ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.3—XXXX
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-reputation—

Part 3:Mechanisms using asymmetric techniques

(ISO/IEC 13888-3:2020,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 2
1　范围 3
2　规范性引用文件 3
3　术语和定义 3
4　符号和缩略语 3
4.1　符号 3
4.2　缩略语 4
5　要求 4
6　可信第三方的参与 4
7　数字签名 5
8　抗抵赖令牌 5
9　由终端实体生成证据的机制 6
9.1　概述 6
9.2　原发抗抵赖机制 6
9.3　交付抗抵赖机制 7
10　由交付机构生成证据的机制 8
10.1　概述 8
10.2　提交抗抵赖机制 8
10.3　传输抗抵赖机制 9
11　时间保证机制 10
11.1　概述 10
11.2　采用时间戳的机制 10
11.3　采用时间公证服务的机制 11
参考文献 12

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》。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) 在 5 中增加了关于数字签名的安全性要求，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) 删除了原 5.1 至 5.6 节，改为列项；

d) 将原 8.1、8.2、8.3、8.4 的内容调整为 9.2.1、9.3.1、10.2.1、10.3.1；

e) 增加了 9.1、10.1 概述，以消除悬置段；

f) 新增了 11，11 规定了时间保证机制，包含原 A.1 中的部分内容，删除了原附录 A；

本文件修改采用 ISO/IEC 13888-3:2020《信息技术 安全技术 抗抵赖 第 1 部分：采用非对称技术的机制》。

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

a) 使用对应的国家标准 GB/T 15851 和 GB/T 17902 替代了规范性引用文件 ISO/IEC 9796 和 ISO/IEC 14888，GB/T 15851 和 GB/T 17902 分别规定了带消息恢复的数字签名和带附录的数字签名；

b) 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；

c) 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。

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、张妍、王蕊、刘丽敏、张立廷、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 17903.3-2008；

——本次为第一次修订。

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 15851（所有部分）信息技术 安全技术 带消息恢复的数字签名方案

GB/T 17902（所有部分）信息技术 安全技术 带附录的数字签名

GB/T 17903.1 信息技术 安全技术 抗抵赖 第1部分：概述

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

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

3 术语和定义

GB/T 17903.1中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。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 符号和缩略语

4.1 符号

GB/T 17903.1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 $1 \leqq i \leqq n$ 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）（$i \in$ {原发,交付,提交,传输}）

$ID_A, ID_B, ID_C, ID_{Di}$　　实体 A、B、C、D_i 的可区分标识符
$Imp(y)$　　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可区分标识符
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可区分标识符
$SIG_X(y)$　　实体 X 使用其私有密钥对数据 y 生成的已签名消息
T_g　　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，$i \in \{1,2,3,4\}$）
$text$　　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 z 按顺序的连接

4.2 缩略语

GB/T 17903.1界定的缩略语适用于本文件。

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记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；
——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，可信赖地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。

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前面方案机制，还应分别遵循 GB/T 15851、GB/T 17902 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 11 章。

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如图 1 所示。与图 1 中模型相关的各类型的抗抵赖令牌的详细定义见 9 章。其中用于生成 NROT 和 NRDT 的可信第三方 C 是可选的。

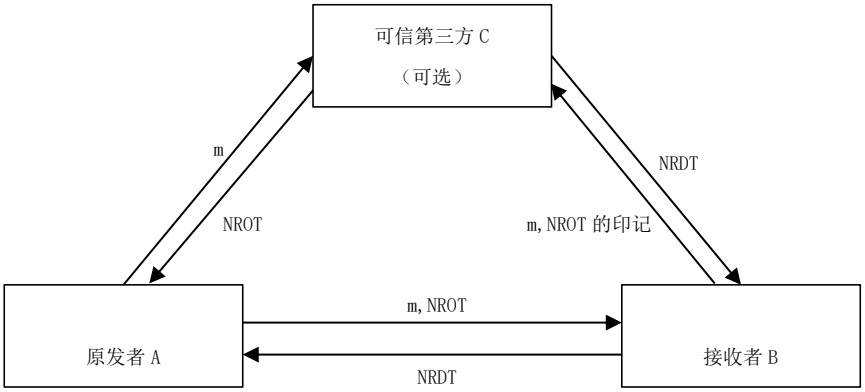

图 1　无交付机构参与时的抗抵赖令牌

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

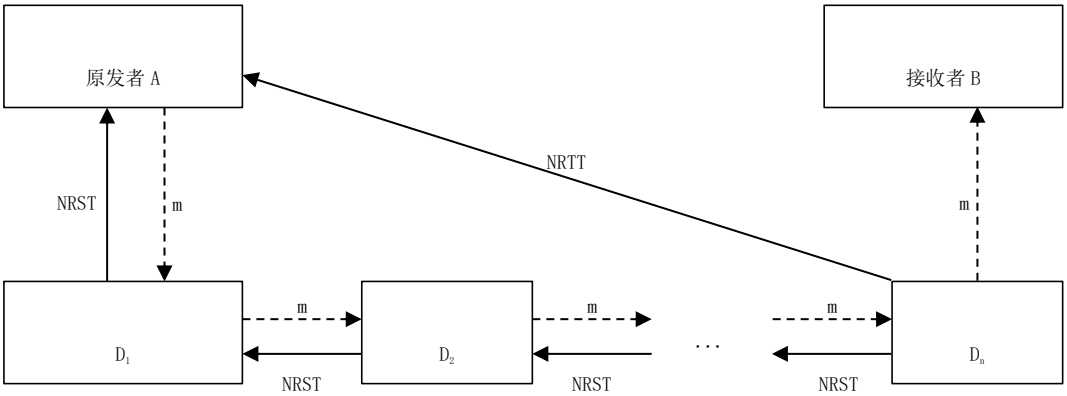

图 2　有交付机构参与时的抗抵赖令牌

9　由终端实体生成证据的机制

9.1　概述

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。如图 1 所示，实体 A 欲发送消息 m 给实体 B，于是实体 A 就成为抗抵赖传输的原发者，实体 B 为接收者。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。

