ICS 35.040
L 80

中华人民共和国国家标准

GB 15843.2—1997
idt ISO/IEC 9798-2:1994

信息技术　安全技术　实体鉴别
第2部分：采用对称加密算法的机制

Information technology—Security techniques—Entity authentication—Part 2: Mechanisms using symmetric encipherment algorithms

1997-09-02 发布　　1998-04-01 实施

国家技术监督局　发布

目　　次

前言 …… Ⅲ
ISO/IEC 前言 …… Ⅳ
1　范围 …… 1
2　引用标准 …… 1
3　定义和记法 …… 1
4　要求 …… 1
5　不涉及可信第三方的机制 …… 2
6　涉及可信第三方的机制 …… 5
附录 A(提示的附录)　文本字段的使用 …… 8
附录 B(提示的附录)　时变参数 …… 8
附录 C(提示的附录)　参考文献 …… 9

前　言

本标准等同采用国际标准 ISO/IEC 9798-2:1994《信息技术　安全技术　实体鉴别　第 2 部分:采用对称加密算法的机制》。

该标准规定了用对称加密算法实现的实体鉴别机制,它适合于我国使用。

GB 15843 在总标题《信息技术　安全技术　实体鉴别机制》下由下列部分组成:

——第 1 部分:一般模型

GB 15843 在总标题《信息技术　安全技术　实体鉴别》下还由下列部分组成:

——第 2 部分:采用对称加密算法的机制

——第 3 部分:采用公开密钥算法的实体鉴别

——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

本标准中的附录 A、附录 B、附录 C 都是提示的附录。

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:电子工业部第三十研究所、电子工业部标准化研究所。

本标准主要起草人:龚奇敏,方姝妹,杜明钰,李桂茹,向维良。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC 1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。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 9798-2 是由联合技术委员会 ISO/IEC JTC 1(信息技术)的分委员会 SC 27(IT 安全技术)起草的。

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别机制》下由下列部分组成:

——第 1 部分:一般模型

——第 3 部分:采用公开密钥算法的实体鉴别

ISO/IEC 9798 在总标题《信息技术　安全技术　实体鉴别》下还由下列部分组成:

——第 2 部分:采用对称加密算法的机制

——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

注:上述第 1 部分和第 3 部分之前的总标题在下一个修订版中将调整为第 2、第 4 和第 5 部分之前的总标题。

也可能还有其他部分跟随其后。

本标准的附录 A、附录 B 和附录 C 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2部分：采用对称加密算法的机制

GB 15843.2—1997
idt ISO/IEC 9798-2:1994

Information technology—Security techniques—Entity authentication—Part 2: Mechanisms using symmetric encipherment algorithms

1　范围

本标准规定了采用对称加密算法的实体鉴别机制。其中有四种是两个实体间无可信第三方参与的鉴别机制，而这四种机制中有两种是单个实体鉴别（单向鉴别），另两种是两个实体相互鉴别。其余的机制都要求有一个可信第三方参与，以便建立公共的秘密密钥，实现相互或单向的实体鉴别。

本标准中规定的机制采用诸如时间标记、顺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。

如果没有可信第三方参与，又采用时间标记或顺序号，则对于单向鉴别只需传送一次信息，而要达到相互鉴别必须传送两次。如果没有可信第三方参与，又采取使用随机数的询问—应答方法时，单向鉴别需传送两次信息，而相互鉴别则需要传送三次。如果有可信第三方参与，则一个实体与可信第三方之间的任何一次附加通信都需要在通信交换中增加两次传送。

2　引用标准

下列标准所包含的条文，通过在本标准中引用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。

GB 15843.1—1995　信息技术　安全技术　实体鉴别机制　第1部分：一般模型（idt ISO/IEC 9798-1:1991）

3　定义和记法

本标准使用GB 15843.1中的定义和记法。

4　要求

本标准规定的鉴别机制中，待鉴别的实体通过表明它拥有某秘密鉴别密钥来证实其身份，这可由该实体用其秘密密钥加密特定数据达到，共享其秘密鉴别密钥的任何实体都可以将加密后的数据解密。

