ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.1—2008/ISO/IEC 9798-1:1997
代替 GB/T 15843.1—1999

信息技术 安全技术 实体鉴别 第1部分:概述

Information technology—Security techniques—Entity authentication—Part 1:General

(ISO/IEC 9798-1:1997,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

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1部分，等同采用ISO/IEC 9798-1:1997《信息技术　安全技术　实体鉴别　第1部分：概述》(英文版)，仅有编辑性修改。

本部分代替GB/T 15843.1—1999《信息技术　安全技术　实体鉴别　第1部分：概述》。本部分与GB 15843.1—1999相比，主要变化如下：

——本部分标准修订了第3章中的部分术语、定义和记法。

——本部分对第6章“一般要求和约束”中的部分叙述进行了文字修订。

——本部分删除了ISO/IEC前言，增加了引言。

——本部分删除了原附录D，增加了参考文献。

本部分的附录A、附录B和附录C均为资料性附录。

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、向继、高能、夏鲁宁。

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。

引　言

本部分等同采用国际标准 ISO/IEC 9798-1:1997，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。

本部分给出了 GB/T 15843 的所有部分中使用的术语和符号，并给出了它们的定义。

本部分给出了实体鉴别机制的一般模型，各种鉴别机制的细节在 GB/T 15843 后续部分中规定。本部分还给出了实体鉴别机制的一般要求和约束，各种鉴别机制的具体要求分别在 GB/T 15843 的其他各部分中规定。

本部分中还给出了在实体鉴别机制中使用文本字段、时变参数和证书的一般要求。

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1部分:概述

1 范围

本部分规定了一个鉴别模型以及采用安全技术的实体鉴别机制的一般要求和约束。这些机制用于证实某个实体就是他所声称的实体。待鉴别的实体通过表明它确实知道某个秘密来证明其身份。这些机制定义实体间的信息交换以及需要时与可信第三方的信息交换。

这些机制的细节和鉴别交换的内容未在本部分中规定,而在GB/T 15843的其他部分中规定。

GB/T 15843其他各部分规定的机制能用于帮助提供GB/T 17903中规定的抗抵赖服务。抗抵赖服务的有关内容不在GB/T 15843的范围之内。

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 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 18794.2—2002 信息技术 开放系统互连 开放系统安全框架 第2部分:鉴别框架(idt ISO/IEC 10181-2:1996)

3 术语和定义

3.1 GB/T 9387.2中确立的下列术语和定义适用于本部分。

3.1.1

密码校验值 cryptographic check value

通过在数据单元上执行密码变换而得到的信息。

3.1.2

数字签名(签名) digital signature (signature)

附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据或变换允许数据单元的接收者确认数据单元的来源和完整性,并防止数据单元被人(例如接收者)伪造。

3.1.3

冒充 masquerade

一个实体伪装成另一个实体。

3.2 GB/T 18794.2中确立的下列术语和定义适用于本部分。

3.2.1

声称方 claimant

以鉴别为目的,是本体本身或者是代表本体的实体。一个声称方包含了代表本体从事鉴别交换所必需的功能。

3.2.2

本体 principal

其身份能被鉴别的实体。

3.2.3

可信第三方 trusted third party

在安全相关的活动中，被其他实体所信任的安全机构或其代理。在 GB/T 15843 中，为了鉴别的目的，可信第三方被声称方和(或)验证方所信任。

3.2.4

验证方 verifier

要求鉴别声称方身份的实体本身或是代表它的实体。验证方包含了从事鉴别交换所必需的功能。

3.3 下列术语和定义适用于 GB/T 15843。

3.3.1

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变换，另一种是由私有密钥定义的私有变换。两种变换具有以下特性：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。

注：基于非对称密码技术的系统可能是加密系统、签名系统，加密与签名组合在一起的系统，或密钥协商系统。非对称密码技术有四种基本变换：签名系统的签名和验证，加密系统的加密和解密。签名和解密变换是拥有方专用的，而相应的验证和加密变换是公开发布的。现在已有仅通过两种变换就可获得四项基本功能的非对称密码系统(如 RSA)：一个私有变换可同时实现对消息的签名和解密，而一个公开变换可同时实现对消息的验证和加密。然而，由于一般情况并非如此，在 GB/T 15843 中，这四项基本变换及相应的密钥都是分开的。

