ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17903.3—2008/ISO/IEC 13888-3:1997
代替 GB/T 17903.3—1999

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 13888-3:1997, IDT)

2008-07-02 发布　　2008-12-01 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。

本部分为 GB/T 17903 的第 3 部分，等同采用 ISO/IEC 13888-3:1997《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》，仅有编辑性修改。ISO/IEC 13888-3:1997 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。

本部分代替 GB/T 17903.3—1999《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》。本部分与 GB/T 17903.2—1999 相比，主要差异如下：

——本部分根据第 1 部分的修订，更改部分术语。

——本部分对部分叙述进行了文字修订，修正了 9.2 中的“NROT”。

本部分的附录 A 是资料性附录。

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 17903.3—1999。

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

抗抵赖服务旨在生成、收集、维护、利用和验证有关已声称事件或动作的证据,以解决有关该事件或动作的已发生或未发生的争议。本部分使用非对称技术规定了用于提供一些特定的、与通信有关的抗抵赖服务机制。

抗抵赖机制可以提供以下四种抗抵赖服务:

a)　原发抗抵赖;

b)　交付抗抵赖;

c)　提交抗抵赖;

d)　传输抗抵赖。

抗抵赖机制涉及到各种抗抵赖服务所规定的抗抵赖权标的交换。抗抵赖权标由数字签名和附加数据组成。抗抵赖权标可作为抗抵赖信息予以存储,以备之后发生争议时使用。

依据特定应用下有效的抗抵赖策略以及该应用操作所处的法律环境,抗抵赖信息可能包括以下附加信息:

a)　包括时间戳机构提供的可信时间戳在内的证据;

b)　公证人提供的证据,以确保动作或事件是由一个或多个实体执行或参与的。

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。

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 16264.8—2005　信息技术　开放系统互连　目录　第8部分:鉴别框架(ISO/IEC 9594-8:2001,IDT)

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 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 17903.1—2008　信息技术　安全技术　抗抵赖　第1部分:概述(ISO/IEC 13888-1:2004,IDT)

3　术语和定义

GB/T 17903.1—2008的术语和定义适用于本部分。

4 符号和缩略语

4.1 符号

A	消息原发者 A 的可区分标识符
B	消息接收者 B 的可区分标识符
f_i	标明抗抵赖服务类型的数据项(标记)
$Imp(y)$	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	实体 A 发送给实体 B 的消息,抗抵赖服务针对该消息提供
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,如消息 m、签名机制或散列函数的可区分标识符
S_X	使用签名算法和实体 X 的私有密钥的签名操作
T_i	事件或动作发生的日期和时间
T_g	证据生成的日期和时间
$text$	包含附加信息的可选数据项,例如密钥标识符和(或)消息标识符
$y \parallel z$	y 和 z 按顺序的连接

4.2 缩略语

DA	Delivery Authority 交付机构,一个可信第三方
NRD	Non-Repudiation of Delivery 交付抗抵赖
NRDT	Non-Repudiation of Delivery Token 交付抗抵赖权标
NRO	Non-Repudiation of Origin 原发抗抵赖
NROT	Non-Repudiation of Origin Token 原发抗抵赖权标
NRS	Non-Repudiation of Submission 提交抗抵赖
NRST	Non-Repudiation of Submission Token 提交抗抵赖权标
NRT	Non-Repudiation of Transport 传输抗抵赖
NRTT	Non-Repudiation of Transport Token 传输抗抵赖权标
TSA	Time-Stamping Authority 时间戳机构
TST	Time-Stamping Token 时间戳权标

