ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34953.4—2020

信息技术　安全技术　匿名实体鉴别 第4部分:基于弱秘密的机制

Information technology—Security techniques—Anonymous entity authentication—Part 4: Mechanisms based on weak secrets

(ISO/IEC 20009-4:2017,MOD)

2020-04-28 发布　　2020-11-01 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

前　言

GB/T 34953《信息技术　安全技术　匿名实体鉴别》分为4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4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 20009-4:2017《信息技术　安全技术　匿名实体鉴别　第4部分：基于弱秘密的机制》。

本部分与ISO/IEC 20009-4:2017相比结构上有调整，调整6.3为6.2，其他条编号依次修改。

本部分与ISO/IEC 20009-4:2017的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的GB/T 15852.2代替ISO/IEC 9797-2，并规定使用的杂凑算法应遵循相关国家标准和行业标准；
- 用等同采用国际标准的GB/T 34953.1代替ISO/IEC 29000-1；
- 用修改采用国际标准的GB/T 36624—2018代替ISO/IEC 19772:2009；
- 删除ISO/IEC 10118-3，ISO/IEC 10118-3规定了本部分机制使用的杂凑算法，并规定使用的杂凑算法应遵循相关国家标准和行业标准；
- 删除ISO/IEC 18033-4，ISO/IEC 18033-4规定了本部分机制使用的序列密码算法，并规定使用的序列密码算法应遵循相关国家标准和行业标准。

——增加了缩略语“MAC”和“PAEA”（见4.1）。

——删除了ISO/IEC 20009-4:2017中包含国际专利的6.2:SKI机制，以使本部分更好地适用于我国当前的应用环境（见ISO/IEC 20009-4:2017的6.2）。

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：中国科学院软件研究所、公安部第三研究所、北京数字认证股份有限公司、中国科学院数据与通信保护研究教育中心、中国电子技术标准化研究院。

本部分主要起草人：张振峰、张立武、张严、冯登国、杨明慧、刘丽敏、王惠莅、陈景燕、江伟玉、杨糠。

引　言

自从计算机问世以来，通过输入用户标识和口令的方式进行用户身份鉴别得到了广泛的应用并且一直是最为普遍的鉴别方式。每天都有数以亿计的口令鉴别在网络空间中发生。口令鉴别被广泛接纳的原因之一在于不需要额外的辅助设施并且用户只需要记住口令即可在任意时间任意地点进行身份鉴别的轻便性。ISO/IEC 11770-4:2016 描述了基于口令(口令通常是弱秘密)的密钥管理方案。这些方案可以被用来实现基于口令的实体鉴别。

同时，网络空间的个人隐私安全正受到被越来越多的关注。在网络空间中进行实体鉴别时对用户隐私进行保护是个人隐私保护的关键步骤。GB/T 34953 系列标准规范了实体鉴别隐私保护的技术，用于支持匿名实体鉴别。本部分关注基于弱秘密的匿名实体鉴别机制。特别是，本部分描述了基于口令的匿名实体鉴别(PAEA)机制，PAEA 能够为口令鉴别过程提供隐私保护。

PAEA 机制需要解决的主要问题是如果将口令等弱秘密直接应用于那些基于强秘密构造的匿名鉴别机制，则会因口令的弱秘密性质泄露秘密，导致用户隐私无法受到保护。本部分描述了两种 PAEA 机制：仅采用口令的 PAEA 和基于辅助存储设施的机制。在仅采用口令的 PAEA 机制中，用户在服务器注册并记住其用于鉴别的口令数据，然后与在非匿名口令鉴别机制中一样地使用其口令进行鉴别。在基于辅助存储设施的机制中，用户不仅要记住他们的口令，还要同时持有一个口令包裹，该口令包裹可以暴露给敌手但是不会危害用户的隐私安全。同时用户口令的验证信息将不储存于服务器中。上述两种机制在不同的应用场景下具有其各自的优势。

信息技术　安全技术　匿名实体鉴别
第4部分:基于弱秘密的机制

1　范围

GB/T 34953的本部分规定了基于弱秘密的匿名实体鉴别机制、每种机制的具体操作步骤以及详细的输入输出。

本部分适用于服务器在无法获取可用来识别用户具体身份信息的情况下对用户进行校验,确认其属于特定用户群组的场景。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 15852.2　信息技术　安全技术　消息鉴别码　第2部分:采用专用杂凑函数的机制(GB/T 15852.2—2012,ISO/IEC 9797-2:2002,MOD)

GB/T 34953.1　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 20009-1:2013,IDT)

GB/T 36624—2018　信息技术　安全技术　可鉴别的加密机制(ISO/IEC 19772:2009,MOD)

ISO/IEC 11770-4:2006　信息技术　安全技术　密钥管理　第4部分:基于弱秘密的机制(Information technology—Security techniques—Key management—Part 4:Mechanisms based on weak secrets)

3　术语和定义

GB/T 34953.1界定的以及下列术语和定义适用于本文件。

3.1

交换群　abelian group

满足对S中的所有元素a与b,有$a*b=b*a$的群(S,*)。

3.2

可鉴别的加密　authenticated encryption

使用密码学算法对数据进行的(可逆)操作,使得生成的密文不能被非授权实体在不被探测到的情况下修改,即:提供数据机密性、数据完整性与数据源鉴别。

3.3

鉴别凭证　authentication credential

包含可用来对实体进行鉴别的信息的凭证。

3.4

认证器　authenticator

作为鉴别机制的一部分被发送,并且被另一方验证的数据串。