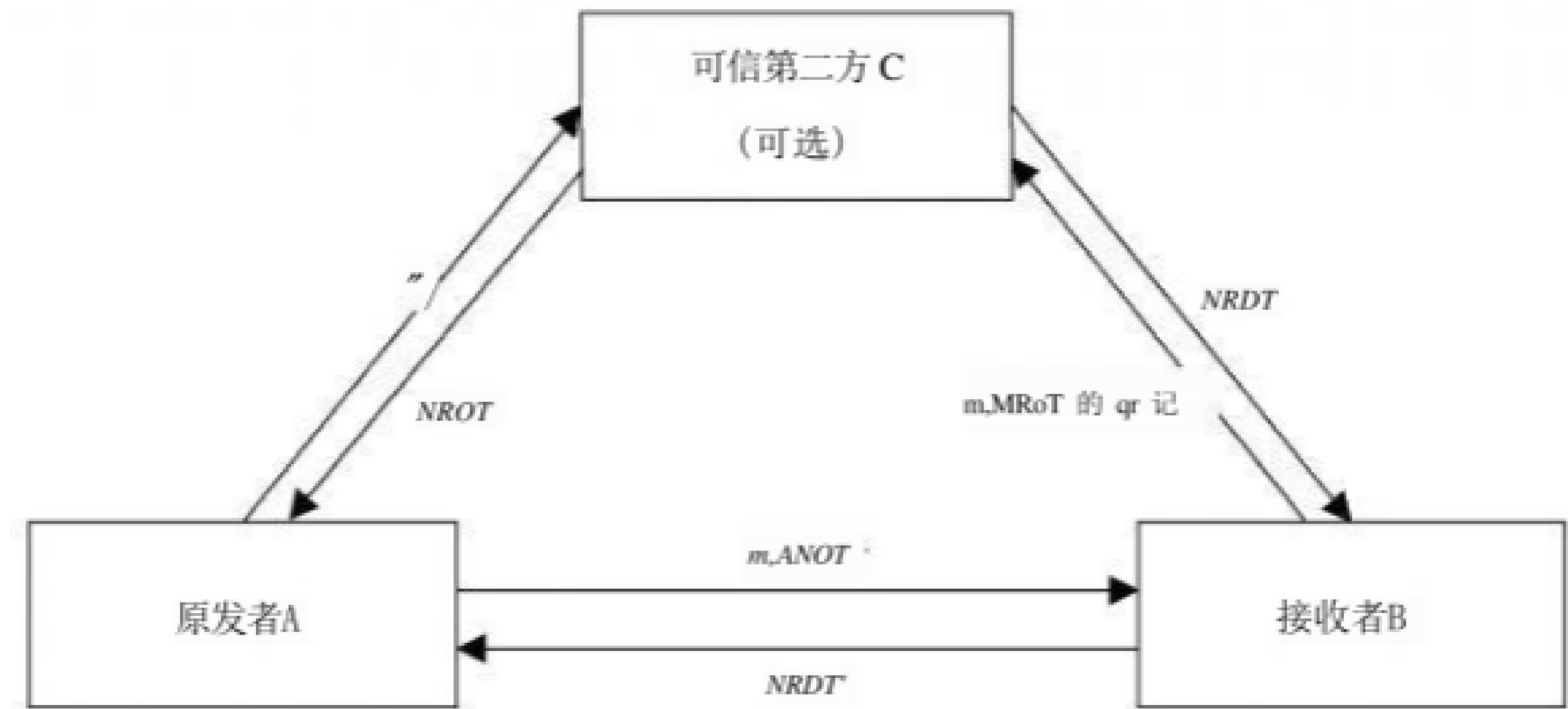


图 1 无交付机构参与时的抗抵赖令牌

在有第三方交付机构参与时，各种抗抵赖令牌的使用方法见图2。与图2中模型相关的各类型的抗抵赖令牌的定义见第10章。

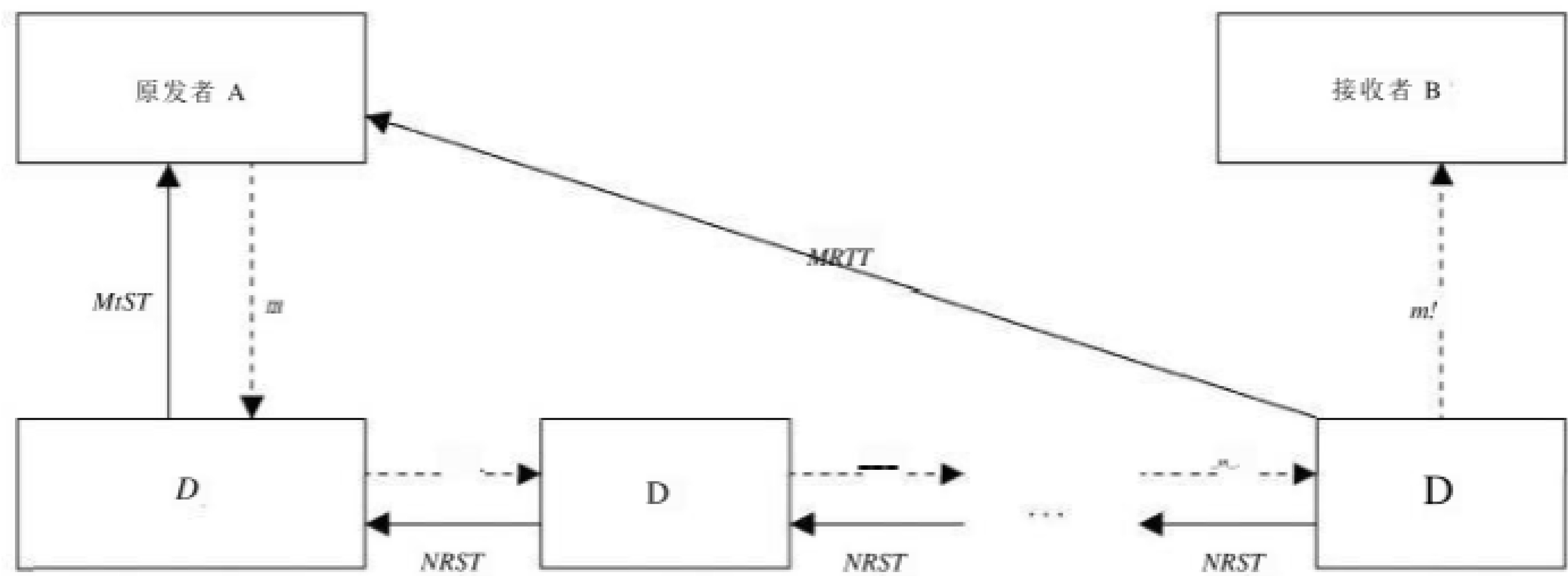


图 2 有交付机构参与时的抗抵赖令牌

9 由终端实体生成证据的机制

9.1 一般规则

本章规定的抗抵赖机制允许在没有交付机构参与的情况下生成原发抗抵赖和交付抗抵赖证据。实体 A 欲发送消息 m 给实体 B，则实体 A 就成为抗抵赖传输的原发者，实体 B 为接收者(见图1)。

对于本章规定的机制，假定实体 A 知道自己的签名密钥，实体 B 也知道自己的签名密钥，并且所有相关实体都知道对应的验证密钥。

如果机制中包含可选的可信第三方 C，C 应保存其生成的所有 NROT，并记录每个 NROT 是否用于生成 NRDT。

本章将描述两种类型的抗抵赖机制：原发抗抵赖机制(9.2)和交付抗抵赖机制(9.3)。

9.2 原发抗抵赖机制

9.2.1 原发抗抵赖令牌

原发抗抵赖令牌用于防止原发者否认其已经发送的消息。

NROT 具有以下性质：

- 由消息 m 的原发者 A 或可信第三方 C 生成；
- 由原发者 A 发送给接收者 B；
- 验证后由接收者 B 存储。

NROT 的结构为：

$$NROT = (text_1, x_1, SIG_4(z_1))$$

其中

$$x_1 = (Pol, fotgin, IDa, ID\mu, IDc, Tg, T_1, Q, Imp(m))$$

NROT 所需数据字段信息 x_1 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_{origin} 标明原发抗抵赖的标记；
- IDa 消息 m 的原发者的区分性标识符；
- ID 消息 m 的预定接收者的区分性标识符(可选项)；