5 要求

下列要求适用于本部分中抗抵赖交换所涉及的实体,这些要求与生成抗抵赖权标的基本机制有关,与抗抵赖机制所支持的抗抵赖服务无关。

5.1 抗抵赖交换中的实体应信任同一个可信第三方(TTP),在抗抵赖协议许可下,该 TTP 可以由若干独立的 TTP 组成。

5.2 实体的签名密钥必须由该实体秘密持有。

5.3 所用数字签名机制应该满足策略所规定的安全要求。

5.4 在生成证据之前,证据生成者必须知道证据的生成所应该遵循的抗抵赖策略、证据的类型以及证据的验证机制。

5.5 特定抗抵赖交换中的实体可得到生成或验证证据的机制,或者存在一个可信机构来提供这些机制。

5.6 证据生成者和证据验证者可能需要访问可信时间戳或者公证设施。

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一个或多个角色。

a) 交付机构(DA)可信赖地将消息交付给预定的接收者,并提供提交抗抵赖权标或者传输抗抵赖权标;

b) 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,正如 GB/T 16264.8—2005 所指出的那样;

c) 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;

d) 时间戳机构(TSA)用于提供可信时间戳。TSA 也可用于保证抗抵赖权标在签署该权标的密钥泄漏或者撤消之后仍然是有效的;

e) 公证机构用于证实所涉及的实体、证实所传输的数据,或者用于将现有权标的生命期延长到期满和撤消之后;

f) 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身份参与到抗抵赖的各个过程中。当交换证据时,双方必须都知道或者同意适用于证据的抗抵赖策略。

7 数字签名

抗抵赖权标是使用数字签名创建的。GB 15851—1995 和 GB/T 17902 规定了两种数字签名,即:

a) 带消息恢复的签名,其中验证过程可以恢复消息以及特定的冗余信息。

b) 带附录的签名,其中验证过程需要把消息作为其输入的一部分。

签名机制的选取由采用的策略来决定,本部分不予考虑。

签名算法和密钥有事先定义的生命周期,在证书机构颁发的密钥证书中规定。因此,本部分所定义的权标也有明确的、由抗抵赖策略规定的生命周期。A.2 中描述的机制可用于延长权标的生命期。

8 抗抵赖权标

各种抗抵赖权标的使用方法如图 1 中所示。

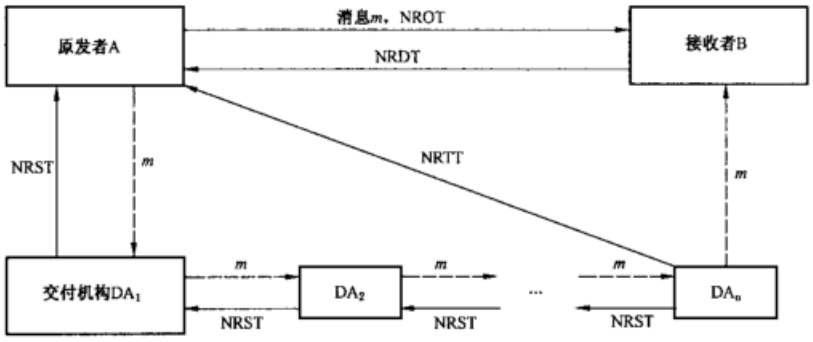

图 1 抗抵赖权标及其应用

8.1 原发抗抵赖(NRO)权标

NRO 权标用于防止原发者否认其已经发送的消息。

NRO 权标:

a) 由消息 m 的原发者 A 或机构 C 生成;

b) 由 A 发送给接收者 B;

c) 验证后由接收者 B 存储。

NRO 权标的结构为:

$$\mathrm{NROT}=text_1 \parallel z_1 \parallel S_A(z_1),\text{其中}$$

$$z_1 = Pol \parallel f_1 \parallel A \parallel B \parallel C \parallel T_g \parallel T_1 \parallel Q \parallel Imp(m)。$$

NRO 权标所需信息 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_1	标明原发抗抵赖的标记
A	消息 m 的原发者的可区分标识符
B	消息 m 的预定接收者的可区分标识符(可选项)
C	所涉及机构的可区分标识符(可选项)。如果权标由机构 C 生成，那么本数据项是强制的，而且 NRO 权标中的签名 $S_A(z_1)$ 应替换为 $S_C(z_1)$
T_g	权标生成的日期和时间，取决于权标的生成者
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、签名机制或散列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 的散列码构成

