ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.4—2024
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）

2024-03-15 发布　　2024-10-01 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

国家图书馆 收用

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 15843《信息技术　安全技术　实体鉴别》的第4部分。GB/T 15843已经发布了以下部分：

——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：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。

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，除结构调整和编辑性改动之外，主要技术变化如下：

a) 更改了第1章的范围(见第1章)；

b) 增加了拼接符号(见第4章)；

c) 增加了对鉴别密钥和密码校验值的安全要求[见第5章d)和e)]；

d) 增加了两次传递双向鉴别机制步骤a)和步骤b)的具体内容(见6.3.1)；

e) 更改了三次传递双向鉴别机制的流程中步骤b)的描述文字为：A 产生随机数 R_A，产生并向 B 发送令牌 TokenAB(见6.3.2)。

本文件修改采用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》。

本文件与ISO/IEC 9798-4:1999相比，做了下列结构调整：

a) 增加了第4章“符号与缩略语”，后续章编号顺延；

b) 将ISO/IEC 9798-4:1999第5章下的悬置段调整为6.1，后续条号顺延；

c) 本文件的附录A、附录B分别对应ISO/IEC 9798-4:1999的附录B、附录A。

本文件与ISO/IEC 9798-4:1999存在技术差异及其原因如下：

——用规范性引用的GB/T 15843.1—2017替换了ISO/IEC 9798-1:1997(见第3章、第4章)，和GB/T 15843文件保持一致，其收录的技术包含但不限于ISO/IEC 9798-1:1997。

本文件与ISO/IEC 9798-4:1999相比，做了下列编辑性改动：

a) 用资料性引用的GB/T 15852(所有部分)替换了ISO/IEC 9797(所有部分)(见第1章)；

b) 用资料性引用的GB/T 16263.1替换了ISO/IEC 8825-1(见第4章)；

c) 用资料性引用的GB/T 15843.1—2017替换了ISO/IEC 9798-1:1997(见6.1、6.2.1、6.2.2、6.3.1、6.3.2、附录B)；

d) 附录A修正为资料性，因为附录A在ISO/IEC 9789-4:1999的第5章的注中引用。

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专利的责任。

本文件由全国网络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、中电科网络安全科技股份有限公司、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

国家图书馆

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、中国电子技术标准化研究院。

本文件主要起草人：荆继武、王鹏、林阳荟晨、刘丽敏、寇春静、夏鲁宁、颜雪薇、张立廷、潘文伦、王跃武、张宇、李俊、王平建、张文科、张军昌、雷灵光、李腾飞、王雨田、孙思维、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；

——本次为第二次修订。

国家图书馆 专用

引　言

实体鉴别是构建网络信任体系的基础和共性技术，是网络交互的第一道安全防线。GB/T 15843旨在描述实体鉴别的模型及采用对称密码算法、数字签名技术、密码校验函数、零知识技术和人工数据传递的具体实体鉴别机制。拟由六部分构成。

——第1部分：总则。目的在于给出实体鉴别的一般模型，作为GB/T 15843的其他部分中使用密码技术具体实体鉴别机制的一般模型。

——第2部分：采用对称加密算法的机制。目的在于给出采用对称加密算法的具体实体鉴别机制。

——第3部分：采用数字签名技术的机制。目的在于给出采用数字签名技术的具体实体鉴别机制。

——第4部分：采用密码校验函数的机制。目的在于给出采用密码校验函数的具体实体鉴别机制。

——第5部分：使用零知识技术的机制。目的在于使用零知识技术的具体实体鉴别机制。

——第6部分：采用人工数据传递的机制。目的在于采用人工数据传递的具体实体鉴别机制。

GB/T 15843.4—1999已经发布实施二十余年，2008年进行了第一次修订，随着GB/T 15843的广泛应用以及实体鉴别技术的发展，有必要修订完善GB/T 15843.4。本次对GB/T 15843.4的修订，对其中的术语和表达方式进行了重新梳理，增加了更为明确的安全要求，更改了部分容易产生歧义的文字，同时加强了和现有国家标准的联系。

国家图书馆 样本

国家图书馆 专用

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。

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。

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。

密码校验函数的示例见GB/T 15852(所有部分)。

国家图书馆专用

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(ISO/IEC 9798-1：2010，IDT)

3　术语和定义

GB/T 15843.1—2017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界定的以及下列符号和缩略语适用于本文件。

$X \| Y$：数据项“X”和“Y”以“X”在左“Y”在右的顺序拼接的结果。

注：当两个或者多个数据项的拼接作为密码校验函数的输入时，保证拼接结果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，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定义的编码规则。

5　安全要求

本文件规定的鉴别机制，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他实体校验，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他实体掌握；

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，应和其他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，宜在用于计算密码校验值的数据项中包含以下元素：