<i>IDc</i>	所涉及机构的区分性标识符(可选项), 如果令牌由可信第三方C 生成, 那么本数据项是强制的, 且NROT 中的签名SIGA(x1) 应替换为 SIGc(x ₁);
<i>Tg</i>	NROT 生成的日期和时间, 取决于令牌的生成者;
<i>T₁</i>	消息m 发送的日期和时间, 取决于原发者(可选项);
<i>Q</i>	包括附加信息的可选数据项, 如消息 m、签名机制或杂凑函数的区分性标识符, 以及有关证书和公开密钥合法性的信息;
<i>Imp(m)</i>	消息m 的印迹, 由消息m 或者m 的杂凑码(及使用的杂凑函数的标识符)构成。

9.2.2 原发抗抵赖令牌机制

原发抗抵赖令牌由消息的原发者A 生成, 并发送给消息的接收者B。

步骤: 从A 到B

- a) 如果使用可信第三方C(可选), 则:
 - 1) A 请求C 为消息m 生成NROT;
 - 2) C 接收消息m 并检查其作为NROT 请求的有效性;
 - 3) C 生成如9.2.1所规定的 NROT;
 - 4) C 将 NROT 发送给A 并保存NROT 的副本;
 - 5) A 从 C 处接收到 NROT。

否则, A 直接生成如9.2.1 所规定的 NROT。

- b) A 将 NROT (与消息 m 一起)发送给 B;
B 按照如下操作检查 NROT 及其内容的有效性:
 - NROT 中数据项类型与值的有效性, 以及;
 - NROT 中签名的有效性。

如果上述校验均通过, 则 B 留存NROT 作为原发抗抵赖的证据。

9.3 交付抗抵赖机制

9.3.1 交付抗抵赖令牌

交付抗抵赖令牌用于防止接收者否认其已经接收到消息m 并认可消息的内容。

NRDT 具有以下性质:

- 由消息m 的接收者B 或可信第三方C 生成;
- 由接收者B 发送给原发者A 及其他相关实体;
- 验证后由原发者 A 存储。

NRDT 的结构为:

NRDT = (text₂, x₂, SIGg(x₂))

其中,

≈2=(Pol,fathey,IDA,IDμ,IDc,T₄,T₂,Q,Imp(m))。

NRDT 所需数据字段信息z₂ 包括以下数据项:

<i>Pol</i>	适用于证据的抗抵赖策略的区分性标识符;
<i>f_{delivery}</i>	标明交付抗抵赖的标记;
<i>ID₄</i>	B 声称的消息m 的原发者的区分性标识符(可选项);
<i>IDβ</i>	消息 m 的预定接收者的区分性标识符;
<i>IDc</i>	所涉及机构的区分性标识符(可选项);如果令牌由可信第三方C 生成, 那么本数据项是强制的, 且 NRDT 中的签名 SIGg(x ₂) 应替换为 SIGc(x ₂);

- T_g NRDT 生成的日期和时间, 取决于令牌的生成者;
- T_1 消息 m 接收的日期和时间, 取决于接收者(可选项);
- Q 包括附加信息的可选数据项, 如消息 m 、签名机制或杂凑函数的区分性标识符, 以及有关证书和公开密钥合法性的信息;
- $Imp(m)$ 消息 m 的印迹, 由消息 m 或 m 的杂凑码(及使用的杂凑函数的标识符)构成。

