ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.1—2017/ISO/IEC 9798-1:2010
代替 GB/T 15843.1—2008

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

(ISO/IEC 9798-1:2010,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》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：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1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 15843.1—2008《信息技术　安全技术　实体鉴别　第1部分：概述》，与GB/T 15843.1—2008相比，主要变化如下：

——将标准名称改为《信息技术　安全技术　实体鉴别　第1部分：总则》；

——前言增加了GB/T 15843的第6部分；

——修改了术语“非对称加密方法”“非对称签名方法”“挑战”“解密”“加密”“主体”“私有解密密钥”“对称加密算法”“令牌”的定义；

——增加了附录B的B.1内容，原有章条序号依次后移。

本部分使用翻译法等同采用ISO/IEC 9798-1:2010《信息技术　安全技术　实体鉴别　第1部分：总则》。

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。

本部分主要起草单位：中国科学院数据与通信保护研究教育中心、普华诚信信息技术有限公司。

本部分主要起草人：王雷、查达仁、向继、沈嘉荟、李丹仪、荆继武、郭晓博、谢超。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.1—1995、GB/T 15843.1—1999、GB/T 15843.1—2008。

引　言

在实时通信系统中，实体鉴别是一项重要的基础安全服务。针对特定应用与安全目标，实体鉴别机制即可通过一次传输协议来实现单向鉴别，又可通过多次传递协议完成通信实体间的单向或双向鉴别。

实体鉴别机制的目的是证实某一身份的声称方是否为其所声称的实体。在密码学上，该目标的实现基于一个能够将实体身份与公开密钥关联起来的基础设施(如，公钥基础设施 PKI)，但是该类基础设施的建立并不属于 GB/T 15843 的内容范围。

实体鉴别机制拥有两种主要模型，一种模型是通过声称方与验证方的直接通信确认声称方身份；另一种模型是通过可信第三方来证实声称方身份。

GB/T 15843 详细说明了实体鉴别机制中不同种类的实体鉴别协议。实体鉴别协议的选择基于系统的安全特性，包括以下几点：

——是否抗重放攻击；

——是否抗反射攻击；

——是否抗暴力延迟；

——单向或双向鉴别；

——是否存在预设的秘密信息可以使用，或者是否需要可信第三方帮助建立共享秘密信息。

例如，不关注重放攻击的特定系统，声称方与验证方之间仅需简单的传输协议即可实现实体鉴别；而可能发生中间人攻击或重放攻击的复杂通信系统，则需要某个多次传输协议来确保安全。

信息技术　安全技术　实体鉴别
第1部分:总则

1　范围

GB/T 15843的本部分详细指明了实体鉴别机制中的鉴别模型和一般性约束要求,并基于此验证实体身份真实性,待鉴别的实体通过展示某个私密信息来证明身份。实体鉴别机制确定了如何进行实体间的信息交换,以及实体与可信第三方的信息交换。

