ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.3—1998
idt ISO/IEC DIS 9798-3:1997

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

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

1998-12-14 发布　　1999-08-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC DIS 9798-3:1997《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》。

本标准规定的单方鉴别和相互鉴别机制用于保证信息交换的安全。

该系列标准在总标题《信息技术　安全技术　实体鉴别》下,由以下几个部分组成:

第 1 部分:概述

第 2 部分:用对称加密算法的机制

第 3 部分:用非对称签名技术的机制

第 4 部分:用密码检验函数的机制

第 5 部分:用零知识技术的机制

将来增加的部分可跟随其后。

本标准的附录 A 是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位:电子工业部标准化研究所、电子工业部第三十研究所。

本标准主要起草人:向维良、龚奇敏、吴世宗、雷利民、陶仁骥、郝伟刚。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)共同组成一个世界标准化专门系统。ISO 或 IEC 的国家成员体,通过涉及特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准开发。ISO 和 IEC 的技术委员会在共同感兴趣的领域内合作,与 ISO 和 IEC 有联络的其他官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO 和 IEC 已建立了一个联合技术委员会 ISO/IEC JTCI。由联合技术委员会采纳的国际标准草案需分发给各国家成员体表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC DIS 9798-3 是由联合技术委员会 ISO/IEC JTCI“信息技术”的 SC 27 分委会“IT 安全技术”制定的。

这个第二版取代了第一版(ISO/IEC 9798-3:1993),对它作了技术上的修订。

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别》下,由以下几部分组成:

——第 1 部分:概述

——第 2 部分:用对称加密算法的机制

——第 3 部分:用非对称签名技术的机制

——第 4 部分:用密码检验函数的机制

——第 5 部分:用零知识技术的机制

将来增加的部分可跟随其后。

本标准的附录 A 只作为信息提供。

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：用非对称签名技术的机制

GB/T 15843.3—1998
idt ISO/IEC DIS 9798-3:1997

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

1　范围

本标准规定了用非对称签名技术的实体鉴别机制。有两种鉴别机制属单个实体(单向)的鉴别，其余的属两个实体相互鉴别的机制。数字签名用于验证实体的身份，也可能有可信的第三方参与。

本标准中规定的机制，使用时变参数，如：时间标记、顺序号或随机数，可防止先前有效的鉴别信息以后又被接受。

若使用时间标记或顺序号，则单向鉴别只需要一次传递，而完成相互鉴别则需两次传递。若使用带有随机数的询问和响应方法，则单向鉴别需要两次传递，而当完成相互鉴别，则需要三次或四次传递(依赖于所使用的机制)。

2　引用标准

下列标准所包含的条文，通过在本标准中引有而构成为本标准的条文，本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

ISO/IEC 9798-1:1997　信息技术　安全技术　实体鉴别　第1部分：概述

3　定义和记法

本标准采用 ISO/IEC 9798-1 中描述的定义和记法。

4　要求

本标准规定的鉴别机制中，待鉴别的实体要通过表明他知道某秘密签名密钥来证实其身份。这要由实体使用其秘密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认证密钥的任何实体来验证。

鉴别机制有以下的要求：

a) 验证者应拥有声称者的有效公开密钥；

b) 声称者应拥有仅由他自己知道和使用的秘密签名密钥。

若这两者之一未能满足，则鉴别进程会受到损害，或者不能成功地完成。

注：获得有效公开密钥的一种途径是用证书的方式(见 ISO/IEC 9798-1:1997 的附录 C)。证书的产生、分发和撤消都超出了本标准的范围。为了这个目的，这里可以存在可信的第三方。另一种获得有效公开密钥的途径是利用可信的信使。

国家质量技术监督局 1998-12-14 批准　　1999-08-01 实施

5 机制

规定的实体鉴别机制利用了时变参数，如时间标记、顺序号或随机数(见 ISO/IEC 9798-1:1997 的附录 B)。

假设权标定义如下：

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

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

若权标的签名数据中含有的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中所含的信息不能从签名中恢复，则它应包含在权标未签名的文本字段中。