3.3.2

非对称加密体制 asymmetric encipherment system

基于非对称密码技术的体制，其公开变换用于加密，而私有变换用于解密。

3.3.3

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。

3.3.4

非对称签名体制 asymmetric signature system

基于非对称密码技术的体制，其私有变换用于签名，而公开变换用于验证。

3.3.5

激励 challenge

由验证方随机选择并发送给声称方的数据项；声称方使用此数据项连同其拥有的秘密信息产生一个响应发送给验证方。

3.3.6

密文 ciphertext

经过变换隐藏其信息内容的数据。

3.3.7

密码校验函数 cryptographic check function

以秘密密钥和任意字符串作为输入，并以密码校验值作为输出的密码变换。不知道秘密密钥就不可能正确计算校验值。

3.3.8

解密 decipherment

一个相应的加密过程的逆过程。

3.3.9

可区分标识符 distinguishing identifier

不含糊地区别一个实体的信息。

3.3.10

加密 encipherment

为了产生密文,即隐藏数据的信息内容,由密码算法对数据进行的(可逆)变换。

3.3.11

实体鉴别 entity authentication

证实一个实体就是所声称的实体。

3.3.12

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导出的信息进行冒充。

3.3.13

密钥 key

控制密码变换操作(例如:加密、解密、密码校验函数计算、签名生成或签名验证)的符号序列。

3.3.14

相互鉴别 mutual authentication

向双方实体提供对方身份保证的实体鉴别。

3.3.15

明文 plaintext

未加密的信息。

3.3.16

私有解密密钥 private decipherment key

定义私有解密变换的私有密钥。

3.3.17

私有密钥 private key

一个实体的非对称密钥对中只由该实体使用的密钥。

注:在非对称签名体制中,私有密钥定义签名变换;而在非对称加密体制中,私有密钥定义解密变换。

3.3.18

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。

3.3.19

公开加密密钥 public encipherment key

定义公开加密变换的公开密钥。

3.3.20

公开密钥 public key

一个实体的非对称密钥对中能够被公开的密钥。

注:在非对称签名体制中,公开密钥定义验证变换;而在非对称加密体制中,它定义加密变换。密钥是"公开的"并不意味着谁都可以获得。密钥可能只有某个事先确定的团体的所有成员才可使用。

3.3.21

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

实体的公钥信息,它由认证机构签名,因而不可伪造(参见附录 C)。

3.3.22

公钥信息 public key information

关于单个实体的特定信息,它至少包括该实体的可区分标识符,且至少包括该实体的一个公开密钥。它还可包括有关认证机构、实体及其所含的公开密钥的其他一些信息,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等(参见附录 C)。

3.3.23

公开验证密钥 public verification key

定义公开验证变换的公开密钥。

3.3.24

随机数 random number

其值不可预测的时变参数(参见附录 B)。

3.3.25

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。

3.3.26

重放攻击 replay attack

使用以前发送的消息的一种冒充攻击手段。

3.3.27

序号 sequence number

其值取自一个在一定时期内不重复的特定序列的时变参数(参见附录 B)。

3.3.28

对称密码技术 symmetric cryptographic technique

原发者变换和接收者变换使用同一秘密密钥的密码技术。如果不知道秘密密钥,推导出原发者或接收者变换在计算上是不可行的。

3.3.29

对称加密算法 symmetric encipherment algorithm

原发者变换和接收者变换使用同一秘密密钥的加密算法。

3.3.30

时间戳 time stamp

相对于一个公共时间基准的时间点的时变参数(参见附录 B)。

3.3.31

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(参见附录 B)。

3.3.32

权标 token

由与特定的通信相关的数据字段构成的消息,它包含使用密码技术进行变换了的信息。

3.3.33

单向鉴别 unilateral authentication

只向一个实体提供另一个实体的身份保证,而不向后者提供前者身份保证的实体鉴别。

4 符号

下列符号适用于 GB/T 15843 的本部分：

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；

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；

$\left.\begin{matrix} T_X \\ N_X \end{matrix}\right\}$：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 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 的权标；

TVP：时变参数；

$S_{S_X}(Z)$：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。所有的实体及交换不一定在每一个鉴别机制中都出现。

关于 GB/T 15843 其他各个部分规定的鉴别机制，对于单向鉴别，把实体 A 视为声称方，实体 B 视为验证方。而对于相互鉴别，A 和 B 既是声称方，又是验证方。

为了鉴别，实体产生并交换称作权标的标准化消息。在单向鉴别中至少要交换一个权标，而在相互鉴别中至少要交换两个权标。如果不得不发送激励以启动鉴别交换，可能需要增加一次传递。如涉及可信第三方，可能需要再增加几次传递。

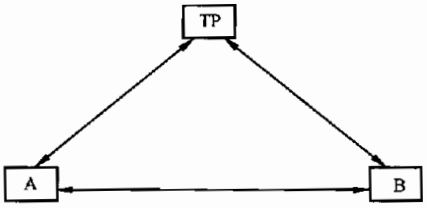

图 1 鉴别模型

图 1 中的连线指示可能存在的信息流。实体 A 和实体 B 可以彼此直接交互，或直接同可信第三方 TP 交互，或分别通过 B 或 A 间接与可信第三方交互，或利用可信第三方发布的信息。

GB/T 15843 鉴别机制的细节在后续各部分中规定。

6 一般要求和约束

为了使一个实体能鉴别另一个实体，二者应使用共同的密码技术和参数集。

在密钥的可操作生命周期中，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。

使用鉴别机制期间，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包括标识符来实现，或者可以从所使用机制的上下文环境中明显看出。

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的通信手段结合使用（如完整性服务）。

附 录 A
（资料性附录）
文本字段的使用

GB/T 15843 后续各部分规定的权标包含文本字段。在一次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依赖于应用。

文本字段可以包含附加的时变参数。例如，如果已使用了序号，那么在权标的文本字段中可以包含时间戳。这样，通过要求消息接收者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，就可以检测出受迫延迟（参见附录 B）。

