ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.3—20XX/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，IDT）

（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。）

（征求意见稿）

（本稿完成日期：2020-12-08）

××××-××-××发布　　××××-××-××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的第3部分。GB/T 15843已发布了以下部分：

——第1部分：概述；

——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：采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，主要技术变化如下：

a) 增加了“概述”（见第5章）；

b) 增加了“单向鉴别”（见8.2）；

c) 增加了“七次传递鉴别”（见8.3.4）；

d) 增加了“text字段的用法”（见附录C）。

本文件使用翻译法等同采用ISO/IEC 9798-3:2019《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》，仅有编辑性修改。

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、无线网络安全技术国家工程实验室、WAPI产业联盟（中关村无线网络安全产业联盟）、北京数字认证股份有限公司、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。

本文件主要起草人：曹军、杜志强、李琴、黄振海、王月辉、张变玲、铁满霞、张璐璐、胡霄亮、郑骊、赖晓龙、赵晓荣、颜湘、张国强、罗鹏、简练、陈晓龙、周涛、李玉娇。

本文件所代替文件的历次版本发布情况为：

——GB/T 15843.3—2008。

——GB/T 15843.3—2016。

引　言

本文件定义了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，又分为一次传递鉴别、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。目的在于规范采用对称加密算法的实体鉴别机制，包括适用于不同应用场景的多种机制。

第 3 部分：采用数字签名技术的机制。目的在于规范采用数字签名技术的实体鉴别机制，包括适用于不同应用场景的多种机制。

第 4 部分：采用密码校验函数的机制。目的在于规范采用密码校验函数的实体鉴别机制，包括适用于不同应用场景的多种机制。

第 5 部分：使用零知识技术的机制。目的在于规范使用零知识技术的实体鉴别机制，包括适用于不同应用场景的多种机制。

第 6 部分：采用人工数据传递的机制。目的在于规范采用人工数据传递的实体鉴别机制，包括适用于不同应用场景的多种机制。

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

本文件的发布机构提请注意，声明符合本文件时，可能涉及到与第 8 章相关的 CN201510654832.X、CN200910024191.4、CN200910023774.5、CN200910023735.5、CN200910023734.0、CN200810150949.4、CN200810150951.1、CN200710199241.3、CN200710018920.6 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。

该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。该专利持有人的声明已在本文件发布机构备案。相关信息可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

请注意除了上述专利外，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

本文件规定了采用基于非对称技术的数字签名的实体鉴别机制。数字签名用于验证实体的身份。

本文件规定了两类机制，第一类共五种机制不引入在线可信第三方，第二类共五种机制引入在线可信第三方。在这两类机制中，分别各有两种机制实现单向鉴别，各有三种机制实现双向鉴别。

本文件适用于指导实体鉴别技术研究以及相关产品和系统的研发与应用。

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：概述（ISO/IEC 9798-1:1997，IDT）

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）

GB/T 16263.1—2006 信息技术 ASN.1 编码规则 第1部分：基本编码规则（BER）、正则编码规则（CER）和非典型编码规则（DER）规范（ISO/IEC 8825-1:2002，IDT）

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）

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，这种数据或变换允许数据单元的接收者用以证明数据单元的来源和完整性，并保护数据单元的发送者和接收者以防止数据被第三方伪造，保护发送者以防止被接收者伪造。

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

可为双方提供彼此身份保证的实体鉴别。

[来源：GB/T 15843.1—2017，3.18]

3.6

权标 token

由与特定的通信相关的数据字段构成的消息，它包含经过密码技术进行变换后的信息。

3.7

可信第三方 trusted third party

在安全相关活动中，被参与实体所信任的安全机构或其代理。

注：GB/T 15843 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]

3.8

单向鉴别 unilateral authentication

只是其中一个实体向另一个实体提供身份保证信息，而不反向进行的实体鉴别方式。

[来源：GB/T 15843.1—2017，3.39]

3.9

验证方 verifier

要求鉴别其他实体身份的实体本身或实体代表。

3.10

三元对等架构 Tri-Element Peer Architecture

TePA

一种基于三元对等理念的安全架构，面向网络空间连接双方提供对等安全保障。提供包括密码算法、安全机制、安全管理等一系列关键基础机制，鉴别、访问控制、机密性、完整性、抗抵赖等一系列基础安全功能，以及面向 TCP/IP 四层模型中每一层网络安全协议技术。

3.11

三元对等实体鉴别 TePA-based entity authentication

TePA-EA

基于三元对等架构，采用非对称密码算法，实现通信实体之间的对等鉴别。

4 符号与缩略语

4.1 符号

下列符号适用于本文件。

$Cert_X$ 实体 X 的证书。

I_X 表示实体X的标识符，可能是i_X或$Cert_X$。

i_X 字符串，用于标识实体 X 的标识。

M 作为数字签名算法的输入的数据串。

P_X 实体X的公开密钥。

Res_X 对实体X的公开密钥或者公开密钥证书的验证结果。

SID_{m}^{i} 用于唯一标识机制 m 及该机制中的签名字符串（i）的常量。

$sS_X(M)$ 使用实体 X 的私有签名密钥对数据串 M 产生的签名。签名应该使 M 能够被恢复。

$\frac{T_X}{N_X}$ 实体X使用的时变参数，可以是序列号N_X或时间戳T_X。

$X \| Y$ 按指定顺序将数据项 X 和 Y 连接在一起的结果。 如果将连接两个或多个数据项的

结果作为本文件中指定的机制之一的一部分进行签名，则应对连接结果进行组合，以便可将其唯一地解析为其组成数据所对应的字符串，即不存在进行解释时存在歧义的可能性。

注：可以根据应用以各种不同的方式实现后一种属性。例如，可以通过以下方式来保证：a）在使用该机制的整个字段中固定每个子字符串的长度，或b）使用保证唯一解码的方法（例如，使用区分编码）对串联字符串的序列进行编码，可参照ISO/IEC 8825-1[3]中定义的规则。

4.2 缩略语

下列缩略语适用于本文件。

CR	Challenge Response（挑战/响应）
MUT	Mutual（双向）
TS	Time Stamp（时间戳）
TP	Third Party（第三方，即可信第三方）
UNI	Unilateral（单向）

