ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.3—2016/ISO/IEC 9798-3:1998
代替 GB/T 15843.3—2008

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 9798-3:1998,IDT)

2016-04-25 发布　　2016-11-01 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 15843《信息技术　安全技术　实体鉴别》目前分为五个部分：

——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。

本部分为GB/T 15843的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 15843.3—2008《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》。本部分与GB/T 15843.3—2008相比，主要技术变化如下：

——增补了引入在线可信第三方的鉴别机制(见第6章)；

——增补了OID和ASN.1语法(见附录B)。

其中，对GB/T 15843.3—2008修改时涉及的有关章条的信息如下：

修改项号	GB/T 15843.3—2008章条号	修改说明
1	第1章	替换了第1章的第三段文字
2	第3章	在第3章最后增加了三个术语说明
3		在第5章的后面增加第6章
4	附录A	替换了附录A的第一段文字
5		在附录A的后面增加附录B

本部分使用翻译法等同采用ISO/IEC 9798-3:1998《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》及其Amd.1:2010《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　第1号修改单：引入在线可信第三方的鉴别机制》，仅有编辑性修改。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：西安西电捷通无线网络通信股份有限公司、国家密码管理局商用密码检测中心、信息安全国家重点实验室、中国电子技术标准化研究所、国家无线电监测中心检测中心、西安电子科技大学、西安邮电大学、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、中国信息安全认证中心、国家信息安全工程技术研究中心、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、公安部第一研究所、工业和信息化部通信计量中心、公安部信息安全等级保护评估中心、国防科技大学、北京市政务网络管理中心、重庆邮电大学、宇龙计算机通信科技(深圳)有限公司、中国人民大学、中国人民解放军信息安全测评认证中心、中国电信集团公司、国家信息中心、北京大学深圳研究生院、中国电力科学研究院、北京中电华大电子设计有限责任公司、东南大学、中国移动通信集团设计院有限公司、中国人民解放军信息工程大学、江南计算技术研究所、北京邮电大学、上海龙照电子有限公司、北京五龙电信技术公司、北京网贝合创科技有限公司、深圳市宏电技术股份有限公司、北大方正集团公司、海尔集团公司、北京广信融科技术有限公司、北京六合万通微电子技术有限公司、弘浩明传科技(北京)有限公司、北京城市热点资讯有限公司、北京华安广通科技发展有限公司、迈普通信技术有限公司、长春吉大正元信息技术股份有限公司、清华大学、北京天一集成科技有限公司、桂林电子科技大学、西安

立人科技股份有限公司、宽带无线 IP 标准工作组、WAPI 产业联盟。

本部分主要起草人：黄振海、赖晓龙、李大为、冯登国、宋起柱、铁满霞、曹军、李建东、林宁、舒敏、朱志祥、陈晓桦、郭晓雷、李京春、余亚莉、王育民、张变玲、肖跃雷、高波、高昆仑、潘峰、胡亚楠、蒋庆生、肖雳、朱建平、贾焰、施伟年、李琴、李广森、吴亚非、梁朝晖、梁琼文、罗旭光、龙昭华、沈凌云、张伟、徐平平、马华兴、高峰、仇洪冰、朱跃生、王雅辉、兰天、王志坚、杜志强、张国强、田小平、田辉、张永强、寿国梁、毛立平、曹竹青、郭志刚、高宏、韩康、王钢、白国强、陈志峰、李建良、李大伟、王立仁、高原、岳林、井经涛。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.3—1998、GB/T 15843.3—2008。

引　言

GB/T 15843 的本部分定义了采用数字签名技术的实体鉴别机制，分为单向鉴别和相互鉴别两种。其中单向鉴别按照消息传递的次数，又分为一次传递鉴别和两次传递鉴别；相互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、两次传递并行鉴别、五次传递鉴别。

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

本部分凡涉及密码算法的相关内容，按国家有关法规实施。

本文件的发布机构提请注意，声明符合本文件时，可能涉及第 6 章与“一种实体双向鉴别方法”“一种基于可信第三方的实体双向鉴别方法及其系统”等相关的专利的使用。

本文件的发布机构对于该专利的真实性、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保证，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：

