ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 15843.3—2023/ISO/IEC 9798-3:2019
代替 GB/T 15843.3—2016

# 信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制

**Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques**

（ISO/IEC 9798-3:2019,IT Security techniques—Entity authentication—Part 3:Mechanisms using digital signature techniques,IDT）

2023-03-17 发布　　2023-10-01 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 15843《信息技术　安全技术　实体鉴别》的第3部分。GB/T 15843已经发布了以下部分:

——第1部分:总则;

——第2部分:采用对称加密算法的机制;

——第3部分:采用数字签名技术的机制;

——第4部分:采用密码校验函数的机制;

——第5部分:使用零知识技术的机制;

——第6部分:采用人工数据传递的机制。

本文件代替GB/T 15843.3—2016《信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制》,与GB/T 15843.3—2016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“符号与缩略语”(见第4章);

b) 增加了“通则”(见第5章);

c) 增加了“单向鉴别”(见8.2);

d) 增加了“七次传递鉴别”(见8.3.4);

e) 增加了“使用指南”(见附录B)。

本文件等同采用ISO/IEC 9798-3:2019《IT安全技术　实体鉴别　第3部分:采用数字签名技术的机制》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系协调,将标准名称改为《信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制》;

——为符合我国技术表达习惯,将TP(第三方)统一改为TTP(可信第三方);

——为方便理解,分别在5.1、8.1、8.2.1增加了资料性说明的注。

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:西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、国家信息技术安全研究中心、中国移动通信集团有限公司、中能融合智慧科技有限公司、中国南方电网有限责任公司、北京数字认证股份有限公司、中国科学院软件研究所、公安部第一研究所、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、广西大学、中国广播电视网络集团有限公司、广西诚新慧创科技有限公司、格尔软件股份有限公司、广西通量能源技术有限公司、中国通用技术研究院、北京计算机技术及应用研究所。

本文件主要起草人:曹军、杜志强、张璐璐、王宏、陈宇、李琴、黄振海、王月辉、张变玲、铁满霞、张阳、王力、侯鹏亮、胡霄亮、郑骊、沙学松、赖晓龙、赵晓荣、颜湘、张国强、陈宝仁、张立武、张严、蒋才平、简练、周涛、李冬、李国友、陶洪波、尹玉昂、罗鹏、邓开勇、卢泉、李爽、韦利娜、郑强、韦昌才、刘科伟、于光明、王锐、李玉娇、朱正美、赵慧、贾嘉、刘鸿运、何双羽、李楠、井经涛、潘琪、陈维刚、白琨鹏、张芝军、孙硕、陈晓龙、芦亮、郭金发、田玉存。

本文件及其所代替文件的历次版本发布情况为:

——1998年首次发布为GB/T 15843.3—1998,2008年第一次修订,2016年第二次修订;

——本次为第三次修订。

# 引　言

本文件规定采用数字签名技术的实体鉴别机制，分为单向鉴别和双向鉴别两类。其中单向鉴别按照消息传递的次数，分为一次传递鉴别、两次传递鉴别和四次传递鉴别；双向鉴别根据消息传递的次数，分为两次传递鉴别、三次传递鉴别、五次传递鉴别和七次传递鉴别。

GB/T 15843 旨在规范实体鉴别技术，由 6 部分组成。

——第 1 部分：总则。目的在于规范实体鉴别技术的模型、框架以及通用要求。

——第 2 部分：采用对称加密算法的机制。目的在于规范六种基于对称加密算法的实体鉴别机制及关要求。

——第 3 部分：采用数字签名技术的机制。目的在于规范十种基于数字签名技术的实体鉴别机制及相关要求。

——第 4 部分：采用密码校验函数的机制。目的在于规范四种基于密码校验函数的实体鉴别机制及相关要求。

——第 5 部分：使用零知识技术的机制。目的在于规范五种基于零知识技术的实体鉴别机制及相关要求。

——第 6 部分：采用人工数据传递的机制。目的在于规范八种基于人工数据传递的实体鉴别机制及相关要求。

由于签名所使用的证书分发方式超出本文件范围，证书的发送在所有机制中是可选的。

本文件的发布机构提请注意，声明符合本文件时，可能涉及与第 8 章相关的 CN201510654832.X、US10，652，029B2、JP6543768B2、EP16853050.9、KR10-2107918、CN200910024191.4、US8，751，792B2、JP5425314B2、EP2472772、KR10-1405509、CN200910023774.5、CN200910023735.5、US8，763，100B2、JP5468138B2、KR10-1471259、CN200910023734.0、US8，732，464B2、JP5468137B2、KR10-1471827、CN200810150949.4、CN200810150951.1、CN200710199241.3、US8，417，955B2、JP5323857B2、KR10-1139547、RU2445741C2、CN200710018920.6、US8，356，179B2、EP2214429B1、JP5099568B2、KR10-1117393、RU2458481C2、CN201510654785.9、US10，615，978B2、JP6687728、EP16853041.8、KR10-2141289、CN201510654784.4 等专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

上述专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。上述专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：王丽珍

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

# 信息技术　安全技术　实体鉴别
# 第3部分:采用数字签名技术的机制

## 1　范围

本文件规定了两类采用数字签名技术的实体鉴别机制。第一类不引入在线可信第三方,包括两种单向鉴别机制和三种双向鉴别机制;第二类引入在线可信第三方,也包括两种单向鉴别机制和三种双向鉴别机制。

本文件适用于指导采用数字签名技术的实体鉴别机制的研究,以及相关产品和系统的研发与应用。

附录A定义了本文件规范的实体鉴别机制的对象标识符。

## 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 15843.1—2017　信息技术　安全技术　实体鉴别　第1部分:总则(ISO/IEC 9798-1:2010,IDT)

ISO/IEC 9796(所有部分)　信息技术　安全技术　带消息恢复的数字签名方案(Information technology—Security techniques—Digital signature schemes giving message recovery)

注:GB/T 15851.3—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)

ISO/IEC 14888(所有部分)　信息技术　安全技术　带附录的数字签名(Information technology—Security techniques—Digital signatures with appendix)

注:GB/T 17902.2—2005　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/T 17902.3—2005　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)

## 3　术语和定义

下列术语和定义适用于本文件。

3.1

**原子性业务　atomic transaction**

不能再进一步拆分为多个更小业务的业务。

3.2

**声称方　claimant**

被鉴别的实体本身或者为了实现验证目标的某代表性实体。

注:声称方拥有鉴别交换时所需的参数和私有数据。

[来源:GB/T 15843.1—2017,3.6]

3.3

**数字签名　digital signature**

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，以使数据单元的接收者能够验证数据单元的来源和完整性。

3.4

**实体鉴别　entity authentication**

证实一个实体就是所声称的实体。

[来源：GB/T 15843.1—2017，3.14]

3.5

**双向鉴别　mutual authentication**

为参与的双方提供相互身份证实的实体鉴别。

3.6

**令牌　token**

包含经过密码技术变换后的数据字段的消息。

3.7

**可信第三方　trusted third party**

在网络安全相关活动中，被参与实体所信任的安全机构或其代理。

注：GB/T 15843.1—2017 中指出，可信第三方在实体鉴别过程中被声称方和(或)验证方所信任。

[来源：GB/T 15843.1—2017，3.38，有修改]

3.8

**单向鉴别　unilateral authentication**

仅为其中一方提供对另一方身份证实的实体鉴别。

[来源：GB/T 15843.1—2017，3.39，有修改]

3.9

**验证方　verifier**

要求验证其他实体身份的实体。



## 4　符号和缩略语

### 4.1　符号

GB/T 15843.1—2017 界定的以及下列符号适用于本文件。

| | |
|---|---|
| $Cert_X$ | 实体 X 的证书。 |
| $I_X$ | 实体 X 的标识符，可能是$i_X$或 $Cert_X$。 |
| $i_X$ | 标识实体 X 的字符串。 |
| M | 输入到数字签名算法的数据串。 |
| $P_X$ | 实体 X 的签名公钥。 |
| $Res_X$ | 对实体 X 的签名公钥或者签名公钥证书的验证结果。 |
| $SID^i_m$ | 唯一标识机制 m 及该机制中的被签名数据(数字 i)的常量。 |
| $sS_X(M)$ | 使用实体 X 的签名私钥对数据串 M 产生的签名。签名应使 M 能够被恢复。 |
| Text | 可选的文本字段。 |
| $\frac{T_X}{N_X}$ | 实体 X 使用的时变参数，或是序列号$N_X$或是时间戳$T_X$。 |
| X ‖ Y | 按指定顺序将数据项 X 和 Y 连接在一起的结果。在本文件规定的机制中，如果对连 |

