ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 15843.4－XXXX
代替 GB/T 15843.4－2008

# 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, MOD）

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

前言 ..... II
1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语和定义 ..... 1
4 符号与缩略语 ..... 1
5 安全要求 ..... 1
6 鉴别机制 ..... 2
6.1 概述 ..... 2
6.2 单向鉴别 ..... 2
6.3 双向鉴别 ..... 3
附录A（资料性）文本字段的使用 ..... 6
附录B（资料性）对象标识符 ..... 7
参考文献 ..... 8

# 前　言

GB/T 15843《信息技术 安全技术 实体鉴别》分为六个部分：

——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：使用零知识技术的机制

——第 6 部分：采用人工数据传递的机制

以后还可能增加其它后续部分。

本文件是 GB/T 15843《信息技术 安全技术 实体鉴别》的第 4 部分，修改采用 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》。

本文件代替 GB/T 15843.4—2008《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》。本文件与 GB/T 15843.4—2008 相比，主要变化如下：

a) 由等同采用 ISO/IEC 9798-4:1999，改为修改采用；

b) 根据 ISO/IEC 9798-4:1999/Cor.1:2009 和 ISO/IEC 9798-4:1999/Cor. 2:2012 勘误文本，修订了部分文字；

c) 调整了部分术语的表述，包括激励-响应改为挑战-响应、权标改为令牌、相互鉴别改为双向鉴别等；

d) 更新了部分规范性引用文件，对 GB/T 15852 以不注日期的形式对其全部文件进行引用；

e) 增加了第 4 章符号和缩略语，加入了拼接符号的说明，以及对拼接数据解析唯一性的注解；

f) 第 5 章增加了对鉴别密钥和密码校验值的安全要求；

g) 第 6 章补充了双向鉴别机制两次传递步骤 a）和步骤 b）的具体内容，避免出现歧义；

h) 第 6 章双向鉴别机制三次传递的流程，步骤 b）的描述文字修改为：*A* 产生随机数 $R_A$，产生并向 *B* 发送令牌 Token*AB*；

i) 增加了附录 B，列出了分配给本文件鉴别机制的对象标识符；

j) 增加了参考文献，为本文件数据编码方式提供标准文本的参考。

本文件的附录 A 和 B 为资料性附录。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国科学院大学、北京数字认证股份有限公司、成都卫士通信息产业股份有限公司、北京信安世纪科技股份有限公司、国民认证科技（北京）有限公司、工业信息安全（四川）创新中心有限公司、浙江大华技术股份有限公司、中国汽车工程研究院股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：荆继武、王鹏、刘丽敏、寇春静、夏鲁宁、颜雪薇、张立廷、潘文伦、张宇、李俊、张文科、张军昌、李腾飞、王雨田、胡建勋、刘为华。

本文件及其所代替文件的历次版本发布情况为：

——1999 年首次发布为 GB/T 15843.4—1999，2008 年第一次修订；

——第一次修订等同采用 ISO/IEC 9798-4:1999;

——本次为第二次修订。

# 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

本文件规定了采用密码校验函数的实体鉴别机制，包括单向鉴别和双向鉴别两种鉴别机制。

本文件适用于使用密码校验函数进行实体鉴别的设计、开发、实施、测试等。

注 1：本文件中规定的机制采用诸如时间戳、序号或随机数等时变参数，目的是防止先前有效的鉴别信息在超过时效后又被接受的问题。

注 2：如果采用时间戳或序号，单向鉴别只需一次传递，而双向鉴别则需两次传递。如果采用随机数的挑战-响应方法，单向鉴别需两次传递，双向鉴别需三次传递。

注 3：密码校验函数的示例见 GB/T 15852。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 15843.1—2017　信息技术 安全技术　实体鉴别　第1部分：总则

