ICS 35.040
L 80
备案号:38318—2013

中华人民共和国密码行业标准

GM/T 0020—2012

证书应用综合服务接口规范

Certificate application integrated service interface specification

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 的规则编写。

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这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准中的附录 A 为规范性附录，附录 B 和附录 C 为资料性附录。

本标准起草单位：北京数字认证股份有限公司、上海格尔软件股份有限公司、北京海泰方圆科技有限公司、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、成都卫士通信息产业股份有限公司、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、国家信息安全工程技术研究中心、国家密码管理局商用密码检测中心。

本标准起草人：刘平、李述胜、谭武征、柳增寿、刘承、徐强、李元正、赵丽丽、王妮娜、孔凡玉、袁峰、李志伟。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

引　言

本标准依托于GM/T 0019—2012《通用密码服务接口规范》,向上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上层的应用系统提供简洁、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,屏蔽了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

本标准规定了面向证书应用的统一服务接口。

本标准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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件,凡是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。

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

PKCS #7 Cryptographic Message Syntax

RFC3275 (Extensible Markup Language) XML-Signature Syntax and Processing

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字证书 digital certificate

由认证权威数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.2

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,包含签名密钥对和加密密钥对。

3.3

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:

API Application Program Interface 应用程序接口,简称应用接口

CA Certification Authority 证书认证机构

CN Common Name 通用名