ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 15843.2—2017/ISO/IEC 9798-2:2008
代替 GB/T 15843.2—2008

# 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**

(ISO/IEC 9798-2:2008,IDT)

2017-12-29 发布　　2018-07-01 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》目前已经或计划发布以下部分：

——第1部分：总则；

——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。

本部分为GB/T 15843的第2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 15843.2—2008《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》，与GB/T 15843.2—2008相比，主要变化如下：

——在第3章中，增加了除引用ISO/IEC 9798-1:1997中定义的术语以外的七个术语的描述；

——将原第3章中的“符号”独立为第4章“符号和缩略语”；

——在第5章“要求”中增加了验证时变参数的要求；

——增加了两个附录：附录A和附录C。

本部分使用翻译法等同采用ISO/IEC 9798-2:2008《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》。

与本部分中规范性引用的国际文件中有一致性对应关系的我国文件如下：

——GB/T 15843.1—2017　信息技术　安全技术　实体鉴别　第1部分：总则(ISO/IEC 9798-1:2010,IDT)

本部分做了下列编辑性修改：

——纳入ISO/IEC 9798-2:2008 TECHNICAL CORRIGENDUM 3:2013的内容；

——并列项编号由“(1)、(2)……”改为“a)、b)……”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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。

本部分起草单位：中国科学院数据与通信保护研究教育中心、北京江南天安科技有限公司、普华诚信信息技术有限公司。

本部分主要起草人：夏鲁宁、张琼露、荆继武、朱家雄、谢超。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.2—1997、GB/T 15843.2—2008。

# 引　言

本部分等同采用 ISO/IEC 9798-2:2008 及其勘误文件 ISO/IEC 9798-2:2008 TECHNICAL CORRIGENDUM 3,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC 27(信息安全技术)起草的。

本部分规定了采用对称加密算法的实体鉴别机制,包括单向鉴别机制和相互鉴别机制,不涉及可信第三方的鉴别机制和涉及可信第三方的鉴别机制,并给出了对这些鉴别机制的要求。

在不涉及可信第三方的情况下,单向鉴别机制包括一次传递鉴别和两次传递鉴别两种,相互鉴别机制包括两次传递鉴别和三次传递鉴别两种。如果涉及可信第三方,相互鉴别机制则需要进行四次或者五次传递。

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2部分:采用对称加密算法的机制

## 1　范围

GB/T 15843的本部分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,这四种机制中有两种是由一个实体针对另一个实体的单向鉴别,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。

如果没有可信第三方参与同时又采用时间戳或序号,则对于单向鉴别只需传递一次信息,而要实现相互鉴别需传送两次。如果没有可信第三方参与同时又采用使用随机数的挑战—响应方法时,单向鉴别需传递两次信息,而相互鉴别则需传递三次。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递。

## 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。

ISO/IEC 9798-1　信息技术　安全技术　实体鉴别　第1部分:总则(Information technology—Security techniques—Entity authentication—Part 1:General)

## 3　术语和定义

ISO/IEC 9798-1界定的以及下列术语和定义适用于本文件。

3.1

**可鉴别的加密　authenticated encryption**

通过一种密码算法对数据进行的(可逆)变换,所产生的密文一旦被未授权实体替换,就可被检测出来,也就是说,它提供了数据机密性,数据完整性和数据起源鉴别的保护。

[ISO/IEC 19772:2009]

3.2

**密文　ciphertext**

经过变换的数据,以隐藏其信息内容。

[ISO/IEC 10116:2006]

3.3

**声称方　claimant**

身份可被鉴别的实体,包括其功能以及在鉴别交互中必要的私有数据。

[ISO/IEC 9798-5:2004]

3.4

**消息鉴别码 message authentication code;MAC**

使用消息鉴别码算法产生的输出位串。

注：消息鉴别码有时也被称作密码校验值。

[GB/T 15852.1—2008]

3.5

**消息鉴别码算法 message authentication code(MAC) algorithm**

一种针对位串和密钥进行计算，得到固定长度位串的算法，具有如下特征：

——对于任意密钥和任何输入串，都可以有效计算；

——对于任意固定的密钥，在没有任何关于此密钥先验知识的情况下，计算出任何新输入串的消息鉴别码在计算上都是不可行的。

注1：消息鉴别算法有时也被称为密码校验函数(参见 ISO 7498-2 的示例)。

注2：计算的可行性以来用户的具体安全需求和环境。

[GB/T 15852.1—2008]

3.6

**时间戳 time stamp**

一种时变参数，表示相对于一个通用时间基准的时间点。

[ISO/IEC 18014-1:2008]