接后的结果进行签名，则应对数据项进行组合，使连接结果能够被唯一地解析为原始数据项，不存在歧义。

注：依据应用的不同，存在多种不同的方式实现唯一解析。例如：a)在机制所定义的范围内，固定每个子字符串的长度，或 b)使用能够保证唯一解码的方法(例如，使用可区分的编码)对连接的字符串序列进行编码，可参照 ISO/IEC 8825-1[2] 中定义的规则。

## 4.2 缩略语

GB/T 15843.1—2017 界定的以及下列缩略语适用于本文件。

CR：挑战/响应(challenge response)

MUT：双向(mutual)

TS：时间戳(time stamp)

TTP：可信第三方(trusted third party)

UNI：单向(unilateral)

# 5 通则

## 5.1 时变参数

本文件规定的机制使用数字签名技术实现单向或双向实体鉴别。附录 B 解释了这些机制的安全性，并指导用户为自己的应用选择适当的机制。

为防止有效的身份鉴别信息在当次鉴别后被冒用，可使用时变参数，例如时间戳、序列号或随机数(见 GB/T 15843.1—2017 的附录 B)。

如果使用时间戳或序列号，则单向鉴别至少需要一次传递，双向鉴别至少需要两次传递。如果采用随机数的挑战与响应方法，则单向鉴别至少需要两次传递，双向鉴别至少需要三次或四次传递(取决于所采用的机制)。

注 1：实体可通过在其所要签名的数据块中加入自选的随机数以防止另一实体控制数据块去伪造签名。这种方法利用了随机数的不可预测性以防止非法实体通过预先构造数据去伪造签名。

注 2：时变参数是用于验证消息非重放的数据项。

## 5.2 令牌

本文件中，令牌的定义如下：

$$\text{Token} = X_1 \parallel \cdots \parallel X_i \parallel sS_A(Y_1 \parallel \cdots \parallel Y_j)$$

本文件中，“被签名数据”是指“$Y_1 \parallel \cdots \parallel Y_j$”，它被用作数字签名机制的输入，而“未被签名数据”是指“$X_1 \parallel \cdots \parallel X_i$”。

通常，“未被签名数据”中包含的信息未经过本文件中的实体鉴别机制进行鉴别。

如果令牌的“被签名数据”中包含的信息可以从签名中恢复[使用带消息恢复的签名机制的情况，符合 ISO/IEC 9796(所有部分)]或验证方已经拥有该“被签名数据”，则在发送给声称方的令牌中不需要包含该信息。

如果令牌的“被签名数据”中包含的信息不能从签名中恢复[使用不带消息恢复的数字签名机制的情况，符合 ISO/IEC 14888(所有部分)]，可在相应的签名之前将“被签名数据”M 加入到“未被签名数据”中，即使用由 $M \parallel sS_X(M)$ 代替 $sS_X(M)$。若接收方已拥有“被签名数据”M 中的一部分，则这部分数据可从“未被签名数据”中删除。

## 5.3 Text 字段的用法

本文件所规定机制中的所有 Text 字段均可被其他应用所使用(Text 字段可能为空)。Text 字段

之间的关系和内容取决于特定的应用。有关 Text 字段的使用方法，见附录 C。

## 6 要求

本文件规定的鉴别机制中，声称方通过表明其拥有签名私钥证明其身份。具体过程是，声称方使用签名私钥对特定数据进行签名，任何实体能够使用声称方的签名公钥验证签名。

鉴别机制有下述要求。

a) 验证方应拥有声称方的有效签名公钥，即声称方所声称的实体的有效签名公钥。

获得有效签名公钥的一种途径是用证书方式(见 GB/T 15843.1—2017 的附录 C)。证书的产生、分发和撤销都超出了本文件的范围。为了以证书形式获取有效签名公钥，可引入可信第三方。另一种获得有效签名公钥的途径是使用可信的信使。

由于证书的分发不在本文件的范围之内，因此在所有机制中，证书的分发都是可选的。

b) 声称方应拥有仅由声称方掌握及使用的签名私钥。

c) 在实现本文件规定的机制时，所使用的签名私钥应不同于任何其他应用的密钥。

d) 在鉴别机制中，应组合所有的被签名数据串，以防止它们被互换。

为了实现要求 d)，本文件中的机制在被签名数据中包含了常量 $SID_m^i$。

注：本文件未规定常量 $SID_m^i$ 的具体形式。但为了满足要求 d)，其包括以下数据元素：

- 附录 A 中规定的对象标识符，特别是用于标识 ISO/IEC 标准、系列标准序号和鉴别机制的标识符；
- 在机制中用于唯一标识签名字符串的常量。在仅包含一个签名字符串的机制中，忽略该常量。

签名的接收方应验证被签名数据中的常量 $SID_m^i$ 是否符合预期。

若上述要求中的任何一条没有得到满足，则会导致鉴别过程的安全性降低或不能成功完成鉴别。

## 7 不引入在线可信第三方的机制

### 7.1 单向鉴别

#### 7.1.1 通则

两个实体运用单向鉴别机制完成一方对另一方的鉴别。

#### 7.1.2 UNI.TS 机制 ——一次传递鉴别

该鉴别机制通过产生并检验时间戳或序列号(见 GB/T 15843.1—2017 的附录 B)实现唯一性和时效性。声称方 A 启动鉴别过程，由验证方 B 鉴别 A。

UNI.TS 机制见图 1。

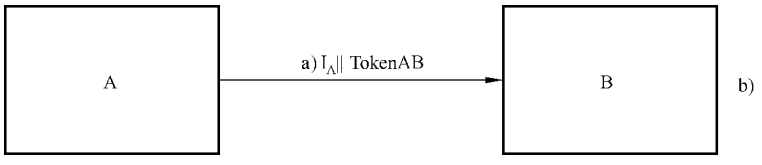


**图 1 UNI.TS 机制**

声称方 A 发送给验证方 B 的令牌(TokenAB)形式是：

$$TokenAB = Text2 \parallel sS_A\left(SID_{UNI.TS}^i \parallel \frac{T_A}{N_A} \parallel i_B \parallel Text1\right)$$

此处声称方 A 用序列号 $N_A$ 或时间戳 $T_A$ 作为时变参数，具体选用哪一个取决于声称方与验证方的

技术能力及使用场景。

注 1：为防止预期验证方之外的任何实体接受令牌，有必要在 TokenAB 的被签名数据中包含标识$i_B$。

注 2：这种机制可用于签名公钥或证书的分发(见 GB/T 15843.1—2017 的附录 A)。

该机制执行下列步骤。

a) A 发送 TokenAB 给 B，并可选地发送 A 的标识符$I_A$。

b) 收到包含 TokenAB 的消息后，B 执行下列步骤：

1) 检查接收到的标识$I_A$，并通过验证 A 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 A 是否可信；

注 3：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认拥有 A 的有效签名公钥；

3) 通过验证令牌中 A 的签名的有效性，检查令牌中的 SID，检查时间戳或序列号，并检查 TokenAB 的被签名数据中的标识字段$i_B$的值是否等于实体 B 的可区分标识符，以验证 TokenAB 的有效性。

### 7.1.3 UNI.CR 机制——两次传递鉴别

该鉴别机制通过产生并检验随机数$R_B$(见 GB/T 15843.1—2017 的附录 B)实现唯一性和时效性。验证方 B 启动鉴别过程，对声称方 A 进行鉴别。

UNI.CR 机制见图 2。

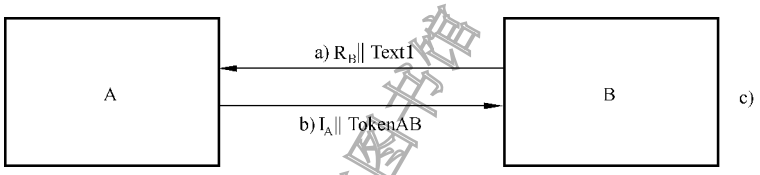


**图 2 UNI.CR 机制**

声称方 A 发送给验证方 B 的令牌(TokenAB)形式是：

$$TokenAB = Text3 \parallel sS_A(SID^1_{UNI.CR} \parallel R_A \parallel R_B \parallel i_B \parallel Text2)$$

注 1：为防止预期验证方之外的任何实体接受令牌(例如，发生中间人攻击时)，在 TokenAB 的被签名数据中需包含标识$i_B$。

注 2：在 TokenAB 的被签名数据中包含随机数$R_A$，可防止 B 在启动鉴别机制之前通过选择数据获得 A 对该选择的数据的签名。

该机制执行下列步骤。

a) B 向 A 发送随机数$R_B$，并可选地发送一个字段 Text1。

b) A 产生并向 B 发送 TokenAB，并可选地发送 A 的标识符$I_A$。

c) 收到包含 TokenAB 的消息后，B 就执行下列步骤：

1) 检查接收到的标识符$I_A$，并通过验证 A 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 A 是否可信；

