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

生成数字签名的行为。复核型数字签名是人工确权型数字签名的形式之一。

3.4

一般数字签名　generic signing

未与签名者交互生成数字签名的行为。

3.5

触发条件　trigger condition

触发交互型签名的前置条件。

3.6

触发特征　trigger-character

触发条件中待签名数据所具备的特征。

3.7

复核信息　message-to-view

从待签名数据提取的供签名者复核的内容。

3.8

人工确权型数字签名设备　manually confirmed signing device

识别待签名数据，符合触发条件时与签名者交互，待签名者确认后使用私钥生成数字签名的设备。

3.9

签名者　signer

人工确权型数字签名设备的使用者。

3.10

交互特征　interaction-character

人工确权型数字签名生成的数字签名区别于一般数字签名生成的数字签名的特征。

3.11

注册方　registration party

使用专用签名密钥对的人工确权型数字签名中，公示和维护签名者与专用签名密钥对公钥的关联的服务方。

3.12

容器　container

密码设备中用于保存密钥所划分的唯一性存储空间。

[来源：GB/T 35291—2017，3.2]

3.13

命令　command

应用接口向设备发出的一条信息，该信息启动一个操作或请求一个应答。

[来源：GM/T 0017—2012，3.3]

3.14

待签名数据　data-to-be-signed

生成数字签名过程中的签名对象。见 3.1。

3.15

含签名数据　signed data

带有数字签名的数据，通常包括待签名数据、签名算法信息以及数字签名。

4　缩略语

下列缩略语适用于本文件。

PIN:个人识别码(Personal Identification Number)

5 总体要求

5.1 过程

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的典型应用见附录A。

人工确权型数字签名包括以下过程:

a) 触发:接收到待签名数据时,人工确权型数字签名设备进行检查,如果满足触发条件,进入交互过程。

b) 交互:人工确权型数字签名设备与签名者进行交互(例如等待签名者确认)。在预定的超时时间内,当签名者给出确认信号(例如按下人工确权型数字签名设备的确认键)时,进入生成过程;否则(例如签名者在预定的超时时间内给出的不是确认信号或未在预定的超时时间内给出信号),结束。

c) 生成:人工确权型数字签名设备生成数字签名。

在触发过程中,如果由于待签名数据导致不满足触发条件(例如待签名数据不具备触发特征或人工确权型数字签名设备无法判断待签名数据是否具备触发特征),可按一般数字签名处理。

在复核型数字签名的交互过程中,人工确权型数字签名设备还从待签名数据提取信息并输出,提示签名者复核。复核型数字签名的超时时间宜不小于1 min。

5.2 触发条件

触发条件包括但不限于:

——满足生成数字签名所需的条件(例如所使用的算法、算法参数、密钥标识等);

——符合生成数字签名所需的权限要求(例如验PIN通过);

——待签名数据具备触发特征。

可根据具体应用情况约定触发特征的判断规则,包括但不限于待签名数据的格式。触发特征的判断规则不得具有二义性。复核型数字签名可根据具体应用情况约定从待签名数据中提取供确认信息的规则,示例见附录B。

5.3 验证数字签名

待验证的含签名数据应符合GB/T 35275—2017中第8章的要求。验证含签名数据中的待签名数据、签名公钥和数字签名时,如果验证通过,应进一步检查待签名数据是否具备触发特征以及数字签名是否具备交互特征。如果符合以下情况之一,验证通过;否则验证不通过:

——待签名数据具备触发特征,且数字签名具备交互特征;

——待签名数据不具备触发特征,且数字签名不具备交互特征。

5.4 安全要求

人工确权型数字签名使用的密码算法应符合国家密码管理部门的规定。

应采取可靠的措施(包括但不限于技术措施)防止交互特征被伪造,包括但不限于:

——防止人工确权型数字签名生成的数字签名被误认为一般数字签名生成的数字签名;

——防止一般数字签名生成的数字签名被误认为人工确权型数字签名生成的数字签名。

应采取可靠的技术措施防止人工确权型数字签名被误触发,包括但不限于:

——人工确权型数字签名设备不得在不满足触发条件时进行人工确权型数字签名;

——人工确权型数字签名设备不得在满足触发条件时不进行人工确权型数字签名。

人工确权型数字签名设备应具备唯一标识(例如序列号)。应采取可靠的技术措施防止人工确权型数字签名设备标识被篡改或窃取、盗用等非授权使用。

5.5 人工确权型数字签名设备

人工确权型数字签名设备应包含与签名者交互所需的部件(包括但不限于按键)。支持复核签名的人工确权型数字签名设备还应包含供签名者查看复核信息所需的部件(包括但不限于显示屏)。典型的人工确权型数字签名设备见附录 A。

人工确权型数字签名设备应支持识别待签名数据是否具备触发特征的功能。支持复核签名的人工确权型数字签名设备还支持应从待签名数据提取供签名者确认所需信息并输出的功能,且应采取可靠的技术措施防止外部对提取和输出复核信息的干扰(例如伪造或篡改复核信息)。

人工确权型数字签名设备应符合 GB/T 37092 规定的密码模块安全要求,等级应不低于二级。人工确权型数字签名设备应使用经国家密码管理部门核准的密码芯片提供密码服务。密码芯片的安全等级应不低于 GM/T 0008 规定的安全等级 2。

人工确权型数字签名设备的应用结构应符合 GB/T 35291—2017 中 5.2 的要求。人工确权型数字签名设备支持的命令应符合 GM/T 0017—2012 的要求。人工确权型数字签名设备应采取可靠的技术措施防止外部对判断人工确权型数字签名触发条件的干扰,包括但不限于:

——不得支持启动交互过程的命令;

——不得支持取消或中止交互过程的命令。

用于网上银行的人工确权型数字签名设备还应符合 GM/T 0074—2019 中 7.5.3.3.2 的要求。

6 人工确权型数字签名密码应用接口

6.1 生成数字签名

生成数字签名接口定义如表 1 所示。

表 1 生成数字签名接口

原型	ULONG DEVAPI SKF_SignData(ULONG idAlg, HCONTAINER hContainer, BYTE * pbData, ULONG ulDataLen, BYTE * pbSignature, ULONG * pulSignLen)	
功能描述	使用 hContainer 指定容器的签名私钥,依据 idAlg 指定的算法,对指定数据 pbData 生成数字签名。数字签名存放到 pbSignature 缓冲区,设置 pulSignLen 为数字签名的长度	
参数	idAlg	[IN] 签名算法标识,定义见 GB/T 33560
	hContainer	[IN] 容器句柄
	pbData	[IN] 待签名数据
	ulDataLen	[IN] 待签名数据的长度
	pbSignature	[OUT] 数字签名
	pulSignLen	[IN/OUT] 数字签名缓冲区的长度/数字签名的长度
返回值	SAR_OK:成功。其他:错误码	
备注	权限要求:用户权限。 如果 hContainer 对应的容器内置的签名私钥与 idAlg 不匹配,应返回错误码 SAR_INVALIDPARAMERR	