GB/T 15852（所有部分） 信息技术 安全技术 消息鉴别码

## 3　术语和定义

GB/T 15843.1—2017中界定的术语和定义适用于本文件。

## 4　符号和缩略语

GB/T 15843.1—2017中界定的符号和缩略语适用于本文件。

$X||Y$：数据项$X$和$Y$以$X$在前而$Y$在后的顺序拼接的结果。

注：当两个或者多个数据项的拼接在本文件鉴别机制中作为密码校验函数的输入时，应该保证拼接结果可以被唯一解析回原来的数据项，即不存在歧义的解释。这一特性可以通过多种方式实现，具体实现与应用相关。例如，可以通过以下方式实现：（a）固定被拼接数据项的长度，并且在鉴别机制执行全过程都保持此长度；（b）使用解码唯一的编码方法处理拼接的数据项序列，例如使用 GB/T 16263.1[1]中定义的编码规则。

## 5　安全要求

本文件规定的鉴别机制中，待鉴别的实体通过表明它拥有某个密钥来证实其身份。这可由该实体使用其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密钥的任何其它实体来校验，校验方式是重新计算密码校验值并与收到的值进行比较，一致则通过校验，否则不通过。

本文件规定的鉴别机制有下述安全要求，违反其中任何一条，则鉴别过程可能会遭受攻击，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用于鉴别的密钥。在正式启动鉴别机制之前，此密钥应被有关各方所掌握，向各相关实体分发密钥的方法不属于本文件的范围；

b) 声称方和验证方共享的鉴别密钥应仅被这两个实体，以及双方都信任的其它实体掌握；

c) 应仔细选取密钥长度、密码校验值长度等参数，以达到所需的安全强度，可以在安全策略中明确规定参数选取的方法和其对应的安全强度；

d) 用于实现本文件任意鉴别机制的密钥，应和其它用途的密钥保持不同；

e) 在鉴别机制中，应确保不同场合使用的密码校验值无法互换。

注：为确保密码校验值无法互换，可以强制要求在用于计算密码校验值的数据项中包含以下元素：附录 B 中规定的对象标识符；能唯一标识密码校验值的常量。如果鉴别机制中仅包含一个密码校验值，则此常量可以省略。密码校验值的接收方应验证对象标识符和常量，以确认密码校验值。

## 6 鉴别机制

### 6.1 概述

本文件规定的鉴别机制中，实体$A$和$B$在进行实体鉴别之前应共享一个密钥，或者两个单向密钥$K_{AB}$和$K_{BA}$。单向密钥$K_{AB}$和$K_{BA}$分别用于$B$对$A$的鉴别和$A$对$B$的鉴别。如无特别说明，本文件也用$K_{AB}$表示实体$A$和$B$共享的一个密钥。

本文件规定的机制要求使用诸如时间戳、序号或随机数等时变参数。时变参数具有很难在鉴别密钥生命周期内重复使用的特性，用于实现唯一性或时效性。详细信息见GB/T 15843.1—2017的附录B。

如何使用以下机制中规定的所有文本字段（可能是空的）超出了本文件的范围，取决于具体应用。有关文本字段使用的信息见附录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获知，或以明文的方式发送，或可从这些途径中推断出来，则文本字段可以只包括在密码校验函数的输入中。

单向鉴别是指使用该机制时两个实体中只有一方被鉴别。

双向鉴别是指两个通信实体运用该机制彼此进行鉴别。

6.3.1 和 6.3.2 分别采用 6.2.1 和 6.2.2 中描述的两种机制以实现双向鉴别，这两种情况都需要增加一次传递，从而分别增加了两个操作步骤。

注：双向鉴别的第三种机制可由 6.2.2 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。

### 6.2 单向鉴别

#### 6.2.1 一次传递

在这种鉴别机制中，声称方$A$发起此过程并由验证方$B$对其进行鉴别。通过产生并检验时间戳或序号（见GB/T 15843.1—2017的附录B）实现唯一性或时效性。

鉴别机制流程如下（见图1）：

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* 的令牌（Token*AB*）形式是：

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

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；$B$是验证方的可区分标识符；Text1 和 Text2 是文本字段。根据 GB/T 15843.1—2017 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 $X$ 计算得到的密码校验值。