实体鉴别机制的细节和鉴别交换的内容不属于本部分标准内容,在GB/T 15843的其他部分中规定。

2　规范性引用文件

本部分不使用任何规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

非对称密码技术　asymmetric cryptographic technique

使用两种相关变换的密码技术:一种是由公开密钥定义的公开转换,另一种是由私有密钥定义的私有变换。

注:在给定公开变换的情况下,推导出私有变换在计算上是不可行的。

3.2

非对称加密方法　asymmetric encryption system

基于非对称密码技术的加密方法,其公开变换用于加密,而私有变换用于解密。

3.3

非对称密钥对　asymmetric key pair

一对相关的密钥,其中私有密钥定义私有变换,公开密钥定义公开变换。

3.4

非对称签名方法　asymmetric signature system

基于非对称密码技术的签名方法,其私有变换用于签名,而公开变换用于验证。

3.5

挑战　challenge

由验证方随机产生并发送给声称方的数据项;声称方将该数据项和其拥有的秘密信息共同产生一个响应发送给验证方。

3.6

声称方　claimant

被鉴别的实体本身或者为了实现验证目标的某代表性实体。

注:声称方拥有鉴别交换时所必需的参数和私有数据。

3.7

密文 ciphertext

为隐藏信息内容进行变换后的数据。

3.8

密码校验函数 cryptographic check function

以秘密密钥和任意字符串为输入，以密码校验值为输出的密码变换过程。

注：缺少秘密密钥就不能正确计算校验值。

3.9

密码校验值 cryptographic check value

数据单元执行密码变换后得到的信息项。

3.10

解密 decryption

一个相应的加密过程的逆过程。

3.11

数字签名(签名) digital signature (signature)

数据单元的附属数据或者是经过密码变换后得到的数据，被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人(例如，接收者)伪造的目的。

3.12

可区分标识符 distinguishing identifier

鉴别交换过程中，用于明确区分实体身份的信息。

3.13

加密 encryption

为隐藏数据信息，通过密码算法对数据进行的一种可逆变换过程，并产生密文。

3.14

实体鉴别 entity authentication

证实一个实体就是所声称的实体。

3.15

插空攻击 interleaving attack

一种冒充攻击手段，它使用从一个或多个正在进行的或先前进行的鉴别交换过程中导出的信息进行冒充。

3.16

密钥 key

控制密码变换操作的符号序列。

注：例如，加密、解密、密码校验函数计算、签名生成或签名验证。

3.17

冒充 masquerade

一个实体伪装成另一个不同实体的现象。

3.18

相互鉴别 mutual authentication

实体双方均向对方提供身份保证信息的实体鉴别机制。

3.19

明文 plaintext

未加密的信息。

3.20

主体 principal

其身份能被鉴别的实体。

3.21

私有解密密钥 private decryption key

针对私有解密变换过程而定义的私有密钥。

3.22

私有密钥 private key

非对称密钥对中只能由该实体使用且被秘密保存的密钥。

3.23

私有签名密钥 private signature key

定义私有签名变换的私有密钥。

注：有时称为秘密签名密钥。

3.24

公开加密密钥 public encryption key

定义公开加密变换的公开密钥。

3.25

公开密钥 public key

非对称密钥对中能够被公开使用的密钥。

3.26

公钥证书(证书) public key certificate(certificate)