6.2 验证数字签名

验证数字签名接口定义如表 2 所示。

表 2 数字签名验签接口

原型	int SAF_VerifySignedData(unsigned char * pucSignedData, unsigned long ulSignedDataLen, BOOL * pblIsInteractive)	
功能描述	基于 pucSignedData 中的含签名数据(包括待签名数据、签名算法标识和签名公钥/数字证书)验证数字签名,并判断数字签名是否为人工确权型数字签名生成	
参数	pucSignedData	[IN] 含签名数据
	ulSignedDataLen	[IN] 含签名数据的长度
	pblIsInteractive	[OUT] 存放“数字签名是否具备交互特征”判断值的标志位指针。TRUE 表示数字签名具备交互特征,FALSE 表示数字签名不具备交互特征。该标志位仅在验签通过的情况下有效
返回值	SAR_OK:成功。其他:错误码	
备注	权限要求:用户权限。 如果 hContainer 对应的容器内置的签名私钥与 idAlg 不匹配,应返回错误码 SAR_INVALID-PARAMERR。 基于人工确权型数字签名的应用应判断验签通过的数字签名是否为人工确权型数字签名生成以及是否与预期相符	

6.3 其他密码应用接口

其他密码应用接口应符合 GB/T 35291—2017 的要求。

7 使用专用签名密钥对的人工确权型数字签名

7.1 概述

使用专用签名密钥对的人工确权型数字签名以签名公钥作为交互特征。使用至少两对签名密钥对,其中一对为专用签名密钥对,用于人工确权型数字签名;其他的签名密钥对用于一般数字签名。进入人工确权型数字签名生成阶段时,使用专用签名密钥对生成数字签名;按一般数字签名处理时,使用其他的签名密钥对生成数字签名。相应地,如果待验证的含签名数据使用专用签名密钥对的公钥验签通过,则含签名数据中的数字签名是由人工确权型数字签名生成的;如果待验证的含签名数据使用其他签名密钥对的公钥验签通过,则含签名数据中的数字签名是由一般数字签名生成的。

使用专用签名密钥对的人工确权型数字签名方案见附录 C。

7.2 人工确权型数字签名应用流程

7.2.1 生成数字签名

生成数字签名流程如下:

a) 签名者将待签名数据发给人工确权型数字签名设备,并指定所使用的容器。人工确权型数字签名设备检查除不涉及待签名数据的触发条件是否满足,如果是,继续;否则返回错误代码(见附录 C)。

b) 人工确权型数字签名设备检查待签名数据是否具备触发特征。如果是，转到 c)；否则按照一般数字签名处理，转到 e)。

c) 人工确权型数字签名设备检查容器中的签名密钥对是否用于人工确权型数字签名。如果是，转到 d)；否则返回错误代码。

d) 人工确权型数字签名设备与签名者交互(例如等待签名者确认)。在预定的超时时间内，当签名者给出确认信号(例如按下人工确权型数字签名设备的确认键)时，使用容器中的签名密钥对生成数字签名；否则(例如签名者在预定的超时时间内给出的不是确认信号或未在预定的超时时间内给出信号)，返回错误代码。

e) 人工确权型数字签名设备检查容器中的签名密钥对是否用于人工确权型数字签名。如果是，返回错误代码；否则，使用容器中的签名密钥对生成数字签名。

7.2.2 验证数字签名

待验证的含签名数据应符合 5.3 的要求。

验证数字签名流程如下：

a) 验证含签名数据中的待签名数据、签名公钥和数字签名。如果验证不通过，结束；否则，进行 b)。

b) 检查含签名数据中的待签名数据是否具备触发特征。如果是，进行 c)；否则，进行 d)。

c) 检查含签名数据中的签名公钥是否用于人工确权型数字签名(例如检查含签名数据中的证书链是否包含专设子 CA 的数字证书，见附录 C。如果是，验证通过；否则，验证不通过。

d) 检查含签名数据中的签名公钥是否用于一般数字签名。如果是，验证通过；否则，验证不通过。

7.3 密钥注册

7.3.1 概述

密钥注册是签名者公示人工确权型数字签名专用公钥的过程。签名者对包含人工确权型数字签名专用公钥的密钥注册消息进行一般数字签名，提交给注册方进行公示；验证方基于注册方公示的信息确定含签名数据中的公钥与签名者的对应关系。

7.3.2 基于数字证书的密钥注册

签名者使用人工确权型数字签名设备为人工确权型数字签名专用密钥对申请数字证书，完成密钥注册。验证方基于数字证书确定签名者与人工确权型数字签名专用公钥的对应关系。申请数字证书的流程应符合 GB/T 25056—2018 中第 12 章的要求。

注册流程如下：

a) 签名者生成申请注册消息，使用一般数字签名密钥对申请注册消息签名，发送给注册方。申请注册消息应符合 GM/T 0014—2012 中 B.4 规定的证书申请消息格式，SubjectPublicKeyInfo 字段包含人工确权型数字签名专用密钥对公钥，extraCerts 字段包含对注册消息签名所用签名密钥对的数字证书。

b) 注册方使用申请注册消息中的数字证书验证申请注册消息中的数字签名的有效性，并验证申请注册消息中的数字证书的有效性。如果验证通过，注册方为申请注册消息中 SubjectPublicKeyInfo 字段中的公钥签发签名数字证书，并保存包含对注册消息签名所用签名密钥对的数字证书，生成注册记录；否则，驳回注册。

数字证书的格式应符合 GB/T 20518—2018 中 5.2 的要求。

7.3.3 基于公钥的密钥注册

签名者使用人工确权型数字签名设备生成包含人工确权型数字签名专用公钥的密钥标识，对包含密钥标识的申请注册消息进行一般数字签名，申请注册消息中包含一般数字签名所用签名密钥对的数字证书。验证方通过数字证书确定人工确权型数字签名专用公钥与签名者的对应关系。

密钥标识包含的信息包括但不限于：

——专用签名密钥对的公钥；

——专用签名密钥对适用的算法标识；

——专用签名密钥对所在的容器 ID 以及应用 ID。

密钥标识不得包含人工确权型数字签名密钥对私钥。

注册流程如下：

a) 签名者生成包含密钥标识的申请注册消息，申请注册消息进行一般数字签名，发送给注册方。申请注册消息中包含一般数字签名所使用的签名密钥对的数字证书。

b) 注册方使用申请注册消息中的数字证书验证申请注册消息的完整性，并验证数字证书的有效性。如果验证通过，注册方保存申请注册消息中的密钥标识和数字证书，生成注册记录；否则，驳回注册。