若在权标的签名数据中的信息(如随机数)对于验证者是已知的，则它不必包含在声称者发送的权标未签名数据中。

在下面机制中规定的所有文本字段，在本标准范围之外的应用中使用是有效的(它们可以是空的)。它们的关系和内容依赖于特定的应用。对于文本字段使用方面的信息见附录 A。

注

1 一个实体对于第二个实体别有用心操纵数据块的签名，这能由第一个实体所签名的数据块中含有它自己的随机数来防止。在这种情况下，是其不可预测性防止了预定义数据的签名。

2 由于证书的分配超出了本标准的范围，因此证书的发送在所有的机制中是可选的。

5.1 单向机制

单向机制意指仅对两个实体中的一个进行鉴别。

5.1.1 一次传递机制

在这种鉴别机制中，由声称者 A 启动进程，并由验证者 B 鉴别。唯一性/时效性由产生和检验时间标记或顺序号来控制(见 ISO/IEC 9798-1:1997 的附录 B)。

该鉴别机制在图 1 中说明。

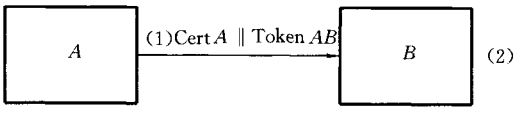

图 1

由声称者 A 发送给验证者 B 的权标(Token AB)的形式是：

$$\text{Token}AB = \begin{matrix} T_A \\ N_A \end{matrix} \| B \| \text{Text 2} \| {}_sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| \text{Text 1} \right)$$

式中：声称者 A 使用顺序号 N_A 或时间标记 T_A 作为时变参数。这种选择依赖于环境以及声称者和验证者的技术能力。

注

1 为了防止意想的验证者之外的任何实体接受权标，在 TokenAB 签名数据中，必须包含标识符 B。

2 在一般情况下，Text 2 不由这个进程鉴别。

3 这种机制的一种应用可能是密钥分配(见 ISO/IEC 9798-1:1997 的附录 A)。

(1) A 发送 TokenAB 给 B。而 A 的证书是否发送，可任选。

(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 A 的签名、检验时间标记或顺序号，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 的区分标识符来验证 TokenAB。

5.1.2 两次传递机制

在这种机制中，验证者 B 启动进程并对声称者 A 进行鉴别。唯一性/时效性是通过产生并检验随机数 R_B（见 ISO/IEC 9798-1:1997 的附录 B）来控制。

该签别机制在图 2 中说明。

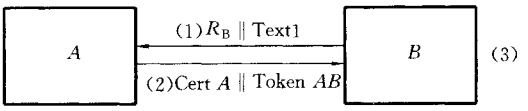

图 2

由声称者 A 发送给验证者 B 的权标(TokenAB)的形式是：

$$\text{Token}AB = R_A \parallel R_B \parallel B \parallel \text{Text } 3 \parallel {}_sS_A(R_A \parallel R_B \parallel B \parallel \text{Text } 2)$$

TokenAB 中是否包含标识符 B 是任选的，它依赖于使用这种鉴别机制的环境。

注

1 在 TokenAB 的签名数据中，包含可选的标识符 B 能防止权标被除意想的验证者之外的任何实体接受(例如中间人的攻击)。

2 随机数 R_A 出现在 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。这种预防方法是需要的，例如当 A 为了实体鉴别之外的其他目的使用同一密钥。

