ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.2—2008/ISO/IEC 9798-2:1999
代替 GB 15843.2—1997

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 algorithm

(ISO/IEC 9798-2:1999,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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和符号 …… 1
4　要求 …… 1
5　不涉及可信第三方的机制 …… 2
5.0　概述 …… 2
5.1　单向鉴别 …… 2
5.2　相互鉴别 …… 3
6　涉及可信第三方的机制 …… 5
6.0　概述 …… 5
6.1　四次传递鉴别 …… 5
6.2　五次传递鉴别 …… 6
附录A（资料性附录）　文本字段的使用 …… 8
参考文献 …… 9

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2部分，等同采用ISO/IEC 9798-2:1999《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》(英文版)，仅有编辑性修改。

本部分代替GB 15843.2—1997《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》。本部分与GB 15843.2—1997相比，主要变化如下：

——本部分更新了第4章"要求"，对加密函数以及与它对应的解密函数应具有的属性提出了要求，同时增加了对时变参数特性的要求。

——本部分在内容上增加了对于基于单向密钥来完成鉴别过程的考虑，因而在对应的各个章条部分都增加了相应的叙述。

——本部分废止了旧版中关于实体A和B之间共享一个秘密密钥K'_{AB}，而K'_{AB}只用于B对A的鉴别的相关叙述。

——本部分删除了ISO/IEC　前言，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、许长志、高能、向继、夏鲁宁。

本部分所代替标准的历次版本发布情况为：

——GB 15843.2—1997。

引　言

本部分等同采用国际标准 ISO/IEC 9798-2:1999,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC 27(IT 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,并给出了这些鉴别机制的 5 项要求。

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

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,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,而要实现相互鉴别必须传递两次。如果没有可信第三方参与同时又采用使用随机数的激励—响应方法时,单向鉴别需传递两次信息,而相互鉴别则需要传递三次。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)

ISO/IEC 11770-2:1996　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

3　术语、定义和符号

GB/T 15843.1 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。

这些鉴别机制有下列要求,若其中任何一个不满足,则鉴别过程就会受到攻击,或者不能成功完成。

a) 向验证方证实其身份的声称方,在应用第5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6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。这些密钥应当在正式启动鉴别机制前就为有关各方知道,达到这一点所采用的方法已超出了本部分的范围。

b) 如果涉及到可信第三方,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。

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

d) 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 应用到字符串 $e_K(X)$ 时，它应该能够使得该字符串的接收者可以检测出数据是否被伪造或者被控制，也就是说，只有秘密密钥 K 的拥有者才能够产生这些字符串，而且只有当这些字符串由解密过程 d_K 检查之后才是能被“接受”。

注 2：在实际应用中，可以通过很多方法来保证上述属性。两个例子如下：

1) 如果数据具有或者附加了足够的冗余信息，并且加密算法是精心挑选的，那么完整性是可以满足的。只有冗余信息的正确性被验证之后，解密的数据才能被接受是正确的。

2) 用密钥 K 推导一对密钥 K′和密钥 K″。用密钥 K′来计算待加密数据的消息鉴别码(MAC)，而密钥 K″用来将该数据和 MAC 级联在一起加密。接收者在确认已解密数据是正确的之前必须先检查 MAC 值是否正确。

e) 本部分中的机制要求使用时变参数，例如时间戳、序号或者随机数。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。

5 不涉及可信第三方的机制

5.0 概述

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} 分别由 B 用来鉴别 A 和 A 用来鉴别 B。

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)。它们的关系与内容取决于具体的应用。有关文本字段使用的信息参见附录 A。

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 GB/T 15843.1—2008 中的附录 B)来控制的。

鉴别机制如图 1 所示。

图 1 不涉及可信第三方的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：

$$Token_{AB} = Text2 \parallel e_{K\,AB}\left(\begin{matrix}T_A\\N_A\end{matrix} \parallel B \parallel Text1\right)$$

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。具体选择哪一个取决于声称方与验证方的技术能力和环境。

在 $Token_{AB}$ 中是否包含可区分标识符 B 是可选的。

注：在 $Token_{AB}$ 中包含可区分标识符 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 B 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标识符省去。

如果使用了单向密钥，该可区分标识符 B 也可以省去。

图 1 中：

(1) A 产生并向 B 发送 $Token_{AB}$；

(2) 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 4 章 d)的要求)并检验可区分标识符 B(如果有)以及时间戳或序号的正确性，从而验证 $Token_{AB}$。