专利权人：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：刘长春

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这些专利的责任。

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

GB/T 15843的本部分规定了采用数字签名技术的实体鉴别机制。有两种鉴别机制是单个实体的鉴别(单向鉴别),其余是两个实体的相互鉴别机制。

本部分中规定的机制采用诸如时间戳、序号或随机数等时变参数,防止先前有效的鉴别信息以后又被接受或者被多次接受。

如果采用时间戳或序号,则单向鉴别只需一次传递,而相互鉴别则需两次传递。如果采用随机数的挑战-响应方法,单向鉴别需两次传递,相互鉴别则需三次、两次传递并行或五次传递(依赖于所采用的机制)。

本部分适用于所有有鉴别需求的应用和设备。

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 15843.1—2008　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 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 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、定义和符号

GB/T 15843.1—2008界定的术语、定义以及下列符号适用于本文件。

I_A:实体A的身份标识,可以是A或者CertA

I_B:实体B的身份标识,可以是B或者CertB

ResX:实体X的证书验证结果或实体X的公钥

4　要求

本部分规定的鉴别机制中,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。这要由实体使用其私有签名密钥对特定数据签名来完成。该签名能够由使用该实体的公开验证密钥的任何实体来验证。

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;

b) 声称方应拥有仅由声称方自己知道的私有签名密钥。

若这两条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。

注 1：获得有效公开密钥的一种途径是用证书方式(见 GB/T 15843.1—2008 的附录 C)。证书的产生、分发和撤销都超出了本部分的范围。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。

注 2：有关数字签名方案的参考文献在 GB/T 15843.1—2008 的参考文献中有描述。

5 机制

5.1 概述

本部分规定的实体鉴别机制使用了时变参数，如时间戳、序号或随机数(见 GB/T 15843.1—2008 的附录 B 和本条的注 1)。

本部分中，权标的(又称令牌)形式如下：

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

本部分中，“签名数据”指的是“$Y_1||\cdots||Y_j$”，它用作数字签名方案的输入，而“未签名数据”指的是“$X_1||\cdots||X_i$”。

若权标签名数据所含信息能从签名中恢复，则它不需要包含在权标的未签名数据中(见 GB 15851—1995)。

若权标签名数据的文本字段所含信息不能从签名中恢复，则它应该包含在权标的未签名文本字段中。

若在权标的签名数据中的信息(如验证方产生的随机数)对于验证方是已知的，则它不必包含在声称方所发送的权标未签名数据中。

以下机制中规定的所有文本字段同样适用于本部分范围之外的应用(文本字段可能是空的)。它们的关系和内容取决于具体应用。有关文本字段使用的信息参见附录 A。

注 1：为了防止一个实体对其签名的数据块是由第二个实体蓄意构造的，第一个实体可在其签名的数据块中包含它自己的随机数。在这种情况下，随机数的加入使得签名值具有了不可预测性，从而防止了对预定义数据的签名。

注 2：由于证书的分发超出了本部分的范围，证书的发送在所有的机制中是可选的。

附录 B 指定了本部分所规定的实体鉴别机制的 OID 和 ASN.1 语法，用于对特定机制的准确引用。

5.2 单向鉴别

5.2.1 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。

5.2.2 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 对它进行鉴别。唯一性和时效性是通过产生并检验时间戳或序号(见 GB/T 15843.1—2008 的附录 B)来控制的。

鉴别机制如图 1 所示。

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：

$$TokenAB = \begin{matrix} T_A \\ N_A \end{matrix} \;||\; B \;||\; Text2 \;||\; sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \;||\; B \;||\; Text1\right)$$

此处声称方 A 用序号 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：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符 B。

