ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34953.1—2017/ISO/IEC 20009-1:2013

信息技术　安全技术　匿名实体鉴别　第1部分:总则

Information technology—Security techniques—Anonymous entity authentication—Part 1: General

(ISO/IEC 20009-1:2013, IDT)

2017-11-01 发布　　2018-05-01 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 34953《信息技术　安全技术　匿名实体鉴别》分为四个部分：

——第1部分：总则；

——第2部分：基于群组公钥签名的机制；

——第3部分：基于盲签名的机制；

——第4部分：基于弱秘密的机制。

本部分为GB/T 34953的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用ISO/IEC 20009-1:2013《信息技术　安全技术　匿名实体鉴别　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。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、WAPI产业联盟、重庆邮电大学、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、中国电子技术标准化研究院、天津市无线电监测站、北京大学深圳研究生院、中国人民解放军信息安全测评认证中心、北京计算机技术及应用研究所、福建省无线电监测站、国家信息技术安全研究中心、北京数字认证股份有限公司、中国电信股份有限公司上海研究院、工业和信息化部宽带无线IP标准工作组。

本部分主要起草人：杜志强、曹军、龙昭华、黄振海、李大为、宋起柱、李琴、张璐璐、李明、铁满霞、张变玲、许玉娜、李楠、朱跃生、李广森、颜湘、张国强、童伟刚、万洪涛、王月辉、高德龙、朱正美、陈志宇、葛培勤、侯鹏亮、许福明、高波、郑骊。

引　言

鉴别通信参与方的合法性是最重要的密码服务之一。有多种加密机制支持这种服务，例如，ISO/IEC 9798 规定的实体鉴别机制和 ISO/IEC 9796 与 ISO/IEC 14888 规定的数字签名机制。

匿名鉴别通信包括向通信对端和/或第三方隐藏被鉴别实体的身份，同时保留能够使验证方确定其通信对端是合法的属性。匿名实体鉴别机制被设计用于支持这些匿名通信。这个机制被定义为实体间信息的交换，在需要时，这些交换将有一个可信第三方参与。

在匿名实体鉴别机制中，被鉴别实体（声称方）提供证据给验证方，该证据证实声称方知晓秘密且不会泄露声称方的身份给任何未授权实体，也就是说，通过在声称方与验证方之间交互的完整信息，未授权实体不能发现待验证实体（即声称方）的身份。同时，验证方可以通过拥有声称方的确定属性（如预定义的群组成员身份）来保证声称方的真实可信。然而，即使被授权的验证方也不可能被授权去获得被鉴别实体的身份。匿名实体鉴别机制允许被授权方执行打开过程，这个过程使被授权方能够获得产生签名的实体的身份。允许打开的机制称为部分匿名实体鉴别机制。

匿名实体鉴别能够应用在许多场景中，如电子商务、电子投票、电子身份（例如，电子驾照、电子健康证明和电子护照）、社交网络、移动支付以及可信计算。在许多这样的服务中，客户的个人身份信息（PII）被透露给服务提供者作为鉴别过程的一部分。其结果是，服务提供者可能将 PII 用于其他目的，但未必对 PII 本身感兴趣。限制服务提供者获取 PII 的一种方法就是使用匿名鉴别机制。匿名实体鉴别的一些用例参见 ISO/IEC 29191 附录 A。

GB/T 34953 由多个部分构成，分别规定了匿名实体鉴别的通用模型和机制，本部分主要规定了匿名实体鉴别的模型，匿名实体鉴别机制的细节和鉴别交互消息不在本部分范围之内，将由其他部分进行规范。

信息技术　安全技术　匿名实体鉴别
第1部分:总则

1　范围

GB/T 34953的本部分规定了用于证实一个实体的合法性的匿名实体鉴别机制的模型、需求和约束条件。

2　术语和定义

下列术语和定义适用于本文件。

2.1

匿名强度　anonymity strength

未经授权的实体可以从给定签名来确定真实签名者的概率。

注:匿名强度为n意味着未经授权的实体可以从一个签名正确猜测真实签名者的概率为$1/n$。

[ISO/IEC 20008-1:2013]

2.2

匿名实体鉴别　anonymous entity authentication

证实一个实体拥有某些特定的属性,但不将该实体从与该实体具有相同属性的其他实体中区分出来。

2.3

匿名数字签名　aonymous digital signature

可以使用一个组公钥或多个公钥进行验证,并且不被包括签名的验证方在内的未经授权的实体追踪到签名者的可区分标识符的签名。

[ISO/IEC 20008-1:2013]

