ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0094—2020

公钥密码应用技术体系框架规范

Public key cryptographic application technology framework specification

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。

本文件起草单位：格尔软件股份有限公司、飞天诚信科技股份有限公司、北京信安世纪科技股份有限公司、长春吉大正元信息技术股份有限公司、上海交通大学、成都卫士通信息产业股份有限公司、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、北京国脉信安科技有限公司、北京握奇智能科技有限公司、国民技术股份有限公司、北京天融信网络安全技术有限公司、山东得安信息技术有限公司。

本文件主要起草人：郑强、朱鹏飞、张庆勇、赵丽丽、李强、罗俊、傅大鹏、蒋红宇、药乐、张渊、付月朋、雷晓峰、马洪富。

公钥密码应用技术体系框架规范

1 范围

本文件规定了公钥密码应用技术体系框架，给出该框架内各组成部分及其逻辑关系。

本文件适用于公钥密码应用技术体系的建设及相关标准的制修订，并指导应用系统的密码应用。

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 35275 信息安全技术 SM2密码算法加密签名消息语法规范

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

属性管理系统 attribute authority system

用来产生、签发、发布、更新和撤销属性证书的管理系统。

3.2

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

3.3

证书认证系统 certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

3.4

通用密码应用支撑 common cryptography application support

向典型密码应用支撑和上层应用提供加解密、签名验签等通用密码功能。

3.5

密码设备 cryptography device

包括密码机、密码卡和智能密码终端等设备。

3.6

身份鉴别 authentication

确认一个实体所声称身份的过程。

3.7

典型密码应用支撑 typical cryptography application support

由电子证据、身份鉴别、电子签章、访问控制和时间戳等组成，为上层应用提供对应的密码应用支撑。

3.8

时间戳　time stamp

对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。

3.9

密码资源池　cryptography resource pool

一组密码物理资源或虚拟密码资源的集合，能够对密码资源进行实时监控、合理分配和负载均衡，具有可扩展性、高性能、低风险等特点。

注：密码资源包括密码运算部件、密钥存储部件和随机数发生器等。

4　公钥密码应用技术体系框架

4.1　概述

公钥密码应用技术体系框架包括密码设备服务层、通用密码应用支撑层、典型密码应用支撑层和基础设施安全支撑平台，四部分有机结合组成公钥密码应用技术体系。该体系通过密码设备服务层为通用密码应用支撑层提供服务，通用密码应用支撑层使用密码设备服务层提供的服务为应用系统提供应用支撑，也可以为典型密码应用支撑层提供服务。典型密码应用支撑层直接为应用系统提供典型的密码应用支撑。基础设施支撑平台为密码设备服务层、通用密码应用支撑层和典型密码应用支撑层提供相关的基础服务。