注 2：在一般情况下，Text2 不由这个过程鉴别。

注 3：这种机制的一种可能的应用是密钥分发(见 GB/T 15843.1—2008 的附录 A)。

(1) A 发送 TokenAB 给 B。是否发送 A 的证书是可选的。

(2) 在接收到含有 TokenAB 的消息时，B 执行下列步骤：

(i) 通过验证 A 的证书或者用其他方式确保拥有 A 的有效公开密钥；

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

5.2.3 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—2008 的附录 B)来控制的。

鉴别机制如图 2 所示。

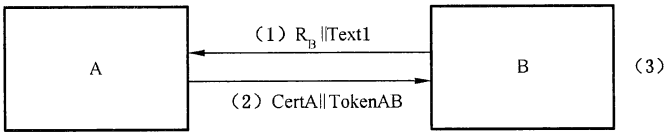

图 2 两次传递单向鉴别机制示意图

由声称方 A 发送给验证方 B 的权标(TokenAB)形式是：

$$TokenAB = R_A \;||\; R_B \;||\; B \;||\; Text3 \;||\; sS_A(R_A \;||\; R_B \;||\; Text2)$$

在 TokenAB 中是否包含可区分标识符 B 是可选的，是否使用依赖于鉴别机制的应用环境。

注 1：在 TokenAB 的签名数据中可选地包含可区分标识符 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。

(1) B 向 A 发送随机数 R_B，并可选地发送一个文本字段 Text1。

(2) A 产生并向 B 发送 TokenAB，并可选地发送 A 的证书。

(3) 一旦收到包含 TokenAB 的消息，B 就执行下列步骤：

(i) 通过验证 A 的证书或者用其他方式确保拥有 A 的有效公开密钥。

(ii) 通过以下方式验证 TokenAB：检验权标中所含的 A 的数字签名；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符字段(B)的值(如果有)，它应等于 B 的可区分标识符。

5.3 相互鉴别

5.3.1 概述

相互鉴别是指两个通信实体运用该机制彼此进行鉴别。

在 5.3.2 和 5.3.3 中，5.2.2 和 5.2.3 中描述的两种机制被扩展以实现相互鉴别。这种扩展增加了一

条消息传递，从而增加了两个操作步骤。

5.3.4 中规定的步骤用了四个消息，但是，这些消息不需要依次的发送。这样，鉴别过程可以加快。

5.3.2 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号（见 GB/T 15843.1—2008 的附录 B）来控制的。

鉴别机制如图 3 所示。

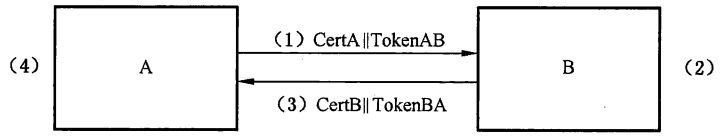

图 3 两次传递相互鉴别机制示意图

由 A 发送给 B 的权标（TokenAB）形式与 5.2.2 所规定的相同。

$$\text{TokenAB} = \begin{matrix} T_A \\ N_A \end{matrix} \,||\, B \,||\, \text{Text2} \,||\, sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \,||\, B \,||\, \text{Text1}\right)$$

由 B 发送给 A 的权标（TokenBA）形式为：

$$\text{TokenBA} = \begin{matrix} T_B \\ N_B \end{matrix} \,||\, A \,||\, \text{Text4} \,||\, sS_B\left(\begin{matrix} T_B \\ N_B \end{matrix} \,||\, A \,||\, \text{Text3}\right)$$

此处声称方 A 用序号 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：在 TokenAB 和 TokenAB 的签名数据中包含标识符 A 和标识符 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。

(1) A 发送 TokenAB 给 B。是否发送 A 的证书是可选的。

(2) 在接收到含有 TokenAB 的消息时，B 执行下列步骤：

(i) 通过验证 A 的证书或者用其他方式确保拥有 A 的有效公开密钥；

(ii) 通过检验包含在权标中的 A 的签名，检验时间戳或序号，以及检验 TokenAB 签名数据中标识符字段（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，是否发送 B 的证书是可选的。

(4) 步骤（3）中的消息处理方式与 5.2.2 的步骤（2）类似。

注：这种机制中两条消息之间除了时效性上有隐含关系外，没有任何联系；该机制独立地两次使用机制 5.2.2 。如果希望这两条消息进一步发生联系，可适当使用文本字段来实现。

