ICS 35.030
L 80

中华人民共和国密码行业标准

GM/T 0113—2021

在线快捷身份鉴别协议

Fast online identity authentication protocol

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　通用在线快捷身份鉴别协议 …… 2
5.1　协议架构 …… 2
5.2　协议消息相关数据结构 …… 5
5.3　协议流程和要求 …… 9
6　双因素在线快捷身份鉴别协议 …… 15
6.1　协议架构 …… 15
6.2　协议消息框架 …… 17
6.3　协议流程和要求 …… 19
附录A（资料性）　安全风险及措施建议 …… 28
附录B（资料性）　可信环境实现方式 …… 31
附录C（资料性）　协议接口 …… 32
参考文献 …… 36

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院数据与通信保护研究教育中心、联想（北京）有限公司、中国科学院大学、国民认证科技（北京）有限公司、北京数字认证股份有限公司、浙江蚂蚁小微金融服务集团有限公司、北京天融信网络安全技术有限公司、中国科学院信息工程研究所、飞天诚信科技股份有限公司、成都卫士通信息产业股份有限公司、中国金融认证中心、吉大正元信息技术股份有限公司、中孚信息股份有限公司、杭州天谷信息科技有限公司、神州融安科技（北京）有限公司、北京握奇智能科技有限公司、郑州信大捷安信息技术股份有限公司、北京眼神智能科技有限公司。

本文件主要起草人：钱文飞、赵欣怡、贾世杰、刘丽敏、柴海新、荆继武、李俊、张永强、宋铮、景鸿理、王平建、牛莹姣、高彪、吕娜、陈天宇、张咪、朱鹏飞、罗俊、孙国栋、赵丽丽、苗功勋、程亮、李登峰、张渊、刘熙胖、杨春林。

在线快捷身份鉴别协议

1 范围

本文件规定了在线快捷身份鉴别协议，包括通用在线快捷身份鉴别协议、双因素在线快捷身份鉴别协议等内容。

本文件适用于在线快捷身份鉴别服务的开发、测试和评估。

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 16262(所有部分) 抽象语法记法(ASN.1)

GB/T 16649.4 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 36651 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GB/T 36651、GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

鉴别客户端 authentication client

在用户代理中处理双因素身份鉴别协议消息的软件组件，用于双因素身份鉴别协议中用户代理与鉴别器之间的通信。

3.2

鉴别客户端接口 authentication client interface

由鉴别客户端提供的协议接口，用于双因素身份鉴别协议中用户代理与鉴别客户端之间的通信。

3.3

生物特征识别密钥管理器标识符 biometric authentication protocol key manager identifier

分配给同一型号生物特征识别密钥管理器的唯一标识符，依赖方可通过该标识符唯一确定厂商公钥。

3.4

用户代理 user agent

安装在用户设备上的浏览器或者其他应用程序。