5 概述

5.1 时变参数

本文件规定的机制使用数字签名来实现单向或双向实体鉴别。附录B提供了指导来解释这些机制的安全性，并指导用户为他们的用例选择适当的机制。

为防止有效的身份鉴别信息再次被接受，应使用时变参数，例如时间戳，序列号或随机数（见GB/T 15843.1—2017 附录B）。

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

注：可以通过第一个实体在其所签名的数据块中包括其自己的随机数来防止一个实体对已经由第二实体操作过的数据块进行签名。在这种情况下，利用了不可预测性防止对预定义数据的签名。

5.2 权标

本文件中，权标（又称令牌）的形式如下：

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

本文件中，“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“未签名数据”是指“$X_1 \parallel \cdots \parallel X_i$”。

通常，“未签名数据”中包含的信息未经过本文件中的机制进行鉴别。

如果权标的“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，应符合GB/T 15851.3—2018的规定）或验证方已经拥有该“签名数据”，则在发送给声称方的权标中不需要包含该信息。

当使用不带消息恢复的数字签名机制时，应在相应的签名之前将“签名数据”M加入到“未签名数据”中，即$sS_X(M)$由$M \parallel sS_X(M)$代替。若接收方已拥有“签名数据”M中的一部分，则这部分数据可从“未签名数据”中删除。

5.3 Text 字段的用法

本文件的机制中规定的所有Text字段均可用于本文件范围之外的应用程序（Text字段可能为空）。它们之间的关系和内容取决于特定的应用。有关Text字段使用的信息，见附录C。

6 要求

本文件规定的鉴别机制中，待鉴别的实体通过表明它拥有某个私有签名密钥来证实其身份，这由实体使用其私有签名密钥对特定数据进行签名来完成。该签名能够由使用该实体的公开密钥的任何实体进行验证。

鉴别机制有下述要求：

a) 验证方应拥有声称方的有效公开密钥，即声称方所声称的实体的有效公开密钥；

获得有效公开密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公开密钥，可以引入可信第三方。另一种获得有效公开密钥的途径是利用可信的信使。

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自己知道的私有签名密钥。

c) 在实现本文件规定的机制时，所使用的私有签名密钥应不同于用于任何其他目的的密钥。

d) 在鉴别机制中，所有的签名数据串必须加以组合，以防止它们互换。

为了实现要求 d)，本文件中的机制在签名数据中包含常量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)，可将其定义为包括以下数据元素：

- 附录A中规定的对象标识符，尤其是用于标识ISO/IEC标准，部分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，可以忽略该常量。

签名的接收方应验证签名数据中的常量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，则鉴别过程会被攻击，或者不能成功完成。

附录A规定了用以标识本文件实体鉴别机制的对象标识符。

7 不引入在线可信第三方的机制

7.1 单向鉴别

7.1.1 概述

单向鉴别是指使用该机制时两个实体中只有一方被鉴别。

7.1.2 机制 UNI.TS —一次传递鉴别

这种鉴别机制中，声称方A启动过程并由验证方B对他进行鉴别。唯一性和时效性是通过产生并检验时间戳或序列号（见GB/T 15843.1-2017的附录B）来控制的。

鉴别机制见图1。

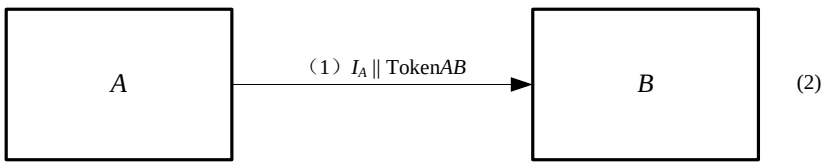

图 1 一次传递单向鉴别机制示意图

声称方A发送给验证方B的权标（TokenAB）形式是：

$$\mathrm{Token}AB = \mathrm{Text2} \| sS_A\left(SID_{UNI.TS}^{1} \| \frac{T_A}{N_A} \| i_B \| \mathrm{Text1}\right)$$

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环境。

注 1：为了防止预期的验证方之外的任何实体接受权标，在TokenAB的签名数据中需包含标识i_B。

注 2：这种机制的一种可能的应用是公开密钥或证书分发（见 GB/T 15843.1-2017 的附录 A）。

该机制执行如下步骤：

（1）A发送TokenAB给B，并可选地发送A的标识符I_A。

（2）收到TokenAB后，B执行如下步骤：

a) 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，或通过其他某种方式来确定实体A是否可信；

注 3：也可以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被视为安全问题。

b) 确认拥有A的有效公开密钥；

c) 通过检验权标中包含的A的签名，检查权标中的SID，检查时间戳或序列号，并检查TokenAB中的签名数据中的标识字段（i_B）的值是否等于实体B的可区分标识符来验证TokenAB。

7.1.3 机制 UNI.CR —两次传递鉴别

在这种鉴别机制中，验证方B启动此过程并对声称方A进行鉴别。唯一性和时效性是通过产生并检验随机数R_B（见 GB/T 15843.1-2017 的附录 B）来控制的。

鉴别机制见图 2。

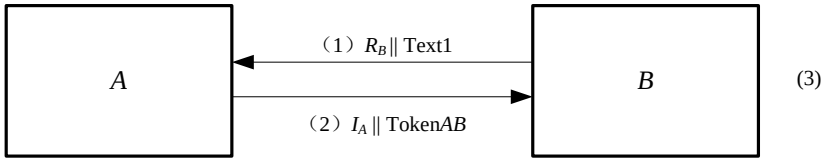

图 2 两次传递单向鉴别机制示意图

由声称方A发送给验证方B的权标（TokenAB）形式是：

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

注 1：在TokenAB的签名数据中可选地包含可区分标识B是为了防止信息被预期的验证方之外的实体所接受（例如，发生中间人攻击时）。

注 2：在TokenAB的签名数据中包含随机数R_A可以防止B在鉴别机制启动之前获得A对由B选择的数据的签名。这种保护方法是需要的，例如当A为了实体鉴别之外的其他目的使用同一密钥时。

该机制执行如下步骤：

（1）B向A发送随机数R_B，并可选地发送一个字段Text1。

（2）A产生并向B发送TokenAB，并可选地发送A的标识符I_A的证书。

（3）一旦收到包含TokenAB的消息，B就执行如下步骤：

a) 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，或通过其他某种方式来确定实体A是否可信；

注 3：也可以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被视为安全问题。

b) 确认拥有A的有效公开密钥；

c) 通过检验包含在权标中的A的签名，检查SID，检验步骤（1）中发送给A的随机数R_B是否与包含在TokenAB签名数据中的随机数相符，检验（TokenAB的签名数据中的标识字段（i_B）的值是否等于B的可区分标识符来验证TokenAB。