注 3：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认拥有 A 的有效签名公钥；

3) 通过验证令牌中 A 的签名的有效性，检查 SID，检验步骤 a)中发送给 A 的随机数$R_B$是否与 TokenAB 的被签名数据中的随机数相等，检验步骤 b)中 TokenAB 的被签名数据中的标识字段$i_B$的值是否等于 B 的可区分标识符，以验证 TokenAB 的有效性。

## 7.2 双向鉴别

### 7.2.1 通则

两个实体运用双向鉴别机制完成相互鉴别。

7.1.2 和 7.1.3 描述的两种机制被扩展以实现双向鉴别。这种扩展增加了一条消息传递，从而增加了两个操作步骤。

7.2.4 规定的步骤使用四条消息，但这些消息不需要依次发送，鉴别过程可因此加快。

### 7.2.2 MUT.TS 机制——两次传递鉴别

该鉴别机制通过产生并检验时间戳或序列号(见 GB/T 15843.1—2017 的附录 B)实现唯一性和时效性。

MUT.TS 机制见图 3。

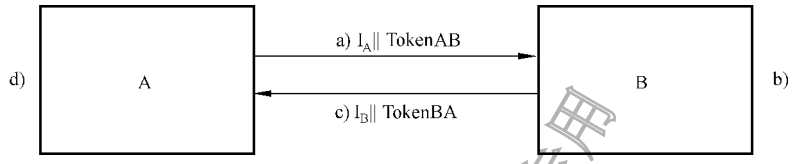


**图 3 MUT.TS 机制**

A 发送给 B 的令牌(TokenAB)格式与 7.1.2 所规定的相似。

$$\text{TokenAB}=\text{Text2}\parallel sS_A\left(SID^1_{MUT.TS}\parallel\frac{T_A}{N_A}\parallel i_B\parallel\text{Text1}\right)$$

B 发送给 A 的令牌(TokenBA)形式为：

$$\text{TokenBA}=\text{Text4}\parallel sS_B\left(SID^2_{MUT.TS}\parallel\frac{T_B}{N_B}\parallel\frac{T_A}{N_A}\parallel i_A\parallel\text{Text3}\right)$$

此处声称方用序列号或时间戳作为时变参数，具体选用哪一个取决于声称方与验证方的技术能力及使用场景。

注 1：为防止验证方之外的任何实体接受令牌，有必要在 TokenBA 和 TokenAB 的被签名数据中包含标识$i_A$和标识$i_B$。

注 2：如果 TokenBA 中省略$\frac{T_A}{N_A}$，则两条消息没有以任何方式绑定在一起。该机制两次独立地使用 7.1.2 机制，时效上存在隐含关系，却不再实现双向鉴别。

该机制执行下列步骤。

a) A 发送 TokenAB 给 B，并可选地发送 A 的标识符$I_A$。

b) 收到包含 TokenAB 的消息后，B 执行下列步骤：

1) 检查接收到的标识符$I_A$，并通过验证 A 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 A 是否可信；

注 3：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认拥有 A 的有效签名公钥；

3) 通过验证令牌中 A 的签名的有效性，检查 SID，检验时间戳或序列号，以及检验 TokenAB 的被签名数据中标识字段$i_B$的值是否等于实体 B 的可区分标识符，以验证 TokenAB 的有效性。

c) B 向 A 发送 TokenBA，并可选地发送 B 的标识符$I_B$。

d) 收到包含 TokenBA 的消息后，A 执行下列步骤：

1) 检查接收到的标识符$I_B$，并通过验证 B 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 B 是否可信；

注 4：A 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认接收到的标识符$I_B$与 TokenAB 中的标识字段$i_B$是否相符；

3) 确认拥有 B 的有效签名公钥；

4) 通过验证令牌中 B 的签名的有效性，检查 SID，检验时间戳或序列号，以及检验 TokenBA 的被签名数据中标识字段$i_A$的值是否等于实体 A 的可区分标识符，以验证 TokenBA 的有效性；

5) 检验 TokenBA 中的$\frac{T_A}{N_A}$是否与步骤 a)中 TokenAB 中的$\frac{T_A}{N_A}$完全相同。

### 7.2.3 MUT.CR 机制——三次传递鉴别

该鉴别机制通过产生并检验随机数(见 GB/T 15843.1—2017 的附录 B)实现唯一性和时效性。MUT.CR 机制见图 4。

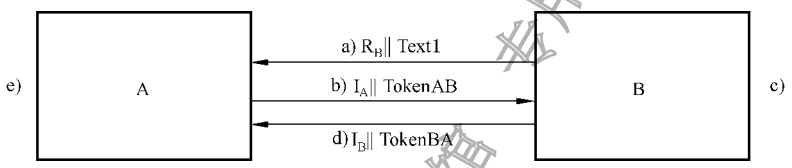


**图 4 MUT.CR 机制**

令牌形式如下：

$TokenAB = Text3 \parallel sS_A(SID^1_{MUT.CR} \parallel R_A \parallel R_B \parallel i_B \parallel Text2)$

$TokenBA = Text5 \parallel sS_B(SID^2_{MUT.CR} \parallel R'_B \parallel R_A \parallel i_A \parallel Text4)$

注 1：当 TokenAB 中不包含标识$i_B$(或者 TokenBA 不包含标识$i_A$)时，A 无法确定 B 是否要对 A 进行鉴别(反之亦然)。此外，也不能保证 Text2 和 Text4 协商一致。

注 2：在 TokenAB 的被签名数据中包含随机数$R_A$，防止了 B 在启动鉴别机制之前通过选择数据获得 A 对该数据的签名。在 TokenBA 的被签名数据中包含$R'_B$也有类似作用。$R'_B$可与$R_B$相同，但这种情况下，在发送 TokenAB 之前，A 能够通过选择数据获得 B 对该数据的签名。

该机制执行下列步骤。

a) B 向 A 发送一个随机数$R_B$，并可选地发送一个字段 Text1。

b) A 向 B 发送 TokenAB，并可选地发送它的标识符$I_A$给 B。

c) 收到包含 TokenAB 的消息后，B 执行下列步骤：

1) 检查接收到的标识符$I_A$，并通过验证 A 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 A 是否可信；

注 3：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认拥有 A 的有效签名公钥；

3) 通过验证令牌中 A 的签名的有效性，检查 SID，检验步骤 a)中发送给 A 的随机数$R_B$是否与 TokenAB 的被签名数据中的随机数相等，检验 TokenAB 的被签名数据中的标识字段$i_B$的值是否等于 B 的可区分标识符，以验证 TokenAB 的有效性。

d) B 向 A 发送 TokenBA，并可选地发送它的标识符$I_B$给 A。

e) 收到包含 TokenBA 的消息后，A 执行下列步骤：

1) 检查接收到的标识符$I_B$，并通过验证 B 的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式确定实体 B 是否可信；

注 4：A 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 确认接收到的标识符$I_B$与 TokenAB 中的标识字段$i_B$是否相符；

3) 确认拥有 B 的有效签名公钥；

4) 通过验证令牌中 B 的签名的有效性，检查 SID，检验步骤 b)中发送给 B 的随机数$R_A$是否与 TokenBA 的被签名数据中的随机数相等，检验 TokenBA 的被签名数据中标识字段$i_A$的值是否等于实体 A 的可区分标识符，以验证 TokenBA 的有效性。

### 7.2.4 MUT.CR.par 机制——两次传递并行鉴别

该鉴别机制是并行执行的，通过产生和检验随机数实现唯一性和时效性(见 GB/T 15843.1—2017 的附录 B)。

MUT.CR.par 机制见图 5。

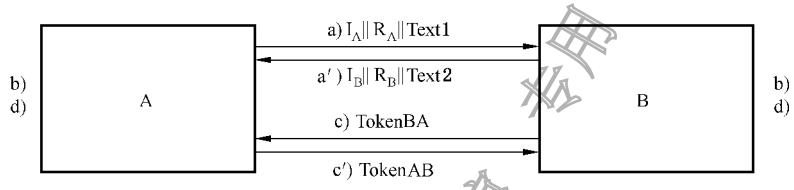


**图 5 MUT.CR.par 机制**

令牌的形式与 7.1.3 中类似：

$TokenAB = Text4 \| sS_A(SID^1_{MUT.CR.par} \| R_A \| R_B \| i_B \| Text3)$

$TokenBA = Text6 \| sS_B(SID^1_{MUT.CR.par} \| R_B \| R_A \| i_A \| Text5)$

注 1：随机数$R_A$包含在 TokenAB 中，防止了 B 在启动鉴别机制之前通过选择数据获得 A 对该数据的签名。基于相同原因，TokenBA 中也包含随机数$R_B$。受步骤 a)和步骤 a′)中消息到达接收端的时间差影响，一方在选择随机数时可能已知另一方的随机数。为防止此类情况发生，双方可分别在 TokenAB 的 Text3 和 Text5 中插入新的随机数$R'_A$和$R'_B$。

