ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.4—2008/ISO/IEC 9798-4:1999
代替 GB/T 15843.4—1999

信息技术　安全技术　实体鉴别
第4部分:采用密码校验函数的机制

Information technology—Security techniques—Entity authentication—Part 4:Mechanisms using a cryptographic check function

(ISO/IEC 9798-4:1999,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　机制 …… 1
5.0　概述 …… 1
5.1　单向鉴别 …… 2
5.1.1　一次传递鉴别 …… 2
5.1.2　两次传递鉴别 …… 2
5.2　相互鉴别 …… 3
5.2.1　两次传递鉴别 …… 3
5.2.2　三次传递鉴别 …… 4
附录A（资料性附录）　文本字段的使用 …… 5

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

以后还可能增加其他后续部分。

本部分为GB/T 15843的第4部分，等同采用ISO/IEC 9798-4:1999《信息技术　安全技术　实体鉴别　第4部分：采用密码校验函数的机制》，仅有编辑性修改。

本部分代替GB/T 15843.4—1999《信息技术　安全技术　实体鉴别　第4部分：采用密码校验函数的机制》。本部分与GB/T 15843.4—1999相比，主要变化如下：

——本部分删除了ISO/IEC前言，并增加了引言。

——本部分根据GB/T 15843.1的修订，更改部分术语。

——本部分为与ISO/IEC 9798-4:1999一致，删除了GB/T 15843.4—1999中的3.1，3.2，3.3。

——本部分删除了GB/T 15843.4—1999的附录B、附录C、附录D，而统一使用GB/T 15843.1的附录B、附录C和参考文献。

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、吕春利、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 15843.4—1999。

引　言

本部分等同采用国际标准 ISO/IEC 9798-4:1999,它是由 ISO/IEC 联合技术委员会 JTC 1(信息技术)的分委员会 SC 27(IT 安全技术)起草的。

本部分定义了采用密码校验函数的实体鉴别机制,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,分为两次传递鉴别和三次传递鉴别。

有关密码校验函数的例子,见 GB 15852。

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4部分:采用密码校验函数的机制

1　范围

本部分规定了采用密码校验函数的实体鉴别机制。其中有两种是单个实体的鉴别(单向鉴别),其余的是两个实体的相互鉴别。

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,对于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,相互鉴别则需三次传递。

密码校验函数的例子见GB 15852。

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 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)

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秘密鉴别密钥来证实其身份。这可由该实体使用其秘密鉴别密钥和密码校验函数对指定数据计算密码校验值来实现。密码校验值可由拥有该实体的秘密鉴别密钥的任何其他实体来校验,其他实体能重新计算密码校验值并与所收到的值进行比较。

这些鉴别机制有下述要求,如果其中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:

a) 向验证方证实其身份的声称方与该验证方共享一个秘密鉴别密钥。在正式启动鉴别机制之前,此密钥应为有关各方所知道。向各个实体分发密钥的方法不属本部分的范围。

b) 声称方和验证方共享的秘密鉴别密钥应仅为这两个实体,以及双方都信任的其他实体所知。

c) 机制的安全强度依赖于密钥的长度和安全性、密码校验函数的特性,以及密码校验值的长度。这些参数应被仔细选取以满足既定的安全级别,参数选取和安全级别可能在安全策略中有明确规定。

5　机制

5.0　概述

这些鉴别机制中,实体A和B在启动鉴别机制之前应共享一个秘密密钥K_{AB}或两个单向秘密密钥

K_{AB}和K_{BA}。在后一种情况下，单向秘密密钥K_{AB}和K_{BA}分别用于由B对A进行鉴别和由A对B进行鉴别。

这些机制要求使用诸如时间戳、序号或随机数等时变参数。这些参数的特性，尤其是它们很难在鉴别密钥生命周期内重复使用的特性，对于这些机制的安全性是十分重要的。详细信息见GB/T 15843.1—2008的附录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。

如果验证方能够独立确定文本字段，例如：文本字段被提前知道，或以明文的方式发送，或可从两个源中的一个或两个推导出来，则文本字段可以只包括在密码校验函数的输入中。

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启动此过程并由验证方B对它进行鉴别。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。

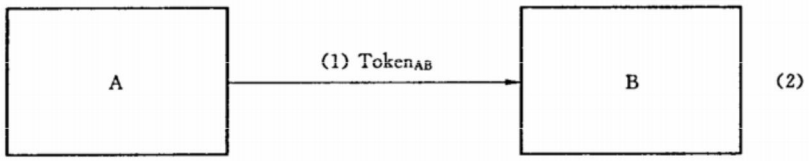

图1 一次传递单向鉴别机制示意图

声称方A发送给验证方B的权标($Token_{AB}$)形式是：

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

此处声称方使用序号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。根据GB/T 15843.1—2008中的定义，$f_K(X)$表示使用密码校验函数f和密钥K对数据X计算的密码校验值。

$Token_{AB}$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是为了防止敌手假冒实体B来对实体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B省去。

