ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0100—2020

人工确权型数字签名密码应用技术要求

Cryptographic application technical requirements for manually confirmed signing

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：飞天诚信科技股份有限公司、北京宏思电子技术有限责任公司、福建省数字安全证书管理有限公司、北京数字认证股份有限公司、数安时代科技股份有限公司、天地融科技股份有限公司、大唐微电子技术有限公司、中国科学院信息工程研究所、北京握奇智能科技有限公司、深圳市文鼎创数据科技有限公司、福建金密网络安全测评技术有限公司。

本文件主要起草人：朱鹏飞、张永强、刘雅静、张文婧、邓福彪、林雪焰、刘磊、牟宁波、龙萌萌、林璟锵、张渊、刘伟丰、贾世杰、李勃、申新波、吴玲玲、于华章、陈国。

引　言

人工确权型数字签名是一种与密码设备紧密结合的密码应用，有助于防止攻击者通过远程控制签名密钥载体的方式生成合法的数字签名。人工确权型数字签名与一般的数字签名生成过程有所区别，在符合约定的触发条件时与签名者进行交互，待签名者确认后方才生成数字签名。在金融行业标准JR/T 0068—2020、JR/T 0114—2015等发布实施的推动下，人工确权型数字签名在网上银行、手机银行等领域得到广泛应用。为规范人工确权型数字签名中的密码技术应用，制定本标准。

人工确权型数字签名密码应用技术要求

1 范围

本文件规定了人工确权型数字签名的总体要求、应用接口以及使用专用签名密钥对的人工确权型数字签名相关要求。

本文件适用于人工确权型数字签名应用、人工确权型数字签名系统以及人工确权型数字签名设备的设计和开发，也可用于指导上述应用、系统及设备的测试。

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 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056—2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275—2017 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35291—2017 信息安全技术 智能密码钥匙密码应用接口规范

GB/T 37092 信息安全技术 密码模块安全技术要求

GM/T 0008 安全芯片密码检测准则

GM/T 0014—2012 数字证书认证系统密码协议规范

GM/T 0017—2012 智能密码钥匙密码应用接口数据格式规范

GM/T 0074—2019 网上银行密码应用技术要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

[来源：GM/Z 4001—2013，2.113]

3.2

人工确权型数字签名 manually confirmed signing

识别待签名数据，符合触发条件时与签名者交互，待签名者确认后生成数字签名的行为。

3.3

复核型数字签名 review-signing

识别待签名数据，符合触发条件时从待签名数据提取特定内容输出供签名者确认，待签名者确认后