ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34953.2—2018/ISO/IEC 20009-2:2013

信息技术　安全技术　匿名实体鉴别 第2部分:基于群组公钥签名的机制

Information technology—Security techniques—Anonymous entity authentication—Part 2:Mechanisms based on signatures using a group public key

(ISO/IEC 20009-2:2013,IDT)

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
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》已发布或计划发布以下部分：

——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2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 20009-2:2013《信息技术　安全技术　匿名实体鉴别　第2部分：基于群组公钥签名的机制》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 34953.1—2017　信息技术　安全技术　匿名实体鉴别　第1部分：总则(ISO/IEC 20009-1:2013,IDT)。

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(中关村无线网络安全产业联盟)、国家密码管理局商用密码检测中心、重庆邮电大学、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、中国通用技术研究院、北京大学深圳研究生院、中国科学院软件研究所、国家计算机网络应急技术处理协调中心、中国网络空间研究院、国家信息技术安全研究中心、国家信息安全工程技术研究中心、中国人民解放军信息安全测评认证中心、公安部第三研究所、北京计算机技术及应用研究所、福建省无线电监测站、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、黄振海、李大为、宋起柱、李琴、龙昭华、冯登国、舒敏、陈晓桦、李京春、葛培勤、郭晓雷、高波、朱跃生、李广森、顾健、李楠、于光明、张璐璐、铁满霞、张变玲、许玉娜、胡亚楠、颜湘、张国强、童伟刚、李明、万洪涛、王月辉、郑骊、彭潇、朱正美、陈志宇、侯鹏亮、许福明。

引　言

GB/T 34593 的本部分定义了基于群组公钥签名的匿名实体鉴别机制，分为有在线可信第三方参与的鉴别机制和无在线可信第三方参与的鉴别机制两类。

本文件的发布机构提请注意，声明符合本文件时，可能涉及第 8 章与 ZL201010546339.3、ZL201010546320.9、CN201210063055.8、CN201210063632.3、CN201210063650.1、ZL200910024191.4、ZL200910023774.5、ZL200910023735.5 等相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利持有人姓名：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

本文件的发布机构提请注意，本文件等同采用 ISO/IEC 20009-2:2013，因此，除上述声明外，韩国电子通信研究院、英特尔公司针对 ISO/IEC 20009-2:2013 所作出的“专利持有人愿意基于无歧视、合理条件和条款与其他方协商许可”的声明适用于本文件。相关信息可通过以下联系方式获得：

专利持有人姓名：Electronics and Telecommunications Research Institute

地址：161, Gajeong-dong, Yuseong-gu, Daejeon, 305-700, KOREA

联系人：Hanchul Shin

电子邮件：vip123@etri.ke.kr

电话：+82-042-860-5797

传真：+82-042-860-3831

网址：http://www.etri.re.kr

专利持有人姓名：Intel Corporation

地址：Intel Legal and Corporation Affairs 2200 Mission College Blvd., RNB-150, Santa Clara, CA 95054

联系人：James Kovacs

电子邮件：Standards.Licensing@intel.com

电话：408-765-1170

传真：408-613-7292

网址：http://www.intel.com/standards/licensing.html

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

信息技术　安全技术 匿名实体鉴别
第2部分:基于群组公钥签名的机制

1　范围

GB/T 34953的本部分定义了基于群组公钥签名的匿名实体鉴别机制,验证方基于群组签名机制验证对端身份的合法性且不需要获得对端的身份信息。

本部分规定了:

——基于群组公钥签名的匿名实体鉴别机制的通用描述;

——多种匿名鉴别机制。

本部分描述了:

——群组成员发布过程;

——无在线可信第三方参与的匿名实体鉴别机制;

——有在线可信第三方参与的匿名实体鉴别机制。

另外,本部分还规定了:

——群组成员身份打开的过程(可选);

——群组成员签名连接的过程(可选)。

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。

ISO/IEC 20008-1 信息技术　安全技术　匿名签名服务　第1部分:总则(Information technology—Security techniques—Anonymous digital signatures—Part 1:General)

ISO/IEC 20008-2 信息技术　安全技术　匿名签名服务　第2部分:采用群组公钥的机制(Information technology—Security techniques—Anonymous digital signatures—Part 2:Mechanisms using a group public key)

ISO/IEC 20009-1 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)

3　术语和定义

ISO/IEC 20008-1、ISO/IEC 20009-1界定的以及下列术语和定义适用于本文件。

3.1

绑定属性　binding-property

在通信实体的消息间提供绑定保证的属性。

3.2

认证机构　certification authority

受信任的创建和颁发公钥证书的实体。

[ISO/IEC 11770-1:2010,定义2.3]