5.1.2 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 GB/T 15843.1—2008 中的附录 B)来控制的。

鉴别机制如图 2 所示。

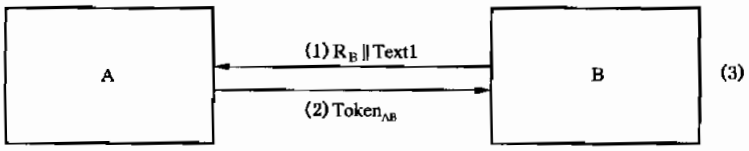

图 2 不涉及可信第三方的两次传递单向鉴别机制示意图

由声称方 A 发送给验证方 B 的权标($Token_{AB}$)形式是：

$$Token_{AB} = Text3 \| e_{K_{AB}}(R_B \| B \| Text2)$$

在 $Token_{AB}$ 中是否包含可区分标识符 B 是可选的。

注 1：为了防止可能的已知明文攻击(即一种密码分析攻击，密码破译者知道一个或者多个密文字符串的完整明文)，实体 A 可以在 Text2 中包含一个随机数 R_A。

注 2：在 $Token_{AB}$ 中包含可区分标识符 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 将激励随机数 R_B“反射”给 B。包含可区分标识符之所以作为可选项，是因为在不会出现这类攻击的环境中可将标识符省去。

如果使用了单向密钥，该可区分标识符 B 也可以省去。

图 2 中：

(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 产生并向 B 发送 $Token_{AB}$。

(3) 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 4 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(1)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 $Token_{AB}$。

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递，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 中规定的机制的两个实例构成，一种由实体 A 启动，另一种由 B 启动。

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 中的附录 B)来控制的。

鉴别机制如图 3 所示。

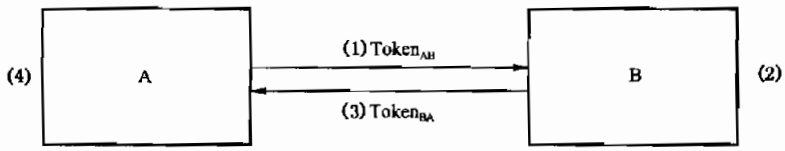

图 3 不涉及可信第三方的两次传递相互鉴别机制示意图

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

$$Token_{AB} = Text2 \parallel e_{K_{AB}}(\begin{matrix}T_A\\N_A\end{matrix} \parallel B \parallel Text1)$$

由 B 发送给 A 的权标($Token_{BA}$)形式是:

$$Token_{BA} = Text4 \parallel e_{K_{AB}}(\begin{matrix}T_B\\N_B\end{matrix} \parallel A \parallel Text3)$$

在 $Token_{AB}$ 中是否包含可区分标识符 B,在 $Token_{BA}$ 中是否包含可区分标识符 A,是分别可选的。

注 1: $Token_{AB}$ 中的可区分标识符 B 是为防止敌手假冒实体 B 对实体 A 重用 $Token_{AB}$。由于同样的原因,Token 包含可区分标识符 A。包含可区分标识符之所以作为可选项,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,可区分标识符 A 和 B 也可以省去。

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。

图 3 中:步骤(1)和(2)与 5.1.1 中规定的一次传递鉴别相同。

(3) B 产生并向 A 发送 $Token_{BA}$。

(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效性的隐含关系外没有任何绑定关系;该机制两次独立使用机制 5.1.1,可以通过使用适当的文本字段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} 用密钥 K_{BA} 代替,并且在步骤(4)中使用对应的密钥。

5.2.2 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检验随机数(见 GB/T 15843.1—2008 中的附录 B)来控制的。

鉴别机制如图 4 所示。

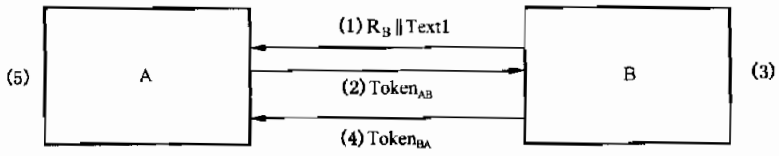

图 4 不涉及可信第三方的三次传递相互鉴别机制示意图

权标形式如下:

$$Token_{AB} = Text3 \parallel e_{K_{AB}}(R_A \parallel R_B \parallel B \parallel Text2)$$

$$Token_{BA} = Text5 \parallel e_{K_{AB}}(R_B \parallel R_A \parallel Text4)$$

$Token_{AB}$ 中是否包含可区分标识符 B 是可选的。

注: 在 $Token_{AB}$ 中包含可区分标识符 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 将激励随机数 R_B"反射"给 B。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将标识符省去。