8.2 交付抗抵赖(NRD)权标

NRD 权标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。

NRD 权标：

a) 由接收者 B(或机构 C)生成；

b) 由 B 发送给包括消息的原发者 A 在内的一个或多个实体；

c) 验证后由这些实体存储。

NRD 权标的结构为：

$$NRDT = text_2 \parallel z_2 \parallel S_B(z_2)，其中$$

$$z_2 = Pol \parallel f_2 \parallel A \parallel B \parallel C \parallel T_g \parallel T_2 \parallel Q \parallel Imp(m)。$$

NRD 权标所需信息 z_2 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_2	标明交付抗抵赖的标记
A	B 声称的消息 m 的原发者的可区分标识符(可选项)
B	消息 m 的接收者的可区分标识符
C	所涉及机构的可区分标识符(可选项)。如果权标由机构 C 生成，那么本数据项是强制的，并且 NRD 权标中的签名 $S_B(z_2)$ 应替换为 $S_C(z_2)$
T_g	权标生成的日期和时间，取决于权标的生成者
T_2	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、签名机制或散列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 的散列码构成

8.3 提交抗抵赖(NRS)权标

NRS 权标由交付机构创建。此时证据生成者是交付机构 DA。原发者 A 或前一个交付机构 X 发送消息 m 给交付机构 DA。交付机构 DA 接收消息 m，并发送 NRS 权标给原发者 A 或前一个传输代理 X，从而提供证据表明消息已经提交以向前递送。

NRS 权标：

a) 由交付机构 DA 生成；

b) 由 DA 发送给消息的原发者 A 或前一个交付机构 X；

c) 验证后由 A 或 X 存储。

NRS 权标的结构为：

$$NRST = text_3 \| z_3 \| S_{DA}(z_3)，其中$$

$$z_3 = Pol \| f_3 \| A \| B \| C \| D \| E \| T_g \| T_3 \| Q \| Imp(m)。$$

NRS 权标所需信息 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_3	标明提交抗抵赖的标记
A	消息 m 的原发者的可区分标识符(可选项)，DA 可能验证过标识符 A 的合法性，也可能没有验证
B	消息 m 的预定接收者的可区分标识符
C	交付机构(DA)的可区分标识符
D	交付机构 X 的可区分标识符(如果存在)
E	交付机构 Y 的可区分标识符(如果存在)
T_g	权标生成的日期和时间，取决于权标的生成者
T_3	消息 m 提交的日期和时间，取决于权标的生成者
Q	包括附加信息的可选数据项，如消息 m、签名机制或散列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 的散列码构成

8.4 传输抗抵赖(NRT)权标

NRT 权标是由消息的原发者使用的证据，以证明消息 m 已经由交付机构 DA 递送给 B。此时，证据的生成者是交付机构 DA。原发者 A 或前一个交付机构 X 发送消息 m 给交付机构 DA。交付机构 DA 把消息 m 递送给接收者 B 或下一个交付机构。将消息 m 递送给接收者 B 的交付机构 DA 发送 NRT 权标给消息 m 的原发者 A，从而提供证据以表明消息 m 已被递送给 B。

NRT 权标：

a) 由交付机构 DA 生成；

b) 由 DA 发送给消息的原发者 A；

c) 验证后由 A 存储。

NRT 权标的结构为：

$$NRTT = text_4 \| z_4 \| S_{DA}(z_4)，其中$$

$$z_4 = Pol \| f_4 \| A \| B \| C \| D \| T_g \| T_4 \| Q \| Imp(m)$$

NRT 权标所需信息 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_4	标明传输抗抵赖的标记
A	消息 m 的原发者的可区分标识符(可选项)，DA 可能验证过标识符 A 的合法性，也可能没有验证
B	消息 m 的预定接收者的可区分标识符
C	交付机构 DA 的可区分标识符
D	交付机构 X 的可区分标识符，如果存在(可选项)
T_g	权标生成的日期和时间，取决于权标的生成者
T_4	消息交付的日期和时间，取决于权标的生成者
Q	包括附加信息的可选数据项，如消息 m、签名机制或散列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 的散列码构成

