ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43779—2024

网络安全技术　基于密码令牌的主叫用户可信身份鉴别技术规范

Cybersecurity technology—Technical specification for caller identity authentication using crypto tokens

2024-04-25 发布　　2024-11-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院大学、中国电信集团有限公司、中国电子技术标准化研究院、中国移动通信集团有限公司、中国信息通信研究院、北京数字认证股份有限公司、华为技术有限公司、北京小米移动软件有限公司、OPPO广东移动通信有限公司、中兴通讯股份有限公司、北京三星通信技术研究有限公司、微位(深圳)网络科技有限公司、广东省电子商务认证有限公司、深圳市电子商务安全证书管理有限公司、中科信息安全共性技术国家工程研究中心有限公司、联通智慧安全科技有限公司、北京信安世纪科技股份有限公司、联通(广东)产业互联网有限公司、国民认证科技(北京)有限公司、郑州信大捷安信息技术股份有限公司、数安时代科技股份有限公司、工业信息安全(四川)创新中心有限公司、成都亚信网络安全产业技术研究院有限公司、武汉大学。

本文件主要起草人：荆继武、王跃武、刘紫千、上官晓丽、刘丽敏、魏亮、詹榜华、寇春静、任兰芳、郑学欣、王平建、颜雪薇、常新苗、雷灵光、黄钱红、李根、王榕、王鹏、华孝泉、吴越、鲍博武、陈木来、梁宁宁、吴昊、李彦峰、王志辉、胡建勋、金刚、张宇、吕召彪、李俊、刘为华、廖正赟、周蔚林、罗影、张文科、吴强、陈晶、赵文博。

引　言

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5章、第6章与可信身份凭证签发、传送、鉴别与信息展示，以及令牌消息传送服务相关的专利的使用。

本文件的发布机构对于上述专利的真实性、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承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就符合本文件规定的方式使用给予免费的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：中国科学院大学

地址：北京市石景山区玉泉路19号甲

专利持有人姓名：微位(深圳)网络科技有限公司

地址：深圳市南山区粤海街道高新区社区科技南路18号深圳湾科技生态园12栋A座601

专利持有人姓名：艾迪通证技术(北京)有限公司

地址：深圳市南山区粤海街道高新区社区科技南路18号深圳湾科技生态园12栋A座601

请注意除了上述专利外，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专利的责任。

网络安全技术　基于密码令牌的主叫用户可信身份鉴别技术规范

1　范围

本文件规定了在通信中基于密码令牌传输、验证和显示主叫用户可信身份的技术要求，描述了相应的测试评价方法。

本文件适用于指导传输、验证和显示主叫用户可信身份的系统设计、生产和测试。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15843.2　信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制

GB/T 15843.3　信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制

GB/T 16262.1　信息技术　抽象语法记法

GB/T 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 32905　信息安全技术　SM3密码杂凑算法

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918.2　信息安全技术　SM2椭圆曲线公钥密码算法　第2部分：数字签名算法

3　术语和定义

下列术语和定义适用于本文件。

3.1

主叫方　caller

呼叫连接的发起方，或呼叫连接发起方的智能终端设备。

3.2

被叫方　called

呼叫连接的接收方，或呼叫连接接收方的智能终端设备。

3.3

运营商　carrier

主叫方或被叫方的网络服务提供商。

注：主叫方运营商和被叫方运营商是相同的或不同的。

3.4

密码令牌　crypto token

由可信用户采用密码技术签名，并提交被叫用户验证的，用以表征自己身份的数据报文。

注：该数据报文也被称为密码身份令牌或身份令牌。