3.7

**可信第三方 trusted third party:TTP**

安全机构或其代理机构，在安全相关活动中，其余的实体都信任它。

[ISO/IEC 18014-1:2008]

## 4 符号和缩略语

下列符号和缩略语适用于本文件。

$A$，$B$：参与鉴别机制的实体的标签。

$d_K$：使用秘密密钥 $K$ 的鉴别解密过程。

$e_K$：使用秘密密钥 $K$ 的鉴别加密过程。

$e_K(X)$：针对数据 $X$ 使用对称加密算法和密钥 $K$ 的加密结果。

$I_U$：实体 $U$ 的可区分标识符。

$K$：用于加密或解密的秘密密钥。

$K_{UV}$：由实体 $U$ 和实体 $V$ 共享的秘密密钥，只在对称加密中使用。

$N_U$：由实体 $U$ 产生的序号。

$P$：用以表示可信第三方的符号。

$R_U$：由实体 $U$ 产生的随机数。

$TN_U$：由实体 $U$ 产生的时变参数，可以是时间戳 $T_U$ 或序号 $N_U$。

$Token_{UV}$：从实体 $U$ 向实体 $V$ 发送的令牌。

$T_U$：由实体 $U$ 产生的时间戳。

$TVP_U$：由实体 $U$ 产生的时变参数，可以是时间戳 $T_U$ 或序号 $N_U$ 或随机数 $R_U$。

$X \| Y$：数据项 $X$ 和 $Y$ 按照给定顺序级联的结果。当两个或多个数据项级联的结果在本部分的某个机制中被加密使用时，级联结果应该是组合的，以便可被唯一地解析为原来的构成项，也就是说解析的时候不存在歧义。在不同的应用中，这可以通过多种方式实现，例如(a)要求被级联的每个数据项的

长度是固定且全程保持不变的，或(b)采用某种方式对级联的序列进行编码，以确保正确解码，比如说采用 ISO/IEC 8825-1 定义的可辨识编码规则(DER)。

注：不仅是数据项级联，有序元组也是需要的。通常这样来表示有序元组：$[X_1, X_2, \cdots, X_n]$。

## 5 要求

本部分规定的鉴别机制中，待鉴别的实体通过表明它知道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，与其共享秘密鉴别密钥的任何实体都可以将加密后的数据解密。被解密的数据必须包含时变参数，时变参数可通过下列途径得到验证。

1. 如果时变参数是随机数，那么接收方应确保它与声称方发送的随机挑战是等同的，有关随机数的产生以及使用，可参考 ISO/IEC 18031 以及相关的中华人民共和国国家标准。
2. 如果时变参数是时间戳，那么接收方应能够验证时间戳的有效性。
3. 如果时变参数是序号，那么接收方应能够将其与之前接收或存储的序号进行比较，以确保它不是重放的。

本部分所规定的鉴别机制有下列要求，若其中任何一个不满足，则鉴别过程就会面临潜在的攻击，或不能成功完成。

a) 向验证方证实其身份的声称方，在应用第 6 章的机制时，应和该验证方共享一个秘密鉴别密钥，在应用第 7 章的机制时，每个实体应和公共的可信第三方都分别共享一个秘密鉴别密钥。这些密钥应当在启动鉴别机制之前就为有关各方所知道，做到这一点所采用的方法已超出了本部分的范围，关于共享密钥的管理，在 ISO/IEC 11770-1 和 ISO/IEC 11770-2 中提供了指导。

b) 如果涉及可信第三方，它应得到声称方与验证方的共同信任。

c) 声称方与验证方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，应仅为这两方或双方都信任的其他方所知。若为双方都信任的其他方所知，则其他方不应误用密钥，即不应冒充双方之一来使用密钥。

注：加密算法与密钥生命期的选择应保证密钥在其生命期内就被推算出来在计算上是不可行的。此外，在选择密钥生命期时还应防止已知明文和选择明文攻击。

d) 在机制中使用的令牌即使在已知旧令牌的情况下也不可被伪造，也就是说，在任何情况下旧令牌都不应被部分或全部重用来构造新令牌。对于秘密密钥 $K$ 的任何取值，加密函数 $e_K$ 以及与它对应的解密函数 $d_K$ 应具有如下的属性：当解密过程 $d_K$ 被应用到串 $e_K(X)$ 时，它应能够使得该串的接收方可以检测出数据是否被伪造或被控制，也就是说，只有秘密密钥 $K$ 的拥有者才能够产生可通过解密过程 $d_K$ 被“接受”的串。