这些鉴别机制有下列要求，若其中任何一个不满足，则鉴别进程就会受到损害或根本不能实现。

a）向验证者证实其身份的声称者，在应用第5章的机制时，应和该验证者共享一个秘密鉴别密钥，在应用第6章的机制时，每个实体和公共的可信第三方都分别共享一个秘密鉴别密钥。这些密钥应当在正式启动鉴别机制前就为有关各方掌握，达到这一点所采用的方法已超出了本标准的范围。

b）如果涉及到可信第三方，它应得到声称者与验证者的共同信任。

c）声称者与验证者共享的秘密鉴别密钥，或实体与可信第三方共享的秘密鉴别密钥，应仅为这两

国家技术监督局1997-09-02批准　　1998-04-01实施

方或双方都信任的其他方所知。

注 1：加密算法与密钥生存期的选择应满足密钥在其生存期内就被推算出来在计算上是不可行的。此外，在选择密钥生存期时还应防止已知明文和选择明文的攻击。

d）在 d1)或 d2)两条假设中需满足一条。

d1）鉴别机制中使用的加密算法与工作方式应能向接收方提供检测数据被伪造或篡改过的方法。这就要求数据有足够的冗余度，并要求明文的任何修改都将导致不可预测的大量密文位的修改。

提供足够冗余度的一种可能的方法就是在数据加密前附上一个散列码。

注 2：散列函数已在 ISO/IEC 10118 中标准化。

如果加密使用块密码算法且块长度小于被加密的数据长度，那么任何一个块的更换都应是可检测的。

d2）应由独立的数据完整性机制来确保已加密数据的完整性。

注 3：数据完整性机制已在 GB 15852 中标准化。

5 不涉及可信第三方的机制

这些鉴别机制中，实体 A 和 B 在开始具体运行鉴别机制之前应共享一个公共的秘密鉴别密钥 K_{AB}。

这些机制要求使用诸如时间标记、顺序号或随机数这样的时变参数。这些参数的特性，尤其是它们很难在鉴别密钥生存期内重复的特性，对于这些机制的安全性是十分重要的。附加信息见附录 B。

以下机制中规定的所有文本字段同样适用于本标准范围之外的应用(它们可能是空的)。它们的关系与内容取决于具体的应用。有关文本字段使用的信息见附录 A(提示的附录)。

5.1 单向鉴别

单向鉴别是指使用该机制时两实体中只有一方被鉴别。

5.1.1 一次传送鉴别

这种鉴别机制中，由声称者 A 启动此进程并被验证者 B 鉴别。唯一性/时间性是通过产生并校验时间标记或顺序号(见附录 B(提示的附录))来控制的。

鉴别机制示于图 1。

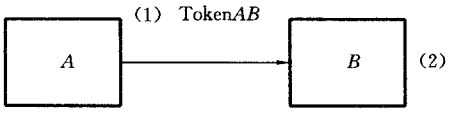

图 1

声称者 A 发送给验证者 B 的权标(TokenAB)形式是：

$$\text{Token}AB = \text{Text2} \parallel eK_{AB}\left(\begin{matrix}T_A \\ N_A\end{matrix} \parallel B \parallel \text{Text1}\right)$$

此处声称者 A 或者用顺序号 N_A，或者用时间标记 T_A 作为时变参数。具体选择哪一个取决于声称者与验证者的技术能力及环境。

在 TokenAB 中是否包含区分标识符 B 是任选的。

注：在 TokenAB 中包含区分标识符 B 是为防止敌人假冒实体 B 重复使用实体 A 的 TokenAB。这种包含之所以被作成可任选，是因为在不会出现这类攻击的环境中可将标识符省去。如果实体 A 和 B 共享一个秘密密钥 K'_{AB}，而 K'_{AB} 只用于 B 对 A 的鉴别，那么标识符 B 也可省去。权标则变为：

$$\text{Token}AB = \text{Text2} \parallel eK'_{AB}\left(\begin{matrix}T_A \\ N_A\end{matrix} \parallel \text{Text1}\right)$$

