ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0020—2023
代替 GM/T 0020—2012

证书应用综合服务接口规范

Certificate application integrated service interface specification

2023-12-04 发布　　2024-06-01 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。

本文件代替GM/T 0020—2012《证书应用综合服务接口规范》，与GM/T 0020—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语“数字证书”（见2012年版的3.1）；

b) 增加了Base64格式数据的更明确描述（见6.5）；

c) 增加了接口“证书登出 SOF_Logout”（见7.1.35）、“证书登录状态检测 SOF_IsLogin”（见7.1.36）；

d) 增加了接口“数据摘要 SOF_HashData”（见7.1.31、7.2.37、7.3.38）“文件摘要 SOF_HashFile”（见7.1.32、7.2.38、7.3.39）“摘要值签名 SOF_SignHashData”（见7.1.33、7.2.39、7.3.40）“摘要值验签 SOF_VerifySignedHashData”（见7.1.34、7.2.40、7.3.41）；

e) 删除了接口“SOF_EncryptFile”（见2012年版的7.1.23）“SOF_DecryptFile”（见2012年版的7.1.24）；

f) 增加了“客户端JavaScript脚本接口”（见7.4）。

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：北京数字认证股份有限公司、格尔软件股份有限公司、北京海泰方圆科技股份有限公司、上海市数字证书认证中心有限公司、无锡江南信息安全工程技术中心、中电科网络安全科技股份有限公司、长春吉大正元信息技术股份有限公司、兴唐通信科技有限公司、山东得安信息技术有限公司、北京国脉信安科技有限公司、国家密码管理局商用密码检测中心、中国电子技术标准化研究院。

本文件主要起草人：刘伟、赵永省、刘平、刘蕾、李述胜、郑强、谭武征、蒋红宇、柳增寿、许涛、寇建波、赵丽丽、王妮娜、马洪富、孔凡玉、袁峰、罗鹏、肖秋林、张绍博、上官晓丽、蔡一鸣、黄晶晶。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布版为GM/T 0020—2012；

——本次是第一次修订。

引　言

本文件依托于GM/T 0019《通用密码服务接口规范》,为应用层规定了统一的高级密码服务接口。

证书应用综合服务接口为应用系统提供简洁、易用的证书应用接口,屏蔽了各类密码设备(服务器密码机和智能密码钥匙等)的设备差异性,以及各类密码设备的密码应用接口之间的差异性,实现应用与密码设备无关性,可简化应用开发的复杂性。证书应用综合服务接口分成客户端服务接口和服务器端服务接口两类,可满足B/S和C/S等多种架构的应用系统的调用需求,有利于密码服务接口产品的开发,有利于应用系统在密码服务过程中的集成和实施,有利于实现各应用系统的互联互通。

证书应用综合服务接口规范

1 范围

本文件规定了面向证书应用的综合服务接口。

本文件适用于公钥密码应用技术体系下密码应用服务产品的开发,密码应用支撑平台的研制及检测,也可用于指导直接使用密码设备和密码服务的应用系统的集成和开发。

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 25061—2020 信息安全技术 XML 数字签名语法与处理规范

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0019 通用密码服务接口规范

GM/Z 4001 密码术语

PKCS #1 RSA 加密标准(RSA Cryptography Standard)

PKCS #7 加密消息语法标准(Cryptographic Message Syntax Standard)

IETF RFC 3275 (可扩展标记语言)XML 签名语法和处理[(Extensible Markup Language)XML-Signature Syntax and Processing]

IETF RFC 4648 Base16、Base32 和 Base64 数据编码(The Base16, Base32, and Base64 Data Encodings)

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

用户密钥 user key

存储在设备内部的用于应用密码运算的非对称密钥对。

注:用户密钥包含签名密钥对和加密密钥对。

3.2

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。

4 缩略语

下列缩略语适用于本文件。