2.4

质询　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给验证方的应答。

[ISO/IEC 9798-1:2010]

2.5

声称方　claimant

为了进行鉴别,本身是本体或者代表本体的实体。声称方具备代表本体进行鉴别交换所必需的各种功能。

[ISO/IEC 9798-1:2010]

2.6

密钥　key

一种用于控制密码变换操作(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。

[ISO/IEC 9798-1:2010]

2.7

链接方　linker

执行链接过程的实体。例如,它链接两个或两个以上的匿名实体鉴别的实例。

2.8

链接过程　linking

揭示两个或两个以上的匿名实体鉴别的实例是由同一实体生成的过程。

2.9

打开方　opener

执行打开过程的被授权实体。例如,打开过程获得特定匿名实体鉴别机制实例中参与方的身份。

注:打开方就是 ISO/IEC 29191 中提及的特定打开方。

2.10

打开过程　opening

被授权实体获得特定匿名实体身份鉴别机制实例中参与方的身份的过程。

注:打开过程就是在 ISO/IEC 29191 中提及的重鉴定。

2.11

双向匿名鉴别　mutual anonymous authentication

向双方实体提供对方实体身份合法性保证的匿名实体鉴别。

2.12

部分匿名鉴别　partially anonymous authentication

允许被授权的实体执行打开过程的匿名实体鉴别机制。

2.13

本体　principal

其身份能够被鉴别的实体。

[ISO/IEC 9798-1:2010]

2.14

随机数　random number

其值不可预测的时变参数。

[ISO/IEC 9798-1:2010]

2.15

序列数　sequence number

一种时变参数,其值取自于指定的序列并在确定时间内不会重复。

[ISO/IEC 9798-1:2010]

2.16

时间戳　time stamp

相对于公共时间基准的时间点的时变参数。

[ISO/IEC 9798-1:2010]

2.17

时变参数　time variant parameter

用于验证消息非重放的数据项,如随机数、序列号、时间戳。

[ISO/IEC 9798-1:2010]

2.18

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过的信息。

[ISO/IEC 9798-1:2010]

2.19

可信第三方 trusted third party

安全机构或其代理,在关于安全相关的活动中,它被其他实体所信任。

[ISO/IEC 9798-1:2010]

2.20

单向匿名鉴别 unilateral anonymous 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匿名实体鉴别。

2.21

单向匿名双向鉴别 unilateral-anonymous mutual authentication

参与双方在一个方向上进行匿名实体鉴别,而同时在另一个方向进行实体鉴别的过程。

2.22

验证方 verifier

需要验证另外一个实体(声称方)合法性的实体。

3 符号和缩略语

3.1 符号

下列符号适用于本文件。

A:参与匿名实体鉴别机制的实体。

B:参与匿名实体鉴别机制的实体。

3.2 缩略语

下列缩略语适用于本文件。

TTP:可信第三方(Trusted Third Party)

4 匿名实体鉴别模型

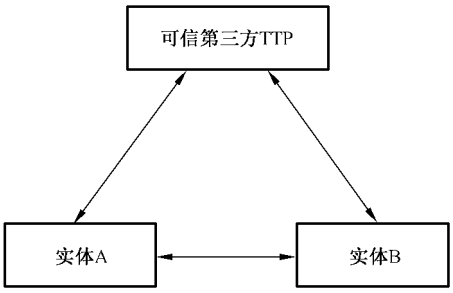

图 1 匿名实体鉴别模型

图 1 所示为匿名实体鉴别机制的通用模型,这个模型中的实体和消息交互并非对于所有鉴别机制都是必需的。

对于在 GB/T 34953 中其他部分叙述的匿名实体鉴别机制,如单向匿名鉴别中,实体 A 作为声称

方,实体 B 作为验证方。在双向匿名鉴别机制中,实体 A 和实体 B 同时承担声称方和验证方两个角色。在单向匿名双向鉴别机制中,实体 A 和实体 B 同时承担声称方和验证方的角色,不同的是,该鉴别机制在一个方向上是匿名的,而在另一个方向上非匿名(例如,A 验证 B 的有效身份,而 B 仅验证 A 属于一个预定义实体群组的成员。)

TTP 的角色依赖于使用它的机制的类型。一些机制可能不使用可信第三方。作为一种选择,TTP 可以离线的方式参与鉴别过程,例如,在使用一个机制之前,为 A 和 B 中的一方或者两方提供用于鉴别的信息以支撑该机制的使用。作为可选择的第三方,TTP 可能会主动的通过与鉴别实体中的一方或者两方交换信息来参与到鉴别机制中。TTP 也可能会参与打开过程或链接过程。如果 TTP 参与,无论在线或是离线的,参与匿名鉴别机制的双方都必须是信任它的。