图 1 中：(1) A 向 B 发送 TokenAB。

(2) 一旦收到包含 TokenAB 的消息，B 便将加密部分解密并检验区分标识符 B(如果有的话)以及

时间标记或顺序号的正确性，从而验证 TokenAB。

5.1.2 两次传送鉴别

这种鉴别机制中，验证者 B 启动此进程并对声称者 A 进行鉴别。唯一性/时间性是通过产生并检验随机数 R_B（见附录 B）来控制的。

鉴别机制示于图 2。

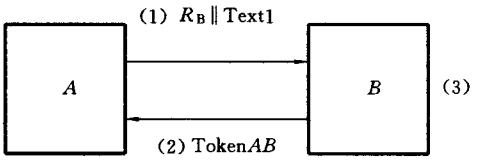

图 2

由声称者 A 发送给验证者 B 的权标（TokenAB）形式是：

$$Token AB = Text3 \| eK_{AB}(R_B \| B \| Text2)$$

在 TokenAB 中是否包含区分标识符 B 是任选的。

注：在 TokenAB 中包含区分标识符 B 是为防止所谓的反射攻击，这种攻击的特性是入侵者假冒 A 将询问 R_B“反射”给 B。区分标识符的包含之所以做成可任选，是因为在不会出现这类攻击的环境中可将标识符省去。

如果实体 A 和 B 共享一个秘密密钥 K'_{AB}，而 K'_{AB} 只用于 B 对 A 的鉴别，那么区分标识符 B 也可省去。权标则变为：

$$Token AB = Text3 \| eK'_{AB}(R_B \| Text2)$$

图 2 中：(1) B 向 A 发送一个随机数 R_B，并可任选地发送一个文本字段 Text1。

(2) A 向 B 发送 TokenAB。

(3) 一旦收到包含 TokenAB 的消息，B 便将加密部分解密并检验区分标识符 B（如果有的话）的正确性以及在步骤(1)中发送给 A 的随机数 R_B 是否与 TokenAB 中所含的随机数相符，从而验证 TokenAB。

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。

5.2.1 和 5.2.2 分别采用 5.1.1 和 5.1.2 中描述的两种机制，以实现相互鉴别。这两种情况都要求增加一次传送，从而增加了两个操作步骤。

注：相互鉴别的第三种机制可由 5.1.2 中规定的机制的两种情况构成，一种由实体 A 启动，另一种由 B 启动。

5.2.1 两次传送鉴别

这种鉴别机制中，唯一性/时间性是通过产生并检验时间标记或顺序号（见附录 B）来控制的。

鉴别机制示于图 3。

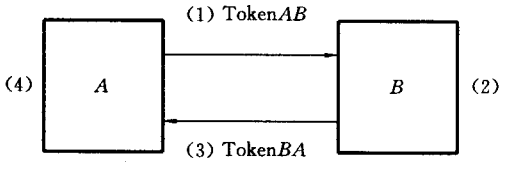

图 3

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

$$Token AB = Text2 \| eK_{AB}\left(\begin{matrix}T_A \\ N_A\end{matrix} \| B \| Text1\right)$$

由 B 发送给 A 的权标（TokenBA）形式是：

$$Token BA = Text4 \| eK_{AB}\left(\begin{matrix}T_B \\ N_B\end{matrix} \| A \| Text3\right)$$

在 TokenAB 中是否包含区分标识符 B，在 TokenBA 中是否包含区分标识符 A，是可(独立地)任选的。

注 1：TokenAB 中的区分标识符 B 是为防止敌人假冒实体 B 重用实体 A 的 TokenAB。同样的原因，TokenBA 包含区分标识符 A。区分标识符的包含之所以作成可任选，是因为在不会出现这类攻击的情况下将其中之一或二者都省去。如果实体 A 和 B 共享两个秘密密钥 K'_{AB}和 K'_{BA}，它们分别用于 B 对 A 和 A 对 B 的鉴别，则区分标识符 A 与 B 可省去。权标变为：

$$\text{Token}AB = \text{Text2} \parallel eK'_{AB}\left(\begin{matrix}T_A\\N_A\end{matrix} \parallel \text{Text1}\right)$$

$$\text{Token}BA = \text{Text4} \parallel eK'_{BA}\left(\begin{matrix}T_B\\N_B\end{matrix} \parallel \text{Text3}\right)$$