7.4 人工确权型数字签名设备

7.4.1 逻辑结构

人工确权型数字签名设备应至少包含 2 个容器(如图 1 所示)，其中一个用于存储专用签名密钥对。存储专用签名密钥对的容器不得包含其他密钥。可使用约定的容器标识(例如容器 ID 或容器名称)作为专用签名密钥对的标识。

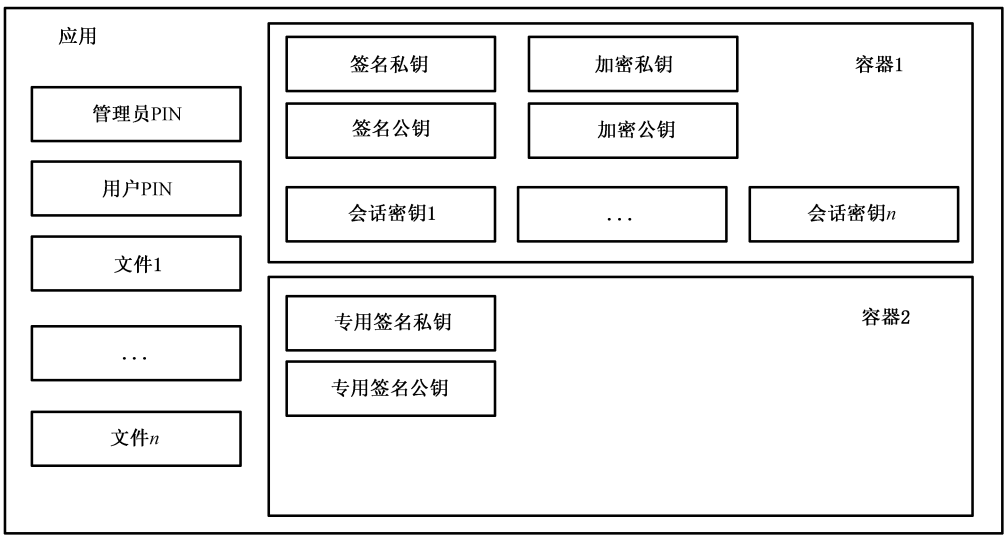

图 1 使用专用签名密钥对的人工确权型数字签名设备逻辑结构

7.4.2 生成专用签名密钥对命令

该命令用于生成专用签名密钥对。如表 3 所示。

表 3　生成专用签名密钥对命令

字段	长度	值	备注
CLA	1 字节	0x80	
INS	1 字节	0xC6	
P1	1 字节	0x00	
P2	1 字节	0x00	
Lc	1 字节	Data 字段长度	
Data	Lc	应用 ID(2 字节)＋容器 ID(2 字节)＋算法标识(4 字节)＋参数(可选)	算法标识应符合 GB/T 33560 的要求
Le	1 字节	0x00	

响应为公钥数据。RSA 算法的情况下,响应数据应符合 GM/T 0017—2012 中 9.6.4.5 的要求。SM2 算法的情况下,响应数据应符合 GM/T 0017—2012 中 9.6.12.5 的要求。

7.4.3　其他密码应用命令

其他密码应用命令应符合 GM/T 0017—2012 的要求。

附 录 A
（资料性）
典型的人工确权型数字签名应用

A.1 人工确权型数字签名的典型应用场景

A.1.1 网上银行

根据金融行业标准 JR/T 0068—2012 的定义，网上银行系统是商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供各种金融服务的信息系统。网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网、移动通信网络、其他开放性公众网络或专用网络向客户进行延伸，是商业银行等金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系变革等的重要举措，提高了商业银行等金融机构的社会效益和经济效益。网上银行系统主要由客户端、增强安全机制、通信网络和服务器端组成，并通过不同类型的通信网络连接到外部系统，开展各类业务。该标准所指网上银行系统，不仅包括传统方式的网上银行系统，还包括通过手机、平板电脑、智能电视等方式访问网上银行系统。

JR/T 0068—2012 中，涉及人工确权型数字签名的要求包括：

——资金类交易中，应具有防范客户端数据被篡改的机制，应由客户确认资金类交易关键数据（至少包含转入账号和交易金额），并采取有效确认方式以保证待确认的信息不被篡改，例如，通过发送包含确认信息的短信验证码，在 USB Key（即智能密码钥匙）内完成确认等（见 JR/T 0068—2012 中 6.3.2.2）。

——USB Key 应能够防远程劫持，具有屏幕显示或语音提示以及按键确认等确认功能，可对交易指令完整性进行校验、对交易指令合法性进行鉴别、对关键交易数据进行输入、确认和保护（见 JR/T 0068—2012 中 6.1.2.1）。

——USB Key 应能够自动识别待签名数据的格式，识别后在屏幕上显示或语音提示交易数据，保证屏幕显示或语音提示的内容与 USB Key 签名的数据一致（见 JR/T 0068—2012 中 6.1.2.1）。

——应采取有效措施防止签名数据在客户最终确认前被替换（见 JR/T 0068—2012 中 6.1.2.1）。

——未经按键确认，USB Key 不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态（见 JR/T 0068—2012 6.1.2.1）。

随着 JR/T 0068—2012 的发布实施，人工确权型数字签名形式之一的复核型数字签名在网上银行系统中得到普及应用。

A.1.2 互联网服务登录

WebAuthn（Web Authentication 的简写）是由国际标准化组织 W3C 于 2019 年 3 月正式发布的一项规范。WebAuthn 定义了一套 Javascript API，支持互联网服务使用 FIDO（Fast IDentity Online，线上快速身份验证）联盟所定义的基于数字签名的身份鉴别协议。目前，WebAuthn 已经得到了 Google Chrome、Mozilla Firefox，Microsoft Edge 以及 Apple Safari 等浏览器的支持。FIDO 联盟成立于 2012 年，致力于安全强度更高、使用更方便且更易于部署的身份鉴别协议（simpler stronger authentication）。在 FIDO 联盟发起的 FIDO2 项目中，基于 CTAP（Client to Authenticator Protocol，客户端到鉴别器协议）规范将 FIDO 规范中的鉴别器（authenticator）与 WebAuthn API 对接，从而实现了 FIDO 与 WebAuthn 的互通。目前，FIDO2 已经受到了 Windows 10 以及 Android 7.0 以上操作系统的支持。