为了达到匿名实体鉴别的目的,实体产生并交换标准化的消息,该消息称之为权标。单向匿名鉴别至少需要交换一个权标,双向匿名鉴别至少需要交换两个权标。如果必须使用质询来发起匿名实体鉴别过程的话,可能还需要额外的消息交互。如果可信第三方参与鉴别,也可能需要额外的消息交互。

在图 1 中,箭头指明了潜在的信息流向,实体 A 和实体 B 可以直接交互,也可以分别利用可信第三方颁发的信息进行交互。

匿名实体鉴别机制由消息交换所构成,验证方根据声称方提供的其所拥有的确定属性(如预定义的群组成员身份)作为鉴别声称方真实性的证据,该证据是通过对只有真实的实体才能拥有的秘密信息进行密码变换后得到。除此之外,某些机制也允许声称方向验证方说明其拥有除了是真正授权实体所拥有的属性外的一些其他属性。

GB/T 34953 匿名实体鉴别机制的具体细节将在后续部分进行规范。

5 一般要求和限制

为了使一个实体(即验证方)能够匿名的鉴别另外一个实体(即声称方),声称方和验证方都应该使用包含密码技术与参数的公共集合。

在密钥的使用过程中,所有时变参数的值都不能重复(如时间戳、序列数和随机数),或者至少是压倒性的概率不会重复。

假定在使用匿名实体鉴别机制的过程中,实体 A 和实体 B 都知道互相所声称的状态,也就是说,声称方声称的是哪一个群组的成员,以及该声称方的额外特征是否被证明是正确的。声称状态可以从两个实体的交互信息(包含密码运算产生的数据串)中获得,或从机制所使用的环境中推导出来。

声称方身份的真实性只在匿名实体鉴别消息交换时得到验证。为了保证声称方和验证方随后交互的数据的真实性,匿名实体鉴别机制的信息交换过程应采用安全通信的方式进行(如使用数字签名或消息鉴别码来保证通信数据的完整性,其中所使用的密钥、公钥/私钥对都产生自匿名实体鉴别机制)。

如果需要使用部分匿名鉴别,声称方在鉴别交换过程中必须提供足够的数据以确保后续的授权实体执行打开过程。

6 匿名管理

实体的匿名程度由其所使用的匿名实体鉴别机制的特性以及该机制被使用的环境决定。例如,如果实体拥有一个从其使用环境中获得的属性且该属性只被两个实体所拥有,则实体所拥有的匿名程度是极其有限的。这样就产生了匿名强度的概念,其用于表示实体所属集合的大小。在上述例子中,一个拥有唯一属性的实体的匿名强度为 2。

在一些情况下,可使用某种机制来撤销参与到匿名鉴别会话中的实体的匿名性,这种撤销可以是完全的也可以是部分的。链接和打开是两种降低匿名性的具体措施。链接是个过程,由称为链接方的实体执行。通过链接过程,两个或两个以上的匿名实体鉴别实体将被证明是由同一个实体执行的,这明显降低了匿名性。打开过程是由称之为打开方的被授权实体执行,能够获得特定的匿名鉴别机制实例的参与方身份,这说明该实体的匿名性已完全消失,至少对于打开方来说是这样的。需要特别说明的是,并不是所有的机制都需要支持链接和打开。允许被授权实体进行打开的匿名实体鉴别机制称为部分匿名鉴别机制。允许被授权实体进行打开但该打开方不具备链接能力的匿名实体鉴别机制称为部分匿名、部分不可链接鉴别机制。

参 考 文 献

[1] ISO/IEC 9796(all parts) Information technology—Security techniques—Digital signature schemes giving message recovery

[2] ISO/IEC 9798-1(all parts) Information technology—Security techniques—Entity authentication

[3] ISO/IEC 9798-1:2010 Information technology—Security techniques—Entity authentication—Part 1: General

[4] ISO/IEC 14888(all parts) Information technology—Security techniques —Digital signatures with appendix

[5] ISO/IEC 20008-1:2013 Information technology—Security techniques—Anonymous digital signatures—Part 1: General

[6] ISO/IEC 29191:2012 Information technology—Security techniques—Requirements for partially anonymous, partially unlinkable authentication

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 匿名实体鉴别
第1部分:总则
GB/T 34953.1—2017/ISO/IEC 20009-1:2013
*
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.org.cn
服务热线:400-168-0010
2017年11月第一版
*
书号:155066·1-58538

GB/T 34953.1-2017