5.3.3 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—2008 的附录 B）来控制的。

鉴别机制如图 4 所示。

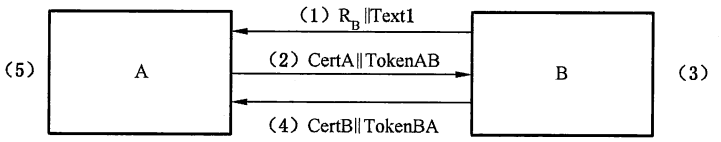

图 4 三次传递相互鉴别机制示意图

权标形式如下：

$$TokenAB = R_A \,||\, R_B \,||\, B \,||\, Text3 \,||\, sS_A(R_A \,||\, R_B \,||\, B \,||\, Text2)$$

$$TokenBA = R_B \,||\, R_A \,||\, A \,||\, Text5 \,||\, sS_B(R_B \,||\, R_A \,||\, A \,||\, Text4)$$

TokenAB 中是否包含标识符 B，以及 TokenBA 中是否包含标识符 A，都是可选的。这依赖于鉴别机制的应用环境。

注：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。这种保护手段是需要的，例如当 A 为了实体鉴别之外的其他目的使用同一密钥时。在 TokenBA 中包含 R_B 也是需要的，它指示 A 应检查其值是否与第一条消息中发送的值相同，但是在 TokenBA 中包含 R_B 可能不会提供类似于上述的在 TokenAB 中包含 R_A 所实现的保护，因为在产生 R_A 之前 A 已经知道了 R_B。如果确实需要实行这类保护，B 可以在文本字段 Text4 和 Text5 之间插入另外一个随机数 R_B'。

(1) B 向 A 发送一个随机数 R_B，并可选地发送一个文本字段 Text1。

(2) A 向 B 发送 TokenAB，并可选地发送它的证书给 B。

(3) 收到包含 TokenAB 的消息后，B 执行下列步骤：

(i) 通过检验 A 的证书或者用别的方式确保拥有 A 的有效公开密钥；

(ii) 通过以下方式验证 TokenAB：检验包含在权标中的 A 的签名；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符字段(B)的值(如果有)是否等于 B 的可区分标识符。

(4) B 向 A 发送 TokenBA，并可选地发送它的证书给 A。

(5) 收到包含 TokenBA 的消息后，A 类似的执行(3)中的步骤(i)和(ii)。此外，A 检验包含在 TokenBA 签名数据中的随机数 R_B 是否与步骤(1)中所接收的随机数相符。

5.3.4 两次传递并行鉴别

在这种机制中，鉴别是并行实行的，唯一性和时效性用产生和检验随机数来控制(见 GB/T 15843.1—2008 的附录 B)。

鉴别机制如图 5 所示。

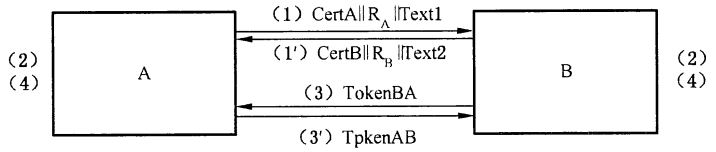

图 5 两次传递并行相互鉴别机制示意图

权标的形式与 5.2.3 中类似：

$$TokenAB = R_A \,||\, R_B \,||\, B \,||\, Text4 \,||\, sS_A(R_A \,||\, R_B \,||\, B \,||\, Text3)$$

$$TokenBA = R_B \,||\, R_A \,||\, A \,||\, Text6 \,||\, sS_B(R_B \,||\, R_A \,||\, A \,||\, Text5)$$

TokenAB 中是否包含标识符 B，以及 TokenBA 中是否包含标识符 A，都是可选的。这依赖于鉴别机制的应用环境。

注：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。这种保护手段是需要的，例如当 A 为了实体鉴别之外的其他目的使用同一密钥时。出于类似的理由，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，可能会已经知道了另一方的随机数。如果不希望如此，则双方可以分别在 TokenAB 的 Text3 和 Text4 之间以及 TokenBA 的 Text5 和 Text6 之间插入另一个随机数 R'_A 和 R'_B。