如果使用单向密钥，那么可区分标识符B也可省去。

(1) A产生并向B发送$Token_{AB}$。

(2) 一旦收到包含$Token_{AB}$的消息，B就检验时间戳或序号，计算

$$f_{K_{AB}}(\begin{matrix}T_A\\N_A\end{matrix} \| B \| Text1)$$

且将其与权标的密码校验值进行比较，并验证可区分标识符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

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。

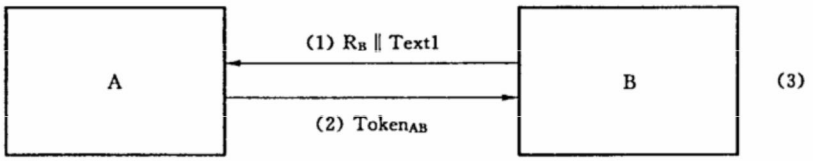

图 2　两次传递单向鉴别机制示意图

由声称方 A 发送给验证方 B 的权标($Token_{AB}$)形式是：

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

在 $Token_{AB}$ 中是否包含可区分标识符 B 是可选的。

注：在 $Token_{AB}$ 中包含可区分标识符 B 是为了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 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 B 省去。

如果使用了单向密钥，则可区分标识符 B 也可省去。

(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 产生并向 B 发送 $Token_{AB}$。

(3)　一旦收到包含 $Token_{AB}$ 的消息，B 就计算

$$f_{K_{AB}}(R_B \| B \| Text2)$$

且将其与权标的密码校验值进行比较，并验证可区分标识符 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 的附录 B)来控制的。

鉴别机制如图 3 所示。

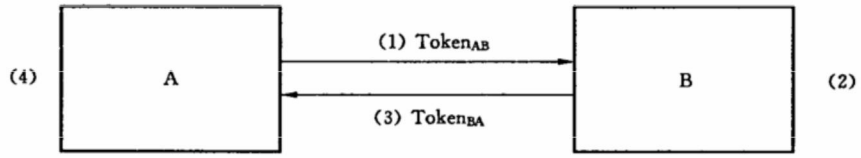

图 3　两次传递相互鉴别机制示意图

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

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

由 B 发送给 A 的权标($Token_{BA}$)形式为：

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

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 都是可选的。

注1：$Token_{AB}$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$Token_{AB}$。因为同样的原因$Token_{BA}$中包含可区分标识符A。对它们的包含为可选的，在不会出现这类攻击的环境下将其中之一或二者都可省去。

如果使用了单向密钥，则可区分标识符A和B也可省去。

在这种机制中，选择时间戳还是序号取决于声称方与验证方的能力及环境。

步骤(1)和步骤(2)与5.1.1一次传递鉴别的规定相同。

(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(见附录A)来实现。

如果使用单向密钥，那么$Token_{BA}$中的密钥K_{AB}用单向密钥K_{BA}代替并在步骤(4)使用相应的密钥。

5.2.2 三次传递鉴别

这种相互鉴别机制中，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。

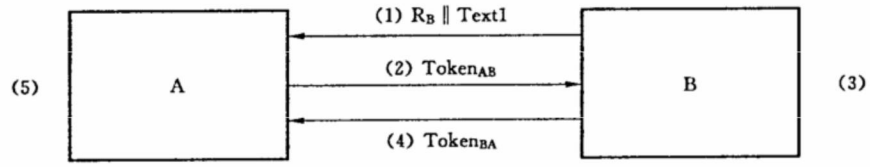

图4 三次传递相互鉴别机制示意图

权标形式如下：

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

$$Token_{BA} = Text5 \| f_{K_{AB}}(R_B \| R_A \| Text4)$$

$Token_{AB}$中是否包含可区分标识符B是可选的。

注：$Token_{AB}$中包含可区分标识符B是为了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B省去。

如果使用单向密钥，那么可区分标识符B也可以省去。

(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产生并向B发送随机数R_A和权标$Token_{AB}$。

(3) 一旦收到包含$Token_{AB}$的消息，B就计算

$$f_{K_{AB}}(R_A \| R_B \| B \| Text2)$$

且将其与权标的密码校验值进行比较，并验证可区分标识符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$Token_{AB}$。

(4) B产生并向A发送$Token_{BA}$。

(5) 一旦收到包含$Token_{BA}$的消息，A就计算

$$f_{K_{AB}}(R_B \| R_A \| Text4)$$

且将其与权标的密码校验值进行比较，并验证在步骤(1)中从B所接收到的随机数R_B是否与$Token_{BA}$中的随机数相符，及在步骤(2)中发给B的随机数R_A是否与$Token_{BA}$中的随机数相符，从而验证$Token_{BA}$。

如果使用单向密钥，那么$Token_{BA}$中的密钥K_{AB}将由单向密钥K_{BA}代替，并在步骤(5)使用相应的密钥。

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。

举例来说，适当的文本字段，例如5.1.1中 $Token_{AB}$ 中的 Text1，其中的信息可以在计算该权标的密码校验值时被用到。通过这种方法，可以为信息提供数据起源鉴别。

关于文本字段的用途的更多示例参见GB/T 15843.1—2008的附录A。