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。