(1) A 向 B 发送 R_A，并可选地发送它的证书和一个文本字段 Text1。

(1′) B 向 A 发送 R_B，并可选地发送它的证书和一个文本字段 Text2。

(2) A 和 B 通过各自验证对方的证书或其他的方式，确保它们拥有对方的有效公开密钥。

(3) A 向 B 发送 TokenAB。

(3′) B 向 A 发送 TokenBA。

(4) A 和 B 执行下列步骤：

它们各自验证所接收到的权标，验证方式是检查权标的签名，并检查权标中的随机数是否与它们先前发送给对方的随机数相符。

注：5.3.4 中的机制的一种替代方案是将 5.2.3 的机制双向运行。在 5.3.4 中的机制的第一个消息中包含证书将允许更早的验证证书，因而能够加速鉴别的过程。

6 引入在线可信第三方的机制

6.1 概述

本章中的鉴别机制要求两个实体 A 和 B 通过拥有 A 和 B 有效公钥的在线可信第三方(具有可区分标识符 TP)来验证对方的公钥。实体 A 和 B 拥有 TP 的有效公钥。而 A 和 B 可不拥有对方的有效公钥。

本章描述了两个五次传递鉴别机制，在实体 A 和 B 之间实现了相互鉴别。在这两个鉴别机制中，有三个元素(A、B 和 TP)，A 和 B 相对 TP 来说是对等鉴别实体。权标和文本字段的格式遵从 5.1 的描述。这两个机制被统称为三元对等鉴别机制 TePA(Tri-element Peer Authentication)，它们使用 ISO/IEC 14888或 GB 15851—1995 定义的签名机制。

6.2 五次传递鉴别 TePA-A(由实体 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—2008 的附录 B)。

鉴别机制如图 6 所示。

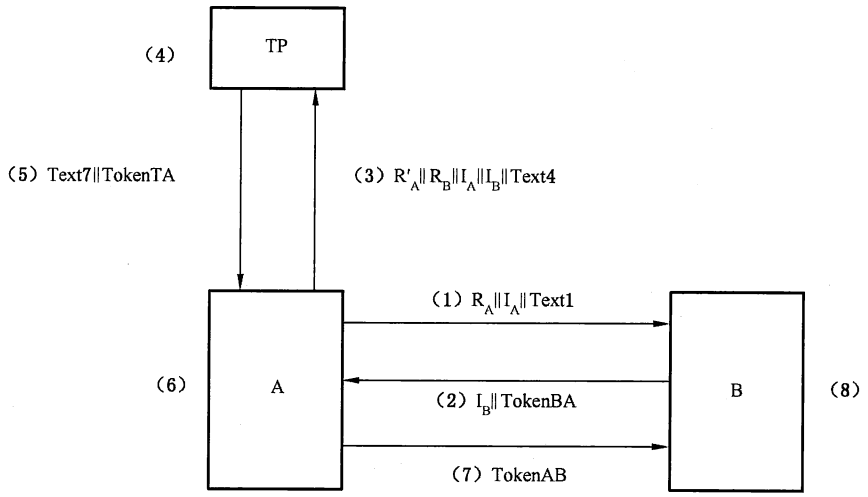

图 6 五次传递鉴别 TePA-A(由实体 A 发起)

权标应为下面的两种形式：

选项 1：

$$\text{TokenAB} = \text{Text9} \,||\, \text{ResA} \,||\, sS_T(R_B \,||\, \text{ResA} \,||\, \text{Text5}) \,||\, sS_A(R_B \,||\, R_A \,||\, \text{B} \,||\, \text{A} \,||\, \text{Text8})$$

$$\text{TokenBA} = R_A \,||\, R_B \,||\, \text{Text3} \,||\, sS_B(\text{B} \,||\, R_A \,||\, R_B \,||\, \text{A} \,||\, \text{Text2})$$

$$\text{TokenTA} = \text{ResA} \,||\, \text{ResB} \,||\, sS_T(R'_A \,||\, \text{ResB} \,||\, \text{Text6}) \,||\, sS_T(R_B \,||\, \text{ResA} \,||\, \text{Text5})$$