7.2 双向鉴别

7.2.1 概述

双向鉴别是指两个通信实体运用该机制彼此进行鉴别。

在 7.1.2 和 7.1.3 中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 中规定的步骤用了四个消息，但是，这些消息不需要依次地发送。这样，鉴别过程可以加快。

7.2.2 机制 MUT.TS—两次传递鉴别

这种鉴别机制中，唯一性和时效性是通过产生并检验时间戳或序列号（见 GB/T 15843.1-2017 的附录 B）来控制的。

鉴别机制见图 3。

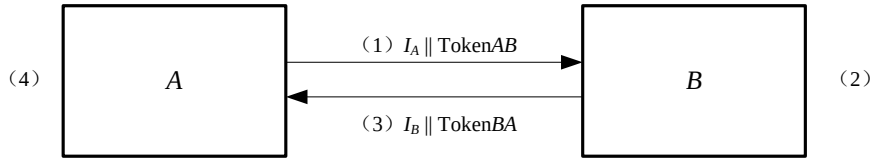

图 3 两次传递双向鉴别机制示意图

由A发送给B的权标（TokenAB）形式与**错误!未找到引用源。**所规定的相同。

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

由B发送给A的权标（TokenBA）形式为：

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

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能力以及环境。

注 1：在TokenBA和TokenAB的签名数据中包含标识i_A和标识i_B是必要的，这可以防止权标被预期的验证方之外的实体所接受。

注 2：如果TokenBA中省略$\frac{T_A}{N_A}$，则此机制的两条消息都不会以任何方式绑定在一起，除了时效上有隐含关系之外。该机制包括两次独立地使用 7.1.2 机制。该机制不再实现双向鉴别。

该机制执行如下步骤：

（1）A发送TokenAB给B，并可选地发送A的标识符I_A。

（2）在接收到含有TokenAB的消息时，B执行如下步骤：

a) 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，或通过其他某种方式来确定实体A是否可信；

注 3：也可以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被视为安全问题。

b) 确认拥有A的有效公开密钥；

c) 通过检验包含在权标中的A的签名，检查SID，检验时间戳或序列号，以及检验TokenAB签名数据中标识字段（i_B）的值是否等于实体B的可区分标识符来验证TokenAB。

（3）B向A发送TokenBA，并可选地发送B的标识符I_B。

（4）在接收到含有TokenBA的消息时，A执行如下步骤：

a) 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，或通过其他某种方式来确定实体B是否可信；

注 4：也可以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被视为安全问题。

b) 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；

c) 确认拥有B的有效公开密钥；

d) 通过检验包含在权标中的B的签名，检查SID，检验时间戳或序列号，以及检验TokenBA签名数据中标识字段（i_A）的值是否等于实体A的可区分标识符来验证TokenBA；

e) 检验TokenBA中的$\frac{T_A}{N_A}$是否等于步骤（1）发送TokenAB中的$\frac{T_A}{N_A}$相同。

7.2.3 机制 MUT.CR—三次传递鉴别

在这种机制中，唯一性和时效性是通过产生并检验随机数（见 GB/T 15843.1-2017 的附录 B）来控制的。

鉴别机制见图 4。

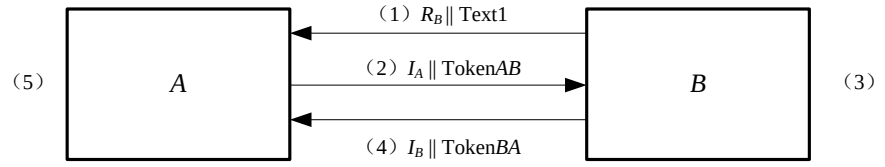

图 4 三次传递双向鉴别机制示意图

权标形式如下：

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

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

注 1：当 TokenAB中不包含标识i_B，或者TokenBA中不包含标识i_A时，A无法确定B是要对A进行鉴别（反之亦然）。另外，Text2和Text4的协商也不能保证。

注 2：在TokenAB的签名数据中包含随机数R_A可以防止B在鉴别机制启动之前获得A对由B选择的数据的签名。在TokenBA的签名数据中包含R'_B也有相同的作用。R'_B可以与R_B相同，但是在这种情况，在发送TokenAB之前，A能获得B对选择的数据的签名。

该机制执行如下步骤：

（1）B向A发送一个随机数R_B，并可选地发送一个字段Text1。

（2）A向B发送TokenAB，并可选地发送它的标识符I_A给B。

（3）收到包含TokenAB的消息后，B执行如下步骤：

a) 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，或通过其他某种方式来确定实体A是否可信；

注 3：也可以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被视为安全问题。

b) 确认拥有A的有效公开密钥；

c) 通过检验包含在权标中的A的签名，检查SID，检验步骤（1）中发送给A的随机数R_B是否与包含在TokenAB签名数据中的随机数相符，检验TokenAB的签名数据中的标识字段（i_B）的值是否等于B的可区分标识符来验证TokenAB。

（4）B向A发送TokenBA，并可选地发送它的标识符I_B给A。

（5）收到包含TokenBA的消息后，A执行如下步骤：

a) 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，或通过其他某种方式来确定实体B是否可信；

注 4：也可以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被视为安全问题。

b) 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；

c) 确认拥有B的有效公开密钥；

d) 通过检验包含在权标中的B的签名，检查SID，检验步骤（2）中发送给B的随机数R_A是否与包含在TokenBA签名数据中的随机数相符，检验TokenBA签名数据中标识字段（i_A）的值是否等于实体A的可区分标识符来验证TokenBA。