在权威认证机构标记过的实体公开密钥信息，不可伪造。

注：参见附录C。

3.27

公钥信息 public key information

可以特指某个实体的信息，它至少包括该实体的可区分标识符和一个公开密钥。

注：其他有关认证机构、实体及其所含的公开密钥的信息都包含在公开密钥证书中，诸如公开密钥的有效期、相关私有密钥的有效期、所涉及算法的标识符(参见附录C)。

3.28

公开验证密钥 public verification key

实现公开验证变换过程的公开密钥。

3.29

随机数 random number

其值不可预测的时变参数。

注：参见附录B。

3.30

反射攻击 reflection attack

将以前发送的消息发回给其原发者的一种冒充攻击手段。

3.31

重放攻击 replay attack

使用以前发送过的有效消息的一种冒充攻击手段。

3.32

序号 sequence number

一种时变参数,其值取自在一定时期内不重复出现的特定序列。

注:参见附录B。

3.33

对称密码技术 symmetric cryptographic technique

源发者和接收者使用同一秘密密钥进行变换的密码技术。

注:在秘密密钥未知的情况下,不能通过计算推导出源发者或接收者。

3.34

对称加密算法 symmetric encryption algorithm

源发者和接收者使用同一秘密密钥进行变换的加密算法。

3.35

时间戳 time stamp

一种时变参数,代表公共时间基准下的某一个时间点。

注:参见附录B。

3.36

时变参数 time variant parameter

一种用来验证消息非重放的数据项,如随机数、序号、时间戳。

注:参见附录B。

3.37

令牌 token

由与特定通信相关的数据字段构成的消息,它包含经过密码技术进行变换后的信息。

3.38

可信第三方 trusted third party

安全相关活动中,被参与实体所信任的安全机构或其代理。

注:GB/T 15843中指出,可信第三方在实体鉴别过程中被声称方和(或)验证方所信任。

3.39

单向鉴别 unilateral authentication

只是其中一个实体向另一个实体提供身份保证信息,而不反向进行的实体鉴别方式。

3.40

验证方 verifier

要求鉴别其他实体身份的实体本身或实体代表。

注:验证方拥有从事鉴别交换所必需的参数。

4 符号和缩略语

下列符号和缩略语适用于本文件。

A:实体A的可区分标识符;

B:实体B的可区分标识符;

TP:可信第三方的可区分标识符;

TTP:可信第三方;

K_{XY}:实体 X 和实体 Y 之间共享的秘密密钥,只用于对称密码技术;

P_X:与实体 X 相关的公开验证密钥,只用于非对称加密技术;

S_X:与实体 X 相关的私有签名密钥,只用于非对称加密技术;

N_X:由实体 X 给出的序号;

R_X:由实体 X 给出的随机数;

T_X:由实体 X 给出的时间戳;

$\begin{matrix}T_X\\N_X\end{matrix}$:由实体 X 原发的时变参数,它或者是时间戳 T_X,或者是序号 N_X;

$Y \| Z$:数据项 Y 和 Z 以 Y 在前而 Z 在后的顺序拼接的结果;

$e_k(Z)$:用密钥 K,对数据 Z 应用对称加密算法加密的结果;

$d_k(Z)$:用密钥 K,对数据 Z 应用对称加密算法解密的结果;

$f_k(Z)$:使用以秘密密钥 K 和任意数据串 Z 作为输入的密码校验函数 f 所产生的密码校验值;

$Cert_X$:由可信第三方签发给实体 X 的证书;

$Token_{XY}$:实体 X 发给实体 Y 的令牌;

TVP:时变参数;

$s_{S_X}(Z)$:使用私有签名密钥 S_X 对数据 Z 进行私有签名变换所产生的签名。

5 鉴别模型

实体鉴别机制的一般模型如图 1 所示。所有实体及交换不需要在每一个鉴别机制中都出现。

GB/T 15843 其他部分涉及的鉴别机制中,单向鉴别中实体 A 被视为声称方,实体 B 被视为验证方;双向鉴别中,实体 A 和实体 B 两者既是声称方,又是验证方。

鉴别过程中,实体产生并交换称作令牌的标准化消息。单向鉴别至少需要交换一个令牌,而双向鉴别则至少要交换两个令牌。如果要通过发送挑战来初始化鉴别机制,就需要增加一次传递。如涉及可信第三方,可能需要再增加几次传递。

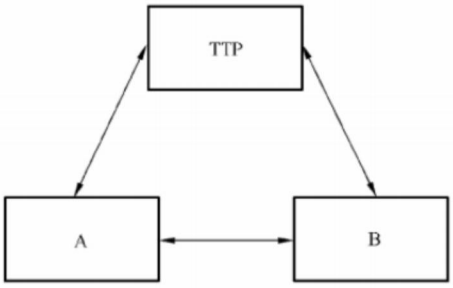

图 1 鉴别模型

图 1 中的连线表示潜在信息流。实体 A 和实体 B 之间可以直接交互,也可以分别通过 B 或 A 间接与可信第三方交互,或直接利用可信第三方发布的信息。

鉴别机制的细节将在 GB/T 15843 后续各部分中规定。

6 一般性要求和限制

为了实现实体间的身份鉴别，实体应使用共同的密码技术和参数集。

在密钥的可操作生命期中，用于密钥操作的所有时变参数值（即：时间戳、序号和随机数）应该是不重复的，至少重复的可能性是极小的。

鉴别机制使用的前提是假定实体 A 和 B 都知道对方声称的身份。这可以通过在两个实体之间交换的信息中添加标识符来实现，或者可以从所使用机制的上下文环境中显示出来。