注：在实际应用中，可以通过很多方法来保证上述属性。推荐的方式是在一种经过验证的能同时提供机密性和完整性保护的加密技术下使用秘钥 $K$，该机制可参见 ISO/IEC 19772。

e) 本部分中的机制要求使用时变参数，例如时间戳、序号或随机数。这些参数的特性，尤其是它们在秘密鉴别密钥的生命周期内极不可能重复的特性，对于这些机制的安全性是十分重要的。有关时变参数的更多信息，参见 ISO/IEC 9798-1:1997 的附录 B。

f) 用来执行本部分所定义的任一鉴别机制的秘密鉴别密钥应与被用于其他用途的密钥区分开来。

g) 在一个鉴别机制中，如果一个数据串在多处被加密使用，那么它不应是组合的，以便在这些被使用处可互换。

注：这可以通过在每个被加密数据串中包含下列元素来约束：

——附录 A 定义的对象标识符，特别是标识了 ISO 标准、本部分序号和鉴别机制编号的标识符；

——在一个鉴别机制内唯一标识被加密数据串的常数，如果机制中仅包含一个被加密数据串，则这个常数可以

被略去。

被加密数据串的接收方应验证对象标识符和标识被加密数据串的常数，确认其是否与预期值相符。

h) 在第 7 章定义的机制中，$K_{AP}$ 或 $K_{BP}$ 密钥的持有者应总是以相同的方式使用密钥，也就是说要么作为 TPP $P$，要么作为实体 $A$ 或 $B$。这意味着，该密钥持有者不应使用相同的密钥，在一个鉴别协议执行实例中作为 TPP 参与，而在该鉴别协议的另一个执行实例中作为实体 $A$ 或 $B$ 参与。

## 6 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 $K_{AB}$，或者两个单向秘密密钥 $K_{AB}$ 和 $K_{BA}$。在后续的实例中，单向密钥 $K_{AB}$ 和 $K_{BA}$ 分别被 $B$ 用来鉴别 $A$ 和被 $A$ 用来鉴别 $B$。

以下机制中指定的所有文本域在具体的鉴别应用中被赋予含义，有关这些应用的描述超出本部分范围。这些文本域也可以是空的，它们的关系与内容取决于具体的应用。有关文本域的使用参见附录 B。

### 6.1 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。

#### 6.1.1 机制 1——单次传递鉴别

这种鉴别机制中，由声称方 $A$ 启动此过程并被验证方 $B$ 鉴别。唯一性和时效性是通过产生并检验时间戳或序号(见 ISO/IEC 9798-1:1997 的附录 B)来控制的。

鉴别机制如图 1 所示。


图 1 机制 1——单次传递鉴别

声称方 $A$ 发送给验证方 $B$ 的令牌($Token_{AB}$)形式是：

$$Token_{AB} = Text_2 \parallel e_{K_{AB}}(TN_A \parallel I_B \parallel Text_1)$$

此处声称方 $A$ 或者用序号 $N_A$，或者用时间戳 $T_A$ 作为时变参数 $TN_A$。具体选择哪一个取决于声称方与验证方的技术能力及环境。

在 $Token_{AB}$ 中是否包含可区分标识符 $I_B$ 是可选的。

注：在 $Token_{AB}$ 中包含可区分标识符 $I_B$ 是为防止敌手假冒实体 $B$ 对实体 $A$ 重用 $Token_{AB}$。包含可区分标识符 $I_B$ 之所以被作为可选项，是因为在不会出现这类攻击的环境中可将标识符省去。如果使用了单向密钥，该可区分标识符 $I_B$ 也可以被省去。

下面是对机制 1——单次传递鉴别的描述：

a) $A$ 产生并向 $B$ 发送 $Token_{AB}$；

b) 一旦收到包含 $Token_{AB}$ 的消息，$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_B$(如果有)以及时间戳或序号的正确性，从而验证 $Token_{AB}$。

#### 6.1.2 机制 2——两次传递鉴别

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 ISO/IEC 9798-1:1997 中的附录 B)来控制的。

鉴别机制如图 2 所示。

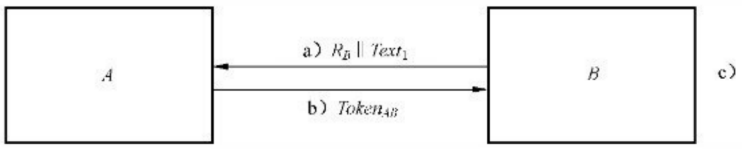


**图 2 机制 2——两次传递鉴别**

由声称方 $A$ 发送给验证方 $B$ 的令牌($Token_{AB}$)形式是:

$Token_{AB} = Text_3 \| e_{K_{AB}}(R_B \| I_B \| Text_2)$

在 $Token_{AB}$ 中是否包含可区分标识符 $I_B$ 是可选的。

注 1:为了防止可能的选择明文攻击(即一种密码分析攻击,密码破译者知道一个或多个密文串对应的完整明文),实体 $A$ 可以在 $Text_2$ 中包含一个随机数 $R_A$。