(1) B 发送随机数 R_B 给 A，并可任选文本字段 Text1。

(2) A 发送 TokenAB 给 B，而 A 的证书是否发送，可任选。

(3) 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，若有的话，它应等于 B 的区分标识符。

5.2 相互鉴别

相互鉴别的方式是指两个通信实体相互进行鉴别。

在 5.1.1 和 5.1.2 中描述的两种机制，分别地扩展到 5.2.1 和 5.2.2 中来完成相互鉴别，这通过传送一个消息而引入两个额外的步骤。

在 5.2.3 中规定的步骤用了四个消息，但是，这些消息不需要全部顺序地发送。这样，鉴别进程可以加快。

5.2.1 两次传递鉴别

在这种鉴别机制中，唯一性/时效性是用产生和检验时间标记或顺序号来控制(见 ISO/IEC 9798-1:1997 的附录 B)。

该鉴别机制在图 3 中说明。

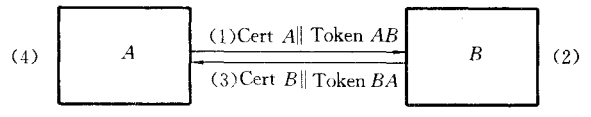

图 3

由 A 发送给 B 的权标(TokenAB)形式与 5.1.1 中规定的相同。

$$\text{Token}AB = \begin{matrix} T_A \\ N_A \end{matrix} \parallel B \parallel \text{Text } 2 \parallel {}_sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \parallel B \parallel \text{Text } 1\right)$$

由 B 发送给 A 的权标(TokenBA)形式是：

$$\text{Token}BA = \begin{matrix} T_B \\ N_B \end{matrix} \parallel A \parallel \text{Text } 4 \parallel {}_sS_B\left(\begin{matrix} T_B \\ N_B \end{matrix} \parallel A \parallel \text{Text } 3\right)$$

在这种机制中选择使用时间标记或顺序号，依赖于环境以及声称者和验证者的技术能力。

注 1：在 TokenAB 和 TokenBA 的签名数据中，必须分别含有标识符 A 和标识符 B，以防止权标被意想的验证者之外的任何别的实体接受。

步骤(1)和(2)与 5.1.1 一次传递鉴别的规定相同。

(3) B 发送 TokenBA 给 A，并且 B 的证书是否发送，可任选。

(4) 在步骤(3)中的消息按 5.1.1 步骤(2)类似的方法处理。

注 2：这种机制的两个消息除了隐含的时效性的约束之外，不受任何其他方式的约束；该机制包含独立使用机制 5.1.1进行两次传递。若要进一步约束这些消息，可通过适当使用文本字段来完成。

5.2.2 三次传递鉴别

在这种机制中，唯一性/时效性是用产生和检验随机数来控制(见 ISO/IEC 9798-1:1997 的附录 B)。

该鉴别机制在图 4 中说明。

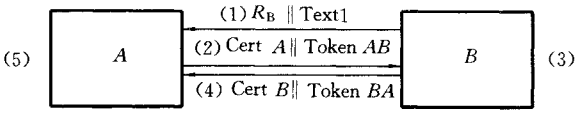

图 4

权标是下面的形式：

$$\text{Token}AB = R_A \| R_B \| B \| \text{Text 3} \| {}_sS_A(R_A \| R_B \| B \| \text{Text 2})$$

$$\text{Token}BA = R_B \| R_A \| A \| \text{Text 5} \| {}_sS_B(R_B \| R_A \| A \| \text{Text 4})$$

在 TokenAB 中是否包含参数 B 和 TokenBA 中是否包含参数 A 都是任选的。它们取决于该机制使用的环境。

注：随机数 R_A 应出现在 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。这种预防方法是需要的，例如，当 A 为了实体鉴别之外其他目的还将使用同一密钥。出于类似的理由，TokenBA 也使用了随机数 R_B。但是，因为 R_B 在选择 R_A 时为已知，A 可能事先就知道 TokenBA 中签名的完整数据。若这是不希望有的，则 B 可在 TokenBA 的 Text 4 和 Text 5 字段中插入一个附加的随机数 R'_B。此外，出于安全考虑，检验随机数 R_B 在第一个与第三个消息中的随机数是否相同也是必要的。

(1) B 发送随机数 R_B 给 A，并可任选文本字段 Text1。

(2) A 发送 TokenAB 给 B，而 A 的证书是否发送，可任选。

(3) 在接收到含有 TokenAB 的消息时，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 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，若有的话，它应等于 B 的区分标识符。

(4) B 发送 TokenAB 给 A，而 B 的证书是否发送，可任选。

(5) 在接收到含有 TokenBA 的消息时，A 类似地执行在(3)中列出的步骤(i)和(ii)。此外，A 检验包含在 TokenBA 签名数据中的随机数 R_B 是否与在步骤(1)中所接收的随机数相符。

