ICS 35.040
L 80

中华人民共和国国家标准

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

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

(ISO/IEC 9798-3:1998,IDT)

2008-06-19 发布　　2008-11-01 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》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

可能还会增加其他后续部分。

本部分为GB/T 15843的第3部分，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》，仅有编辑性修改。

本部分代替GB/T 15843.3—1998《信息技术　安全技术　实体鉴别　第3部分：用非对称签名技术的机制》。本部分与GB 15843.3—1998相比，主要变化如下：

——本部分修改了名称。

——本部分根据GB/T 15843.1的修订，更改了部分术语。

——本部分删除了ISO/IEC前言，并增加了引言。

本部分的附录A为资料性附录。

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：中国科学院数据与通信保护研究教育中心(信息安全国家重点实验室)。

本部分主要起草人：荆继武、王平建、夏鲁宁、高能、向继。

本部分所代替标准的历次发布情况为：

——GB/T 15843.3—1998。

引　言

本部分等同采用国际标准 ISO/IEC 9798-3:1998,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC27(IT 安全技术)起草的。

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、三次传递鉴别和两次传递并行鉴别。

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。

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),其余的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。如果采用使用随机数的激励—响应方法,单向鉴别需两次传递,相互鉴别则需三次或四次传递(依赖于所采用的机制)。

2　规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注明日期的引用文件,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/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)

3　术语、定义和符号

GB/T 15843.1—2008 中确立的术语、定义和符号适用于本部分。

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

5.0　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 和下面的注1)。

本部分中,权标的形式如下:

$$Token = X_1 \| \cdots \| X_i \| s_{S_A}(Y_1 \| \cdots \| Y_j)。$$

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。

5.1 单向鉴别

单向鉴别是指使用该机制时两个实体中只有一方被鉴别。

5.1.1 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（$Token_{AB}$）形式是：

$$Token_{AB} = \begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text2 \| s_{S_A}(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1)$$

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$Token_{AB}$的签名数据中必须包含标识符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$Token_{AB}$给B。是否发送A的证书是可选的。

(2) 在接收到含有$Token_{AB}$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$Token_{AB}$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$Token_{AB}$。

5.1.2 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。

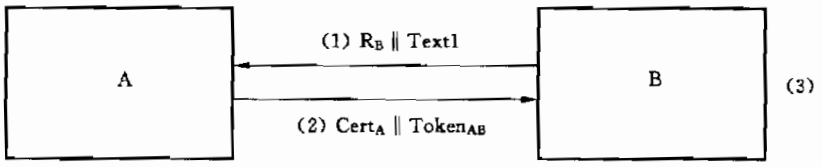

图 2 两次传递单向鉴别机制示意图

由声称方 A 发送给验证方 B 的权标($Token_{AB}$)形式是：

$$Token_{AB} = R_A \| R_B \| B \| Text3 \| s_{S_A}(R_A \| R_B \| B \| Text2)$$

在 $Token_{AB}$ 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 $Token_{AB}$ 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 $Token_{AB}$ 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 $Token_{AB}$，并可选地发送 A 的证书。

(3) 一旦收到包含 $Token_{AB}$ 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 $Token_{AB}$：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 $Token_{AB}$ 签名数据中的随机数相符；检验 $Token_{AB}$ 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。

5.2 相互鉴别

相互鉴别是指两个通信实体运用该机制彼此进行鉴别。

在 5.2.1 和 5.2.2 中，5.1.1 和 5.1.2 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。

5.2.3 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。

5.2.1 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。

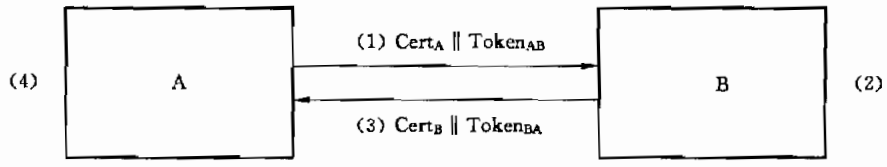

图 3 两次传递相互鉴别机制示意图

由 A 发送给 B 的权标($Token_{AB}$)形式与 5.1.1 所规定的相同。

$$Token_{AB} = \frac{T_A}{N_A} \| B \| Text2 \| s_{S_A}(\frac{T_A}{N_A} \| B \| Text1)$$