注 2:在 $Token_{AB}$ 中包含可区分标识符 $I_B$ 是为了防止任何第三方将 $Token_{AB}$ 用作 $Token_{BA}$。对可区分标识符 $I_B$ 的包含之所以是可选的,是因为在不可能发生此类攻击的环境中,可以将其省去;如果使用了单向密钥,可区分标识符 $I_B$ 也可以被省去。

下面是对机制 2——两次传递鉴别的描述:

a) $B$ 产生一个随机数 $R_B$ 并向 $A$ 发送,并可选地发送一个文本字段 $Text_1$ 给 $A$;

b) $A$ 产生并向 $B$ 发送 $Token_{AB}$;

c) 一旦收到包含 $Token_{AB}$ 的消息,$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $B$(如果有)的正确性以及在步骤 a)中发送给 $A$ 的随机数 $R_B$ 是否与 $Token_{AB}$ 中所含的随机数相符,从而验证 $Token_{AB}$。

## 6.2 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。

6.2.1 和 6.2.2 分别采用 6.1.1 和 6.1.2 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 6.1.2 中规定的机制的两个实例构成,一个由实体 $A$ 启动,另一个由 $B$ 启动。

### 6.2.1 机制 3——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校验时间戳或序号(见 ISO/IEC 9798-1:1997 附录 B)来控制的。

鉴别机制如图 3 所示。

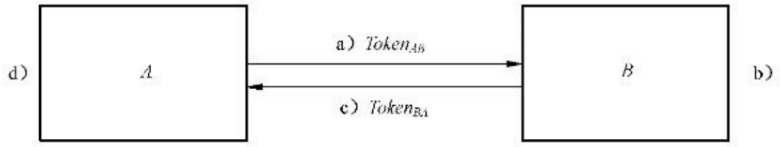


**图 3 机制 3——两次传递鉴别**

由 $A$ 发送给 $B$ 的令牌($Token_{AB}$)形式与 6.1.1 规定的相同。

$Token_{AB} = Text_2 \| e_{K_{AB}}(TN_A \| I_B \| Text_1)$

由 $B$ 发送给 $A$ 的令牌($Token_{BA}$)形式是:

$Token_{BA} = Text_4 \| e_{K_{AB}}(TN_B \| I_A \| Text_3)$

在 $Token_{AB}$ 中是否包含可区分标识符 $I_B$，在 $Token_{BA}$ 中是否包含可区分标识符 $I_A$，是分别可选地。

注 1：$Token_{AB}$ 中的可区分标识符 $I_B$ 是为防止敌手假冒实体 $B$ 对实体 $A$ 重用 $Token_{AB}$。同样的原因，$Token_{BA}$ 包含可区分标识符 $I_A$。可区分标识符的包含之所以作为可选项，是因为在不会出现这类攻击的环境中可以将其中之一或二者都省去。如果使用了单向密钥，可区分标示符 $I_A$ 和 $I_B$ 也可以被省去。

这种机制中，选择使用时间戳还是序号取决于声称方与验证方的技术能力和环境。

下面是对机制 3——两次传递鉴别的描述：

a) $A$ 产生并向 $B$ 发送 $Token_{AB}$；

b) 一旦收到包含 $Token_{AB}$ 的消息，$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_B$(如果有)以及时间戳或序号的正确性，从而验证 $Token_{AB}$；