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：

$NROT = (text_1, z_1, SIG_A(z_1))$

其中

$z_1 = (Pol, f_{origin}, ID_A, ID_B, ID_C, T_g, T_1, Q, Imp(m))$

NROT 所需数据字段信息 z_1 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_{origin}　　标明原发抗抵赖的标记

ID_A　　消息 m 的原发者的可区分标识符

ID_B 消息 m 的预定接收者的可区分标识符（可选项）

ID_C 所涉及机构的可区分标识符（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 $SIG_A(z_1)$ 应替换为 $SIG_C(z_1)$

T_g $NROT$ 生成的日期和时间，取决于令牌的生成者

T_1 消息 m 发送的日期和时间，取决于原发者（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可区分标识符，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

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，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；
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 及其它相关实体；

——验证后由原发者 A 存储。

NRDT 的结构为：

$NRDT = (text_2, z_2, SIG_B(z_2))$

其中

$z_2 = (Po1, f_{delivery}, ID_A, ID_B, ID_C, T_g, T_2, Q, Imp(m))$

NRDT 所需数据字段信息 z_2 包括以下数据项：

$Po1$ 适用于证据的抗抵赖策略的可区分标识符

$f_{delivery}$ 标明交付抗抵赖的标记

ID_A B 声称的消息 m 的原发者的可区分标识符（可选项）

ID_B 消息 m 的预定接收者的可区分标识符

ID_C 所涉及机构的可区分标识符（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 $SIG_B(z_2)$ 应替换为 $SIG_C(z_2)$

T_g　　*NRDT* 生成的日期和时间，取决于令牌的生成者

T_I　　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可区分标识符，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*，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* 中包含的印记对应的 *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　概述

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 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 NRST 和 NRTT 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 $i \in \{1,2,\cdots,n-1\}$ 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，对于 X 为 D_i 时则指 D_{i+1})。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+1} 发送给 D_i 的 NRST，其结构为：

$NRST = (text_3, z_3, SIG_{Di+1}(z_3))$

其中

$z_3 = (Pol, f_{submission}, ID_A, ID_B, D_1, D_2, \cdots, D_i, D_{i+1}, T_g, T_3, Q, Imp(m))$

NRST 所需数据字段信息 z_3 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

$f_{submission}$　标明提交抗抵赖的标记

ID_A　消息 m 的原发者的可区分标识符（可选项）,C 可能验证过标识符辖的合法性，也可能没有验证

ID_B　消息 m 的预定接收者的可区分标识符

D_i　交付机构，$i \in \{1,2,\cdots,n\}$

T_g　NRST 生成的日期和时间，取决于令牌的生成者

T_3　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可区分标识符，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

本机制的步骤 1 中，发送实体 X（X 可能是 A 或 D_i，其中 $i \in \{1,2,\cdots,n-1\}$ 中的某一个）把消息发送给交付机构 Y(Y 是 X 的后续代理，X 为 A 时，Y 指 D_1，对于 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_n。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_n 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_n 生成；

——由 D_n 发送给原发者 A；

——验证后由原发者 A 存储。

NRTT 的结构为：

$NRTT = (text_4, z_4, SIG_{Dn}(z_4))$

其中

$z_4 = (Pol, f_{transport}, ID_A, ID_B, D_1, D_2, \cdots, D_n, T_g, T_4, Q, Imp(m))$

NRTT　所需数据字段信息 z_4 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

$f_{transport}$　标明传输抗抵赖的标记

ID_A　消息 m 的原发者的可区分标识符（可选项）

ID_B　消息 m 的预定接收者的可区分标识符

D_i　交付机构，$i \in \{1, 2, \cdots, n\}$

T_g　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可区分标识符，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

本机制的步骤 1 中，发送实体 X 把消息 m 发送给交付机构以向前传递。步骤 2 中，D_n 发送消息给接收者 B。步骤 3 中，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_n 到实体 B

D_n 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；

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；

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　概述

本文件规定的所有 NRT 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，因此需要采用时间保证机制来证明 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。类似地，如果用于对 NRT 进行签名的证书被撤销，同样需要时

间保证机制来描述NRT中签名的生成时间早于证书被撤销的时间。

时间保证机制确保了NRT的有效期在证书过期或被撤销后仍能够被有效验证。

11.2 采用时间戳的机制

可采用时间戳来实现时间保证机制，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。

在本机制的步骤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 = ($text_5$, y)

$text_5$可包含：

——时间公证机构的可区分标识符；

——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 = ($text_6$, recording number)

$text_6$可包含：

——数据y；

——生成记录时的日期和时间；

——$text_5$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或任何授权实体可以通过提交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；

——$text_5$的全部或一部分；

——时间保证授予策略。

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] GB/T 16264.8-2005 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
[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/IEC 10118-4 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 10181-4:1997 Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework — Part 4:
[9] ISO/IEC TR 14516:2002 Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[10] ISO 14641 Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications
[11] ISO/IEC 15945:2002 Information technology — Security techniques — Specification of TTP services to support the application of digital signatures