这种机制中，选择时间标记还是顺序号取决于声称者与验证者的能力及环境。

图 3 中：步骤(1)和(2)与 5.1.1 中规定的一次传送鉴别相同。

(3) B 向 A 发送 TokenBA。

(4) 步骤(3)中的消息处理方式与 5.1.1 步骤(2)类似。

注 2：这种机制中两条消息之间除了时间上有隐含关系外，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(见附录 A)来进行。

5.2.2 三次传送鉴别

这种鉴别机制中，唯一性/时间性是通过产生并检验随机数(见附录 B)来控制的。

鉴别机制示于图 4。

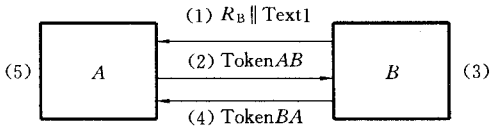

图 4

权标形式如下：

$$\text{Token}AB = \text{Text3} \parallel eK_{AB}(R_A \parallel R_B \parallel B \parallel \text{Text2})$$

$$\text{Token}BA = \text{Text5} \parallel eK_{AB}(R_B \parallel R_A \parallel \text{Text4})$$

注 1：TokenBA 中包含 R_B 是为防止由 TokenAB 导出 TokenBA。

TokenAB 中是否包含区分标识符 B 是可任选的。

注 2：TokenAB 中的区分标识符 B 是为防止所谓的反射攻击。这种攻击的特性是入侵者假冒 A 将询问 R_B“反射”给 B。区分标识符 B 的包含之所以作成可任选，是因为在不会出现此类攻击的环境中可以将其省去。

如果实体 A 和 B 共享两个秘密密钥 K'_{AB}和 K'_{BA}，它们分别用于 B 对 A 和 A 对 B 的鉴别，区分标识符 B 亦可省去。权标则为：

$$\text{Token}AB = \text{Text3} \parallel eK'_{AB}(R_A \parallel R_B \parallel \text{Text2})$$

$$\text{Token}BA = \text{Text5} \parallel eK'_{BA}(R_B \parallel R_A \parallel \text{Text4})$$

图 4 中：(1) B 向 A 发送一个随机数 R_B 和可任选地发送一个文本字段 Text1。

(2) A 向 B 发送 TokenAB。

(3) 一旦收到包含 TokenAB 的消息，B 便将加密部分解密并检验区分标识符 B(如果有的话)的正确性以及步骤(1)中发给 A 的随机数 R_B 是否与 TokenAB 中含的随机数相符，从而验证 TokenAB。

(4) B 向 A 发送 TokenBA。

(5) 一旦收到包含 TokenBA 的消息，A 便将加密部分解密并检验在步骤(1)中来自 B 的随机数 R_B 是否与 TokenBA 中的随机数相符以及在步骤(2)中发送给 B 的随机数 R_A 是否与 TokenBA 中的随机数相符。

6 涉及可信第三方的机制

这些鉴别机制均不需要两个实体在鉴别过程前共享秘密密钥，而是利用一个可信第三方(带区分标识符 TP)，它与实体 A 和 B 分别共享秘密密钥 K_{AT}和 K_{BT}。每个机制中，先由一个实体向可信第三方申请密钥 K_{AB}。此后再分别采用 5.2.1 和 5.2.2 中描述的机制。

按照下面的描述，如果只要求单向鉴别，则可省略每个机制中的某些传送。

注：这些机制不向可信第三方提供任何有关实体 A 和 B 身份的保证。此外，如果鉴别失败，也不会有任何信息指出哪一次交换被入侵者修改或产生。

这些机制要求使用时变参数，如时间标记、顺序号或随机数。这些参数的特性，尤其是它们在鉴别密钥生存期限内极难重复的特性，对于这些机制的安全性是十分重要的。附加信息见附录 B。

以下机制中规定的所有文本字段都可用于本标准范围之外的应用(它们可能是空的)。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见附录 A。