c) $B$ 产生并向 $A$ 发送 $Token_{BA}$；

d) 步骤 c)中的 $A$ 对消息的处理方式与步骤 b)类似。

注 2：这种机制中两条消息之间除了时效性的隐含关系外没有任何绑定关系；该机制独立地两次使用机制 6.1.1，可以通过使用适当的文本域来进一步绑定这些消息。

如果使用了单向密钥，那么 $Token_{BA}$ 中的密钥 $K_{AB}$ 被密钥 $K_{BA}$ 代替，并且在步骤 d)中使用对应的密钥。

### 6.2.2 机制 4——三次传递鉴别

这种鉴别机制中，唯一性和时效性是通过产生并校验随机数(见 ISO/IEC 9798-1:1997 中的附录 B)来控制的。

鉴别机制如图 4 所示。

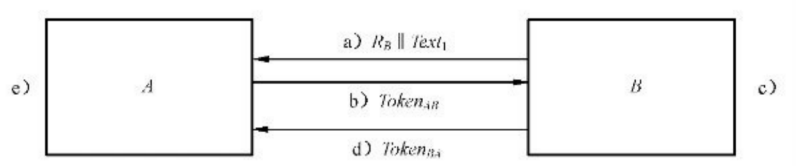


图 4 机制 4——三次传递鉴别

令牌形式如下：

$Token_{AB} = Text_3 \| e_{K_{AB}}(R_A \| R_B \| I_B \| Text_2)$

$Token_{BA} = Text_5 \| e_{K_{AB}}(R_B \| R_A \| Text_4)$

$Token_{AB}$ 中是否包含可区分标识符 $I_B$ 是可选的。

注：当 $Token_{AB}$ 中包含可区分标识符 $I_B$ 时，是为防止所谓的反射攻击，这种攻击的特征是入侵者假冒 $A$ 将挑战随机数 $R_B$“反射”给 $B$。可区分标识符 $I_B$ 的包含之所以作为可选项，是因为在不会出现这类攻击的环境中可将其省去。如果使用了单向密钥，该可区分标识符 $I_B$ 也可以被省去。

下面是对机制 4——三次传递鉴别的描述：

a) $B$ 产生一个随机数 $R_B$ 并向 $A$ 发送，并可选地发送一个文本字段 $Text_1$ 给 $A$；

b) $A$ 产生一个随机数 $R_A$，然后产生 $Token_{AB}$ 并发送给 $B$；

c) 一旦收到包含 $Token_{AB}$ 的消息，$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_B$(如果有)的正确性以及步骤 a)中发给 $A$ 的随机数 $R_B$ 是否与 $Token_{AB}$ 中含的随机数相符，从而验证 $Token_{AB}$；

d) $B$ 产生并向 $A$ 发送 $Token_{BA}$；

e) 一旦收到包含 $Token_{BA}$ 的消息，$A$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验在步骤 a)中来自 $B$ 的随机数 $R_B$ 是否与 $Token_{BA}$ 中的随机数相符以及在步骤 b)中发送给 $B$ 的随机数 $R_A$ 是否与 $Token_{BA}$ 中的随机数相符。

如果使用了单向密钥，那么 $Token_{BA}$ 中的密钥 $K_{AB}$ 被密钥 $K_{BA}$ 代替，并且在步骤 e)中使用对应的密钥。

## 7 涉及可信第三方的机制

本章中所述的鉴别机制不是利用两个实体在鉴别过程前共享的秘密密钥，而是利用一个可信第三方(用 $P$ 表示)，实体 $A$ 和 $B$ 分别与它共享秘密密钥 $K_{AP}$ 和 $K_{BP}$。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 6.2.1 和 6.2.2 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递。

以下机制中规定的所有文本域同样适用于本标准范围之外的应用(文本域可能是空的)。它们的关系和内容取决于具体应用。有关文本域使用的信息参见附录 B。

### 7.1 机制 5——四次传递鉴别

本机制与 ISO/IEC 11770-2:2008 中的密钥建立机制 8 等同。

鉴别机制如图 5 所示。

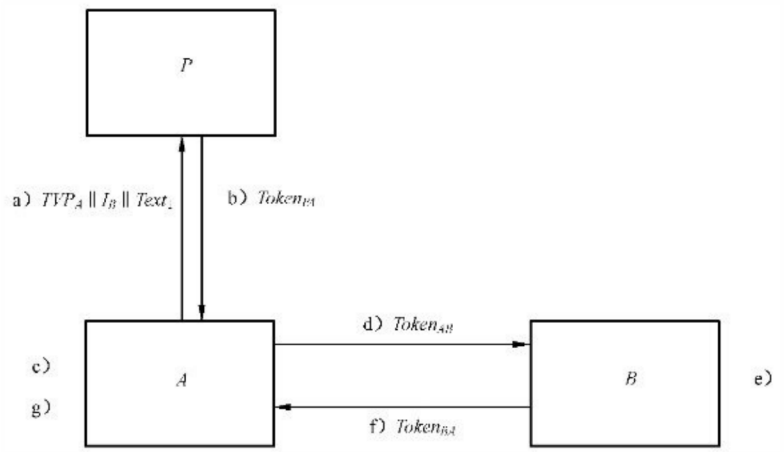


**图 5 机制 5——四次传递鉴别**

由 $P$ 发送给 $A$ 的令牌($Token_{PA}$)形式是：

$$Token_{PA} = Text_4 \| e_{K_{AP}}(TVP_A \| K_{AB} \| I_B \| Text_3) \| e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2)$$

由 $A$ 发送给 $B$ 的令牌($Token_{AB}$)形式是：

$$Token_{AB} = Text_6 \| e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2) \| e_{K_{AB}}(TN_A \| I_B \| Text_5)$$