9.3.2 交付抗抵赖令牌机制

交付抗抵赖令牌由消息的接收者 B 在接收到消息 m 后生成, 并发送给消息的原发者 A 。

步骤1: 从实体 A 到实体 B

A 向 B 发送消息 m 并请求NRDT。

步骤2: 从实体 B 到实体 A

- a) B 接收消息 m , 校验 NRDT 请求的有效性。
- b) 如果使用可信第三方 C (可选), 则:
 - 1) B 向 C 发送 m 或 $(m, Imp(NROT))$ (如果 A 发送了NROT 且 NROT 由 C 生成), 请求 C 为消息 m 生成NRDT;
 - 2) C 接收消息 m 或 $(m, Imp(NROT))$, 如果NROT 存在, 则 C 校验NROT 由 C 生成且与 NROT 中包含的印迹对应的NRDT 未被生成, 如果校验不通过, C 拒绝NRDT 请求;
 - 3) C 生成如9.3.1所规定的NRDT, 并记录与NRDT 对应的NROT;
 - 4) C 将 NRDT 发送给 B ;
 - 5) B 从 C 处接收到 NRDT。否则, B 直接生成如9.3.1 所规定的 NRDT。
- c) B 将 NRDT 发送给 A 。
 A 按照如下操作检查NRDT 及其内容的有效性:
 - NRDT 中数据项类型与值的有效性, 以及;
 - NRDT 中签名的有效性。如果上述校验均通过, 则 A 留存NRDT 作为 B 接收到消息 m 的证据。

10 由交付机构生成证据的机制

10.1 一般规则

本章规定了一系列由可信的交付机构生成证据的额外证据产生机制。本章中规定的机制可与第9章中规定的机制共同使用, 以满足特定的抗抵赖需求。

本章中使用的提交抗抵赖令牌和传输抗抵赖令牌的概念如下:

- NRST 允许原发者或前一个交付机构得到证据, 证明消息在一个存储与传送系统中已经提交以便进行传递;
- NRTT 允许原发者得到证据, 证明消息已经由交付机构交付给了预定的接收者。

10.2 提交抗抵赖机制

10.2.1 提交抗抵赖令牌

在本机制中, NRST 由交付机构创建。此时证据生成者是交付机构。原发者 A 或前一个交付机构 $X(X$ 可能是 A 或 D_i , 其中 $i \in \{1, 2, \dots, n-1\}$ 中的某一个) 发送消息 m 给交付机构 $Y(Y$ 是 X 的后续代

理，X 为 A 时，Y 指 D_1 , X 为 D_i 时则指 D_i)。交付机构 Y 接收消息 m 后，Y 向 X 发送 NRST，从而

提供证据表明消息已经提交以便向前递送。

NRST 具有以下性质：

- 由交付机构 Y 生成；
- 由交付机构 Y 发送给 X (消息原发者 A 或交付机构 D_i)；
- X 使用 Y 的公钥证书验证 NRST 后，由 X 留存。

对于由 D_i 发送给 D_j 的 NRST，其结构为：

NRST = (text_a, \geq a, SIG_{pi+i}(z₃))

其中，

$\geq g = (Pol, fwbmisim, IDA, IDg, D_1, D_2, \dots, D_i, D+i, Tg, T_3, Q, Imp(m))$ 。

NRST 所需数据字段信息 z₃ 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；
- fsbmisin 标明提交抗抵赖的标记；
- IDA 消息 m 的原发者的区分性标识符(可选项), C 可能验证过标识符籍的合法性，也可能没有验证；
- ID_β 消息 m 的预定接收者的区分性标识符；
- D_i 交付机构, $i \in \{1, 2, \dots, n\}$ (n 为消息传输过程中涉及的交付机构的数量)；
- T_g NRST 生成的日期和时间，取决于令牌的生成者；
- T₃ 消息 m 提交的日期和时间，取决于原发者；
- Q 包括附加信息的可选数据项，如消息 m、签名机制或杂凑函数的区分性标识符，以及有关证书和公开密钥合法性的信息；
- Imp(m) 消息 m 的印迹，由消息 m 或 m 的杂凑码(及使用的杂凑函数的标识符)构成。