如果使用了单向密钥,该可区分标识符 B 也可以省去。

图 4 中:

(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 产生一个随机数 R_A,然后产生 $Token_{AB}$ 并发送给 B。

(3) 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 4 章 d)的要求)并检验可区分标识符 B(如果有)的正确性以及步骤(1)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 $Token_{AB}$。

(4) B产生并向A发送 $Token_{BA}$。

(5) 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4章d)的要求)并检验在步骤(1)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(2)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} 用密钥 K_{BA} 代替，并且在步骤(5)中使用对应的密钥。

6 涉及可信第三方的机制

6.0 概述

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(其可区分标识符为TP)，实体A和B分别与它共享秘密密钥 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递。

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见附录A。

6.1 四次传递鉴别

在这种相互鉴别机制中，唯一性和时效性是通过使用时变参数(见GB/T 15843.1—2008中的附录B)控制的。本机制与ISO/IEC 11770-2:1996中的密钥建立机制8等同。

鉴别机制如图5所示。

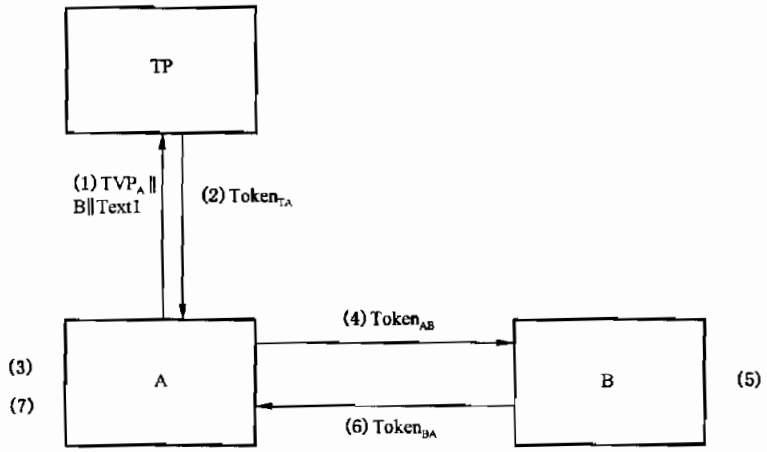

图5 涉及可信第三方的四次传递相互鉴别机制示意图

由TP发送给A的权标($Token_{TA}$)形式是：

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

由A发送给B的权标($Token_{AB}$)形式是：

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

由B发送给A的权标($Token_{BA}$)形式是：

$$Token_{BA} = Text8 \| e_{K_{AB}}\left(\begin{matrix}T_{B}\\N_{B}\end{matrix} \| A \| Text7\right)$$

在本机制中选择使用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 $Token_{TA}$ 可能被重用。

注：时变参数 TVP_A 可以是一个随机数。但是与本部分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，由此，不重复的计数器值同样适用于产生该随机数。

图 5 中：

(1) A 产生并向可信第三方 TP 发送一个时变参数 TVP_A、可区分标识符 B 以及可选地发送一个文本字段 Text1。

(2) 可信第三方 TP 产生并向 A 发送 $Token_{TA}$。

(3) 一旦收到包含 $Token_{TA}$ 的消息，A 便将使用 K_{AT} 加密的数据解密（此时加解密意味着满足第 4 章 d）的要求）并检验可区分标识符 B 的正确性以及在步骤(1)中发送给 TP 的时变参数是否与 $Token_{TA}$ 中的时变参数相符，从而验证 $Token_{TA}$。此外，A 提取出秘密鉴别密钥 K_{AB}，然后再从 $Token_{TA}$ 中取出

$$e_{K_{BT}}\left(\begin{matrix}T_{TP}\\N_{TP}\end{matrix} \| K_{AB} \| A \| Text2\right)$$

并以此来构造 $Token_{AB}$。

(4) A 产生并向 B 发送 $Token_{AB}$。

(5) 一旦收到包含 $Token_{AB}$ 的消息，B 便将加密部分解密（此时加解密意味着满足第 4 章 d）的要求）并检验可区分标识符 A 和 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}。

(6) B 产生并向 A 发送 $Token_{BA}$。

(7) 一旦收到包含 $Token_{BA}$ 的消息，A 便将加密部分解密（此时加解密意味着满足第 4 章 d）的要求）并检验可区分标识符 A 以及时间戳或序号的正确性，从而验证 $Token_{BA}$。