由 $B$ 发送给 $A$ 的令牌($Token_{BA}$)形式是：

$$Token_{BA} = Text_8 \| e_{K_{AB}}(TN_B \| I_A \| Text_7)$$

在本机制中选择时间戳还是序号取决于相关实体的技术能力和环境。

在图 5 中步骤 a)～步骤 c)中的时变参数 $TVP_A$ 的使用方法与通常的有所不同，它允许 $A$ 将响应消息 b)与请求消息 a)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 $Token_{PA}$ 被重用。

注：时变参数 $TVP_A$ 可以是一个随机数。但是与本标准中某些机制所使用的随机数不同的是，该随机数对于第三方不必是不可预测的，不重复的计数器值同样适用于产生该随机数。

下面是对机制 5——四次传递鉴别的描述：

a) $A$ 产生并向可信第三方 $P$ 发送一个时变参数 $TVP_A$、可区分标识符 $I_B$ 以及可选地发送一个文本域 $Text_1$。

b) 可信第三方 $P$ 产生并向 $A$ 发送 $Token_{PA}$。

c) 一旦收到包含 $Token_{PA}$ 的消息，$A$ 便将使用 $K_{AP}$ 加密的数据解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_B$ 的正确性以及在步骤 a)中发送给 $P$ 的时变参数是否与 $Token_{PA}$ 中的时变参数相符，从而验证 $Token_{PA}$。此外，$A$ 提取出秘密鉴别密钥 $K_{AB}$，然后再从 $Token_{PA}$ 中取出

$$e_{K_{BP}}(TN_P \parallel K_{AB} \parallel I_A \parallel Text_2)$$

并以此来构造 $Token_{AB}$。

d) $A$ 产生并向 $B$ 发送 $Token_{AB}$。

e) 一旦收到包含 $Token_{AB}$ 的消息，$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_A$ 和 $I_B$ 以及时间戳或序号的正确性，从而验证 $Token_{AB}$。此外，$B$ 提取出秘密鉴别密钥 $K_{AB}$。

f) $B$ 产生并向 $A$ 发送 $Token_{BA}$。

g) 一旦收到包含 $Token_{BA}$ 的消息，$A$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_A$ 以及时间戳或序号的正确性，从面验证 $Token_{BA}$。

如果只要求 $B$ 对 $A$ 的单向鉴别，步骤 f)和 g)可省去。

## 7.2 机制 6——五次传递鉴别

在这种相互鉴别机制中，唯一性和时效性是用随机数(见 ISO/IEC 9798-1:1997 的附录 B)来控制的。本机制与 ISO/IEC 11770-2:2008 中的密钥建立机制 9 等同。

鉴别机制如图 6 所示。

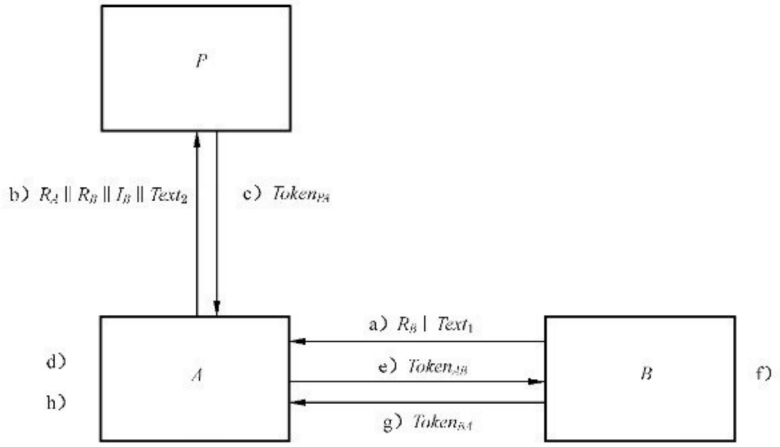


**图 6 机制 6——五次传递鉴别**

由 $P$ 发送给 $A$ 的令牌($Token_{PA}$)形式是：

$$Token_{PA} = Text_5 \parallel e_{K_{AP}}(R_A \parallel K_{AB} \parallel I_B \parallel Text_4) \parallel e_{K_{BP}}(R_B \parallel K_{AB} \parallel I_A \parallel Text_3)$$

由 $A$ 发送给 $B$ 的令牌($Token_{AB}$)形式是：

$$Token_{AB} = Text_7 \parallel e_{K_{BP}}(R_B \parallel K_{AB} \parallel I_A \parallel Text_3) \parallel e_{K_{AB}}(R'_A \parallel R_B \parallel Text_6)$$

由 $B$ 发送给 $A$ 的令牌($Token_{BA}$)形式是：

$$Token_{BA} = Text_9 \parallel e_{K_{AB}}(R_B \parallel R'_A \parallel Text_8)$$