7.2.4 机制 MUT.CR.par—两次传递并行鉴别

在这种机制中，鉴别是并行进行的，唯一性和时效性用产生和检验随机数来控制（见 GB/T 15843.1-2017 的附录 B）。

鉴别机制见图 5。

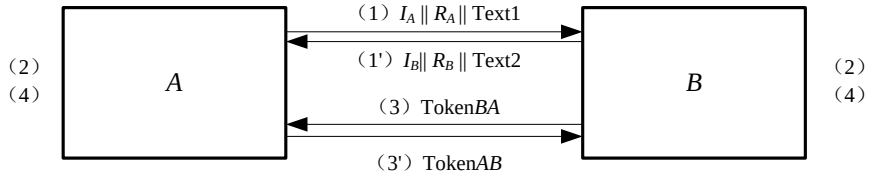

图 5 两次传递并行双向鉴别机制示意图

权标的形式与**错误!未找到引用源。**中类似：

$$\text{Token}AB = \text{Text4} \| sS_A\left(SID^1_{MUT.CR.par} \| R_A \| R_B \| i_B \| \text{Text3}\right)$$

$$\text{Token}BA = \text{Text6} \| sS_B\left(SID^1_{MUT.CR.par} \| R_B \| R_A \| i_A \| \text{Text5}\right)$$

注 1：随机数R_A应包含在TokenAB中，以防止B在鉴别机制启动之前获得A对由B选择的数据的签名。基于相同原因，TokenBA中也包含随机数R_B。依赖于步骤（1）和步骤（1'）中发送的消息到达接收端的相对时差，当一方选择随机数时，可能已知另一方的随机数。为防止此情况发生，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：因为消息顺序不固定，所以在这个机制里两个签名包括相同的标识$SID^1_{\text{MUT.CR.par}}$。

该机制执行如下步骤：

（1）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。

（1'） 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。

（2）A和B各执行如下步骤：

a) 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，或通过其他某种方式来确定对方实体是否可信；

注 3：它们也可以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被视为安全问题。

b) A和B各自确认拥有对方的有效公开密钥。

（3）A向B发送TokenAB，它包括步骤（2）A所信任的B的标识字段（i_B）。

（3'） B向A发送TokenBA，它包括步骤（2）B所信任的A的标识字段（i_A）。

（4）A和B执行如下步骤：

a) 它们各自检验包含在权标中的签名（使用步骤（2）中公开密钥）和检查SID验证所接收到的权标；
b) 它们各自检查之前发送的随机数是否与包括在权标中的签名数据中的第一个随机数相同；
c) 它们各自检查之前接收的随机数（在步骤（1））是否与包括在权标中的签名数据的第二个随机数相同；
d) 它们各自检查包括在权标中的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 概述

本章中机制的实现应使用ISO/IEC 14888（所有部分）或GB/T 15851.3—2018中定义的签名方案之一。

在本章中规范的系列TePA-EA实体鉴别机制中，权标和Text字段的形式遵循第3章和第5章中的描述。此外，在本章中规范的机制中，字段Res_A，Res_B，Status和Failure的值应具有以下形式：

— $Res_A = (Cert_A \parallel \text{Status})$，$(i_A \parallel P_A)$或Failure。
— $Res_B = (Cert_B \parallel \text{Status})$，$(i_B \parallel P_B)$或Failure。
— Status = True或Failure。如果进行证书验证（例如，根据ISO/IEC 9594-8[4]，ITU-T X.509[7]或TP所在域的安全策略）失败，则该字段的值应设置为Failure。否则，该字段的值设置为True。
— Failure：如果TP无法找到公开密钥或实体X的证书，则$Res_X\left(X \in \{A, B\}\right)$将设置为Failure。

在本章定义的机制中，如果TP确认X$\left(X = \{A, B\}\right)$的身份与公开密钥$P_X$的映射，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$Cert_X$允许被用于作为一种标识，则应有一种预安排的方式允许TP区分这两种类型的标识。$Res_X\left(X = \{A, B\}\right)$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	$(Cert_X \| \| \text{Status})$ 或 Failure

8.2 单向鉴别

8.2.1 概述

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TP）来验证对方的公开密钥。该可信第三方应具有验证A（或B）公开密钥的真实性的能力。实体A（或B）必须拥有TP公开密钥的可靠副本。

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TP的实体鉴别、原发鉴别和鉴别结果的防重放。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 GB/T 15851.3-2018 中规定的签名机制之一。

8.2.2 机制 TP.UNI.1—四次传递鉴别（A发起）

在本机制中，声称方B被验证方A所鉴别，该机制由A发起，使用可信第三方TP参与鉴别，TP能够验证实体B的公开密钥，实体A拥有TP的公开密钥。

鉴别机制见图 6。

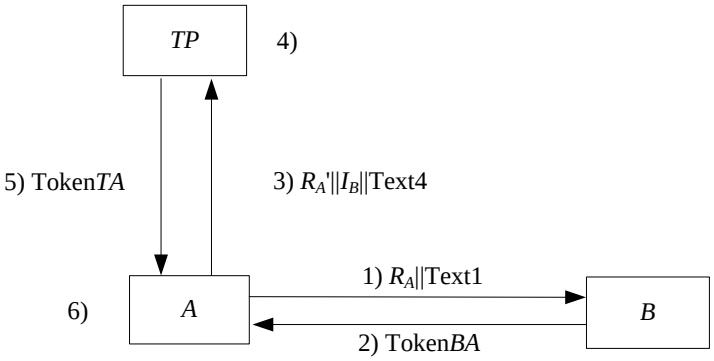

图 6 四次传递鉴别（A发起）

权标结构如下：

TokenBA = Text2 ‖ M ‖ $sS_B(SID^1_{TP.UNI.1} ‖ R_B ‖ R_A ‖ i_A ‖ \text{Text3})$

TokenTA = Text5 ‖ M ‖ $sS_T(SID^2_{TP.UNI.1} ‖ R'_A ‖ Res_B ‖ \text{Text6})$

该机制执行如下步骤：

（1）A发送随机数R_A及可选文本Text1给B。

（2）B发送权标TokenBA给A。

（3）A发送随机数R'_A，标识符I_B以及可选文本Text4给TP。

（4）TP收到A在步骤（3）发来的消息后，执行如下步骤：如果I_B是i_B，TP提取P_B；如果I_B是$Cert_B$，TP检查证书Cert_B的有效性。TP检查证书有效性的过程需要防止dos攻击。提供保护的机制超出了本标准的范围。

（5）TP发送TokenTA给A，TokenTA中的Res_B字段必须为：B的证书及其状态；或者是B的可区分标识符及其公开密钥；或者是Failure失败标识。

（6）实体A收到TP在步骤（5）发来的消息后，执行下列操作：

a) 通过校验包含在TokenTA中的TP的签名，检查SID，检查签名数据中包含的R'_A是否与在步骤（3）中发送给TP的R'_A相等，并检查Res_B不为Failure来验证TokenTA；