选项 2：

$$TokenAB = R'_A \,||\, Text9 \,||\, TokenTA \,||\, sS_A(R_B \,||\, R_A \,||\, B \,||\, A \,||\, Text8)$$

$$TokenBA = R_A \,||\, R_B \,||\, Text3 \,||\, sS_B(B \,||\, R_A \,||\, R_B \,||\, A \,||\, Text2)$$

$$TokenTA = ResA \,||\, ResB \,||\, sS_T(R'_A \,||\, R_B \,||\, ResA \,||\, ResB \,||\, Text5)$$

I_A、I_B、ResA、ResB、Status 和 Failure 字段的值应为下列形式：

I_A = A 或 CertA

I_B = B 或 CertB

ResA = (CertA||Status),(A||P_A)或 Failure

ResB = (CertB||Status),(B||P_B)或 Failure

Status = True 或 False。如果证书是被撤销的，该字段的值应为 False；否则该字段的值应为 True。

Failure：当公钥或实体 X 的证书不能被 TP 获得，ResX(X={A, B})应为 Failure。

如果 TP 确认 X(X={A,B})的身份和公钥 P_X 的映射，则 I_X = X；否则 I_X = CertX，且 X 应等于 CertX 的可区分标识符字段值；如果 X 或 CertX 允许被用于作为一种身份，则应有一种预安排的方式允许 TP 区分这两种类型的身份标识。ResX(X={A, B})的值应按表 1 确定。

表 1 ResX 的值

域	选项 1	选项 2
I_X	X	CertX
ResX	(X||P_X)或 Failure	(CertX||Status)或 Failure

本机制的执行过程如下：

(1) A 发送随机数 R_A、身份 I_A 和可选文本字段 Text1 到 B。

(2) B 发送 TokenBA 和身份 I_B 到 A。

(3) A 发送随机数 R'_A、随机数 R_B、身份 I_A、身份 I_B 以及可选文本字段 Text4 到 TP。

(4) 收到来自步骤(3)中 A 的消息后，TP 执行下列步骤：如果 I_A = A，且 I_B = B，则 TP 提取 P_A 和 P_B；如果 I_A = CertA，且 I_B = CertB，则 TP 检查 CertA 和 CertB 的有效性。TP 校验证书有效性的过程可能需要防范拒绝服务攻击。提供该保护机制的描述超出了本部分的范围。

(5) TP 发送可选文本字段 Text7 和 TokenTA 到 A。TokenTA 中的 ResA 和 ResB 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 执行下列步骤：

(i) 通过下列方式校验 TokenTA：验证包含在 TokenTA 中 TP 的签名，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。

(ii) 从消息中提取 B 的公钥，通过下列方式校验在步骤(2)中收到的 TokenBA：验证包含在 TokenBA 中 B 的签名检查包含在 TokenBA 中的 B 的签名数据中的标识符字段(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。

(7) A 发送 TokenAB 到 B。

(8) 收到来自步骤(7)中 A 的消息后，B 执行下列步骤：

(i) 通过下列方式校验 TokenTA：验证包含在 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_B 与在步骤(2)中发送给 A 的随机数 R_B 是否一致。

(ii) 从消息中提取 A 的公钥，通过下列方式校验 TokenAB：验证包含在 TokenAB 中 A 的

签名，检查包含在 TokenAB 中的 A 的签名数据中的标识符字段(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。

6.3 五次传递鉴别 TePA-B(由实体 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—2008 的附录 B)。

该鉴别机制如图 7 所示。

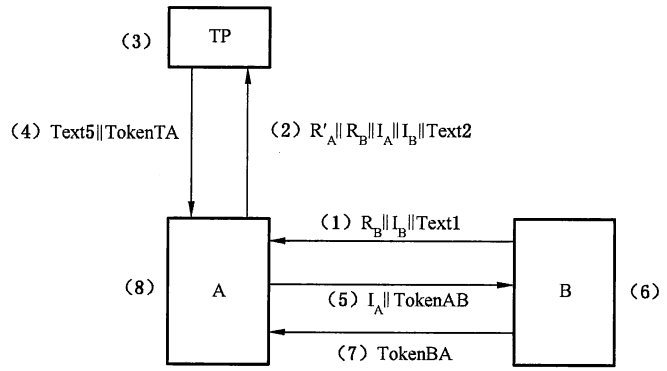

图 7 五次传递鉴别 TePA-B(由实体 B 发起)