下面是对机制 6——五次传递鉴别的描述：

a) $B$ 产生并向 $A$ 发送一个随机数 $R_B$，可选地发送一个文本域 $Text_1$。

b) $A$ 产生随机数 $R_A$，并向可信第三方 $P$ 发送 $R_A$、随机数 $R_B$、可区分标识符 $I_B$ 以及可任选地发送一个文本域 $Text_2$。

c) 可信第三方 $P$ 产生并向 $A$ 发送 $Token_{PA}$。

d) 一旦收到包含 $Token_{PA}$ 的消息，$A$ 便将使用 $K_{AP}$ 加密的数据解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_B$ 的正确性以及在步骤 b)中发给 $P$ 的随机数 $R_A$ 是否与 $Token_{PA}$ 中的随机数相符，从而验证 $Token_{PA}$。此外，$A$ 提取出秘密鉴别密钥 $K_{AB}$，然后再从 $Token_{PA}$ 中取出

$$e_{K_{BP}}(R_B \parallel K_{AB} \parallel I_A \parallel Text_3)$$

以此来构造 $Token_{AB}$。

e) $A$ 产生第二个随机数 $R'_A$，然后产生并向 $B$ 发送 $Token_{AB}$。

f) 一旦收到包含 $Token_{AB}$ 的消息，$B$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验可区分标识符 $I_A$ 的正确性以及在步骤 a)中发给 $A$ 的随机数 $R_B$ 是否与 $Token_{AB}$ 中的该随机数的两个副本相符，从而验证 $Token_{AB}$。此外，$B$ 还提取出秘密鉴别密钥 $K_{AB}$。

g) $B$ 产生并向 $A$ 发送 $Token_{BA}$。

h) 一旦收到包含 $Token_{BA}$ 的消息，$A$ 便将加密部分解密[此时解密意味着满足第 5 章 d)的要求]并检验在步骤 a)从 $B$ 收到的随机数 $R_B$ 是否与 $Token_{BA}$ 中包含的那个随机数相符，以及在步骤 e)中发送给 $B$ 的随机数 $R'_A$ 是否与 $Token_{BA}$ 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 g)和 h)可以被省去。

# 附 录 A
（规范性附录）
OID 和 ASN.1 语法

## A.1 形式化定义

```
EntityAuthenticationMechanisms-2 {
    iso(1) standard(0) e-auth-mechanisms(9798) part2(2)
      asn1-module(0) object-identifiers(0) }
    DEFINITIONS EXPLICIT TAGS ::= BEGIN
--EXPORTS All;--
--IMPORTS None;--
OID ::= OBJECT IDENTIFIER--alias

--Synonyms--
is9798-2 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part2(2) }
mechanism OID ::= { is9798-2 mechanisms(1) }

--不涉及可信第三方的单向或相互实体鉴别机制--
ua-one-pass OID ::= { mechanism 1 }
ua-two-pass OID ::= { mechanism 2 }
ma-two-pass OID ::= { mechanism 3 }
ma-three-pass OID ::= { mechanism 4 }

--涉及可信第三方的相互实体鉴别机制 -
ttp-ma-four-pass OID ::= { mechanism 5 }
ttp-ma-five-pass OID ::= { mechanism 6 }
END--EntityAuthenticationMechanisms-2--
```

## A.2 对象标识符的后续使用

本部分中所有的实体鉴别机制都使用对称加密技术。因此，在实体鉴别机制的对象标识符之后，可能会跟有一个对象标识符来指定所使用的加密技术，例如在 ISO/IEC 19772 中所定义的各个机制的对象标识符。

## A.3 符合 ASN.1 基本编码规则(BER)的编码示例

根据 ISO/ISC 8825-1，一个对象标识符由一个或多个字节序列构成，每个字节序列都编码了一个数字。

——如果字节序列包含一个以上字节，则首个字节的第 8 位设置为 1，最后一个字节的第 8 位设置为 0；

——字节序列用所有字节的低 7 位共同编码一个数字，每个数字应使用最少的字节数进行编码，这意味着，字节'80'在字节序列中不是一个有效的首字节；

——第一个数字表示标准号；如果存在第二个数字，则它表示多部分标准的第几部分。

本文档所定义的每个机制都分别由一个对象标识符表示。

——为标识一个 ISO 标准，首个字节被设置为十六进制'28'，即十进制 40；

——接下来的两个字节被设置为'CC46'，这是因为 9798 的十六进制值是'2646'，即二进制 0010 0110 0100 0110，也就是两个 7 位组：1001100 1000110。在对每个字节的第 8 位设置相应的值后，字节序列变成了 11001100 01000110，也就是'CC46'。