6.1 四次传送鉴别

在这种相互鉴别机制中，唯一性/时间性是通过使用时变参数(见附录 B)控制的。

鉴别机制示于图 5。

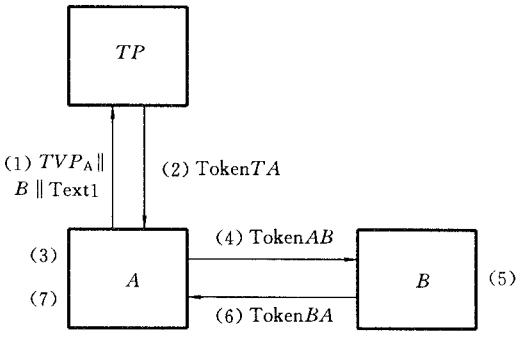

图 5

由 TP 发送给 A 的权标(TokenTA)形式是：

$$\text{Token}TA = \text{Text4} \| eK_{AT}(TVP_A \| K_{AB} \| B \| \text{Text3}) \| eK_{BT}\left(\begin{matrix}T_{TP}\\N_{TP}\end{matrix} \| K_{AB} \| A \| \text{Text2}\right)$$

由 A 发送给 B 的权标(TokenAB)形式是：

$$\text{Token}AB = \text{Text6} \| eK_{BT}\left(\begin{matrix}T_{TP}\\N_{TP}\end{matrix} \| K_{AB} \| A \| \text{Text2}\right) \| eK_{AB}\left(\begin{matrix}T_{A}\\N_{A}\end{matrix} \| B \| \text{Text5}\right)$$

由 B 发送给 A 的权标(TokenBA)形式是：

$$\text{Token}BA = \text{Text8} \| eK_{AB}\left(\begin{matrix}T_{B}\\N_{B}\end{matrix} \| A \| \text{Text7}\right)$$

在这种机制中选择时间标记还是顺序号取决于有关实体的能力和环境。

在图 5 的步骤(1)到步骤(3)中规定的时变参数 TVP_A 的使用方法与通常的有所不同。它允许 A 将响应消息(2)与请求消息(1)联系起来。此处时变参数的重要特性是它的不可重复性，以限制先前用过的 TokenTA 可能被重用。

图 5 中：(1) A 向可信第三方 TP 发送一个时变参数 TVP_A、区分标识符 B 以及可任选地发送一个文本字段 Text1。

(2) 可信第三方 TP 向 A 发送 TokenTA。

(3) 一旦收到包含 TokenTA 的消息，A 便将在 K_{AT}下加密的数据解密并检验区分标识符 B 的正确性以及在步骤(1)中发送给 TP 的时变参数是否与 TokenTA 中的时变参数相符，从而验证

TokenTA。此外，A 提取出秘密鉴别密钥 K_{AB}，然后再从 TokenTA 中取出 $eK_{BT}\left(\begin{matrix}T_{TP}\\N_{TP}\end{matrix}\| K_{AB}\| A\| \text{Text2}\right)$ 并构造 TokenAB。

(4) A 向 B 发送 TokenAB。

(5) 一旦收到包含 TokenAB 的消息，B 便将加密部分解密并检验区分标识符 A 和 B 以及时间标记或顺序号的正确性，从而验证 TokenAB。此外，B 提取出秘密鉴别密钥 K_{AB}。

(6) B 向 A 发送 TokenBA。

(7) 一旦收到包含 TokenBA 的消息，A 便将加密部分解密并检验区分标识符 A 以及时间标记或顺序号的正确性，从而验证 TokenBA。

如果只要求 B 对 A 的单向鉴别，步骤(6)和(7)可省去。

6.2 五次传送鉴别

这种相互鉴别机制中，唯一性/时间性是用随机数(见附录 B)来控制的。

鉴别机制示于图 6。

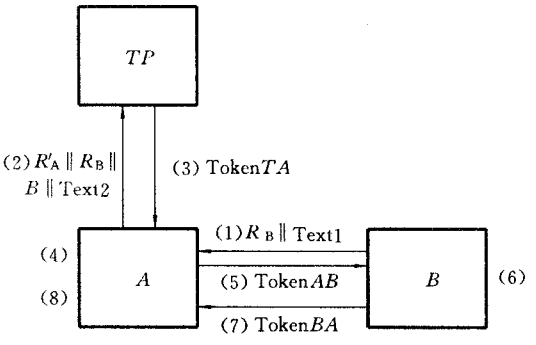

图 6

TP 发送给 A 的权标(TokenTA)形式是：

$$\text{Token}TA = \text{Text5} \| eK_{AT}(R'_A \| K_{AB} \| B \| \text{Text4}) \| eK_{BT}(R_B \| K_{AB} \| A \| \text{Text3})$$