注 2：因消息顺序不固定，所以在这个机制的两个签名中采用相同的标识 $SID^1_{MUT.CR.par}$。

该机制执行下列步骤。

a) A 向 B 发送$R_A$，并可选地发送它的标识符$I_A$和一个字段 Text1。

a′) B 向 A 发送$R_B$，并可选地发送它的标识符$I_B$和一个字段 Text2。

b) A 和 B 各自执行下列步骤：

1) A 和 B 各自检查接收到的标识符$I_X$，并通过验证对方的证书或将其与所存储的可信实体列表进行匹配，或通过其他方式来确定对方实体是否可信；

注 3：A 和 B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) A 和 B 各自确认拥有对方的有效签名公钥。

c) A 向 B 发送 TokenAB，其中包括步骤 b)中 A 所信任的 B 的标识字段$i_B$。

c′) B 向 A 发送 TokenBA，其中包括步骤 b)中 B 所信任的 A 的标识字段$i_A$。

d) A 和 B 执行下列步骤：

1) 它们各自验证令牌中签名的有效性(使用步骤 b)中的签名公钥)和检查 SID 所接收到的令牌；

2) 它们各自检查之前发送的随机数是否与令牌中被签名数据中的第一个随机数相等；

3) 它们各自检查之前(在步骤 a))接收的随机数是否与令牌中被签名数据的第二个随机数相等；

4) 它们各自检查令牌中被签名数据中的标识符$I_X$是否与自己的标识相同。

## 8 引入在线可信第三方的机制

### 8.1 通则

本章中的机制应使用 ISO/IEC 14888(所有部分)或 ISO/IEC 9796(所有部分)中定义的签名算法实现。

在本章规范的三元对等实体鉴别 TePA-EA 系列机制中，令牌和 Text 字段的形式遵循第 3 章和第 5 章的描述。此外，在本章规范的机制中，字段$Res_A$、$Res_B$、Status 和 Failure 的值应具有以下形式：

——$Res_A=(Cert_A \parallel Status),(i_A \parallel P_A)$或 Failure；

——$Res_B=(Cert_B \parallel Status),(i_B \parallel P_B)$或 Failure；

——Status=True 或 False。如果证书验证(例如，根据 ISO/IEC 9594-8[3]，ITU-T X.509 [5]或 TTP 所在域的安全策略)失败，则设置该字段的值为 False，否则设置该字段的值为 True；

——Failure：如果 TTP 无法找到签名公钥或实体 X 的证书，则$Res_X$(X∈{A，B})将设置为 Failure。

注：三元对等实体鉴别 TePA-EA(TePA-based entity authentication)是基于三元对等架构实现通信实体之间对等鉴别的系列安全机制。其中，三元对等架构 TePA(Tri-element peer architecture)是一种为网络连接双方提供对等安全的架构，其核心是引入可信第三方，为在连接建立前需要通过对端实体访问可信第三方的一端和对端之间提供对等安全保障。

在本章定义的机制中，如果 TTP 确认掌握 X(X∈{A，B})的身份与签名公钥$P_X$的映射关系，则$I_X=i_X$；否则$I_X=Cert_X$，且$i_X$应等于$Cert_X$的可区分标识符字段值；如果 X 或$Cert_X$被允许作为一种标识，则应预先定义一种方法使得 TTP 能够区分这两种类型的标识。$Res_X$(X={A，B})的值应按表 1 确定。

**表 1 $Res_X$的值**

| 域 | 选项 1 | 选项 2 |
|---|---|---|
| $I_X$ | $i_X$ | $Cert_X$ |
| $Res_X$ | $(X\|\|P_X)$或 Failure | $(Cert_X\|\|Status)$或 Failure |

### 8.2 单向鉴别

#### 8.2.1 通则

8.2 中的实体鉴别机制要求两个实体 A(或 B)使用在线可信第三方(可区分标识符为 TTP)验证对方的签名公钥。该可信第三方应具有验证 A(或 B)签名公钥的真实性的能力。实体 A(或 B)应拥有 TTP 签名公钥的可靠副本。

注：签名公钥的可靠副本是指与签名公钥完全相同的一段数据。

8.2 中规定了两种四次传递鉴别机制，它们都实现了实体 A 和 B 之间的单向鉴别。8.2 中的机制还提供了对 TTP 的实体鉴别、原发鉴别和鉴别结果的防重放功能。四次传递鉴别是一种原子性业务。

机制的实现应使用 ISO/IEC 14888(所有部分)或 ISO/IEC 9796(所有部分)中规定的签名机制之一。

### 8.2.2 TTP.UNI.1 机制——四次传递鉴别(A 发起)

该鉴别机制中,声称方 B 被验证方 A 鉴别。该机制由 A 发起,A 拥有可信第三方 TTP 签名公钥的可靠副本,借助 TTP 参与鉴别。TTP 能够验证实体 B 的签名公钥的有效性。

TTP.UNI.1 机制见图 6。

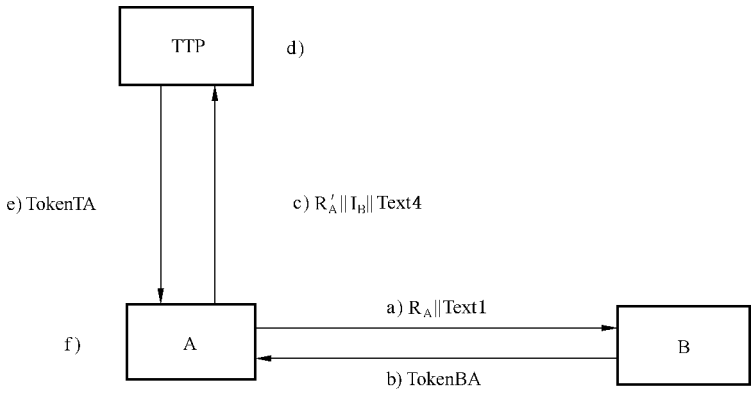


**图 6 TTP.UNI.1 机制**

令牌结构如下:

$TokenBA = Text2 \| M \| sS_B(SID^1_{TTP.UNI.1} \| R_A \| i_A \| Text3)$

$TokenTA = Text5 \| M \| sS_{TTP}(SID^2_{TTP.UNI.1} \| R'_A \| Res_B \| Text6)$

该机制执行下列步骤。

a) A 发送随机数$R_A$及可选文本 Text1 给 B。

b) B 发送令牌 TokenBA 给 A。

c) A 发送随机数$R'_A$,标识符$I_B$以及可选文本 Text4 给 TTP。

d) TTP 收到 A 在步骤 c)发来的消息后,执行下列步骤:如果$I_B$是$i_B$,TTP 提取$P_B$;如果$I_B$是$Cert_B$,TTP 检查证书$Cert_B$的有效性。TTP 检查证书有效性的过程可能需要防范拒绝服务攻击,具体的防范方法超出了本文件的范围。

e) TTP 发送 TokenTA 给 A,TokenTA 中的$Res_B$字段应为:B 的证书及其状态,或者是 B 的可区分标识符及其签名公钥,或者是 Failure 失败标识。

f) 实体 A 收到 TTP 在步骤 e)发来的消息后,执行下列操作:

1) 通过验证 TokenTA 中的 TTP 的签名的有效性,检查 SID,检查被签名数据中包含的随机数$R'_A$是否与在步骤 c)中发送给 TTP 的随机数$R'_A$相等,并检查$Res_B$不为 Failure 来验证 TokenTA;

**注**:A 也能检查接收到的标识是否与自己的标识一致。在许多应用中,实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取实体 B 的签名公钥,通过校验在步骤 b)收到的令牌中实体 B 的签名,检查 SID,检查 TokenBA 中的标识字段$i_A$的值是否等于实体 A 的可区分标识符,并检查 TokenBA 中的随机数$R_A$是否与在步骤 a)发送给 B 的随机数相等,以验证 TokenBA 的有效性。

### 8.2.3 TTP.UNI.2 机制——四次传递鉴别(B 发起)

该鉴别机制中,声称方 A 被验证方 B 鉴别,该机制由实体 B 发起,B 拥有可信第三方 TTP 签名公钥的可靠副本,借助 TTP 参与鉴别。TTP 能够验证实体 A 的签名公钥的有效性。