注：也可以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被视为安全问题。

b) 从消息中提取实体B的公开密钥，通过校验在步骤（2）收到的权标中实体B的签名，检查SID，检查TokenBA中的标识字段（i_A）是否与实体A的可区分标识符相等，并检查TokenBA中的随机数R_A是否与在步骤（1）发送给B的随机数相等来验证TokenBA。

8.2.3 机制 TP.UNI.2—四次传递鉴别（B发起）

在本机制中，声称方A被验证方B所鉴别，该机制由实体B发起，使用可信第三方TP参与鉴别。该可信第三方应具有验证A的公开密钥的真实性的能力。实体B必须拥有TP公开密钥的可靠副本。

鉴别机制见图 7。

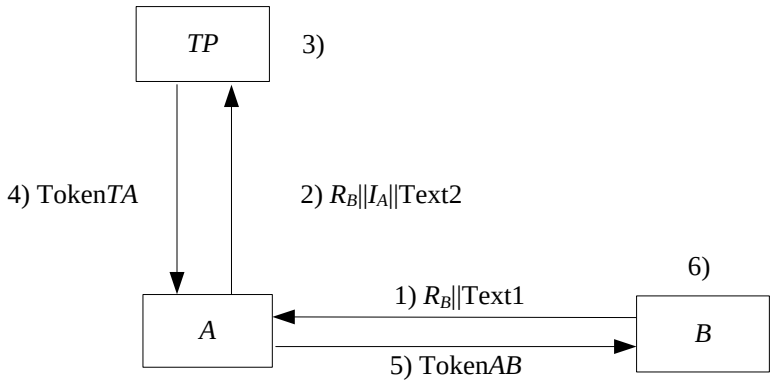

图 7 四次传递鉴别（B发起）

权标结构如下：

TokenTA = Text3 ‖ M ‖ $sS_T(SID^1_{TP.UNI.2}$ ‖ R_B ‖ Res_A ‖ Text4)

TokenAB = Text5 ‖ M ‖ $TokenTA$ ‖ $sS_A(SID^2_{TP.UNI.2}$ ‖ R_A ‖ R_B ‖ i_B ‖ Text6)

该机制执行如下步骤：

（1）B发送随机数R_B及可选文本Text1给A。

（2）A发送R_B，I_A和可选字段Text2给TP。

（3）收到A在步骤（2）中发来的消息后，TP执行如下操作：如果I_A是i_A，TP提取P_A；如果I_A是$Cert_A$，TP检查证书$Cert_A$的有效性。TP检查证书有效性的过程需要防止拒绝服务攻击。提供保护的机制超出了本文件的范围。

（4）TP发送TokenTA给A。TokenTA中的Res_A必须为：A的证书及其状态；或者是A的可区分标识符及其公开密钥；或者是Failure失败标识。

（5）A发送权标TokenAB给B。

（6）收到A在步骤（5）中发来的消息后，B执行如下操作：

a) 通过校验包含在TokenTA中的TP的签名，检查SID，检查签名数据中包含的R_B是否与在步骤（1）中发送给A的R_B相等，并检查Res_A不为Failure来验证TokenTA。

注：也可以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被视为安全问题。

b) 从消息中提取实体A的公开密钥，通过校验包含在权标中的实体A的签名，检查SID，检查TokenAB中的标识字段(i_B)是否与实体B的可区分标识符相等，并检查TokenAB中的随机数R_B是否与在步骤（1）发送给A的随机数相等来验证TokenAB。

8.3 双向鉴别

8.3.1 概述

8.3 中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来验证彼此的公开密钥。

如果仅使用单个在线可信第三方，则由TP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TP_A和TP_B表示。仅通过TP_A验证A的公开密钥的真实性，仅通过TP_B验证B的公开密钥的真实性。实体A信任TP_A（A认为由TP_A签名的任何断言都是有效的），并应拥有TP_A的公开密钥的可靠副本。实体B信任TP_B（B认为TP_B签名的任何断言都是有效的），并应拥有TP_B的公开密钥的可靠副本。TP_A和TP_B互相信任。TP_A具有TP_B的公开密钥的可靠副本，且TP_B具有TP_A的公开密钥的可靠副本。

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TP，TP_A或TP_B的实体鉴别，以及原发鉴别和鉴别结果的防重放。五次传递鉴别和七次传递鉴别都是一种原子性业务。

注 1：8.3 中规定的机制使用在封闭的环境里，所有的实体共享同一个TP，拥有TP公开密钥的可靠副本。如果使用选项 1，TP只提供证书校验服务。如果使用选项 2，TP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。

注 2：如果选项 1 应用在B（或A）知晓TP正在校验A（或B）的身份，选项 1 中的TP签名里的Text字段应该各自包括I_A（或I_B）。更具体地讲，TP使I_A作为TokenTA第一个签名的Text字段部分，同样地，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TP应该就Text字段中包括的I_A（或I_B）位置和格式达成共识。

8.3.2 机制 TP.MUT.1—五次传递鉴别（A发起）

在这种鉴别机制中，唯一性/时效性通过产生和检查随机数来控制（见GB/T 15843.1-2017的附录B）。鉴别机制见图 8 示。

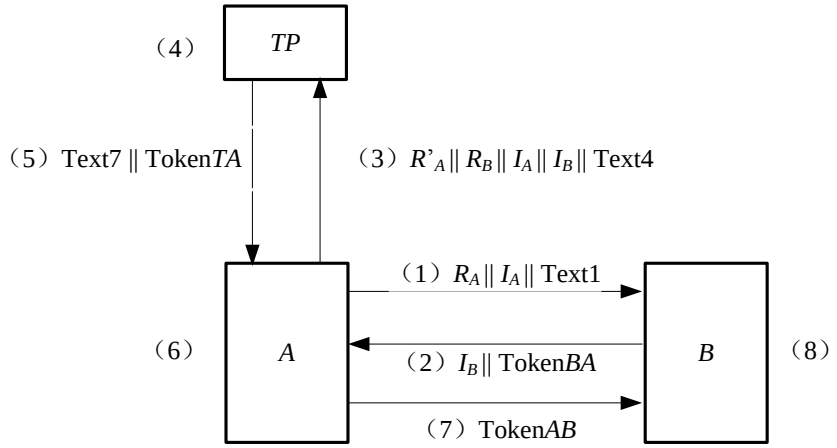

图 8 五次传递鉴别机制（A发起）

权标结构如下：

选项 1：

$$\text{Token}BA = \text{Text3} \parallel sS_B(SID^1_{\text{TP.MUT.1}-1} \parallel i_B \parallel R_A \parallel R_B \parallel i_A \parallel \text{Text2})$$