A 发送给 B 的权标(TokenAB)形式是：

$$\text{Token}AB = \text{Text7} \| eK_{BT}(R_B \| K_{AB} \| A \| \text{Text3}) \| eK_{AB}(R_A \| R_B \| \text{Text6})$$

B 发送给 A 的权标(TokenBA)形式是：

$$\text{Token}BA = \text{Text9} \| eK_{AB}(R_B \| R_A \| \text{Text8})$$

图 6 中：(1) B 向 A 发送一个随机数 R_B 和可任选地发送一个文本字段 Text1。

(2) A 向可信第三方 TP 发送随机数 R_B 和 R'_A、区分标识符 B 以及可任选地发送一个文本字段 Text2。

(3) 可信第三方 TP 向 A 发送 TokenTA。

(4) 一旦收到包含 TokenTA 的消息，A 便将在 K_{AT} 下加密的数据解密并检验区分标识符 B 的正确性以及在步骤(2)中发送给 TP 的随机数 R'_A 是否与 TokenTA 中的随机数相符，从而验证 TokenTA。此外，A 提取出秘密鉴别密钥 K_{AB}，然后再从 TokenTB 中取出 $eK_{BT}(R_B \| K_{AB} \| A \| \text{Text3})$，并构造 Token$AB$。

(5) A 向 B 发送 TokenAB。

(6) 一旦收到包含 TokenAB 的消息，B 便将加密部分解密并检验区分标识符 A 的正确性以及在步骤(1)中发送给 A 的随机数 R_B 是否与 TokenAB 中的该随机数的两个副本相符，从而验证 TokenAB。此外，B 还提取出秘密鉴别密钥 K_{AB}。

(7) B 向 A 发送 TokenBA。

(8) 一旦收到包含 TokenBA 的消息，A 便将加密部分解密并检验在步骤(1)中从 B 收到的随机数

R_B 是否与 TokenBA 中包含的那个随机数相符，以及在步骤(5)中发送给 B 的随机数 R_A 是否与 TokenBA 中包含的那个随机数相符。

如果只要求 B 对 A 的单向鉴别，步骤(7)和(8)可以省去。

附 录 A
（提示的附录）
文本字段的使用

本标准的第5章和第6章规定的权标包含了文本字段。在给定传送中不同文本字段的实际使用及各文本字段间的关系取决于具体应用。以下给出一些实例。

如果权标不包含(足够的)冗余度，已加密的文本字段可用于提供附加冗余度。

要求保密性或数据源鉴别的任何信息都应放在该权标的加密部分处。

文本字段可以包含附加的时变参数。例如，在机制5.1.1中，如果已用了顺序号，那么Token*AB*的文本字段可以包含时间标记。这样通过要求消息接收者验证消息中的任何时间标记是否都在一个预先规定的时间窗口内的方法，可以检测出人为延迟(见附录B)。

如果有效密钥不止一个，那么明文文本字段应包括密钥标识符；如果可信第三方不止一个，那么文本字段可用于包括所涉及的那个可信第三方的区分标识符。

文本字段也可用于密钥分配(见ISO/IEC 11770-2)。

假如本标准规定的任何一种机制嵌入到这样一种应用，即如果该机制启动之前，它允许一个实体采用附加消息开始鉴别，那么有些入侵攻击就变得可能。为了抵抗这类攻击，可用文本字段说明哪个实体要求鉴别。这类攻击的特性是入侵者可能重用一个非法获得的权标。

附 录 B
（提示的附录）
时 变 参 数

时变参数是用于控制唯一性/时间性的。它们能使先前发送过的消息再使用时被检测出来。为实现这一点，每次使用机制时，其鉴别信息都应不同。验证者应直接或间接地控制其变化。