9 不使用交付机构的机制

本章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(NRO)和交付抗抵赖

(NRD)证据。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。

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。

下面描述两种抗抵赖机制。

9.1 原发抗抵赖机制

原发抗抵赖(NRO)权标由消息的原发者 A 生成,并发送给消息的接收者 B。

步骤:从实体 A 到实体 B

a) 实体 A 生成 8.1 规定的 NRO 权标;

b) 实体 A 发送 NRO 权标(与消息 m 一起)给实体 B。

实体 B 检验 NRO 权标及其内容的有效性。如果是有效的,则存储 NRO 权标作为原发抗抵赖的证据;如果是无效的,实体 B 要求 A 重新发送 NRO 权标。

9.2 交付抗抵赖机制

交付抗抵赖(NRD)权标由消息的接收者 B 生成,B 在收到消息 m 后把 NRD 权标发送给原发者 A。

步骤 1:从消息的原发者 A 到消息的接收者 B

实体 A 向 B 发送消息 m 并请求 NRD 权标。

步骤 2:从实体 B 到实体 A

a) 实体 B 接收消息 m 并验证该 NRD 权标请求的有效性;

b) 实体 B 生成 8.2 规定的 NRD 权标;

c) 实体 B 发送 NRD 权标给实体 A;

d) 实体 A 检验 NRD 权标及其内容的有效性。如果是有效的,则存储 NRD 权标作为 B 已经接收到消息 m 的证据;如果是无效的,实体 A 要求 B 重新发送 NRD 权标。

10 使用交付机构的机制

在抗抵赖过程中有许多其他机制使用可信第三方。这些机制结合第 9 章的基本机制,可满足安全策略的要求。

交付机构在发布抗抵赖(NRS/NRT)权标时,使用术语"提交"或"传输"。

a) NRS 权标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;

b) NRT 权标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。

10.1 提交抗抵赖机制

本机制的第一步,发送实体 X 把消息发送给交付机构 DA 以向前传递。第二步,交付机构发送 NRS 权标给实体 X。提交抗抵赖在第二步建立。

步骤 1:从实体 X 到交付机构 DA

实体 X 发送消息 m 给 DA 并向 DA 请求 NRS 权标。

步骤 2:从 DA 到实体 X

a) DA 生成 8.3 规定的 NRS 权标;

b) DA 向实体 X 发送 NRS 权标;

c) 实体 X 检验 NRS 权标及其内容。如果是有效的,则存储 NRS 权标作为提交抗抵赖(即消息已经提交)的证据。

10.2 传输抗抵赖机制

本机制的第一步,发送实体 X 把消息发送给交付机构以向前传递。第二步,DA 发送消息给接收者 B。第三步,DA 生成 NRT 权标并发送给消息 m 的原发者,即实体 A。传输抗抵赖在第三步建立。

步骤 1:从实体 X 到交付机构 DA

实体 X 发送消息 m 给 DA。

步骤 2:从交付机构 DA 到实体 B

DA 发送消息 m 给实体 B。

步骤 3:从交付机构 DA 到实体 A

a) DA 生成 8.4 规定的 NRT 权标;

b) DA 发送 NRT 权标给实体 A;

c) 实体 A 验证 NRT 权标及其内容。如果是有效的,则存储 NRT 权标作为传输抗抵赖(即消息已经交付给预定的接收者 B)的证据。

附 录 A
（资料性附录）
其他抗抵赖服务机制

根据特定应用的有效抗抵赖策略和该应用操作所处的法律环境，可能需要以下机制来完成抗抵赖服务：

a) 时间戳服务机制，提供包含可信时间戳（由时间戳机构生成）在内的证据；

b) 公证服务机制，提供证据以确保所执行的事件或动作；

c) 证据记录服务机制，以维护某操作的记录，供将来解决争执时恢复证据。

A.1 时间戳服务机制

本章中，TTP 通过生成时间戳权标（TST）的方式提供时间戳服务。如果需要可信的时间参照，而权标生成者提供的时钟又不可信，就需要依赖一个可信第三方，即时间戳机构（TSA），其职责是对消息进行会签，建立进一步的证据以表明签名是何时生成的。