实体的真实性只是在进行鉴别交换的时刻被确认。为了保证后续通信数据的真实性，鉴别交换必须与一种安全通信手段结合使用（如完整性服务）。

附 录 A
（资料性附录）
文本字段的使用

GB/T 15843 后续各部分涉及的令牌包含文本字段。在一次给定传递中不同文本字段的用途及各文本字段间的关系依赖于具体应用实例。

文本字段可以包含附加的时变参数。例如，如果实体鉴别机制使用序号，那么在其令牌的文本字段中就包含时间戳。消息接收者可通过验证消息中的任何时间戳是否都在一个预先规定的时间窗口内来检测受迫延迟（参见附录 B）。

如果存在多个有效密钥，每个密钥的标识符就包含在明文的文本字段中；如果存在多个可信第三方，那么作为区分可信第三方的标识符就包含在文本字段中。

文本字段也可用于密钥分配（见 ISO/IEC 11770-2 和 ISO/IEC 11770-3）。

假如 GB/T 15843 后续各部分规定的任何一种机制被嵌入到这样一种应用，即允许两个实体中的任一方在启动机制之前采用附加消息初始化鉴别，那么就会使得一些入侵攻击成为可能，这类攻击的特性是入侵者可能重复使用一个非法获得的令牌（见 ISO/IEC 10181-2）。为了避免这类攻击，可用文本字段说明哪个实体被要求鉴别。

上述给出的例子不是完备的。

附 录 B
（资料性附录）
时变参数

B.1 三类时变参数

时变参数用于控制唯一性和时效性，他们能够检测消息的重放。为实现这一点，不同信息交换实例的鉴别信息应不一样。

某些类型的时变参数可以用来检测“受迫延迟”（由敌手引入通信媒体的延迟）。在涉及一次以上的消息传递机制中，也可通过其他方法（如采用“超时时钟”来强行规定特定消息间可允许的最大时间间隙）检测受迫延迟。

GB/T 15843 后续各部分使用的三类时变参数分别是时间戳、序号和随机数。在不同的应用中可根据实现需要选择最可取的时变参数，也可以适当选用多种时变参数（如同时选择时间戳和序号）。有关参数选择的细节不属于本部分范围。

B.2 时间戳

涉及时间戳的机制主要是采用同一个时间基准在逻辑上连接声称方和验证方。建议使用的基准时钟是国际标准时间（UTC）。验证方使用固定大小的接受窗口。验证方通过计算接收到的已验证令牌中的时间戳与验证方收到令牌的时间差值来控制时效性。如果差值落在窗口内，消息就被接受。记录当前窗口的所有消息，拒收第二次和后续出现在同一个时间窗内的相同消息，基于以上两点实现唯一性。

应该采用某种机制确保通信各方的时钟同步，而且时钟同步性能要足够好，这样可以使得重放攻击出现的可能性低到可接受的程度。除此之外，还应确保与验证时间戳有关的所有信息，特别是通信双方的时钟，不会被篡改。

使用时间戳的机制可检测受迫延迟。

B.3 序号

序号可用于验证方检测消息的重放，从而控制唯一性。声称方和验证方预先就如何以特定方式给消息编号达成一致，基于序号检测消息重放的基本思想是特定编号的消息只能被接受一次（或在规定时间内只接受一次）。使用上述策略检查与消息一同发过来的序号，从而判断该消息是否可接受。如果此序号不符合上述策略，该消息则被拒绝。

使用序号时可要求附加“簿记”。声称方应记载先前用过的序号和（或）将来仍将有效使用的序号。声称方也应为所有他希望与之通信的潜在验证方保存上述记录。同样，验证方也应为所有可能的声称方保存这些记录。当正常定序被破坏时（如系统故障），则需要专用程序来重置或重新启动序号计数器。