TTP.UNI.2 机制见图 7。

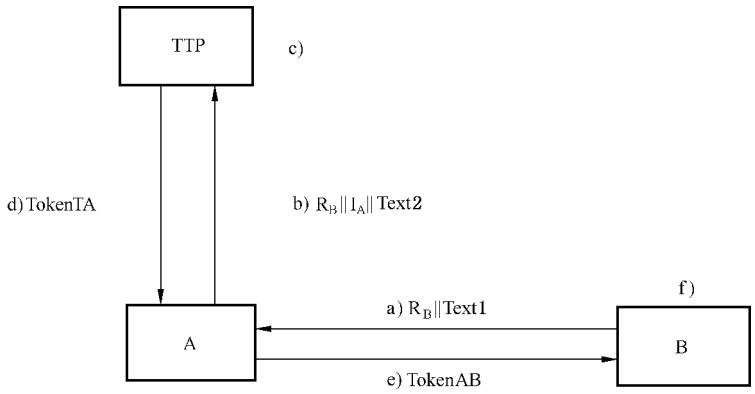


**图 7　TTP.UNI.2 机制**

令牌结构如下：

$TokenTA = Text3 \| M \| sS_{TTP}(SID^1_{TTP.UNI.2} \| R_B \| Res_A \| Text4)$

$TokenAB = Text5 \| M \| TokenTA \| sS_A(SID^2_{TTP.UNI.2} \| R_B \| i_B \| Text6)$

该机制执行下列步骤。

a) B 发送随机数$R_B$及可选文本 Text1 给 A。

b) A 发送$R_B$，$I_A$和可选字段 Text2 给 TTP。

c) 收到 A 在步骤 b)中发来的消息后，TTP 执行如下操作：如果$I_A$是$i_A$，TTP 提取 $P_A$；如果$I_A$是$Cert_A$，TTP 检查证书$Cert_A$的有效性。TTP 检查证书有效性的过程可能需要防范拒绝服务攻击，具体的防范方法超出了本文件的范围。

d) TTP 发送 TokenTA 给 A。TokenTA 中的$Res_A$应为：A 的证书及其状态，或者是 A 的可区分标识符及其签名公钥，或者是 Failure 失败标识。

e) A 发送令牌 TokenAB 给 B。

f) 收到 A 在步骤 e)中发来的消息后，B 执行如下操作：

1) 通过验证 TokenTA 中 TTP 的签名的有效性，检查 SID，检查被签名数据中包含的随机数$R_B$是否与在步骤 a)中发送给 A 的随机数$R_B$相等，并检查$Res_A$是否为 Failure 来验证 TokenTA；

**注**：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取实体 A 的签名公钥，通过验证令牌中实体 A 的签名的有效性，检查 SID，检查 TokenAB 中的标识字段$i_B$的值是否等于实体 B 的可区分标识符，并检查 TokenAB 中的随机数$R_B$是否与在步骤 a)发送给 A 的随机数相等，以验证 TokenAB 的有效性。

## 8.3　双向鉴别

### 8.3.1　通则

8.3 中规定的鉴别机制要求两个实体 A 和 B 使用一个或两个在线可信第三方验证彼此签名公钥的有效性。

如果仅使用一个在线可信第三方，则由 TTP 表示其可区分标识符。

如果使用两个在线可信第三方，则它们的可区分标识符分别用$TTP_A$和$TTP_B$表示。仅通过$TTP_A$验证 A 的签名公钥的有效性，仅通过$TTP_B$验证 B 的签名公钥的有效性。实体 A 信任$TTP_A$(A 认为由$TTP_A$签名的任何断言都是有效的)，并应拥有$TTP_A$的签名公钥的可靠副本。实体 B 信任$TTP_B$(B 认

为$TTP_B$签名的任何断言都是有效的),并应拥有$TTP_B$的签名公钥的可靠副本。$TTP_A$和$TTP_B$互相信任。$TTP_A$具有$TTP_B$的签名公钥的可靠副本,且$TTP_B$具有$TTP_A$的签名公钥的可靠副本。

8.3 中规定了两种五次传递鉴别机制和一种七次传递鉴别机制。所有这些机制均实现了实体 A 和 B 之间的双向鉴别。此外,这些机制还提供了对 TTP,$TTP_A$或$TTP_B$的实体鉴别,以及原发鉴别和鉴别结果的防重放功能。五次传递鉴别和七次传递鉴别都是一种原子性业务。

注:8.3 中规定的机制在封闭的场景中使用。所有的实体共享同一个 TTP,拥有 TTP 公开密钥签名公钥的可靠副本。如果使用选项 1,TTP 只提供证书校验服务。如果使用选项 2,TTP 除了提供证书校验服务之外,还提供实体 A 和 B 之间的鉴别服务。

如果选项 1 应用于 B(或 A)知道 TTP 正在为 B(或 A)验证 A(或 B)身份的场景中,选项 1 中 TTP 签名的 Text 字段宜包括$I_A$(或$I_B$)。更具体地讲,TTP 使用$I_A$作为 TokenTA 第一个签名的 Text 字段部分,使用$I_B$作为 TokenTA 第二个签名的 Text 字段部分。在这种情况下,A、B 和 TTP 宜就 Text 字段中包括的$I_A$(或$I_B$)格式和位置达成共识。

### 8.3.2 TTP.MUT.1 机制——五次传递鉴别(A 发起)

该鉴别机制通过产生和检查随机数实现唯一性和时效性(见 GB/T 15843.1—2017 的附录 B)。

TTP.MUT.1 机制见图 8。

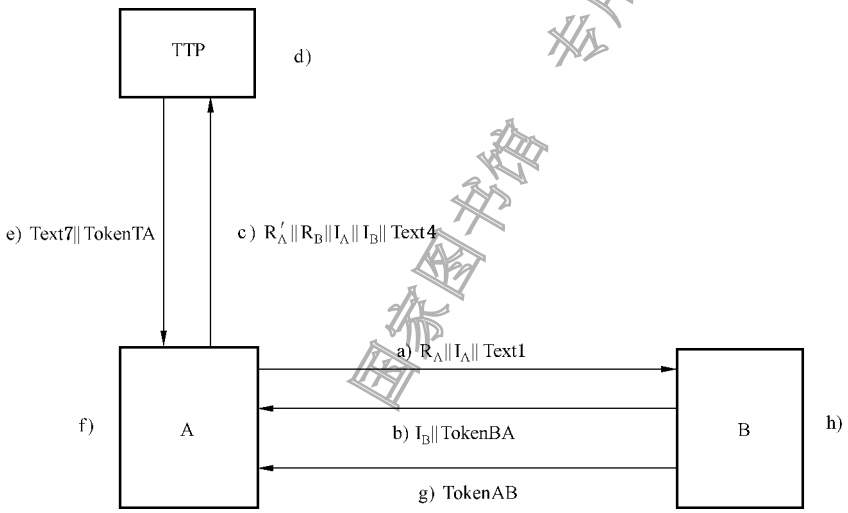


**图 8 TTP.MUT.1 机制**

令牌结构如下:

选项 1:

$TokenBA = Text3 \| sS_B(SID^1_{TTP.MUT.1-1} \| i_B \| R_A \| R_B \| i_A \| Text2)$

$TokenTA = sS_{TTP}(SID^2_{TTP.MUT.1-1} \| R'_A \| ReS_B \| Text6) \| sS_T(SID^3_{TTP.MUT.1-1} \| R_B \| ReS_A \| Text5)$

$TokenAB = Text9 \| sS_{TTP}(SID^3_{TTP.MUT.1-1} \| R_B \| ReS_A \| Text5) \| sS_A(SID^4_{TTP.MUT.1-1} \| R_B \| R''_A \| i_B \| i_A \| Text8)$

选项 2:

$TokenBA = Text3 \| sS_B(SID^1_{TTP.MUT.1-2} \| i_B \| R_A \| R_B \| i_A \| Text2)$

$TokenTA = sS_{TTP}(SID^2_{TTP.MUT.1-2} \| R'_A \| R_B \| ReS_A \| ReS_B \| Text5)$

$TokenAB = Text9 \| TokenTA \| sS_A(SID^3_{TTP.MUT.1-2} \| R_B \| R''_A \| i_B \| i_A \| Text8)$

注 1:该机制的实现者能选择支持一个或者两个上述选项。

注 2:随机数$R_A$包含在 TokenAB 中,防止了 B 在启动鉴别机制之前通过选择数据获得 A 对该数据的签名。出于类似的原因,TokenBA 中也包含随机数$R_B$。