权标应为如下两种形式：

选项 1：

$TokenAB = Text7||R_A||ResA||sS_T(R_B||ResA||Text3)||sS_A(R_B||R_A||B||A||Text6)$

$TokenBA = R_A||R_B||Text9||sS_B(A||R_A||R_B||B||Text8)$

$TokenTA = ResA||ResB||sS_T(R'_A||ResB||Text4)||sS_T(R_B||ResA||Text3)$

选项 2：

$TokenAB = R'_A||Text7||TokenTA||sS_A(R_B||R_A||B||A||Text6)$

$TokenBA = R_A||R_B||Text9||sS_B(R_A||R_B||A||B||Text8)$

$TokenTA = ResA||ResB||sST(R'_A||R_B||ResA||ResB||Text3)$

I_A、I_B、ResA、ResB、Status 和 Failure 字段的值如下：

I_A = A 或 CertA

I_B = B 或 CertB

ResA = (CertA||Status)，(A||P_A)或 Failure

ResB = (CertB||Status)，(B||P_B)或 Failure

Status = True 或 False。如果证书是被撤销的，该字段的值应为 False；否则该字段的值应为 True。

Failure：当公钥或实体 Y 的证书不能被 TP 获得，ResY(Y = {A，B})应为 Failure。

如果 TP 确认 Y(Y = {A，B})的身份和公钥 P_Y 的映射，则 I_Y = Y；否则 I_Y = CertY，且 Y 应等于 CertY 的可区分标识符字段值；如果 Y 或 CertY 允许被用于作为一种身份，则应有一种预安排的方式允许 TP 区分这两种类型的身份标识。ResY(Y = {A，B})的值应按表 2 确定。

表 2 ResY 的值

域	选项 1	选项 2
I_Y	Y	CertY
ResY	(Y||P_Y) 或 Failure	(CertY || Status)或 Failure

本机制的执行过程如下：

(1) B 发送随机数 R_B、身份 I_B 和可选文本字段 Text1 到 A。

(2) A 发送随机数 R'_A、随机数 R_B、身份 I_A、身份 I_B 以及可选文本字段 Text2 到 TP。

(3) 收到来自步骤(2)中 A 的消息后，TP 执行下列步骤：如果 I_A=A，且 I_B=B，则 TP 提取 P_A 和 P_B；如果 I_A=CertA，且 I_B=CertB，则 TP 检查 CertA 和 CertB 的有效性。TP 校验证书有效性的过程可能需要防范拒绝服务攻击。提供该保护机制的描述超出了本部分的范围。

(4) TP 发送可选文本字段 Text5 和 TokenTA 到 A。TokenTA 中的 ResA 和 ResB 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 执行下列步骤：

(i) 通过下列方式校验 TokenAB：验证包含在 TokenAB 中 TP 的签名，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。

(ii) 从消息中提取 A 的公钥，通过下列方式校验 TokenAB：验证包含在 TokenAB 中 A 的签名，检查包含在 TokenAB 中的 A 的签名数据中的标识符字段(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。

(7) B 发送 TokenBA 到 A。

(8) 收到来自步骤(7)中 B 的消息后，A 执行下列步骤：

(i) 通过下列方式校验 TokenTA：验证包含在 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。

(ii) 从步骤(4)中 TP 发送的消息中提取 B 的公钥，通过下列方式校验 TokenBA：验证包含在 TokenBA 中 B 的签名，检查包含在 TokenBA 中的 B 的签名数据中的标识符字段(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 相一致。

附 录 A
（资料性附录）
文本字段的使用

本部分第5章和第6章规定的权标包括了文本字段。在一次给定传递中不同文本字段的实际用途及各文本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—2008的附录A。