FIDO 协议包括注册和登录两个阶段。在注册阶段，进行以下操作：

——系统提示用户选择符合互联网服务策略的可用的 FIDO 鉴别器（用于生成密钥对和计算数字签名的密码模块）。

——用户使用指纹传感器、第二因子设备上的按钮、安全输入的 PIN 或其他方法解锁 FIDO 鉴别器。

——用户设备（内置鉴别器的设备）创建一对针对用户设备、互联网服务和用户账户的独有的全新公/私钥对。

——系统将公钥发送给互联网服务，并将其与用户的账户关联。私钥和本地身份鉴别方法相关信息（例如生物特征识别数据）不会离开用户设备。

在登录阶段，进行以下操作：

——互联网服务要求用户使用之前注册过的并与服务策略相符的设备登录；

——用户使用与注册时相同的方法解锁 FIDO 鉴别器；

——设备使用由服务器提供的用户的账户标识来选择正确的密钥并对服务器发出的挑战生成数字签名；

——设备将挑战值连带数字签名发送回服务器，由其使用存储的公钥进行验证，然后即可允许用户登录。

在 FIDO 协议中，生成数字签名前，用户使用设备上的按钮解锁。因此 FIDO 协议中生成数字签名的过程属于人工确权型数字签名。

A.2 典型的人工确权型数字签名设备

A.2.1 可视按键型智能密码钥匙

可视按键型智能密码钥匙在智能密码钥匙的基础上增设显示屏和按键。应用于网上银行的可视按键型智能密码钥匙通常包括确定、取消、上翻和下翻四个按键，内置交易报文解析引擎，能够解析交易报文，提取并显示账号、户名等交易要素，等候用户复核确认。用户复核完毕按键确认之后，再生成数字签名。除了 USB 接口之外，可视按键型智能密码钥匙还可支持蓝牙等接口。外观样式如图 A.1 所示。

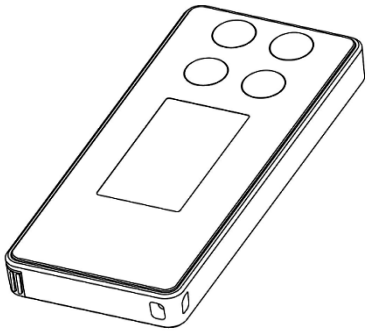

图 A.1 可视按键型智能密码钥匙示意图

A.2.2 集成外设 IC 卡

集成外设 IC 卡是将若干类型的设备（包括但不限于电池、显示屏、传感器、按键/键盘等）集成于 IC 卡形成的新型 IC 卡。ISO/IEC 18328-2 规定了集成外设 IC 卡的通用物理特性及测试方法。由于集成了可与使用者交互的设备，集成外设 IC 卡无需依赖读卡机具就能够独立与使用者进行交互，可作为人工确权型数字签名设备使用。目前较为成熟的集成外设 IC 卡包括集成电池、显示屏和按键的可视卡

（如图 A.2 所示）以及集成指纹传感器的指纹卡（如图 A.3 所示）等。

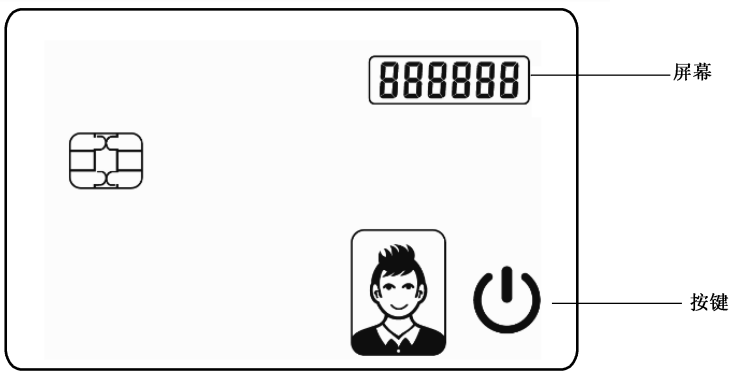

图 A.2　可视卡示意图

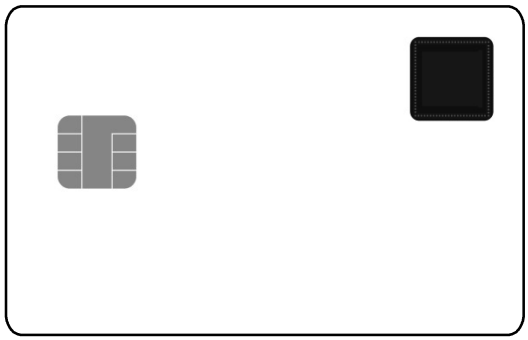

图 A.3　指纹卡示意图

附 录 B
（资料性）
人工确权型数字签名方案设计指南

B.1 概述

人工确权型数字签名特有的安全威胁称作“骗签”，即5.4中的“一般数字签名生成的数字签名被误认为人工确权型数字签名生成的数字签名”以及“人工确权型数字签名生成的数字签名被误认为一般数字签名生成的数字签名”。为了尽量降低骗签风险，人工确权型数字签名方案的设计和实现应关注以下要点：

——设计逻辑完备的报文格式规则定义（例如B.2）并实现，避免出现二义性或者逻辑漏洞，防止在判断是否触发人工确权型数字签名时出现误判；

——人工确权型数字签名和一般数字签名应具备区别特征（例如第7章使用专用签名密钥对的人工确权型数字签名方案），即使在判断是否触发人工确权型数字签名时出现误判，在验证签名阶段也能够准确无误地判断出数字签名是否经人工确权型数字签名生成，进一步降低安全风险。

B.2 人工确权型数字签名报文格式规则示例

B.2.1 概述

本报文格式规则适用于网上银行系统的交易类业务。报文基于XML格式，采用UTF-8编码。XML元素标签采用单英文字母大写形式，元素属性采用单英文字母小写形式。交易报文中不包括换行、空格缩进。

触发特征可描述为：

——XML格式；

——根元素为〈R〉，包含最多一个子元素〈S〉或至少一个子元素〈E〉；

——元素〈S〉或〈E〉中包含至少一个子元素〈V〉；

——元素〈V〉中包含最多一个子元素〈D〉，或元素〈V〉中包含至少一个子元素〈T〉。

B.2.2 交易报文元素

交易报文元素包括：

——〈R〉：根元素。交易报文中有且仅有一个。可以有语言标识属性xml:lang。

——〈S〉：〈R〉的子元素，标识批量签名的交易信息总计部分。交易报文中最多有一个。如果〈S〉元素存在，则应位于所有〈E〉元素之前，并且〈S〉后的〈E〉元素只参与签名，不参与显示。

——〈E〉：〈R〉的子元素，标识一笔交易。交易报文中有一个或多个。如果没有〈S〉元素，则所有〈E〉元素都参与显示。

——〈V〉：〈S〉和〈E〉的子元素，标识交易中显示的一个条目。交易报文中有任意个，其中〈S〉中至少有一个。可以有键值属性k和类别属性t。

——〈I〉：〈S〉和〈E〉的子元素，标识交易中不参与显示的一个条目。交易报文中有任意个。可以有键值属性k。

——〈D〉:〈V〉和〈I〉的子元素,标识条目中数据。〈V〉中最多有一个,〈I〉中有一个。

——〈T〉:〈V〉的子元素,标识条目中显示的文本片段,交易报文中有任意个。

B.2.3 交易报文元素属性

交易报文元素的基本键值属性列表如表 B.1 所示:

表 B.1 基本键值属性列表

序号	属性名称	属性标识
1	交易序号	transId
2	付款账号	outAccountId
3	收款账号	inAccountId
4	交易金额	amount
5	付款日期	payDate
6	交易笔数	count
7	交易总金额	sum

交易报文元素的属性包括:

——xml:lang:说明 xml 文本的自然语言属性,用于提示显示的语言,仅在根元素有效。需要符合 xml 和 RFC1766 规范,例如:en、en-US、zh-CN,缺省为 zh。

——k:〈V〉和〈I〉的属性,标识条目的键值,在〈E〉中应唯一。

——t:〈V〉和〈I〉的属性,标识条目中数据的类型,用于提示显示数据的方式。t 的有效值如下,缺省为 s。

——s:字符串类型,内容可能已经根据语言做本地化处理。

——d:十进制数值类型,内容可能已经根据语言做本地化处理,例如金额在中文、英文下显示为 1,234,567.56,在德文下显示为 1.234.567,56。可有“+”、“-”号。

——t:日期、时间类型,内容可能已经根据语言做本地化处理,内容可以只有日期、只有时间或两者都有。日期格式为年月日顺序,时间格式为 24 小时制,毫秒可选。如:2010-09-18、2010/09/18 00:00:00、2010/09/18 21:30:45.500、14:30:15、23:59:59.999。

——b:布尔类型,值为大小写不敏感的“true”“false”或者“1”(对应“true”)、“0”(对应“false”)。

B.2.4 报文样例

无总计报文样例:

〈? xml version="1.0" encoding="UTF-8"?〉〈R xml:lang="zh"〉〈E〉〈I k="transId"〉〈D〉111111〈/D〉〈/I〉〈V k="outAccountId"〉〈T〉付款账号:〈/T〉〈D〉1234567890123456〈/D〉〈/V〉〈V k="amount" t="d"〉〈T〉付款金额:〈/T〉〈D〉1234.23〈/D〉〈T〉元〈/T〉〈/V〉〈V k="payDate" t="t"〉〈T〉付款日期:〈/T〉〈D〉2014-10-21〈/D〉〈/V〉〈V k="inAccountId"〉〈T〉收款账号:〈/T〉〈D〉100000067782〈/D〉〈/V〉〈/E〉〈/R〉

上述报文对应的显示内容如下所示:

付款账号:1234567890123456

付款金额:1234.23 元

付款日期:2014-10-21

收款账号:100000067782

有总计报文样例：

〈? xml version="1.0" encoding="UTF-8"?〉〈R xml:lang="zh"〉〈S〉〈V k="count" t="d"〉〈T〉交易笔数：〈/T〉〈D〉2〈/D〉〈/V〉〈V k="sum" t="d"〉〈T〉总金额：〈/T〉〈D〉3000〈/D〉〈T〉元〈/T〉〈/V〉〈/S〉〈E〉〈I k="transId"〉〈D〉111111〈/D〉〈/I〉〈I k="outAccountId"〉〈D〉1234567890123456〈/D〉〈/I〉〈I k="amount"〉〈D〉1，000〈/D〉〈/I〉〈I k="payDate"〉〈D〉2010-09-10〈/D〉〈/I〉〈V k="inAccountId"〉〈T〉收款账号：〈/T〉〈D〉100000067782〈/D〉〈/V〉〈/E〉〈E〉〈I k="transId"〉〈D〉111112〈/D〉〈/I〉〈I k="outAccountId"〉〈D〉1234567890123456〈/D〉〈/I〉〈I k="amount"〉〈D〉2，000〈/D〉〈/I〉〈I k="payDate"〉〈D〉2010-09-10〈/D〉〈/I〉〈V k="inAccountId"〉〈D〉100000067783〈/D〉〈/V〉〈/E〉〈/R〉

上述报文对应的显示内容如下所示：

交易笔数：2

总金额：3 000 元

B.2.5 基于 JSON 的等效格式

B.2.4 中的 XML 报文可转换成等效的 JSON 报文，因此本报文格式规则也可基于 JSON 格式。无总计报文样例如下：


```
{
  "R": {
    "-xml:lang": "zh",
    "E": {
      "I": {
        "-k": "transId",
        "D": "111111"
      },
      "V": [
        {
          "-k": "outAccountId",
          "T": "付款账号：",
          "D": "1234567890123456"
        },
        {
          "-k": "amount",
          "-t": "d",
          "T": [
            "付款金额：",
            "元"
          ],
          "D": "1234.23"
        },
        {
          "-k": "payDate",
          "-t": "t",
          "T": "付款日期：",
          "D": "2014-10-21"
```

```
        },
        {
          "-k": "inAccountId",
          "T": "收款账号:",
          "D": "100000067782"
        }
      ]
    }
  }
}
```

有总计报文样例：

```
{
  "R": {
    "-xml:lang": "zh",
    "S": {
      "V": [
        {
          "-k": "count",
          "-t": "d",
          "T": "交易笔数:",
          "D": "2"
        },
        {
          "-k": "sum",
          "-t": "d",
          "T": [
            "总金额:",
            "元"
          ],
          "D": "3000"
        }
      ]
    },
    "E": [
      {
        "I": [
          {
            "-k": "transId",
            "D": "111111"
          },
          {
            "-k": "outAccountId",
            "D": "1234567890123456"
          },
          {
```

```
                "-k": "amount",
                "D": "1,000"
              },
              {
                "-k": "payDate",
                "D": "2010-09-10"
              }
            ],
            "V": {
              "-k": "inAccountId",
              "T": "收款账号:",
              "D": "100000067782"
            }
          },
          {
            "I": [
              {
                "-k": "transId",
                "D": "111112"
              },
              {
                "-k": "outAccountId",
                "D": "1234567890123456"
              },
              {
                "-k": "amount",
                "D": "2,000"
              },
              {
                "-k": "payDate",
                "D": "2010-09-10"
              }
            ],
            "V": {
              "-k": "inAccountId",
              "D": "100000067783"
            }
          }
        ]
      }
    }
```

B.3 人工确权型数字签名的安全性分析方法

B.3.1 人工确权型数字签名及骗签的形式化描述

数字签名的生成过程是一个从待签名数据到数字签名的映射，包含预处理和密码运算两个子映射。将待签名数据记作 m，数字签名记作 s，密钥记作 k，预处理记作 h，密码运算记作 c，则数字签名的生成过程可以形式化地表述为 $s=c(h(m),k)$。实际的数字签名设备可以支持多种预处理方式、多种密码运算方式(算法)或多个(种)密钥。因此，实际的数字签名设备可以表示为三元组 (C,H,K)。其中 C 是密码运算方式(算法)的集合，H 是预处理映射的集合，K 是密钥的集合。