某些类型的时变参数也允许检测“人为延迟”(由敌人引入通信媒体的延迟)。在涉及一次以上传送的机制中，可通过其他方法(如采用“超时计时法”来强行规定具体消息间可允许的最大时间间隙)检测人为延迟。

本标准使用的三类时变参数是时间标记、顺序号和随机数。在不同的应用中可根据实现需要选择最可取的时变参数，有时也可以适当选用一种以上时变参数(如同时选择时间标记和顺序号)。有关选择参数的细节不在本标准范围之内。

B1 时间标记

涉及时间标记的机制利用逻辑上链接通信双方的同一个时间基准。建议使用的基准时钟是国际标准时间(UTC)。验证者使用某种固定大小的接收窗口。验证者通过计算接收到的已验证权标中的时间标记与验证者在收到权标时的时间之差来控制时间性。如果差值落在窗口内，消息就被接收。通过在当前窗口中登录所有消息，并拒收第二次和以后出现的与该窗口中同样的消息的方法来验证唯一性。

应该采用某种机制确保通信各方的时钟同步，以便时间基准处在验证者的(间接)控制之下。而且，时钟同步性能要足够好，使通过重用达到冒名顶替的可能性小到可接受的程度。还应确保与验证时间标记有关的所有信息，特别是通信双方的时钟，不会被篡改。

时间标记可用来检测人为延迟。

B2 顺序号

因为顺序号可以使验证者检测消息的重用，可以用顺序号控制唯一性。声称者和验证者预先就如何以特定方式给消息编号的策略达成一致，基本思想是特定编号的消息只能被接受一次(或在规定时间内只接受一次)。然后再检验验证者收到的消息，根据上述策略判断消息中的顺序号是否可接受。这样，顺序号就在验证者的(间接)控制之下。如果顺序号不符合上述策略，该消息则被拒绝。

使用顺序号时可要求附加"簿记"。声称者应维护先前用过的顺序号和/或将来可用的有效顺序号的记录。该声称者应为所有他希望与之通信的潜在验证者保存上述记录。同样，验证者也应为所有可能的声称者保存这些记录。当正常定序被破坏的情况(如系统故障)发生时，则需要有专用程序来重置和/或重新启动顺序号计数器。

声称者使用顺序号不能保证验证者能检测出人为延迟。对于涉及两个或两个以上消息的机制，如果消息发送者能检测出消息发送与预期的回复接收之间的时间间隔，并在延迟超过预先规定的时间间隙时拒绝此消息，就可以测出人为延迟。

B3 随机数

本标准规定的各种机制使用的随机数可防止重用攻击或交错攻击。本标准所述的随机数还包括不可预测的伪随机数。

为防止重用或交错攻击，验证者获得一个发送给声称者的随机数，声称者又将该随机数放在返回权标的加密部分予以响应(这通常称为询问—应答)。这一过程将包含特定随机数的两个消息联系起来。如果同一个随机数被验证者再次使用，记录原始鉴别交换的第三方，就能将记录下的权标发送给验证者，从而使自己假冒为声称者的行为得逞。为防止这类攻击，随机数不重复的概率必须很高。

按照定义，随机数是不可预测的，而且如果随机数从很大范围内取值，则可认为它们的不重复概率可达很高。

声称者使用随机数不能保证验证者能检测人为延迟。

附 录 C
(提示的附录)
参 考 文 献

[1] GB 15852—1995 信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制 (idt ISO/IEC 9797：1994)

[2] ISO/IEC 10118-1：1994 信息技术 安全技术 散列函数 第1部分：概述

[3] ISO/IEC 10118-2：1994 信息技术 安全技术 散列函数 第2部分：采用n位块密码算法的函数

[4] ISO/IEC 11770-2：1995 信息技术 安全技术 密钥管理 第2部分：采用对称技术的机制

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 实体鉴别
第2部分:采用对称加密算法的机制
GB 15843.2—1997
*
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 1 字数 21 千字
1998年4月第一版 1998年4月第一次印刷
印数 1—2 000
*
书号:155066·1-14690 定价 12.00 元
*
标 目 333—29

GB 15843.2-1997