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]