对待签名数据 m 生成的数字签名的可能值是一个集合，表达为

$S(m)=\{s \mid s=c(h(m),k),c \in C,h \in H,k \in K\}$

将 m 的可能值构成的集合记作 M，数字签名设备生成的数字签名集合可形式化地表达为

$S(m)=\{s \mid s=c(h(m),k),m \in M,c \in C,h \in H,k \in K\}$

将含签名数据中的待签名数据记作 m，含签名数据中的数字签名记作 s，则数字签名的验证过程是从二元组(m,s)到集合$\{0,1\}$的映射，可以形式化地表达为

$$V(m,s)=\begin{cases}1, s \in S(m)\\0, s \notin S(m)\end{cases}$$

1 表示被验证方接受，0 表示不被接受。

人工确权型数字签名在生成数字签名的过程中增加触发和交互过程，签名算法、待签名数据、签名密钥等参数的变化与交互过程相独立，而人工确权型数字签名的验签过程与触发、交互过程无关。因此，人工确权型数字签名也适用于上述形式化描述。

对于人工确权型数字签名，待签名数据可分为“需要进行人工确权型数字签名”(触发交互)和“不需要进行人工确权型数字签名”两类。相应地，待签名数据集合 M 可表示为

$M=M_0 \cup M_1$

其中 M_0 是能够触发交互的消息集合，M_1 是其补集。在形式化视角下，“骗签”描述为：

若 $m_0 \in M_0$，$\in M_1$ 且 $m_0 \neq m_1$ 满足 $\exists s_1 \in S(m_1)$ 使得 $V(m_0,s_1)=1$，则存在骗签隐患；若对特定的 $m_0 \in M_0$，$\exists m_1 \in M$ 且 $m_0 \neq m_1$ 满足 $\exists s_1 \in S(m_1)$ 使得 $V(m_0,s_1)=1$，则存在骗签漏洞。

更具体地，若 $m_1 \in M_1$，对应着利用一般数字签名仿冒人工确权型数字签名的情况；若 $m_1 \in M_0$，$m_1 \in M_0$ 对于复核型数字签名意味着可能存在签名结果相同而复核信息不同的情况(即“所见非所签”)。

B.3.2 对一种存在骗签隐患的人工确权型数字签名方案的分析

根据 GB/T 35276—2017 的规定，SM2 签名的预处理过程表示为 $H=\mathrm{SM3}(Z \| M)$。其中 H 为预处理结果，SM3()表示 SM3 杂凑运算，“||”表示拼接，M 为待签名数据，Z 为对使用签名方的用户身份标识和签名方公钥依序拼接后进行 SM3 杂凑运算得到的值(在签名方密钥对等参数不变的前提下，可以将 Z 按固定值处理)。以此为基础设计一种复核型数字签名方案，生成数字签名流程如下：

a) 签名者将待签名数据发给人工确权型数字签名设备。

b) 人工确权型数字签名设备检查待签名数据是否具备触发特征。如果是，转到 c)；否则，转到 d)。

c) 人工确权型数字签名设备从待签名数据中提取复核信息，等待与签名者交互(通过显示屏显示复核信息，等待交互者按下人工确权型数字签名设备上的确认键)。如果签名者确认，将复核信息与待签名数据拼接，对拼接后的数据生成数字签名；否则返回错误码。

d) 人工确权型数字签名设备对待签名数据生成数字签名。

对上述方案进行分析：将待签名数据 m 中可能存在的复核信息记为 m_a。不难理解，若 $m \in M_1$，则 $m_a = \Phi$。上述复核签名方案的预处理过程可以形式化地表示为

$h(m) = \mathrm{SM3}(Z \| M \| m_a)$

将 m_a 的可能取值集合记作 M_a，显然 $M_a \subseteq M$。构造集合

$M_2 = \{m_2 \mid m_2 = m \| m_a, m \in M, m_a \in M_a\} \subseteq M$

则有

$h(m_2) = \mathrm{SM3}(Z \| m_2) = \mathrm{SM3}(Z \| m \| m_a), \forall m_2 \in M_2$

若 $\exists m_0 \in M_0$ 能够构造 $m_3 = m_0 \| m_a$ 满足

$m_2 \in M_2$ 且 $m_3 \notin m_a$

则

$m_3 \neq m_0, S(m_2) IS(m_0) \neq \phi$ 即 $\exists s_1 \in S(m_2)$ 使得 $V(m_0, S_1) = 1$。

由上述分析可知，在该方案中，一旦对触发复核签名的消息范围定义（例如报文格式规则）的设计或实现存在漏洞，有可能在不触发人工确权型数字签名的前提下得到人工确权型数字签名结果。因此，该方案存在骗签隐患。

附 录 C
（资料性）
使用专用签名密钥对的复核型数字签名系统方案

C.1 系统架构

系统包括客户端主机、注册方系统和应用方系统。系统架构如图 C.1 所示。

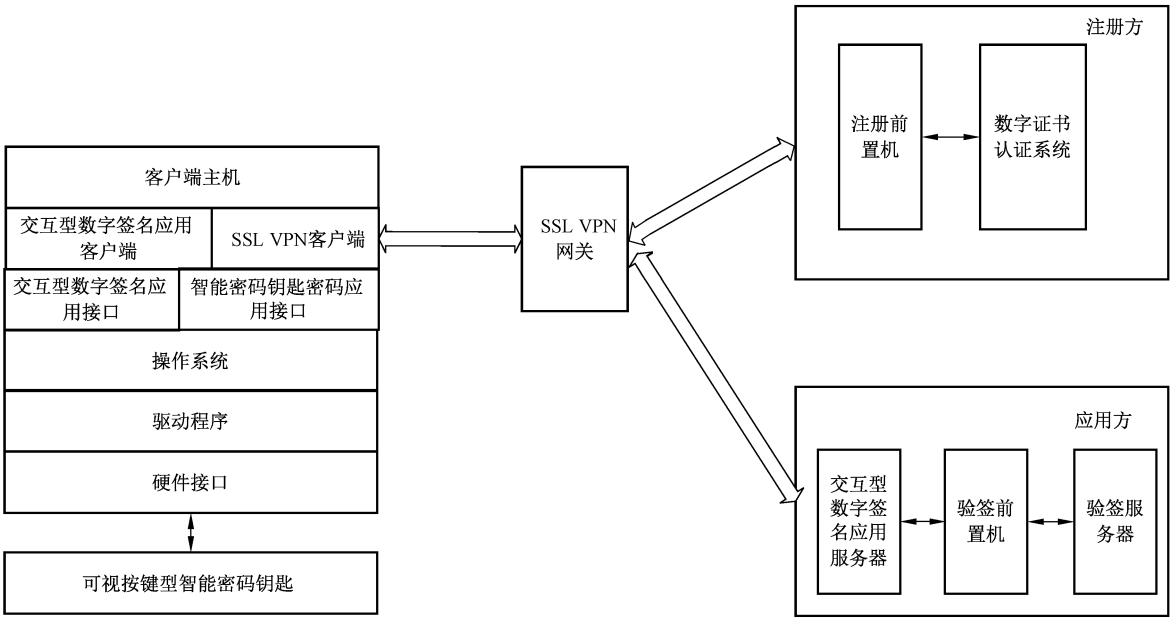

图 C.1 系统架构

使用可视按键型智能密码钥匙作为人工确权型数字签名设备。客户端主机与人工确权型数字签名设备连接，运行人工确权型数字签名应用客户端，按照 7.2.1 的要求生成数字签名。典型的客户端主机包括 PC、智能手机等等。客户端主机还可运行符合 GM/T 0024—2014 要求的 SSL VPN 客户端，与符合 GM/T 0025—2014 要求的 SSL VPN 网关建立加密信道。