10.2.2 提交抗抵赖令牌机制

本机制包含两个步骤。第一步，发送实体 X (X 可能是 A 或 D_i，其中 $i \in \{1, 2, \dots, n-1\}$ 中的某一个) 把消息发送给交付机构 Y (Y 称为 X 的后续代理，X 为 A 时，Y 指 D₁，X 为 D_i 时则指 D_{i+1}) 以向前传递。第二步，交付机构 Y 发送 NRST 给实体 X。提交抗抵赖在步骤 2 建立。

步骤 1: 从实体 X 到交付机构 Y

X 向 Y 发送消息 m 并请求 NRST。

步骤 2: 从交付机构 Y 到实体 X

a) Y 生成如 10.2.1 所规定的 NRST；

b) Y 将 NRST 发送给 X。

X 按照如下操作检查 NRST 及其内容的有效性：

- NRST 中数据项类型与值的有效性，以及；
- NRST 中签名的有效性。

如果上述校验均通过，则 X 留存 NRST 作为 Y 接收到消息 m 的证据。

10.3 传输抗抵赖机制

10.3.1 传输抗抵赖令牌

NRTT 是由消息的原发者使用的证据，以证明消息 m 已经由交付路径中的最终交付机构递送给 B。此时，证据的生成者是图 2 中所示的交付机构 D_j。在此过程中，原发者 A 或交付机构 X 发送消息 m 给下一个交付机构 Y。最终的交付机构 D_j 把消息 m 递送给接收者 B，然后向消息的原发者 A 发送 NRTT，从而提供证据以表明消息 m 已被递送给 B。

- NRTT 具有以下性质：
- 由交付机构 D_i 生成；
 - 由 D_i 发送给原发者 A；
 - 验证后由原发者 A 存储。

NRTT 的结构为：
 $NRTT = (text_4, \geq_4, SIGp(x_4))$

其中，
 $\geq_4 = (Pol, fmmgoa, ID_4, IDg, D_1, D_2, \dots, D_7, T_4, T_4, Q, Imp(m))$ 。

- NRTT 所需数据字段信息 \approx 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... 标明传输抗抵赖的标记；
 - ID 消息 m 的原发者的区分性标识符(可选项)；
 - ID β 消息 m 的预定接收者的区分性标识符；
 - D $_i$ 交付机构， $i \in \{1, 2, \dots, n\}$ (n 为消息传输过程中涉及的交付机构的数量)；
 - T $_o$ NRTT 生成的日期和时间，取决于令牌的生成者；
 - T $_4$ 消息 m 接收的日期和时间，取决于接收者(可选项)；
 - Q 包括附加信息的可选数据项，如消息 m、签名机制或杂凑函数的区分性标识符，以及有关证书和公开密钥合法性的信息；
 - Imp(m) 消息 m 的印迹，由消息 m 或者 m 的杂凑码(及使用的杂凑函数的标识符)构成。

10.3.2 传输抗抵赖令牌机制

本机制包含三个步骤。第一步，发送实体 X(X 可能是 A 或 D_i ，其中 $i \in \{1, 2, \dots, n-1\}$ 中的某一个)把消息 m 发送给交付机构 Y(X 的后续代理，X 为 A 时，Y 指 D_1 ，X 为 D_i 时则指 D_{i+1}) 以向前传递。第二步， D_n 发送消息给接收者 B。第三步， D_n 生成 NRTT 并发送给消息 m 的原发者，即实体 A。传输抗抵赖在步骤 3 建立。

- 步骤 1: 从实体 X 到交付机构 Y
- X 向 Y 发送消息 m。
- 步骤 2: 从交付机构 D_i 到实体 B
- D_i 向 B 发送消息 m。
- 步骤 3: 从交付机构 D_n 到实体 A
- a) D_n 生成如 10.3.1 所规定的 NRTT。
 - b) D_n 将 NRTT 发送给 A。
 - c) A 按照如下操作检查 NRTT 及其内容的有效性：
 - NRTT 中数据项类型与值的有效性，以及；
 - NRTT 中签名的有效性。
 - d) 如果上述校验均通过，则 A 留存 NRTT 作为消息 m 已交付至预定接收者 B 的证据。