验证方不能通过声称方使用序号检测出受迫延迟。对于涉及两次或两次以上消息传递的机制，如果消息发送者能计算出消息发送与预期回复之间的时间间隔，并且延迟超过预先规定的时槽时拒绝消息，就可以检测出受迫延迟。

B.4 随机数

随机数可被 GB/T 15843 后续部分中规定的各种机制用来防止重放或插空攻击。要求 GB/T 15843 中的所有随机数选自于一个足够大的范围，从而使同一个密钥重复使用的概率很小，并且第三方预测正确特定值的概率也很小。GB/T 15843 中使用的术语“随机数”中还包括了满足同样要求的伪随机数。

为防止重放或插空攻击，验证方首先产生一个发送给声称方的随机数，声称方将该随机数放在返回令牌的受保护部分来予以响应(这通常称为挑战——响应)。这一过程将包含特定随机数的两个消息联系起来。如果验证方再次使用了同样的随机数，那么记录了先前鉴别交换的第三方就可以把记录的令牌发送给验证方验证，从而将自己伪装成了声称方并通过验证。为了防止这类攻击，要求随机数重复的概率必须很低。

声称方使用随机数不能保证验证方能检测受迫延迟。

附 录 C
（资料性附录）
证 书

在 GB/T 15843 后面各部分中，公钥证书（证书）能用来保证公开密钥的真实性。在某些实例中，公钥证书包含实体的公钥信息，此信息至少由该实体的可区分标识符和公开密钥组成。公钥信息中还可以包括有关可信第三方、实体和公开密钥的其他信息，例如公钥的有效期、相关私有密钥的有效期或所涉及算法的标识符。公钥证书包含可信第三方的签名。

对证书的验证包括验证可信第三方的签名，如果需要，还要检验与证书的有效性有关的其他条件，如证书是否已撤销或证书有效期。

证书不是确保公开密钥真实性的唯一方式。实体可通过其他方式获得其他实体的公开密钥，所以 GB/T 15843 后续各部分中不同机制对证书的使用是可选的。确保公开密钥真实性有其他方法，如在 ISO/IEC 14888-2 中规定的基于身份的签名方案。

参 考 文 献

[1] ISO/IEC 7498-1:1994 Information technology—Open systems interconnection—Basic reference model: the basic model

[2] ISO 7498-2:1989 Information processing systems—Open systems interconnection—Basic reference model—Part 2: Security architecture

[3] ISO/IEC 8825-1:2002 Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[4] ISO/IEC 9594-8:2005 Information technology—Open systems interconnection—The directory: Public-key and attribute certificate frameworks

[5] ISO/IEC 9796-2:2002 Information technology—Security techniques—Digital signature schemes giving message recovery—Part 2: Integer factorization based mechanisms

[6] ISO/IEC 10181-1:1996 Information technology—Open systems interconnection—Security frameworks for open systems: Overview

[7] ISO/IEC 10181-2:1996 Information technology—Open systems interconnection—Security frameworks for open systems: Authentication framework

[8] ISO/IEC 11770-1:1996 Information technology—Security techniques—Key management—Part 1: Framework

[9] ISO/IEC 11770-2:2008 Information technology—Security techniques—Key management—Part 2: Mechanisms using symmetric techniques

[10] ISO/IEC 11770-3:2008 Information technology—Security techniques—Key management—Part 3: Mechanisms using asymmetric techniques

[11] ISO/IEC 13888-1:2009 Information technology—Security techniques—Non repudiation—Part 1: General

[12] ISO/IEC 14888-1:2008 Information technology—Security techniques—Digital signatures with appendix—Part 1: General

[13] ISO/IEC 14888-2:2008 Information technology—Security techniques—Digital signatures with appendix—Part 2: Integer factorization based mechanisms

[14] ISO/IEC 14888-3:2006 Information technology—Security techniques—Digital signatures with appendix—Part 3: Discrete logarithm based mechanisms

[15] ISO/IEC 18031:2005 Information technology—Security techniques—Random bit generation