注册方由数字证书认证系统和注册前置机组成。其中，注册前置机审核申请注册消息，基于通过审核的注册消息向数字证书认证系统申请签发签名数字证书，实现 7.3.2 规定的密钥注册功能。数字证书认证系统符合 GB/T 25056—2018 的要求。为了区分人工确权型数字签名证书和一般签名密钥数字证书，数字证书认证系统增设证书策略，例如对注册前置机的证书签发申请使用专设的子 CA。

应用方由人工确权型数字签名应用服务器、验签前置机和验签服务器组成。其中，验签服务器符合 GM/T 0029—2014 的要求，验签前置机基于验签服务器实现 7.2.2 规定的数字签名验签功能，人工确权型数字签名应用服务器按照 7.2.2 的要求。

C.2 专用签名密钥对注册

C.2.1 注册之前

注册专用签名密钥对之前，人工确权型数字签名设备内置一般数字签名证书，由注册方按照

GB/T 25056—2018 的要求签发。以预定的容器名称作为专用签名密钥对的标识，生成专用签名密钥对的过程如下：

a) 人工确权型数字签名应用客户端调用 GB/T 35291—2017 中 7.5.2 规定的创建容器接口，使用预定的容器名称创建容器；

b) 人工确权型数字签名应用客户端调用 GB/T 35291—2017 中 7.6.11 规定的生成签名密钥对接口，人工确权型数字签名应用接口向人工确权型数字签名设备发送 7.4.2 规定的生成专用签名密钥对指令，人工确权型数字签名设备生成专用签名密钥对。

C.2.2 客户端到注册前置机

从客户端发给注册前置机的注册消息符合 PKCS#10 规定的 CertificationRequest。

```
CertificationRequest ::= SEQUENCE {
        certificationRequestInfo CertificationRequestInfo,
        signatureAlgorithm AlgorithmIdentifier{{ SignatureAlgorithms }},
        signature              BIT STRING
    }
```

其中，signature 由人工确权型数字签名设备的一般数字签名密钥对生成。

```
CertificationRequestInfo ::= SEQUENCE {
        version             INTEGER { v1(0) } (v1,...),
        subject             Name,
        subjectPKInfo       SubjectPublicKeyInfo{{ PKInfoAlgorithms }},
        attributes          [0] Attributes{{ CRIAttributes }}
    }
```

其中，Name 包括人工确权型数字签名设备的序列号。

```
SubjectPublicKeyInfo { ALGORITHM : IOSet} ::= SEQUENCE {
        algorithm             AlgorithmIdentifier {{IOSet}},
        subjectPublicKey      BIT STRING
    }
```

其中，subjectPublicKey 包括人工确权型数字签名设备的专用签名密钥对公钥。

```
AlgorithmIdentifier {ALGORITHM:IOSet } ::= SEQUENCE {
        algorithm               ALGORITHM.&id({IOSet}),
        parameters              ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
    }
```

从客户端发给注册前置机的注册消息也可符合 GM/T 0014—2012 中 B.3 规定的 PKIMessage 要求。

C.2.3 注册前置机到 CA

注册前置机从注册消息提取序列号，根据序列号检索获得用户信息和公钥，使用公钥验证注册消息的完整性。如果验证通过且用户信息符合证书策略，基于用户信息和注册消息中的公钥生成证书签发请求消息，向 CA 申请签发数字证书。

注册前置机向 CA 申请签发证书的协议符合 GM/T 0014—2012 中 B.4 的要求。

CA 基于用户信息及其专用签名密钥对公钥签发证书，完成专用签名密钥对注册。

C.2.4 专用签名密钥对注销

通过撤销 CA 为用户及其专用签名密钥对签发的数字证书完成专用签名密钥对注销。撤销证书协

议符合 GM/T 0014—2012 中 B.5 的要求。注册方可根据预设策略主动撤销专用签名密钥对数字证书。

C.3 生成数字签名

下列描述中，涉及的状态码的具体含义见 GM/T 0017—2012 附录 A，错误代码的具体含义见 GB/T 35291—2017 附录 C。

生成数字签名流程如下：

a) 人工确权型数字签名应用客户端调用 6.1 中的生成数字签名接口，指定要使用的容器，将待签名数据传给人工确权型数字签名设备。人工确权型数字签名设备检查是否处于用户认证通过状态，如果是，继续；否则，人工确权型数字签名设备回送状态码‘6982’。相应地，生成数字签名接口返回错误代码 SAR_USER_NOT_LOGGED_IN。

b) 人工确权型数字签名设备检查待签名数据是否具备触发特征。如果是，从待签名数据中提取复核信息，转到 c)；否则，转到 e)。

c) 人工确权型数字签名设备检查所指定容器中的签名密钥对是否为专用签名密钥对。如果是，转到 d)；否则，人工确权型数字签名设备回送状态码‘6986’。相应地，生成数字签名接口返回错误代码 SAR_KEYUSAGEERR。

d) 人工确权型数字签名设备显示复核信息，等待签名者按下确认键。在预定的超时时间内，当确认键被按下时，人工确权型数字签名设备使用所指定容器中的签名密钥对生成数字签名，将数字签名回送给生成数字签名接口；否则（例如在超时时间内取消键被按下，或在超时时间内未按键），人工确权型数字签名设备回送状态码‘6986’。相应地，生成数字签名接口返回错误代码 SAR_TIMEOUTERR。

e) 人工确权型数字签名设备检查容器中的签名密钥对是否为一般签名密钥对（是否不为专用签名密钥对）。如果是，人工确权型数字签名设备使用所指定容器中的签名密钥对生成数字签名，将数字签名回送给生成数字签名接口；否则，人工确权型数字签名设备回送状态码‘6986’。相应地，生成数字签名接口返回错误代码 SAR_KEYUSAGEERR。