该机制执行下列步骤。

a) A 发送随机数$R_A$、标识符$I_A$和可选字段 Text1 到 B。

b) B 发送 TokenBA 和标识符$I_B$到 A。

c) A 发送随机数 $R'_A$、随机数$R_B$、标识符$I_A$、标识符$I_B$以及可选字段 Text4 到 TTP。

d) 收到来自步骤 c)中 A 的消息后，TTP 执行下列步骤：如果$I_A=i_A$，且$I_B=i_B$，则 TTP 提取$P_A$和$P_B$；如果$I_A=Cert_A$，且$I_B=Cert_B$，则 TTP 检查$Cert_A$和$Cert_B$的有效性。TTP 检查证书有效性的过程可能需要防范拒绝服务攻击，具体的防范方法超出了本文件的范围。

e) TTP 发送可选字段 Text7 和 TokenTA 到 A。TokenTA 中的$Res_A$和$Res_B$应为 A 和 B 的证书及其状态，或者是 A 和 B 的可区分标识符及其签名公钥，或者是指示符 Failure。

f) 收到来自步骤 e)中 TTP 的消息后，A 执行下列步骤：

1) 通过验证 TokenTA 中 TTP 的签名的有效性，检查 SID，检查步骤 c)中发送给 TTP 的随机数 $R'_A$与 TokenTA 中 TTP 的签名数据中的随机数 $R'_A$是否一致是否相等，以验证 TokenTA 的有效性，宜检查包含$Res_B$的签名，可选地检查不包含$Res_B$的签名，如果检查不包含$Res_B$的签名，则宜检查$R_B$；

注 3：A 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取 B 的签名公钥，通过验证步骤 b)中收到的令牌 B 的签名的有效性，检查 SID，检查 TokenBA 中 B 的签名数据中的标识字段$i_A$的值是否等于 A 的可区分标识符，检查 TokenBA 中随机数$R_A$与在步骤 a)中发送给 B 的随机数$R_A$是否相等，以验证 TokenBA 的有效性。

g) A 发送 TokenAB 到 B。

h) 收到来自步骤 g)中 A 的消息后，B 执行下列步骤：

1) 通过验证 TokenTA(实体 A)或者 TokenAB(实体 B)中 TTP 的签名的有效性，检查 SID，检查 TokenTA 中 TTP 的签名数据的随机数$R_B$与在步骤 b)中发送给 A 的随机数$R_B$是否相等，以验证 TokenTA 的有效性；

注 4：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取 A 的签名公钥，通过验证 TokenAB 中 A 的签名的有效性，检查 SID，检查 TokenAB 中 A 的签名数据中的标识字段$i_B$的值是否等于 B 的可区分标识符，检查 TokenAB 中 A 的签名数据的随机数$R_B$与在步骤 b)中发送给 A 的随机数$R_B$是否相等，以验证 TokenAB 的有效性。

### 8.3.3 TTP.MUT.2 机制——五次传递鉴别(B 发起)

该鉴别机制通过产生和检查随机数实现唯一性和时效性(见 GB/T 15843.1—2017 的附录 B)。TTP.MUT.2 机制见图 9。

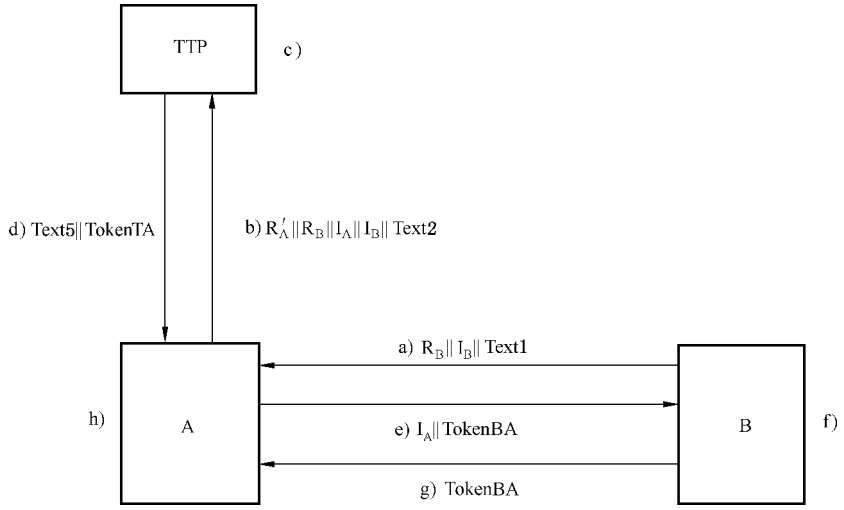


**图 9　TTP.MUT.2 机制**

令牌结构如下：

选项 1：

$TokenTA = sS_{TTP}(SID^1_{TTP.MUT.2-1} \| R'_A \| ReS_B \| Text4) \| sS_{TTP}(SID^2_{TTP.MUT.2-1} \| R_B \| ReS_A \| Text3)$

$TokenAB = Text7 \| sS_{TTP}(SID^2_{TTP.MUT.2-1} \| R_B \| ReS_A \| Text3) \| sS_A(SID^3_{TTP.MUT.2-1} \| R_B \| R_A \| i_B \| i_A \| Text6)$

$TokenBA = Text9 \| sS_B(SID^4_{TTP.MUT.2-1} \| i_A \| R_A \| R'_B \| i_B \| Text8)$

选项 2：

$TokenTA = sS_{TTP}(SID^1_{TTP.MUT.2-2} \| R'_A \| R_B \| ReS_A \| ReS_B \| Text3)$

$TokenAB = Text7 \| TokenTA \| sS_A(SID^2_{TTP.MUT.2-2} \| R_B \| R_A \| i_B \| i_A \| Text6)$

$TokenBA = Text9 \| sS_B(SID^3_{TTP.MUT.2-2} \| R_A \| R'_B \| i_A \| i_B \| Text8)$

**注 1**：该机制的实现者能选择支持一个或者两个上述选项。

该机制执行下列步骤。

a) B 发送随机数$R_B$、标识符$I_B$和可选字段 Text1 到 A。

b) A 发送随机数 $R'_A$、随机数$R_B$、标识符$I_A$、标识符$I_B$以及可选字段 Text2 到 TTP。

c) 收到来自步骤 b)中 A 的消息后，TTP 执行下列步骤：如果$I_A = i_A$，且$I_B = i_B$，则 TTP 提取$P_A$和$P_B$；如果$I_A = Cert_A$，且$I_B = Cert_B$，则 TTP 检查$Cert_A$和$Cert_B$的有效性。TTP 检查证书有效性的过程可能需要防范拒绝服务攻击，具体的防范方法超出了本文件的范围。

d) TTP 发送可选字段 Text5 和 TokenTA 到 A。TokenTA 中的$Res_A$和$Res_B$应为 A 和 B 的证书及其状态，或者是 A 和 B 的可区分标识符及其签名公钥，或者是指示符 Failure。

e) A 发送身份$I_A$和 TokenAB 到 B。

f) 收到来自步骤 e)中 A 的消息后，B 执行下列步骤：

1) 通过验证 TokenAB 中 TTP 的签名的有效性，检查 SID，检查步骤 a)中发送给 A 的随机数$R_B$与 TokenAB 中 TTP 的签名数据中的随机数$R_B$是否相等，以验证 TokenAB 的有效性；

**注 2**：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取 A 的签名公钥，通过验证 TokenAB 中 A 的签名的有效性，检查 SID，检查 TokenAB 中 A 的签名数据的标识字段$i_B$的值是否等于 B 的可区分标识符，检查

TokenAB 中的 A 的签名数据的随机数$R_B$与在步骤 a)中发送给 A 的随机数$R_B$是否相等，以验证 TokenAB 的有效性。

g) B 发送 TokenBA 到 A。

h) 收到来自步骤 g)中 B 的消息后，A 执行下列步骤：

1) 通过验证 TokenTA 中 TTP 的签名的有效性，检查 TokenTA 中 TTP 的签名数据的随机数$R'_A$与在步骤 b)中发送给 TTP 的随机数$R'_A$是否相等，以验证步骤 d)消息中的 TokenTA 的有效性，宜检查包含$Res_B$的签名，可选地检查不包含$Res_B$的签名；

注 3：A 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从步骤 d)的消息中提取 B 的签名公钥，通过验证 TokenBA 中 B 的签名的有效性，检查 TokenBA 中 B 的签名数据中的标识字段$i_A$的值是否等于 A 的可区分标识符，检查 TokenBA 中随机数$R_A$与步骤 e)中发送给 B 的随机数$R_A$是否相等，以验证 TokenBA 的有效性。