$$\text{Token}TA = sS_T(SID^2_{\text{TP.MUT.1}-1} \parallel R'_A \parallel Res_B \parallel \text{Text6}) \parallel sS_T(SID^3_{\text{TP.MUT.1}-1} \parallel R_B \parallel Res_A \parallel \text{Text5})$$

$$\text{Token}AB = \text{Text9} \parallel sS_T(SID^3_{\text{TP.MUT.1}-1} \parallel R_B \parallel Res_A \parallel \text{Text5}) \parallel sS_A(SID^4_{\text{TP.MUT.1}-1} \parallel R_B \parallel R''_A \parallel i_B \parallel i_A \parallel \text{Text8})$$

选项 2：

$$\text{Token}BA = \text{Text3} \parallel sS_B(SID^1_{\text{TP.MUT.1}-2} \parallel i_B \parallel R_A \parallel R_B \parallel i_A \parallel \text{Text2})$$

$$\text{Token}TA = sS_T(SID^2_{\text{TP.MUT.1}-2} \parallel R'_A \parallel R_B \parallel Res_A \parallel Res_B \parallel \text{Text5})$$

$$\text{Token}AB = \text{Text9} \parallel \text{Token}TA \parallel sS_A(SID^3_{\text{TP.MUT.1}-2} \parallel R_B \parallel R''_A \parallel i_B \parallel i_A \parallel \text{Text8})$$

注1：本机制的实现者可以支持一个或者两个上述选项。

注2：随机数R_A应包含在TokenAB中，以防止B在鉴别机制启动之前获得A对由B选择的数据的签名。出于类似的理由，TokenBA中也包含随机数R_B。

该机制执行如下步骤：

（1）A发送随机数R_A、标识符I_A和可选字段Text1到B。

（2）B发送TokenBA和标识符I_B到A。

（3）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TP。

（4）收到来自步骤（3）中A的消息后，TP执行如下步骤：如果$I_A = i_A$，且$I_B = i_B$，则TP提取P_A和P_BP；如果$I_A = Cert_A$，且$I_B = Cert_B$，则TP检查$Cert_A$和$Cert_B$的有效性。TP检查证书有效性的过程可能需要防范拒绝服务攻击。提供保护的机制超出了本文件的范围。

（5）TP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公开密钥，或者是指示符Failure。

（6）收到来自步骤（5）中TP的消息后，A执行如下步骤：

a) 通过校验包含在TokenTA中TP的签名，检查SID，检查步骤（3）中发送给TP的随机数R'_A与包含在TokenTA中的TP的签名数据中的随机数R'_A是否一致来验证TokenTA。

必须检查包含Res_A的签名。可选地检查不包含Res_A的签名。如果检查不包含Res_A的签名，则R_B必须检查。

注 3：也可以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被视为安全问题。

b) 从消息中提取B的公开密钥，通过校验在步骤（2）中收到的权标中B的签名，检查SID，检查包含在TokenBA中的B的签名数据中的标识字段（i_A）与A的可区分标识符是否一致，检查包含在TokenBA中的随机数R_A与在步骤（1）中发送给B的随机数R_A是否一致来验证TokenBA。

（7）A发送TokenAB到B。

（8）收到来自步骤（7）中A的消息后，B执行如下步骤：

a) 通过校验包含在TokenTA（实体A）或者TokenAB（实体B）中TP的签名，检查SID，检查包含在TokenTA中TP的签名数据中的随机数R_B与在步骤（2）中发送给A的随机数R_B是否一致来验证TokenTA。

注 4：也可以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被视为安全问题。

b) 从消息中提取A的公开密钥，通过校验包含在TokenAB中A的签名，检查SID，检查包含在TokenAB中的A的签名数据中的标识字段（i_B）与B的可区分标识符是否一致，检查包含在TokenAB中A的签名数据中的随机数R_B与在步骤（2）中发送给A的随机数R_B是否一致来验证TokenAB。

8.3.3 机制 TP.MUT.2—五次传递鉴别（B发起）

在这种鉴别机制中，唯一性/时效性通过产生和检查随机数来控制（见GB/T 15843.1-2017的附录B）。该鉴别机制见图 9。

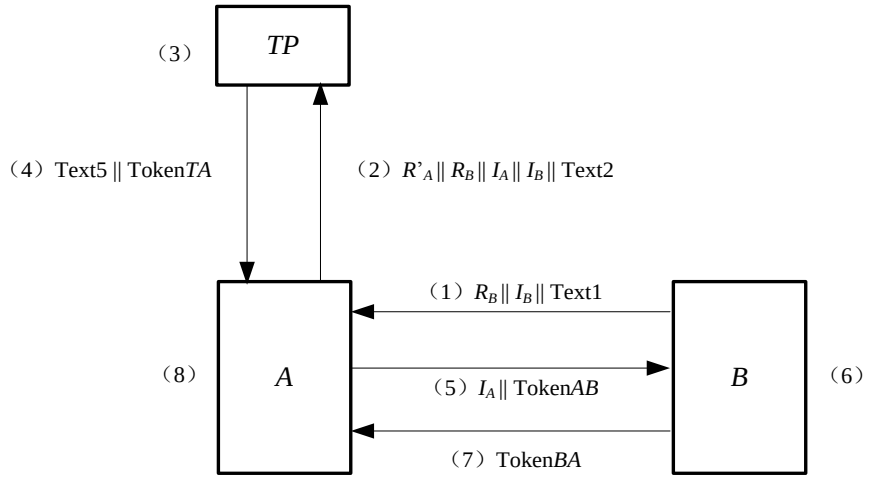

图 9 五次传递鉴别机制（B发起）

权标结构如下：

选项 1：

$$\text{Token}TA = sS_T(SID^1_{\text{TP.MUT.2}-1} \| R'_A \| Res_B \| \text{Text4}) \| sS_T(SID^2_{\text{TP.MUT.2}-1} \| R_B \| Res_A \| \text{Text3})$$

$$\text{Token}AB = \text{Text7} \| sS_T(SID^2_{\text{TP.MUT.2}-1} \| R_B \| Res_A \| \text{Text3}) \| sS_A(SID^3_{\text{TP.MUT.2}-1} \| R_B \| R_A \| i_B \| i_A \| \text{Text6})$$