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* 是为了防止攻击者假冒实体 *B* 对实体 *A* 重用 Token*AB*。由于有些环境中不

存在这类攻击，因此可以将可区分标识符 *B* 作为可选项。

如果使用单向密钥，那么可区分标识符 *B* 也可省去。

a) *A* 产生并向 *B* 发送 Token*AB*；

b) 当收到包含 Token*AB* 的消息后，*B* 检验时间戳或序号，计算

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

并将其与令牌中的密码校验值进行比较，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*。

### 6.2.2 两次传递

在这种鉴别机制中，验证方 *B* 发起此过程并对声称方 *A* 进行鉴别。通过产生并检验随机数 $R_B$（见 GB/T 15843.1—2017 的附录 B）实现唯一性或时效性。

鉴别机制流程如下（见图 2）：

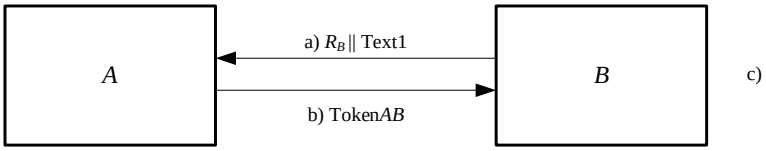


**图 2 两次传递单向鉴别机制示意图**

由声称方 *A* 发送给验证方 *B* 的令牌（Token*AB*）形式是：

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

其中 Text2 和 Text3 是文本字段；$R_B$ 是随机数；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* 将挑战随机数 $R_B$ 反射给 *B*。由于有些环境中不存在这类攻击，因此可以将可区分标识符 *B* 作为可选项。

如果使用了单向密钥，则可区分标识符 *B* 也可省去。

a) *B* 产生并向 *A* 发送一个随机数 $R_B$，还可选择发送一个文本字段 Text1；

b) *A* 产生并向 *B* 发送 Token*AB*；

c) 当收到包含 Token*AB* 的消息后，*B* 进行如下计算

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

并将其与令牌的密码校验值进行比较，验证可区分标识符 *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*。

## 6.3 双向鉴别

### 6.3.1 两次传递

这种鉴别机制，通过产生并检验时间戳或序号（见 GB/T 15843.1—2017 的附录 B）实现唯一性或时效性。

鉴别机制流程如下（见图 3）：

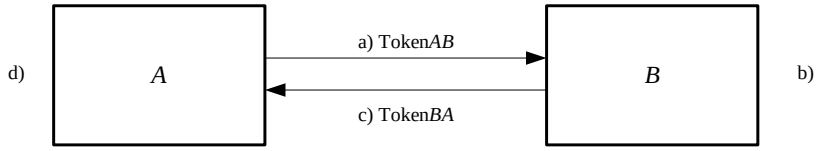


**图 3 两次传递双向鉴别机制示意图**

由 *A* 发送给 *B* 的令牌（Token*AB*）形式与 6.2.1 所规定的相同。

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

类似的，由 $B$ 发送给 $A$ 的令牌（Token$BA$）形式为：

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

Token$AB$ 中是否包含可区分标识符 $B$，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 $B$ 是为防止攻击者对实体 $A$ 重用 Token$AB$ 以假冒实体 $B$。因为同样的原因 Token$BA$ 中包含可区分标识符 $A$。由于有些环境中不存在这类攻击，因此二者都可以作为可选项。

如果使用了单向密钥，则可区分标识符 $A$ 和 $B$ 也可省去。

在这种鉴别机制中，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。

a) $A$ 产生并向 $B$ 发送 Token$AB$；

b) 当收到包含 Token$AB$ 的消息后，$B$ 计算

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

并将其与令牌的密码校验值进行比较，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$AB$；

c) $B$ 产生并向 $A$ 发送 Token$BA$；

d) 当收到包含 Token$BA$ 的消息后，$A$ 计算

$$f_{K_{AB}}(\begin{matrix} T_B \\ N_B \end{matrix} ||A||\text{Text3})$$

并将其与令牌的密码校验值进行比较，验证可区分标识符 $A$（如果有）以及时间戳或序号的正确性，从而验证 Token$BA$。

注 3：步骤 a)和步骤 b)与 6.2.1 一次传递鉴别的规定相同；步骤 c)和步骤 d)与 6.2.1 一次传递鉴别的规定类似。

注 4：这种机制中两条消息之间除了时效性上有隐含关系外，没有其它任何联系；该机制独立地两次使用机制 6.2.1。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 d)使用相应的密钥。