——附录 A 中给出了对象标识符，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在确认密码校验值的同时应验证对象标识符和常量。

6 鉴别机制

6.1 通则

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 B。

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。

鉴别机制流程见图 1。

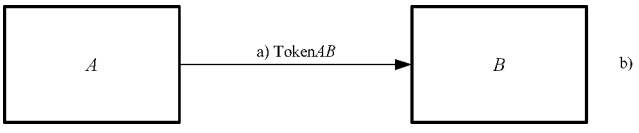

图 1 一次传递单向鉴别机制示意图

国家图书馆藏书专用

声称方 A 发送给验证方 B 的令牌(TokenAB)形式是：

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

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(见附录 B)。$f_K(X)$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。

TokenAB 中是否包含可区分标识符 B 是可选的。

注：在 TokenAB 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 TokenAB。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 TokenAB。

b) 当收到包含 TokenAB 的消息后，B 检验时间戳或序号，计算：

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

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 TokenAB。

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。

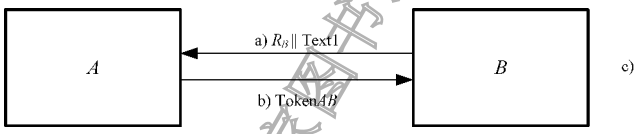

图 2 两次传递单向鉴别机制示意图

由声称方 A 发送给验证方 B 的令牌(TokenAB)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(见附录 B)；R_B 是随机数；TokenAB 中是否包含可区分标识符 B 是可选的。

注：在 TokenAB 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 TokenAB。

c) 当收到包含 TokenAB 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 TokenAB 中所含的随机数相符，从而验证 TokenAB。

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

国家图书馆 专用

效性。

鉴别机制流程见图 3。

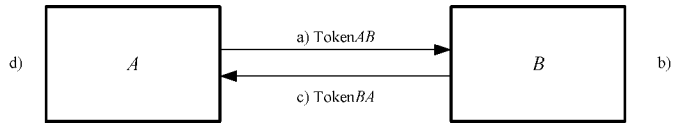

图 3　两次传递双向鉴别机制示意图

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

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

类似的,由 B 发送给 A 的令牌(TokenBA)形式为:

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

TokenAB 中是否包含可区分标识符 B,TokenBA 中是否包含可区分标识符 A,都是可选的。

注 1: TokenAB 中包含可区分标识符 B 是为防止攻击者对实体 A 重用 TokenAB 以假冒实体 B。因为同样的原因 TokenBA 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 TokenAB。

b)　当收到包含 TokenAB 的消息后,B 计算:

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

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 TokenAB;

c)　B 产生并向 A 发送 TokenBA。

d)　当收到包含 TokenBA 的消息后,A 计算:

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

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 TokenBA。

注 2: 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 3: 这种机制中两条消息之间除了时效性上有隐含关系外,没有其他任何联系;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 B)来实现。

如果使用单向密钥,那么 TokenBA 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。

鉴别机制流程见图 4。

国家图书馆 查重

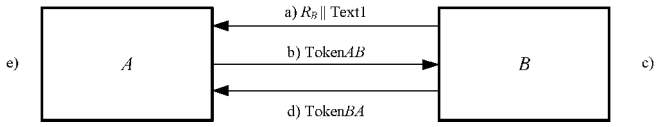

图 4　三次传递双向鉴别机制示意图

令牌形式如下：

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

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

其中 Text2、Text3、Text4 和 Text5 是文本字段(见附录 B)；R_A 和 R_B 是随机数；TokenAB 中是否包含可区分标识符 B 是可选的。

注：TokenAB 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 TokenAB；

c)　当收到包含 TokenAB 的消息后，B 进行如下计算：

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

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 TokenAB 中所含的随机数相符，从而验证 TokenAB；

d)　B 产生并向 A 发送 TokenBA；

e)　当收到包含 TokenBA 的消息后，A 进行如下计算：

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

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 TokenBA 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 TokenBA 中的随机数相符，从而验证 TokenBA。

如果使用单向密钥，那么 TokenBA 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。

国标图书馆专用

附 录 A
（资料性）
对象标识符

以下列出了分配给本文件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 --
```

国家图书馆专用

附 录 B
（资料性）
文本字段的使用

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。声称方能提前和验证方确定 Text1 的内容，声称方也能直接将 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。

国家图书馆 专用

参 考 文 献

[1] GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码

[2] GB/T 16263.1 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

国家图书馆 专用

国家图书馆 专用

中 华 人 民 共 和 国
国 家 标 准
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
GB/T 15843.4—2024
*
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.net.cn
服务热线:400-168-0010
2024 年 3 月第一版
*
书号:155066·1-75233

版权专有 侵权必究

GB/T 15843.4-2024