### 8.3.4 TTP.MUT.3 机制——七次传递鉴别

该鉴别机制包含七条消息的传递，使用两个在线可信第三方($TTP_A$和$TTP_B$)，通过产生和检查随机数实现唯一性和时效性(见 GB/T 15843.1—2017 的附录 B)。

TTP.MUT.3 机制见图 10。

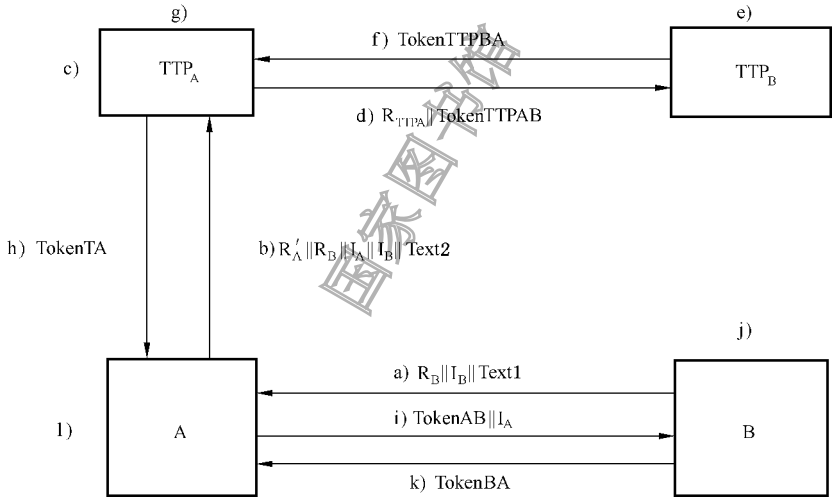


**图 10 TTP.MUT.3 机制**

令牌结构如下：

$TokenTTPAB = M \| sS_{TTPA}(SID^1_{TTP.MUT.3} \| ReS_A \| I_B \| R_B \| Text3)$

$TokenTTPBA = M \| sS_{TTPB}(SID^2_{TTP.MUT.3} \| ReS_A \| R_B \| Text4) \| sS_{TTPB}(SID^3_{TTP.MUT.3} \| Res_B \| R_{TTPA} \| Text5)$

$TokenTA = M \| sS_{TTPA}(SID^4_{TTP.MUT.3} \| ReS_B \| R'_A \| Text6) \| sS_{TTPB}(SID^2_{TTP.MUT.3} \| ReS_A \| R_B \| Text4)$

$TokenAB = M \| sS_{TTPB}(SID^2_{TTP.MUT.3} \| ReS_A \| R_B \| Text4) \| sS_A(SID^5_{TTP.MUT.3} \| R_B \| R_A \| i_B \| i_A \| Text7)$

$TokenBA = M \| sS_B(SID^6_{TTP.MUT.3} \| R_A \| R_B \| i_A \| i_B \| Text8)$

该机制执行下列步骤。

a) B 发送随机数$R_B$、标识符$I_B$和可选字段 Text1 到 A。

b) A 发送随机数 $R'_A$、随机数$R_B$、标识符$I_A$、标识符$I_B$以及可选字段 Text2 到$TTP_A$。

c) 收到来自步骤 b)中 A 的消息后，$TTP_A$执行下列步骤：如果$I_A=i_A$，则$TTP_A$提取$P_A$；如果$I_A=Cert_A$，则$TTP_A$检查$Cert_A$的有效性。$TTP_A$检查证书有效性的过程可能需要防范拒绝服务攻击，具体的防范方法超出了本文件的范围。

d) $TTP_A$发送$R_{TTPA}$和 TokenTTPAB 到$TTP_B$。

e) $TTP_B$收到$TTP_A$发送的消息后，执行下列步骤：

1) 通过验证 TokenTTPAB 中$TTP_A$的签名的有效性，以验证令牌中$TTP_A$的签名的有效性；

2) 如果$I_B=i_B$，则$TTP_B$提取$P_B$；如果$I_B=Cert_B$，则$TTP_B$检查$Cert_B$的有效性。$TTP_B$检查证书有效性的过程可能需要防范拒绝服务攻击，具体的防范方法超出了本文件的范围。

f) $TTP_B$向$TTP_A$发送令牌 TokenTTPBA。

g) $TTP_A$收到$TTP_B$发送的消息后，$TTP_A$通过下列方式校验 TokenTTPBA：验证令牌中$TTP_B$的签名的有效性，检查 TokenTTPBA 中的被签名数据的随机数$R_{TTPA}$与步骤 d)中发送给$TTP_B$的随机数$R_{TTPA}$是否相等。

h) $TTP_A$发送令牌 TokenTA 给 A，TokenTA 中的$Res_A$和$Res_B$应为 A 和 B 的证书及其状态，或者是 A 和 B 的可区分标识符及其签名公钥，或者是指示符 Failure。

i) A 发送 TokenAB 和标识符$I_A$到 B。

j) B 收到步骤 i)的消息后，执行下列步骤：

1) 通过验证 TokenAB 中$TTP_B$的签名的有效性，检查 TokenAB 中被签名数据的随机数$R_B$与步骤 a)中发送给 A 的随机数$R_B$是否相等，以验证$TTP_B$的签名的有效性；

注 1：B 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取 A 的签名公钥，通过验证 TokenAB 中 A 的签名的有效性，检查 TokenAB 中 A 的签名数据中的标识字段$i_B$的值是否等于 B 的可区分标识符，检查 TokenAB 中随机数$R_B$与步骤 a)中发送给 A 的随机数$R_B$是否相等，以验证 TokenAB 的有效性。

k) B 发送 TokenBA 到 A。

l) A 收到 B 的消息后，执行下列步骤：

1) 通过验证 TokenTA 中$TTP_A$的签名的有效性，检查 TokenTA 中被签名数据的随机数 $R'_A$与步骤 b)中发送给$TTP_A$的随机数 $R'_A$是否相等，以验证 TokenTA 的有效性；

注 2：A 也能检查接收到的标识是否与自己的标识一致。在许多应用中，实体针对自身进行鉴别也被视为安全事项。

2) 从消息中提取 B 的签名公钥，通过验证 TokenBA 中 B 的签名的有效性，检查 TokenBA 中 B 的签名数据中的标识字段$i_A$的值是否等于 A 的可区分标识符，检查 TokenBA 中随机数$R_A$与步骤 i)中发送给 B 的随机数$R_A$是否相等，以验证 TokenBA 的有效性。

# 附 录 A
（规范性）
对象标识符

## A.1 形式定义

```
EntityAuthenticationMechanisms-3{
    iso(1)standard(0)e-auth-mechanisms(9798)part3(3)
    asn1-module(0)object-identifiers(0)}
    DEFINITIONS EXPLICIT TAGS ::=BEGIN
  --只有输出,没有输入。--
  OID ::=OBJECT IDENTIFIER
  is9798-3 OID ::={iso(1)standard(0)e-auth-mechanisms(9798)Part3(3)}
  mechanism OID ::={is9798-3 mechanisms(1)}
  --不引入在线可信第三方的机制 --
  nottp-mechanism OID ::={mechanism nottp(1)}
  nottp-uni-mechanism OID ::={nottp-mechanism uni(1)}
  nottp-mut-mechanism OID ::={nottp-mechanism mut(2)}
  uni-ts OID ::={nottp-uni-mechanism 1 }
  uni-cr OID ::={nottp-uni-mechanism 2 }
  mut-ts OID ::={nottp-mut-mechanism1 }
  mut-cr OID ::={nottp-mut-mechanism2 }
  mut-cr-Parallel OID ::={nottp-mut-mechanism3 }
  -- 引入在线可信第三方的机制 --
  ttp-mechanism OID ::={mechanism ttp(2)}
  ttp-uni-mechanism OID ::={ttp-mechanism uni(1)}
  ttp-mut-mechanism OID ::={ttp-mechanism mut(2)}
  ttp-uni-1OID ::={ttp-uni-mechanism1 }
  ttp-uni-2 OID ::={ttp-uni-mechanism2 }
  ttp-mut-1 OID ::={ttp-mut-mechanism 1 }
  ttp-mut-2 OID ::={ttp-mut-mechanism 2 }
  ttp-mut-3 OID ::={ttp-mut-mechanism 3 }
END--EntityAuthenticationMechanisms-3 --
```

## A.2 后续对象标识符的使用

在标示某个机制的对象标识符之后,应立即跟随另外一个标示数字签名算法的对象标识符[例如,在 ISO/IEC 14888(所有部分)或 ISO/IEC 9796(所有部分)中规范的算法]。