### 6.3.2 三次传递

这种双向鉴别机制，通过产生并检验随机数（见 GB/T 15843.1—2017 的附录 B）实现唯一性或者时效性。

鉴别机制流程如下（见图 4）：

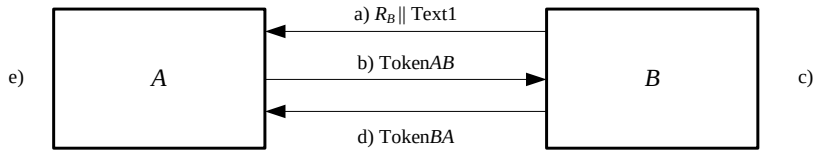


图 4 三次传递双向鉴别机制示意图

令牌形式如下：

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

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

其中 Text2、Text3、Text4 和 Text5 是文本字段；$R_A$ 和 $R_B$ 是随机数；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 $A$ 将挑战随机数 $R_B$ 反射给 $B$。由于有些环境中不存在这类攻击，因此可以将可区分标识符 $B$ 作为可选项。

如果使用单向密钥，那么可区分标识符 $B$ 也可以省去。

a) $B$ 产生并向 $A$ 发送一个随机数 $R_B$，还可选择发送一个文本字段 Text1；

b) $A$ 产生随机数 $R_A$，产生并向 $B$ 发送令牌 Token$AB$；

c) 当收到包含 Token$AB$ 的消息后，$B$ 进行如下计算

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

并将其与令牌的密码校验值进行比较，验证可区分标识符 $B$（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$AB$；

d) $B$ 产生并向 $A$ 发送 Token$BA$；

e) 当收到包含 Token$BA$ 的消息后，$A$ 进行如下计算

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

并将其与令牌的密码校验值进行比较，验证在步骤 a)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 b)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 $K_{AB}$ 用单向密钥 $K_{BA}$ 代替，并在步骤 e)使用相应的密钥。

# 附　录　A
(资料性)
文本字段的使用

本文件第 6 章规定的令牌包括了文本字段。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，6.2.1 中的文本字段 Text1 用于计算令牌 Token*AB* 中的密码校验值，为信息提供数据来源的鉴别。验证方需要获取 Text1 才能进行密码校验值的验证。声称方可以提前和验证方确定 Text1 的内容，声称方也可以直接将 Text1 发送给验证方，例如在文本字段 Text2 中包含 Text1 的信息。

关于文本字段用途的更多示例见 GB/T 15843.1—2017 的附录 A。

# 附　录　B
(资料性)
对象标识符

以下列出了分配给本文件中鉴别机制的对象标识符。

```
EntityAuthenticationMechanisms-4      {iso(1) standard(0) e-auth-mechanisms(9798)
                                       part4(4) asn1-module(0) object-identifiers(0)}

DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias

-- Synonyms --

is9798-4 OID ::= {iso(1) standard(0) e-auth-mechanisms(9798) part4(4)}

mechanism OID ::= {is9798-4 mechanisms(1)}

-- unilateral authentication mechanisms --

ua-one-pass OID ::= {mechanism ua-One-pass(1)}

ua-two-pass OID ::= {mechanism ua-Two-pass(2)}

-- mutual authentication mechanisms --

ma-two-pass OID ::= {mechanism ma-Two-pass(3)}

ma-three-pass OID ::= {mechanism ma-Three-pass(4)}

END -- EntityAuthenticationMechanisms-4 --
```

## 参 考 文 献

[1] GB/T 16263.1-2006 信息技术.ASN.1 编码规则.第 1 部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范