若使用了没有消息恢复的数字签名方案，并且签名的文本字段不是空的，则验证方在检验签名之前要拥有文本。在本附录中，“签名文本字段”指签名数据中的文本字段，而“未签名文本字段”指未签名数据中的文本字段。

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文本字段和（作为一部分放到）未签名文本字段中。

若权标未含有（足够的）冗余，签名文本字段可以用来提供额外的冗余。

签名文本字段可以用来指示，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，另一实体可以在文本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，则需要在签名文本字段和（若必要）未签名文本字段中，包含预期的验证方的身份。

未签名文本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。

附 录 B
（规范性附录）
OID 和 ASN.1 记法

B.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--
ua-one-pass OID::={mechanism 1}
ua-two-pass OID::={mechanism 2}
ma-two-pass OID::={mechanism 3}
ma-three-pass OID::={mechanism 4}
ma-two-pass-Parallel OID::={mechanism 5}
--引入在线可信第三方的机制--
ttp-ma-five-pass-by-A OID::={mechanism 6}
ttp-ma-five-pass-by-B OID::={mechanism 7}
END--EntityAuthenticationMechanisms-3--
```

B.2 后续客体标识符的使用

在标示某个机制的客体标识符之后，应立即跟随另外一个标示数字签名算法的客体标识符（例如，在 ISO/IEC 14888 或 GB 15851—1995 中规范的算法）。

B.3 依据基本编码规则的编码示例

根据 ISO/IEC 8825-1，一个客体标识符包括一个或多个八位位组序列。每一个八位位组序列编码了一个数字。

——当一个八位位组序列包含 2 个及以上的八位位组时，最后的一个八位位组的比特 8（最高有效位）设为 0，其之前的八位位组的比特 8 设为 1。

——某个八位位组序列中的八位位组的比特 7 到比特 1 的级联编码了一个数字。每一个数字应编码为尽可能少的八位位组，也就是说，八位位组‘80’在某个序列的第 1 个位置是无效的。

——第 1 个数字是标准的编号，第 2 个数字（如果有的话）是多部分标准的部分号。

某个客体标识符可以指本部分中定义的任何一个机制。

——为了标示某个 ISO 标准，第 1 个八位位组被设为‘28’，即十进制的 40（见 ISO/IEC 8825-1）。

——接下来的两个八位位组被设为‘CC46’。9798 等于十六进制的‘2646’，即 0010 0110 0100 0110，也即 2 个 7 比特块 10011001000110。在每个八位位组中插入比特 8 的合适的值，该序列的编码因此为 11001100 01000110，即‘CC46’。

——接下来的八位位组被设为‘03’，用于标示第 3 部分。

——接下来的八位位组标示鉴别机制：

——‘01’标示不引入在线可信第三方的一次传递单向鉴别机制；

——‘02’标示不引入在线可信第三方的两次传递单向鉴别机制；

——‘03’标示不引入在线可信第三方的两次传递相互鉴别机制；

——‘04’标示不引入在线可信第三方的三次传递相互鉴别机制；

——‘05’标示不引入在线可信第三方的两次传递并行相互鉴别机制；

——‘06’标示由实体 A 发起的引入在线可信第三方的五次传递相互鉴别机制 TePA-A；

——‘07’标示由实体 B 发起的引入在线可信第三方的五次传递相互鉴别机制 TePA-B。

例如，数据元素‘28 CC 46 03 04’解读{ISO Standard 9798 3 4}，即本部分的第四个机制——不引入在线可信第三方的三次传递相互鉴别机制。数据元素可以按照下面 BER-TLV 数据对象传输（见 GB/T 16263.1—2006 中 ASN.1 的基本编码规则，通用类标签‘06’），其中短横线和大括号仅用于表述更为清楚。

数据对象＝{‘06’-‘05’-‘28 CC 46 03 04’}

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—2016/ISO/IEC 9798-3:1998
*
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
总编室：(010)68533533 发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 30 千字
2016年6月第一版 2016年6月第一次印刷
*
书号：155066·1-54003 定价 21.00 元

GB/T 15843.3-2016

打印日期：2016年7月4日 F009B