# 附 录 B
（资料性）
使用指南

## B.1 安全属性

### B.1.1 实体鉴别

实体鉴别的目的是证实一个实体是其所声称的实体。为了形式化地描述该属性，根据GB/T 15843.1—2017，攻击者将被认为可以执行中间人、重放、反射和强制延迟等攻击方法。有关本文件的广泛安全性分析，见[1]。该报告考虑以下安全属性：

——对方是存活的（存在且正常响应的）；

——与对方在有关代理及其角色方面存在弱共识；

——在可能的情况下，与对方就随机数和 Text 字段达成数据一致。

提供上述属性的机制可抵御中间人攻击、反射攻击和重放攻击（在按照 GB/T 15843.1—2017 附录 B 正确地使用了时变参数的情况下）。对于涉及在线可信第三方的机制，尽管实体 A 和 B 都确信 TTP 的存活性（反之没有），但仅在 A 和 B 之间考虑这些属性，在 TTP 和 A（或 B）之间并没有考虑这些属性。

### B.1.2 单向和双向鉴别

单向鉴别协议仅能保证对等方之一的安全性。例如，向实体 B 保证 A 的存活性、弱共识和数据一致，反之则不然。在双向鉴别中，两个对等方可以确保彼此的存活性、弱共识和数据一致。

注：弱共识和数据一致的要求意味着不能通过简单组合两种单向鉴别机制就实现双向鉴别。

### B.1.3 证书分发与可信

所有机制都允许在消息中包含$I_X$作为可选字段。$I_X$包含证书 $Cert_X$或标识 X。这允许声称方将关于其标识和（或）证书的信息提供给验证方。但是，声称方没有为验证方提供能够对声称方所提供信息加以信任的方法。验证方仍然需要验证证书，或者等效地，需要拥有声称方的签名公钥的可靠副本。但是，此验证步骤超出了本文件的范围。

机制 UNI.TS，UNI.CR，MUT.TS，MUT.CR 和 MUT.CR 中由给 A 和（或）B 进行证书和（或）签名公钥的验证（可能涉及辅助机制，例如与第三方合作的 OCSP）。

TTP.UNI.1，TTP.UNI.2 和 TTP.MUT.1 到 TTP.MUT.3 机制直接包含一个或两个可信第三方（TTP）以验证 A 和 B 的签名公钥或证书。这将验证证书和（或）签名公钥的任务从参与方 A 和 B 转移到 TTP。注意，TTP 如何执行此验证步骤超出了本文件的范围。假定 TTP 的标识和签名公钥对于 A 和 B 都是已知的（或者在两个 TTP 的情况下，每一方都知道各自 TTP 的标识和签名公钥），即，该机制只能在具有固定 TTP 的封闭环境中使用。

TTP 在实体鉴别机制执行期间仅与参与方之一交互，但向双方提供证书验证结果。对于该机制的每次执行，TTP 需要在线可用。而且，TTP 会在每次执行该机制时了解所涉及双方的未经验证的身份。在某些设置中，并不希望第三方获取有关通信双方身份的信息，而不论该信息是否真实。

## B.2 机制的比较和选择

### B.2.1 比较

表 B.1 总结了本文件所有机制的安全属性和协议的已知限制。该表仅在包括所有可选字段时显示属性。省略这些字段会导致较低的安全保证，如相应机制的注释中所述。参考文献[1]中提出的安全性问题已通过(在可能的范围内)使用唯一标识符标记每个签名消息以及在整个机制中确保对串联字符串的唯一解码的方法加以解决。

**表 B.1 机制的安全属性**

| 机制 | 双向 | TTP | 消息条数 | 时效性与唯一性 |
|---|---|---|---|---|
| UNI.TS 机制 | N | N | 1 | $\frac{T_A}{N_A}$ |
| UNI.CR 机制 | N | N | 2 | $R_A$ |
| MUT.TS 机制 | Y | N | 2 | $\frac{T_A}{N_A}$和$\frac{T_B}{N_B}$ |
| MUT.CR 机制 | Y | N | 3 | $R_A$和$R_B$ |
| MUT.CR.par 机制 | Y | N | 4 | $R_A$和$R_B$ |
| TTP.UNI.1 机制 | N | Y | 4 | $R_A$和$R'_A$ |
| TTP.UNI.2 机制 | N | Y | 4 | $R_B$ |
| TTP.MUT.1 机制 | Y | Y | 5 | $R_A$，$R'_A$和$R_B$ |
| TTP.MUT.2 机制 | Y | Y | 5 | $R_A$，$R'_A$和$R_B$ |
| TTP.MUT.3 机制 | Y | Y | 7 | $R_A$，$R'_A$和$R_B$ |



### B.2.2 选择机制的建议

在选择实体鉴别机制时，宜考虑以下几个因素。

——安全通信信道的需求：本文件中的机制不提供任何通信的机密性保护，并且在实体鉴别完成后也未设置用于进一步通信的安全信道。如果需要安全的通信信道，可使用 ISO/IEC 11770[4] 中的密钥建立方法代替本文件中的机制。

——单向或双向鉴别：单向或双向鉴别的需求完全由应用场景决定。

——已知的安全限制：机制 UNI.1 和 MUT.1 通过使用时间戳或序列号确保实体鉴别的时效性/唯一性。如 GB/T 15843.1—2017 中附录 B 的详细说明，这需要同步时钟(用于时间戳)或额外的簿记以验证序列号。若缺少这些附加措施，易遭受攻击。在多数情况下，最好使用挑战—响应机制以避免这些附加措施。

——通信和计算的复杂度：机制的效率取决于各方的通信要求(消息的数量、大小)和计算要求(签名的生成和验证以及随机数的生成)。这些开销在很大程度上取决于用于实施某种机制的平台。可能的影响因素包括网络传输速度和延迟，使用的是单向还是双向通信，双方的处理器和内存大小等。

——证书和密钥验证：如何实现验证不在本文件的范围之内。所有机制都可以用各方可以执行的证书验证机制进行修改(直接或通过另一方间接执行)。在封闭的环境中，可以由单个实体负责验证证书/密钥，可考虑使用 TTP－＊类的机制之一。

# 附 录 C
（资料性）
## Text 字段的使用方法

第 7 章和第 8 章规定的令牌包括 Text 字段。在一次具体地传递中，不同 Text 字段的实际用途及各 Text 字段间的关系取决于具体应用。下面给出一些例子，也可参见 GB/T 15843.1—2017 的附录 A。

若使用不带消息恢复的数字签名方案，且被签名 Text 字段不为空，则要求验证方在检验签名之前已有该 Text 字段。在本附录中，“被签名 Text 字段”指被签名数据中的 Text 字段，而“未被签名 Text 字段”指未在被签名数据中的 Text 字段。

例如，若使用不带消息恢复的数字签名方案，任何需要进行数据起源鉴别的信息都应放到令牌的被签名 Text 字段和（作为一部分放到）未被签名 Text 字段中。

若令牌未含有（足够的）冗余，被签名 Text 字段可以用来提供额外的冗余。

被签名 Text 字段可以用来指示，令牌只有用于实体鉴别目的时才是有效的。宜注意，一个实体可能会蓄意地选择一个“退化”的值来让另一个实体签名。为防范这种可能性，另一实体可以在 Text 字段中引入一个随机数。

假如使用某种算法时，某个声称方对所有与之通信的验证方都使用同一密钥，那么将可能发生潜在的攻击。若认为这种潜在的攻击是一个威胁，则需要在被签名 Text 字段和（若必要）未被签名 Text 字段中，包含预期验证方的身份。

未被签名 Text 字段也可以用于向验证方提供信息，以指明声称方正在声称（但尚未被鉴别）的身份。若不用证书方式分发签名公钥，则要求使用这种信息让验证方确定用哪个签名公钥鉴别声称方。

# 参 考 文 献

[1] David Basin and CasCremers, Evaluation of ISO/IEC 9798 Protocols CRYPTREC Technical Report, Version 2.0, April 2011. Available at https://www.cryptrec.go.jp/estimation/techrep_id2014_2.pdf

[2] ISO/IEC 8825 (all parts) ITU-T Rec. X.690-series, Information technology—ASN.1 Encoding rules

[3] ISO/IEC 9594-8, Information technology—Open systems interconnection—The directory: public-key and attribute certificate frameworks

[4] ISO/IEC 11770(all parts) Information technology—Security techniques—Key management

[5] ITU-T X.509 Information technology—Open systems interconnection—The directory: public-key and attribute certificate frameworks

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 实体鉴别
第3部分:采用数字签名技术的机制
GB/T 15843.3—2023/ISO/IEC 9798-3:2019
*
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
2023年3月第一版
*
书号:155066·1-72565



GB/T 15843.3-2023

码上扫一扫 正版服务到