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

选项 2：

$$\text{Token}TA = sS_T(SID^1_{\text{TP.MUT.2}-2} \| R'_A \| R_B \| Res_A \| Res_B \| \text{Text3})$$

$$\text{Token}AB = \text{Text7} \| \text{Token}TA \| sS_A(SID^2_{\text{TP.MUT.2}-2} \| R_B \| R_A \| i_B \| i_A \| \text{Text6})$$

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

注1：本机制的实现者可以支持一个或者两个上述选项。

该机制执行如下步骤：

（1）B发送随机数R_B、标识符I_B和可选字段Text1到A。

（2）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TP。

（3）收到来自步骤（2）中A的消息后，TP执行如下步骤：如果$I_A = i_A$，且$I_B = i_B$ =，则TP提取P_A和P_B；如果$I_A = Cert_A$，且$I_B = Cert_B$，则TP检查$Cert_A$和$Cert_B$的有效性。TP检查证书有效性的过程可能需要防范拒绝服务攻击。提供保护的机制超出了本文件的范围。

（4）TP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公开密钥，或者是指示符Failure。

（5）A发送身份I_A和TokenAB到B。

（6）收到来自步骤（5）中A的消息后，B执行如下步骤：

a) 通过校验包含在TokenAB中TP的签名，检查SID，检查步骤（1）中发送给A的随机数R_B与包含在TokenAB中的TP的签名数据中的随机数R_B是否一致来验证TokenAB。

注 2：也可以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被视为安全问题。

b) 从消息中提取A的公开密钥，通过验证包含在TokenAB中A的签名，检查SID，检查包含在TokenAB中的A的签名数据中的标识字段（i_B）与B的可区分标识符是否一致，检查包含在

TokenAB中的A的签名数据中的随机数R_B与在步骤（1）中发送给A的随机数R_B是否一致来验证TokenAB。

（7）B发送TokenBA到A。

（8）收到来自步骤（7）中B的消息后，A执行如下步骤：

a) 通过校验包含在TokenTA中TP的签名，检查包含在TokenTA中TP的签名数据中的随机数R'_A与在步骤（2）中发送给TP的随机数R'_A是否一致来验证步骤（4）消息里的TokenTA。必须检查包含Res_B的签名。可选地检查不包含Res_B的签名。

注 3：也可以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被视为安全问题。

b) 从步骤（4）的消息中提取B的公开密钥，通过校验包含在TokenBA中B的签名，检查包含在TokenBA中的B的签名数据中的标识字段（i_A）与A的可区分标识符是否一致，检查包含在TokenBA中的随机数R_A与在步骤（5）中发送给B的随机数R_A是否一致来验证TokenBA。

8.3.4 机制 TP.MUT.3—七次传递鉴别

这种鉴别机制有七条消息的传递，使用两个在线可信第三方（TP_A和TP_B），唯一性/时效性通过产生和检查随机数来控制（见 GB/T 15843.1-2017 的附录 B）。

鉴别机制见图 10。

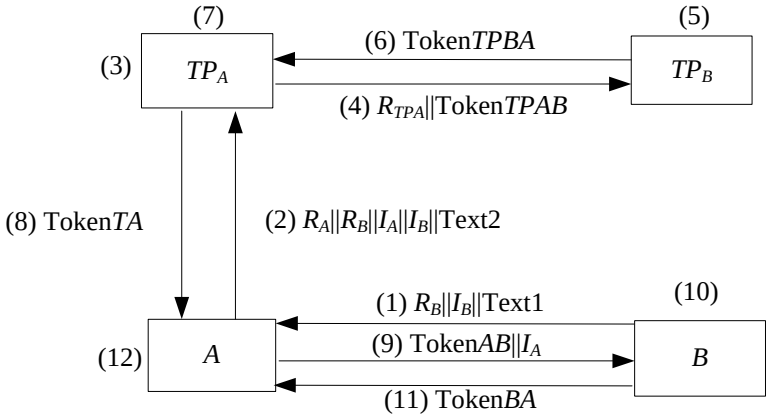

图 10 七次传递鉴别机制

权标结构如下：

$$\text{Token}TPAB = M \parallel sS_{TPA}(SID^{1}_{\text{TP.MUT.3}} \parallel Res_A \parallel I_B \parallel R_B \parallel \text{Text3})$$

$$\text{Token}TPBA = M \parallel sS_{TPB}(SID^{2}_{\text{TP.MUT.3}} \parallel Res_A \parallel R_B \parallel \text{Text4}) \parallel sS_{TPB}(SID^{3}_{\text{TP.MUT.3}} \parallel Res_B \parallel R_{TPA} \parallel \text{Text5})$$

$$\text{Token}TA = M \parallel sS_{TPA}(SID^{4}_{\text{TP.MUT.3}} \parallel Res_B \parallel R'_A \parallel \text{Text6}) \parallel sS_{TPB}(SID^{2}_{\text{TP.MUT.3}} \parallel Res_A \parallel R_B \parallel \text{Text4})$$

$$\text{Token}AB = M \parallel sS_{TPB}(SID^{2}_{\text{TP.MUT.3}} \parallel Res_A \parallel R_B \parallel \text{Text4}) \parallel sS_{A}(SID^{5}_{\text{TP.MUT.3}} \parallel R_B \parallel R_A \parallel i_B \parallel i_A \parallel \text{Text7})$$

$$\text{Token}BA = M \parallel sS_{B}(SID^{6}_{\text{TP.MUT.3}} \parallel R_A \parallel R_B \parallel i_A \parallel i_B \parallel \text{Text8})$$

该机制执行如下步骤：

（1）B发送随机数R_B、标识符I_B和可选字段Text1到A发送的。

（2）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TP_A。

（3）收到来自步骤（2）中A的消息后，TP_A执行如下步骤：如果$I_A = i_A$，则TP_A提取P_A；如果$I_A = Cert_A$，则TP_A检查$Cert_A$的有效性。TP_A检查证书有效性的过程可能需要防范拒绝服务攻击。提供保护的机制超出了本文件的范围。