11 时间保证机制

11.1 一般规则

本文件规定的所有抗抵赖令牌均经过数字签名，由于在证书过期后，CA 不再处理该证书的撤销状态，但 NRT 仍可能被验证，因此需要表明 NRT 中签名的生成时间处于证书有效期内，即 NRT 中的签

名是在证书仍有效时生成的。

如果用于对NRT 进行签名的证书被撤销，需要表明NRT 中签名的生成时间早于证书被撤销的时间。实现的方式包括：采用在 NRT 上应用时间戳令牌或使用时间公证等，时间印记是指安全审计踪迹中包含签名、签名的杂凑值及所使用的杂凑函数标识符的记录；

时间戳和时间公证机制保证 NRT 在以下情况中能够被有效验证：

- a) 用于验证 NRT 中签名的证书过期；
- b) 用于验证 NRT 中签名的证书被撤销。

11.2 采用时间戳的机制

如果采用时间戳机制，实体(请求者)与 TSA 间的通信应符合 GB/T 20520 中的规定。

11.3 采用时间公证服务的机制

使用时间公证服务来实现时间保证机制时，实体 X 与时间公证服务间的通信应通过具有数据源鉴别和完整性保护性质的安全通信信道进行。并遵循以下步骤。

请求者 X 生成待进行时间保证的 NRT 中签名的杂凑值，并附加杂凑函数的标识符，在本节中，这一由杂凑值和杂凑算法标识符组成的数据记作y。

本机制包含两个步骤。在步骤1中，请求实体X 发送想要进行时间保证的数据y，请求公证证明。步骤2 中，公证机构响应步骤1的请求，返回已证实的数据。

步骤1:从实体 X 到时间保证服务

- a) 实体 X 生成如下形式的请求Req:

$Req = (texts, y)$

texts 可包含：

- 时间公证机构的区分性标识符；
- 获取时间保证的策略；
- 请求者 X 的名称。

- b) 实体X 将Req 发送至时间公证服务。

步骤2:从时间公证服务到实体 X

- a) 时间公证服务校验请求的有效性，并将Req 与从可信时间源获取的时间一同留存；
- b) 时间公证服务将数据 Resp 发送至实体X:

$Resp = (texts, recording\ number)$

texts 可包含：

- 数据y；
- 生成记录时的日期和时间；
- texts 的全部或一部分；
- 时间保证授予策略。

recording number 是一个用于查询时间保证信息的标识，在之后的交互过程中，实体X 或任何授权实体通过提交recording number 获取时间保证信息，包括：

- 数据 y；
- 生成记录时的日期和时间；
- texts 的全部或一部分；
- 时间保证授予策略。

参 考 文 献

- [1] GB/T16264.8—2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架
 - [2] ISO 7498-2:1989 Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2:Security Architecture
 - [3] ISO 8601(所有部分) Date and time—Representations for information interchange
 - [4] ISO/IEC 10118-2 Information technology—Security techniques—Hash-functions—Part 2: Hash-functions using an n-bit block cipher
 - [5] ISO/IEC 10118-3 IT Security techniques—Hash-functions—Part 3:Dedicated hash-functions
 - [6] ISO/IEC10118-4 Information technology—Security techniques—Hash-functions—Part 4: Hash-functions using modular arithmetic
 - [7] ISO/IEC 10181-1:1996 Information technology—Open Systems Interconnection—Security frameworks for open systems:Overview
 - [8] ISO/IEC TR 14516:2002 Information technology—Security techniques—Guidelines for the use and management of trusted third party services
 - [9] ISO 14641 Electronic document management—Design and operation of an information system for the preservation of electronic documents—Specifications
 - [10] ISO/IEC 15945:2002 Information technology—Security techniques—Specification of TTP services to support the application of digital signatures
-