如果有多个有效密钥，则一个密钥标识符可包括在明文的文本字段中。如果有多个可信第三方，那么文本字段可用于包括所涉及的那个可信第三方的可区分标识符。

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嵌入到这样一种应用，即如果允许两个实体中的任一个在启动鉴别机制之前采用附加消息，那么有些入侵攻击就会变得可能。为了抵抗这类攻击，可用文本字段说明哪个实体要求鉴别。这类攻击的特性是入侵者可能重复使用一个非法获得的权标（见 GB/T 18794.2）。

上述给出的例子不是完备的。

附 录 B
（资料性附录）
时 变 参 数

时变参数用于控制唯一性和时效性。它们能使先前发送过的消息重放时被检测出来。为实现这一点，对各次交换实例，其鉴别信息都应不同。

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）。在涉及一次以上传递的机制中，也可以通过其他方法（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，有时也可以适当选用一种以上的时变参数（如同时选择时间戳和序号）。有关参数选择的细节不在本部分范围之内。

B.1 时间戳

涉及时间戳的机制利用逻辑上链接声称方和验证方的同一个时间基准。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权标中的时间戳与验证方在收到权标时所察觉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。通过在当前窗口中记录所有消息的日志以及拒收第二次和后续出现在同一个时间窗内的相同消息的方法来验证唯一性。

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，使通过重放达到冒名顶替的可能性小到可接受的程度。还应确保与时间戳验证有关的所有信息，特别是通信双方的时钟不会被篡改。

使用时间戳机制可检测受迫延迟。

B.2 序号

因为序号可以使验证方检测消息的重放，所以可以用序号控制唯一性。声称方和验证方预先就如何以特定方式给消息编号的策略达成一致，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）。然后再检验验证方收到的消息，根据上述策略判断与消息一起发送的序号是否可接受。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”。声称方应维护先前用过的序号和或者或将来使用仍将有效的序号的记录。该声称方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。当发生正常定序被破坏的情况（如系统故障）时，需要专用程序来重置或重新启动序号计数器。

声称方使用序号不能保证验证方能检测出受迫延迟。对于涉及两个或两个以上消息的机制，如果消息发送者能检测出发送消息与接收到预期回复消息之间的时间间隔，并在延迟超过预先规定的时槽时拒绝此消息，就可以测出受迫延迟。

B.3 随机数

GB/T 15843 后续各部分规定的各种机制中使用的随机数可防止重放或插空攻击。因此要求 GB/T 15843 中使用的所有随机数选自于一个足够大的范围，使得与同一个密钥使用时出现重复的概率很小，并且第三方预测出特定值的概率也很小。GB/T 15843 中使用的术语“随机数”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，验证方获得一个发送给声称方的随机数，声称方可以将该随机数放在返回权标的受保护部分予以响应(这通常称为激励—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所记录的权标发送给验证方验证，从而将自己伪装成声称方并通过验证。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 后续各部分中，公钥证书（证书）能用来保证公开密钥的真实性。在这种情况下，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认证机构、实体和公开密钥的其他信息，例如相关私有密钥的有效期或所涉及算法的标识符。证书要包括由可信第三方签名的公钥信息。

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，如证书是否撤销或证书有效期。

证书不是确保公开密钥的真实性的唯一方式。为了使一个实体能通过其他方式获得其他实体的公开密钥，GB/T 15843 后续各部分中各种机制对证书的使用是可选的。确保公开密钥的真实性的其他方法包括诸如在 GB/T 17902.2 中规定的基于身份的签名方案。

参 考 文 献

[1] GB/T 9387.1—1998 信息处理系统 开放系统互连 基本参考模型 第1部分:基本模型(idt ISO/IEC 7498-1:1994)

[2] GB 15851—1995 信息技术 安全技术 带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

[3] GB/T 18794.1—2002 信息技术 开放系统互连 开放系统安全框架:概述(idt ISO/IEC 10181-1:1996)

[4] GB/T 17901.1—1999 信息技术 安全技术 密钥管理 第1部分:框架(idt ISO/IEC 11770-1:1996)

[5] 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

[6] ISO/IEC 11770-3:1996 信息技术 安全技术 密钥管理 第3部分:采用非对称技术的机制

[7] GB/T 17902.1—1999 信息技术 安全技术 带附录的数字签名 第1部分:概述(idt ISO/IEC 14888-1:1998)

[8] GB/T 17902.2—2005 信息技术 安全技术 带附录的数字签名 第2部分:基于身份的机制(idt ISO/IEC 14888-2:1999)

[9] GB/T 17902.3—2005 信息技术 安全技术 带附录的数字签名 第3部分:基于离散对数的机制(idt ISO/IEC 14888-3:1998)

中华人民共和国
国家标准
信息技术 安全技术 实体鉴别
第1部分:概述
GB/T 15843.1—2008/ISO/IEC 9798-1:1997
*
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 22千字
2008年9月第一版 2008年9月第一次印刷
*
书号:155066·1-33388 定价 16.00 元

GB/T 15843.1-2008

打印日期:2009年4月22日