5.2.3 两次传递的并行鉴别

在这种机制中，鉴别是并行实行的，唯一性/时效性用产生和检验随机数来控制(见 ISO/IEC 9798-1:1997 的附录 B)。

该鉴别机制在图 5 中说明。

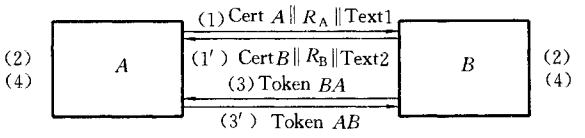

图 5

权标与 5.1.2 中的类似：

$$\text{Token}AB = R_A \| R_B \| B \| \text{Text 4} \| {}_sS_A(R_A \| R_B \| B \| \text{Text 3})$$

$$\text{Token}BA = R_B \| R_A \| A \| \text{Text 6} \| {}_sS_B(R_B \| R_A \| A \| \text{Text 5})$$

TokenAB 中是否包含参数 B 和 TokenBA 中是否包含参数 A 是任选的。它们依赖于使用这种权标的环境。

注 1：随机数应出现在 TokenAB 中，以防止 B 在鉴别机制启动之前获得 A 对由 B 选择的数据签名。这种预防是需要的，例如，当 A 为了实体鉴别之外的其他目的还将使用同一密钥。出于类似的理由，TokenBA 也使用了随机数 R_B。依赖于(1)和(1′)中发送的消息被接受的相对时间，当一方选其随机数时，可能会知道另一方的随机数。若这是不希望有的，则两方可在 TokenAB 的文本字段 Text 3 和 Text 4 中和 TokenBA 的文本字段 Text 5 和 Text 6 中分别插入附加的随机数 R'_A 和 R'_B。

(1) A 发送 R_A 给 B，而 A 的证书和文本字段 Text 1 是否发送，可任选。

(1′) B 发送 R_B 给 A，而 B 的证书和文本字段 Text 2 是否发送，可任选。

(2) A 和 B 确保它们拥有另一实体有效的公开密钥，或者通过验证各自的证书，或者用某种别的方式。

(3) A 发送 TokenAB 给 B。

(3′) B 发送 TokenBA 给 A。

(4) A 和 B 执行下列步骤：

它们各自都验证收到的权标，方式是通过检验包含在权标中的签名，并检验它先前发送给另一实体的那个随机数，看是否与包含在接收的权标签名数据中的随机数相符。

注 2：5.2.3 中机制的一种替代方案是将 5.1.2 的机制双向运行。在机制 5.2.3 的第一个消息中包含证书将允许更早地验证证书，因而能加速鉴别的进程。

附 录 A
（提示的附录）
文本字段的使用

本标准第5章规定的权标含有文本字段。在给定传递中的各种文本字段的实际应用及其之间关系依赖于应用。在下面给出一些例子，也可见ISO/IEC 9798-1:1997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，则验证者在检验签名之前要拥有文本。在本附录中，“签名文本字段”是指签名数据中的文本字段，而“未签名文本字段”是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，要求数据源鉴别的任何信息都应放到权标中的签名文本字段和（作为一部分）未签名文本字段中。

若权标未含有（足够的）冗余，签名的文本字段可以用来提供附加的冗余。

签名的文本字段可用来指示只有为了实体鉴别的目的权标才是有效的。还应注意，鉴于一个实体可能会带有恶意企图选择“退化”的值让另一实体签名，而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，由于某个声称者对所有与之通信的验证者使用同一密钥而使得进行攻击是可能的，并且若认为这种攻击是一个威胁，则在签名文本字段和（若必要）未签名文本字段中，均应含有意想的验证者的身份。

未签名的文本字段也可用于向验证者提供信息，以指明声称者正在声称（但未被鉴别）的身份。若不用证书方式来分配公开密钥，则要求用这种信息让验证者确定用哪一个公开密钥来鉴别声称者。

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:用非对称签名技术的机制
GB/T 15843.3—1998
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电 话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*
开本 880×1230 1/16 印张 3/4 字数 15 千字
1999年8月第一版 1999年8月第一次印刷
印数 1—1 200
*
书号:155066·1-16078 定价10.00元
*
标 目 383—21

GB/T 15843.3-1998