由 B 发送给 A 的权标($Token_{BA}$)形式为：

$$Token_{BA} = \frac{T_B}{N_B} \| A \| Text4 \| s_{S_B}(\frac{T_B}{N_B} \| A \| Text3)$$

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：在 $Token_{AB}$ 和 $Token_{AB}$ 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。

步骤(1)和步骤(2)与 5.1.1 一次传递鉴别的规定相同。

(3) B 向 A 发送 $Token_{BA}$，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 5.1.1 的步骤(2)类似。

注 2：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 5.1.1。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。

5.2.2 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。

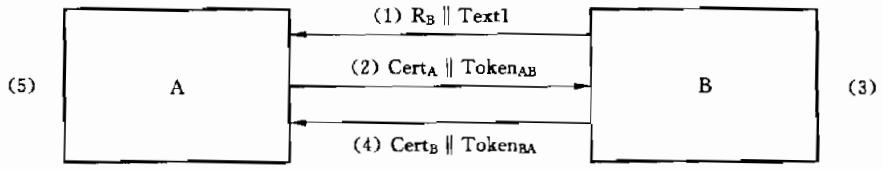

图 4 三次传递相互鉴别机制示意图

权标形式如下：

$$Token_{AB} = R_A \| R_B \| B \| Text3 \| s_{S_A}(R_A \| R_B \| B \| Text2)$$

$$Token_{BA} = R_B \| R_A \| A \| Text5 \| s_{S_B}(R_B \| R_A \| A \| Text4)$$

$Token_{AB}$ 中是否包含标识符 B，以及 $Token_{BA}$ 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 $Token_{AB}$ 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 $Token_{BA}$ 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 $Token_{BA}$ 中包含 R_B 可能不会提供类似于上述的在 $Token_{AB}$ 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 发送随机数权标 $Token_{AB}$，并可选地发送它的证书给 B。

(3) 收到包含 $Token_{AB}$ 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 $Token_{AB}$：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 $Token_{AB}$ 签名数据中的随机数相符；检验 $Token_{AB}$ 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 $Token_{BA}$，并可选地发送它的证书给 A。

(5) 收到包含 $Token_{BA}$ 的消息后，A 类似地执行(3)中的步骤(i)和(ii)。此外，A 检验包含在 $Token_{BA}$ 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。

5.2.3 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。

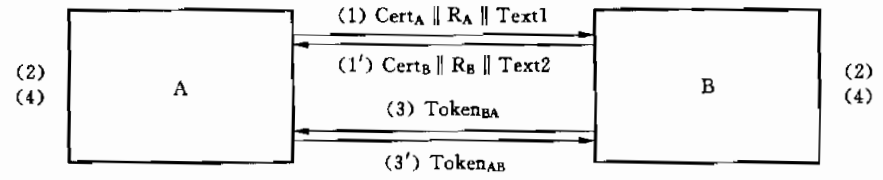

图 5 两次传递并行相互鉴别机制示意图

权标的形式与 5.1.2 中类似：

$$Token_{AB} = R_A \| R_B \| B \| Text4 \| s_{S_A}(R_A \| R_B \| B \| Text3)$$

$$Token_{BA} = R_B \| R_A \| A \| Text6 \| s_{S_B}(R_B \| R_A \| A \| Text5)$$

$Token_{AB}$中是否包含标识符 B，以及 $Token_{BA}$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 1：随机数 R_A 应包含在 $Token_{AB}$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，$Token_{BA}$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 $Token_{AB}$的 Text3 和 Text4 之间以及 $Token_{BA}$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 $Token_{AB}$。

(3′) B 向 A 发送 $Token_{BA}$。

(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 2：5.2.3 中的机制的一种替代方案是将 5.1.2 的机制双向运行。在 5.2.3 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。

附 录 A
（资料性附录）
文本字段的使用

本部分第5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。

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—2008/ISO/IEC 9798-3:1998
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 0.75 字数 16千字
2008年9月第一版 2008年9月第一次印刷
*
书号:155066·1-33390 定价 14.00元

GB/T 15843.3-2008

打印日期:2009年4月22日

GB/T 15843.3—2008/ISO/IEC 9798-3:1998