ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0118—2022

浏览器数字证书应用接口规范

Browser digital certificate application interface specification

2022-11-20 发布　　2023-06-01 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　总体技术框架 …… 2
6　算法标识与数据类型 …… 3
6.1　算法标识 …… 3
6.2　基本数据类型 …… 3
6.3　常量定义 …… 3
6.4　复合数据类型 …… 4
7　接口函数 …… 12
7.1　概述 …… 12
7.2　证书存储区管理接口 …… 13
7.3　UI 接口 …… 19
7.4　SKF 管理接口 …… 20
7.5　与其他接口规范的关系 …… 20
附录 A（规范性）　错误码定义和说明 …… 22
附录 B（资料性）　使用本规范接口的例程 …… 23
B.1　注册 SKF 以及证书存储 …… 23
B.2　SKF 函数指针 …… 25
B.3　加载释放 SKF 动态库 …… 25
B.4　证书使用 …… 26
参考文献 …… 28

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：天津赢达信科技有限公司、北京信安世纪科技有限公司、北京数字认证股份有限公司、北京海泰方圆科技股份有限公司、中国民生银行股份有限公司、北京奇虎科技有限公司、亚数信息科技(上海)有限公司。

本文件主要起草人：张秋璞、曹伟、彭竹、李强强、张永强、张庆勇、蒋红宇、虞刚、刘书洪、袁丽欧、霍海涛、张志磊、翟新元。

浏览器数字证书应用接口规范

1 范围

本文件规定了浏览器SM2数字证书应用接口，描述了在支持国产密码算法应用的浏览器中，数字证书应用接口的函数、数据类型和参数的定义。

本文件适用于浏览器产品的开发、应用和检测，支持SM2数字证书的浏览器应用的开发，安全浏览器密码模块的检测，也可用于指导第三方应用调用不同终端设备中SM2数字证书的集成和开发。

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 信息安全技术 公钥基础设施 数字证书格式

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

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0100 人工确权型数字签名密码应用技术要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

SM2密码算法 SM2 cryptographic algorithm

由GB/T 32918.5定义的公钥密码算法。

3.2

数字证书 digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类型可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.3

数字签名 digital signature

签名者使用私钥对待签名数据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。

3.4

证书上下文 certificate context

一种数据结构，用于保存相关的证书信息，证书信息包括拥有者信息、公开密钥、签发者信息、有效期以及扩展信息等。