得到数字签名后，人工确权型数字签名应用客户端从所指定容器中读取签名数字证书，将待签名数据、签名数字证书和数字签名打包组成含签名数据。含签名数据的数据格式符合 GB/T 35275—2017 第 8 章规定的 SignedData。其中，contentInfo 字段包含待签名数据，certificates 字段包含签名证书链。签名证书链可根据签名数字证书从数字证书认证系统检索获得。

```
SignedData ::= SEQUENCE {
        version Version,
        digestAlgorithms DigestAlgorithmIdentifiers,
        contentInfo ContentInfo,
certificates[0] IMPLICIT ExtendedCertificatesAndCertificates OPTIONAL,
        crls[1] IMPLICIT CertificateRevocationLists OPTIONAL,
        signerInfos SignerInfos
}
```

需要注意的是，如果 contentInfo 字段包含的是待签名数据的杂凑值（或预处理结果）而数字签名具有交互特征，由于无法确定待签名数据是否具备触发特征，验证数字签名将不通过。

如果使用 SM2 签名而待签名数据的长度超出了相关限制（例如超出了 GM/T 0017—2012 中 9.6.14规定的 ECCSign 指令定义的数据长度限制），在 6.1 中的生成数字签名接口中按以下流程执行：

a) 发送 GM/T 0017—2012 中 9.6.35 定义的 DigestInit 指令，摘要算法标识为 SM3，DATA 域包含签名密钥对公钥和用户 ID。人工确权型数字签名设备根据签名密钥对公钥在当前应用检

索确定要使用的签名密钥对所在的容器 ID。

b) 发送 GM/T 0017—2012 中 9.6.37 定义的 DigestUpdate 指令(一条或多条),将待签名数据传输给人工确权型数字签名设备。人工确权型数字签名设备按照 GB/T 35276—2017 第 8 章的要求对待签名数据进行预处理,并根据待签名数据确定是否触发人工确权型数字签名。

c) 待签名数据传输完毕时,发送 GM/T 0017—2012 中 9.6.37 定义的 DigestFinal 指令。人工确权型数字签名设备保存当前预处理结果。

d) 发送 GM/T 0017—2012 中 9.6.14 定义的 ECCSignData 指令,数据域不存在。人工确权型数字签名设备对当前预处理结果生成数字签名(一般数字签名或人工确权型数字签名),清除当前保存的预处理结果。

在上述过程中,人工确权型数字签名设备采取的控制措施包括但不限于:

——如果根据签名密钥对公钥检索得到的容器 ID 不存在,回送状态码'6A91';如果容器 ID 不止一个,回送状态码'6A94';

——如果接收到的 ECCSignData 指令包含数据域,但数据域中的用户 ID 或签名密钥对公钥与 DigestInit 指令中的数据不符,或容器 ID 与人工确权型数字签名设备检索确定的容器 ID 不符,回送状态码'6A80';

——在接收上述指令序列的过程中,如果接收到 GM/T 0017—2012 中定义的其他密码服务指令,不执行相应的密码服务,回送状态码'6985';如果接收到使生成数字签名过程中断的其他指令(例如关闭应用、验证 PIN 等),执行相应指令,清除当前保存的计算结果、容器 ID 等。

C.4 验证数字签名

下列描述中,涉及的错误代码的具体含义见 GM/T 0019—2012 附录 A,响应码的具体含义见 GM/T 0029—2014 附录 C。

验证数字签名流程如下:

a) 人工确权型数字签名应用服务器调用 6.2 规定的验证数字签名接口,将含签名数据发给验签前置机。

b) 验签前置机向验签服务器发送 GM/T 0029—2014 中附录 A.5.13 规定的单包验证消息签名请求,将含签名数据发给验签服务器。如果验签服务器返回的响应码为 GM_SUCCESS,转到 c);否则,验证数字签名接口返回 SAR_CertVerifyErr。结束。

c) 验签前置机从含签名数据中提取待签名数据,检查待签名数据是否具备触发特征。如果是,转到 d);否则,转到 e)。

d) 验签前置机从含签名数据中提取证书链,检查证书链中是否包含专设子 CA 的数字证书且证书链中的所有证书均有效。如果是,验证数字签名接口返回 SAR_OK,且标志位为 TRUE;否则,验证数字签名接口返回 SAR_KeyUsageErr。

e) 验签前置机从含签名数据中提取证书链,检查证书链中是否不包含专设子 CA 的数字证书且证书链中的所有证书均有效。如果是,验证数字签名接口返回 SAR_OK,且标志位为 FALSE;否则,验证数字签名接口返回 SAR_KeyUsageErr。

C.5 人工确权型数字签名设备标识

根据 GM/T 0017—2012 中 9.1.3 的规定,GetDevInfo 指令的响应中包含 cosDEVINFO 数据结构,其中的 DeviceType 字段表示设备类型,可用于区分人工确权型数字签名设备与一般的智能密码钥匙。例如,根据 GM/T 0017—2012 的规定,DeviceType 为 2,表示普通 USBKey,即仅支持一般数字签名的

智能密码钥匙；DeviceType 为 3，表示显示按键 key，可对应带屏幕和按键的人工确权型数字签名设备；DeviceType 为 5，表示指纹 key，可对应支持指纹识别的人工确权型数字签名设备。

除此之外，cosDEVINFO 数据结构还包含序列号，可作为人工确权型数字签名设备标识。为符合 5.4 的要求，在专用签名密钥对存在于人工确权型数字签名设备的情况下，当接收到 GM/T 0017—2012 中 9.1.3 规定的 GetDevInfo 命令时，人工确权型数字签名设备的响应报文中不仅包括 cosDEVINFO 数据，还包括对使用一般数字签名密钥对 cosDEVINFO 数据生成的数字签名，以此防止人工确权型数字签名设备标识被篡改。

参 考 文 献

[1] GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

[2] GM/T 0024—2014 SSL VPN 技术规范

[3] GM/T 0025—2014 SSL VPN 网关产品规范

[4] GM/T 0029—2014 签名验签服务器技术规范

[5] JR/T 0068—2012 网上银行系统信息安全通用规范

[6] JR/T 0114—2015 网银系统USBKey规范 安全技术与测评要求

[7] W3C. Web Authentication: An API for accessing Public Key Credentials Level 1[EB/OL]. https://www.w3.org/TR/webauthn/. 2019-03-04

[8] FIDO Alliance. FIDO2 Project[EB/OL]. https://fidoalliance.org/fido2/. 2018-02-27

[9] FIDO Alliance. Client to Authenticator Protocol (CTAP)[EB/OL]. https://fidoalliance.org/specs/fido-v2.0-id—20180227/fido-client-to-authenticator-protocol-v2.0-id—20180227.html#ctap2-canonical-cbor-encoding-form. 2018-02-27

[10] ISO/IEC 18328-2:2015,Identification cards—ICC-managed devices—Part 2: Physical characteristics and test methods for cards with devices

中华人民共和国密码
行业标准
人工确权型数字签名密码应用技术要求
GM/T 0100—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 58 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35846 定价 36.00 元

GM/T 0100-2020

码上扫一扫 正版服务到