（4）TP_A发送R_{TPA}和Token$TPAB$到TP_B。

（5）TP_B收到TP_A发送的消息后，执行如下步骤：

a) 通过验证Token$TPAB$中TP_A的签名来验证包含在权标中的TP_A的签名

b) 如果$I_B = i_B$，则TP_B提取P_B；如果$I_B = Cert_B$，则TP_B检查$Cert_B$的有效性。TP_B检查证书有效性的过程可能需要防范拒绝服务攻击。提供保护的机制超出了本文件的范围。

（6）TP_B向TP_A发送权标Token$TPBA$。

（7）TP_A收到TP_B发送的消息后，TP_A通过下列方式校验Token$TPBA$：验证包含在权标的TP_B的签名，检查包含在Token$TPBA$中签名数据中的随机数R_{TPA}与在步骤（4）中发送给TP_B的随机数R_{TPA}是否一致。

（8）TP_A发送权标TokenTA给A，包含、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公开密钥，或者是指示符Failure。

（9）A发送TokenAB和标识符I_A到B。

（10）B收到步骤（9）的消息后，执行如下步骤：

a) 通过校验包含在TokenAB中的TP_B的签名，检查包含在TokenAB中签名数据中的随机数R_B与在步骤（1）中发送给A的随机数R_B是否一致来验证TP_B的签名。

注 1：也可以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被视为安全问题。

b) 从消息中提取A的公开密钥，通过校验包含在TokenAB中A的签名，检查包含在TokenAB中的A的签名数据中的标识字段（i_B）与B的可区分标识符是否一致，检查包含在TokenAB中的随机数R_B与在步骤（1）中发送给A的随机数R_B是否一致来验证TokenAB。

（11）B发送TokenBA到A。

（12）A收到B的消息后，执行如下步骤：

a) 通过校验包含在TokenTA中的TP_A的签名，检查包含在TokenTA中签名数据中的随机数R'_A与在步骤（2）中发送给TP_A的随机数R'_A是否一致来验证TokenTA。

注 2：也可以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被视为安全问题。

b) 从消息中提取B的公开密钥，通过校验包含在TokenBA中B的签名，检查包含在TokenBA中的B的签名数据中的标识字段（i_A）与A的可区分标识符是否一致，检查包含在TokenBA中的随机数R_A与在步骤（9）中发送给B的随机数R_A是否一致来验证TokenBA。

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 后续客体标识符的使用

紧随实体鉴别标识符之后的是一个标识数字签名算法的信息对象（如ISO/IEC 14888（全部）或GB/T 15851.3—2018中规范的算法），以及相关参数（如ISO/IEC 10118-3[5]指定的哈希函数）。

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明一个实体是所声称的实体。为了使此属性正式化，根据GB/T 15843.1，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。有关本文件第2版的广泛安全性分析，参见[1]。该报告考虑以下安全属性：

— 对方是存活的；

— 与参与方在有关代理及其角色上的共识较弱；

— 在可能的情况下与对方就随机数和Text字段达成数据协议。

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（假设根据GB/T15843.1附录B正确的使用了时变参数）。对于涉及在线可信第三方的机制，尽管实体A和B都保证了TP的存活性，但仅在A和B之间考虑了这些属性，而在TP和A与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，弱协议和数据协议，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，弱协议和数据协议。

注：弱协议和数据协议的要求意味着不能仅通过两种单向鉴别机制的组合来实现双向鉴别。

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确定其对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，需要拥有声称方的公开密钥的受信任副本。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.将其留给A和（或）B进行证书和（或）公开密钥的验证（可能涉及辅助机制，例如与第三方合作的OCSP）。

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

TP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，TP必须在线可用。而且，TP会在每次执行该机制时了解所涉及的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，而不管该信息是否真实。

B.2 机制的比较和选择

B.2.1 比较

表B.1概述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）通过用唯一标识符标记每个签名消息并通过在整个机制中确保对串联字符串的唯一解码而得到解决。

表 B.1 机制的安全属性

	双向	TP	消息条数	新鲜性与唯一性
UNI.TS 机制	N	N	1	T_A/N_A
UNI.CR 机制	N	N	2	R_A
MUT.TS 机制	Y	N	2	T_A/N_A和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
TP.UNI.1 机制	N	Y	4	R_A和R'_A
TP.UNI.2 机制	N	Y	4	R_B
TP.MUT.1 机制	Y	Y	5	R_A，R'_A和R_B
TP.MUT.2 机制	Y	Y	5	R_A，R'_A和R_B
TP.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，可考虑以下几个因素：

— 需要安全的通信信道时：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[6]中的密钥建立方法来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来决定。

— 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来确保实体鉴别的新鲜性/唯一性。如GB/T 15843.1-2017附录B中的详细说明，这需要同步时钟（用于时间戳）或额外的簿记来验证序列号。缺少这些附加措施将易遭受攻击。在多数情况下，最好使用挑战-响应机制来避免这些附加措施。

— 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速和延迟，使用的是单向还是双向通信，双方的处理器和内存的能力等。

— 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，可以考虑使用TP −*类的机制之一。

附 录 C

（资料性）

Text字段的用法

本文件第 5 章和第 6 章规定的权标包括了 Text 字段。在一次给定传递中不同 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。

若使用了没有消息恢复的数字签名方案，并且签名的 Text 字段不是空的，则验证方在检验签名之前要拥有文本。在本附录中，“签名 Text 字段”指签名数据中的 Text 字段，而“未签名 Text 字段”指未签名数据中的 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权标的签名 Text 字段和（作为一部分放到）未签名 Text 字段中。

若权标未含有（足够的）冗余，签名 Text 字段可以用来提供额外的冗余。

签名 Text 字段可以用来指示，权标只有用于实体鉴别目的时才是有效的。还应注意，一个实体可能会蓄意地企图选择一个“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，则需要在签名 Text 字段和（若必要）未签名 Text 字段中，包含预期的验证方的身份。

未签名 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。若不用证书方式来分发公开密钥，则要求使用这种信息让验证方确定用哪个公开密钥来鉴别声称方。

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 8824 (all parts) | ITU-T Rec. X.680-series, Information technology –Abstract Syntax Notation One (ASN.1)

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

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

[5] ISO/IEC 10118-3, Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions

[6] ISO/IEC 11770 (all parts), Information technology – Security techniques – Key management

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