- 下一个字节设置为十六进制'02'，表示第 2 部分；
- 下一个字节标识一种鉴别机制；
- '01'标识不涉及可信第三方的单次传递单向鉴别机制；
- '02'标识不涉及可信第三方的两次传递单向鉴别机制；
- '03'标识不涉及可信第三方的两次传递相互鉴别机制；
- '04'标识不涉及可信第三方的三次传递相互鉴别机制；
- '05'标识涉及可信第三方的四次传递相互鉴别机制；
- '06'标识涉及可信第三方的五次传递相互鉴别机制。

例如十六进制数据元'28 CC 46 02 05'读为{iso standard 9798 2 5}，意思是 ISO/IEC 9798-2 的第五种机制，即涉及可信第三方的四次传递相互鉴别机制。这个数据元可以以下面的 BER-TLV 数据对象（参见 ASN.1 基本编码规则，ISO/IEC 8825-1，全局类标签'06'）的形式被传输，其中破折号和大括号不重要，使用它们的目的只是为了表达清晰。

数据对象 = {'06'-'05'-'28 CC 46 02 05'}。

# 附 录 B
（资料性附录）
文本域的使用

本部分的第6章和第7章规定的令牌包含了文本域。在给定传递中不同文本域的实际使用及各文本域间的关系取决于具体应用。以下给出一个实例，也可以参考ISO/IEC 9798-1:1997的附录A。

机密性或数据起源鉴别所需的信息应被放在该令牌的被加密部分。

# 附 录 C
（资料性附录）
实体鉴别机制的性质

表 C.1 总结了本部分所描述的实体鉴别机制的主要性质。括号中显示的是可选项，例如机制 5 有一个可选的三次传递单向鉴别版本。

**表 C.1 机制的性质**

| 机制 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 传递的次数 | 1 | 2 | 2 | 3 | 4(或 3) | 5(或 4) |
| 单向/相互鉴别 | 单向 | 单向 | 相互 | 相互 | 相互(单向) | 相互(单向) |
| 保证时效性的变量(注 1) | $TN_A$ | $R_B$ | $TN_A$ 和 $TN_B$ | $R_A$ 和 $R_B$ | $TVP_A$、$TN_B$ 和 $TN_P$ | $R_A$ 和 $R_B$ |
| 发起鉴别机制的实体 | $A$ | $B$ | $A$ | $B$ | $A$ | $B$ |
| 声称方是否获知成功信息(注 2) | 否 | 否 | 仅 $A$ 获知 | 仅 $A$ 获知 | 仅 $A$ 获知 | 仅 $A$ 获知 |

注 1：对于使用随机数来保证时效性的机制 2、4 和 6，两实体间不必维持同步时钟或序号。

注 2：在本部分所描述的鉴别机制中，声称方以加密令牌的形式发送身份证明。某些情况下，对方实体并不返回响应以表明身份证明被成功地接受。表 C.1 中的最后一行表明了协议内在的保证成功鉴别的信息的位置。在其余的情况下，如果声称方需要，则系统向其提供成功信息。

## 参 考 文 献

[1] GB/T 15852.1—2008 信息技术 安全技术 消息鉴别码 第1部分:采用分组密码的机制(ISO/IEC 9797-1:1999,IDT)

[2] ISO/IEC 8825-1 信息技术 ASN.1编码规则:基本编码规则(BER)、标准编码规则(CER)和区分编码规则(DER)规范

[3] ISO/IEC 9798-5:2004 信息技术 安全技术 实体鉴别 第5部分:使用零知识证明技术的机制

[4] ISO/IEC 10116:2006 信息技术 安全技术 $n$ 位块密码算法的工作模式

[5] ISO/IEC 11770-1 信息技术 安全技术 密钥管理 第1部分:框架

[6] ISO/IEC 11770-2:2008 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

[7] ISO/IEC 18014-1:2008 信息技术 安全技术 时间戳服务 第1部分:框架

[8] ISO/IEC 18031 信息技术 安全技术 随机位产生

[9] ISO/IEC 19772:2009 信息技术 安全技术 可鉴别的加密机制

[10] D. Basin, C. Cremers and S. Meier, 'Provably repairing the ISO/IEC 9798 standard for entity authentication'. In: P. Degano, J. D. Guttman (eds.), Principles of Security and Trust—First International Conference, POST 2012, Tallinn, Estonia, March 24—April 1, 2012, Proceedings. Springer LNCS 7215, pp.129-148, 2012.

GB/T 15843.2—2017/ISO/IEC 9798-2:2008

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/T 15843.2—2017/ISO/IEC 9798-2:2008
*
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.org.cn
服务热线:400-168-0010
2018年1月第一版
*
书号:155066·1-58579



GB/T 15843.2-2017