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 GB/T 15843.1—2008 中的附录 B）来控制的。该机制与 ISO/IEC 11770-2:1996 中的密钥建立机制 9 等同。

鉴别机制如图 6 所示。

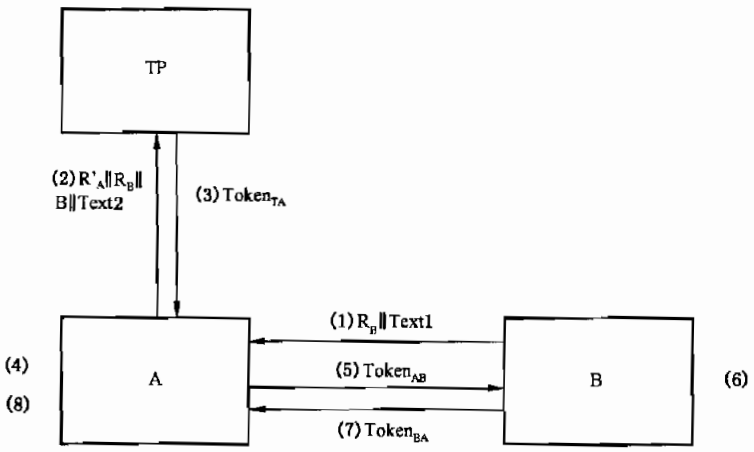

图 6 涉及可信第三方的五次传递相互鉴别机制示意图

TP 发送给 A 的权标（$Token_{TA}$）形式是：

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

A 发送给 B 的权标（$Token_{AB}$）形式是：

$$Token_{AB} = Text7 \| e_{K_{BT}}(R_B \| K_{AB} \| A \| Text3) \| e_{K_{AB}}(R_A \| R_B \| Text6)$$

B 发送给 A 的权标($Token_{BA}$)形式是：

$$Token_{BA} = Text9 \parallel e_{K_{AB}}(R_B \parallel R_A \parallel Text8)$$

图 6 中：

(1) B 产生并向 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 产生 R'_A，并向可信第三方 TP 发送随机数 R_B 和 R'_A、可区分标识符 B 以及可选地发送一个文本字段 Text2。

(3) 可信第三方 TP 产生并向 A 发送 $Token_{TA}$。

(4) 一旦收到包含 $Token_{TA}$ 的消息，A 便将使用 K_{AT} 加密的数据解密(此时加解密意味着满足第 4 章 d)的要求)并检验可区分标识符 B 的正确性以及在步骤(2)中发给 TP 的随机数 R'_A 是否与 $Token_{TA}$ 中的随机数相符，从而验证 $Token_{TA}$。此外，A 提取出秘密鉴别密钥 K_{AB}，然后再从 $Token_{TB}$ 中取出

$$e_{K_{BT}}(R_B \parallel K_{AB} \parallel A \parallel Text3)$$

以此来构造 $Token_{AB}$。

(5) A 产生第二个随机数 R_A，然后产生并向 B 发送 $Token_{AB}$。

(6) 一旦收到包含 $Token_{AB}$ 的消息，B 便将加密部分解密(此时加解密意味着满足第 4 章 d)的要求)并检验可区分标识符 A 的正确性以及在步骤(1)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}。

(7) B 产生并向 A 发送 $Token_{BA}$。

(8) 一旦收到包含 $Token_{BA}$ 的消息，A 便将加密部分解密(此时加解密意味着满足第 4 章 d)的要求)并检验在步骤(1)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(5)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(7)和(8)可以省去。

附 录 A
（资料性附录）
文本字段的使用

本部分的第5章和第6章规定的权标包含了文本字段。在给定传递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，也可以参考GB/T 15843.1—2008的附录。

如果权标不包含(足够的)冗余，已加密的文本字段可用于提供附加冗余。

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。

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] GB/T 18238.1—2000 信息技术 安全技术 散列函数 第1部分:概述(idt ISO/IEC 10118-1:1994)

[3] GB/T 18238.2—2002 信息技术 安全技术 散列函数 第2部分:采用n位块密码的散列函数(idt ISO/IEC FDIS 10118-2:2000)

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—2008/ISO/IEC 9798-2:1999
*
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 1 字数 20 千字
2008年9月第一版 2008年9月第一次印刷
*
书号:155066·1-33389 定价 16.00 元

GB/T 15843.2—2008/ISO/IEC 9798-2:1999

GB/T 15843.2-2008

打印日期:2009年4月22日