时间戳服务也可用于保证：即使用于签署权标的密钥已经泄漏或撤消，抗抵赖权标依然是有效的。

本机制的第一步，请求实体 X 发送数据 y 请求时间戳服务，希望对数据 y 和时间戳进行会签，其中数据 y 可以是消息、抗抵赖权标、消息的散列码、权标的散列码，或者用户希望与时间戳进行会签的任何数据。第二步，时间戳机构响应第一步的请求，发送对数据 y 的时间戳的会签。

步骤 1：从实体 X 到时间戳机构 TSA

a) 实体 X 形成请求 R：

$$R = text \parallel y,$$

其中 $text$ 包括：标明 R 为时间戳服务请求的标记、请求者 X 的可区分标识符、TSA 的可区分标识符、请求策略；

b) 实体 X 把该请求发送给 TSA。

步骤 2：从 TSA 到实体 X

a) TSA 生成时间戳权标（TST）

$$\mathrm{TST} = text \parallel w \parallel S_{TSA}(w),$$

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	标明时间戳权标的标记
TSA	时间戳机构的可区分标识符
T_g	证据生成的日期和时间
Q	需要保护的可选信息，如数据 y、签名机制或者散列函数的可区分标识符，以及有关证书和公开密钥有效性的信息
$Imp(y)$	数据 y 的印迹，由数据 y 或者 y 的散列码构成；

b) TSA 发送 TST 给实体 X；

c) 实体 X 验证 TST。

A.2 公证服务机制

公证服务是由公证机构提供的证据，以证实有关实体和通信数据的性质，并且将现有权标的生命期

延长到期满和撤消之后。

本机制的第一步，请求实体 X 发送想要证实的数据 y，请求公证证明，其中数据 y 可以是消息、抗抵赖权标、消息的散列码、权标的散列码，或者用户希望得到公证机构证实的任何数据。第二步，公证机构响应第一步的请求，返回已证实的数据。

步骤 1：从实体 X 到公证机构

a) 实体 X 形成请求 R：

$$R = text \parallel y。$$

这里 $text$ 可包括：标明 R 为公证服务请求的标记、实体 X 的可区分标识符、公证机构的可区分标识符、以及请求生成的日期和时间；

b) 实体 X 向公证机构发送请求 R 和已签名的请求 $S_X(R)$。

步骤 2：从公证机构到实体 X

a) 公证机构检查该请求的有效性；

b) 公证机构向实体 X 发送已证实数据的公证权标(NT)

$$\mathrm{NT} = text \parallel w \parallel S_{NA}(w),$$

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	实体 X 的可区分标识符
NA	公证机构的可区分标识符
T_g	证据生成的日期和时间
Q	需要保护的可选数据，如数据 y、签名机制或者散列函数的可区分标识符，以及有关证书和公开密钥有效性的信息
$Imp(y)$	数据 y 的印迹，由数据 y 或者数据 y 的散列码构成；

c) 实体 X 检查已证实的数据并存储这些数据。

A.3 证据记录服务机制

证据记录服务可保存操作的记录，用于将来解决争议时恢复数据。证据所有者信任证据记录机构能够记录并安全地保存数据。

本机制的第一步，请求实体 X 发送希望记录的证据 y(可以是消息或者抗抵赖权标)请求证据记录服务。第二步，证据记录机构响应第一步的请求，返回确认信息。

步骤 1：从实体 X 到证据记录机构

a) 实体 X 生成请求 R：

$$R = text \parallel y;$$

其中 $text$ 包括：R 为证据记录服务请求的标记、证据生成者的可区分标识符、请求者 X 的可区分标识符、证据记录机构的可区分标识符，以及请求生成的日期和时间；

b) 实体 X 向证据记录机构发送请求 R 和已签名的请求 $S_X(R)$。

步骤 2：从证据记录机构到实体 X

a) 证据记录机构检查请求的有效性，然后安全地保存正确的时间参照和 R；

b) 证据记录机构向实体 X 发送确认信息；

$$确认信息 = text \parallel 记录号码；$$

其中 *text* 包括：标明数据是证据记录服务的确认信息的数据项、请求 R 的全部或部分信息、适用于证据的策略、证据记录的日期和时间、证据记录机构的签名。