非云计算环境下，密码设备服务层通过密码设备向通用密码应用支撑层提供支撑，基础设施安全支撑平台通过密码设备管理对密码设备进行管理。

云计算环境下，密码设备服务层通过密码资源池向通用密码应用支撑层提供服务。基础设施安全支撑平台通过密码资源管理对密码资源池进行管理，见图 1。

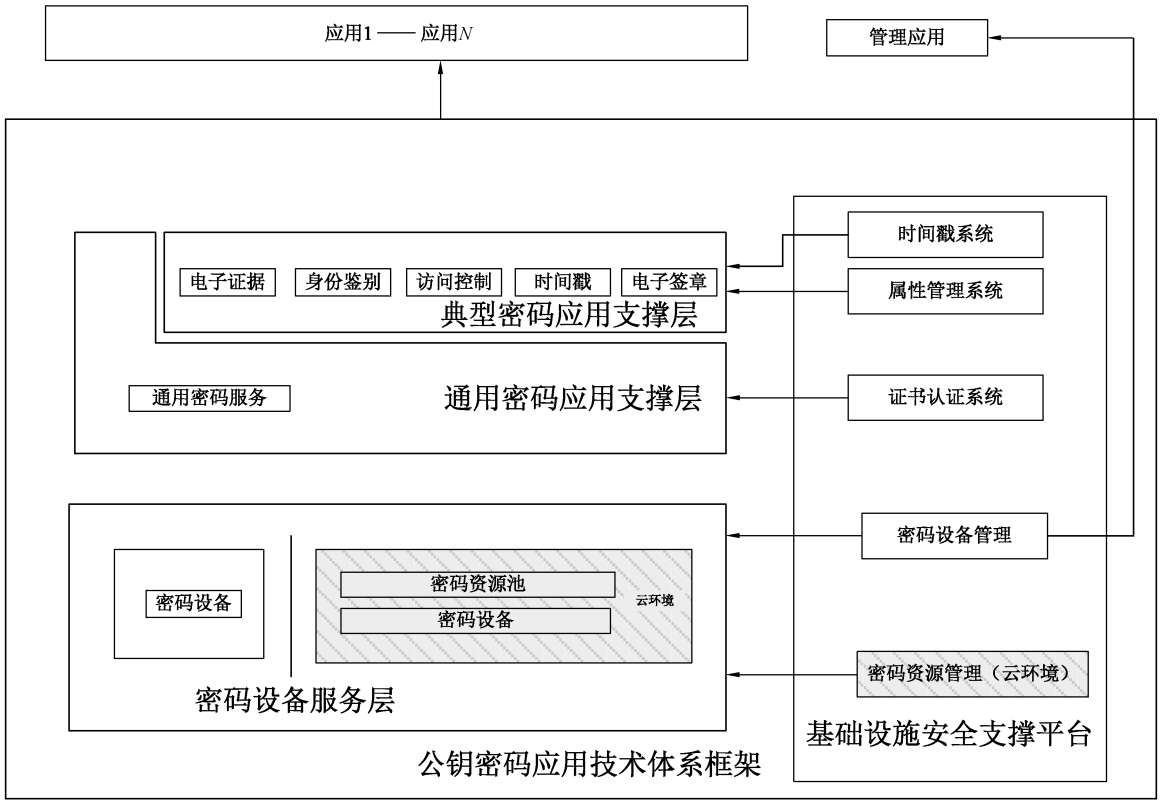

图 1　公钥密码应用技术体系框架图

4.2 密码设备服务层

密码设备服务层由密码模块组成，密码模块包括密码机、密码卡和智能密码终端等设备或密码软件组成，通过密码设备服务接口向通用密码应用支撑层提供密钥管理、密码运算及设备管理等服务，并接受基础设施安全支撑平台的密码设备管理。

在云计算环境下，密码设备服务层由密码设备和密码资源池组成，物理密码设备虚拟化成为虚拟密码设备，按需分配给租户使用。为了对虚拟的密码资源进行有效管理，基础设施安全支撑平台中需要密码资源管理器对密码设备服务层的密码资源进行创建、销毁、配置和漂移等管理。

4.3 通用密码应用支撑层

通用密码服务功能主要包括负责完成与密码设备的安全连接；实现基于数字证书的身份认证，从证书中获取有关信息，实现授权管理、访问控制等安全机制；负责具体与密码设备交互实现具体的密码运算；将数据按照 GB/T 35275 格式进行封装，数据封装格式与应用系统无关性，实现应用系统互联互通和信息共享。

通用密码应用支撑层通过通用密码应用支撑接口，为上层（典型密码应用支撑层和应用层）提供与具体密码设备无关的透明密码应用支撑，将上层的密码应用支撑请求转化为具体的基础密码操作请求，通过统一的密码设备应用接口调用相应密码设备实现具体的密码运算和密钥操作。

通用密码应用支撑包括证书解析、证书认证、信息的机密性、完整性、真实性和不可否认性等密码功能。

通用密码应用支撑层属于中间件，可以单独实现；也可以在保证密钥安全的前提下，采用虚拟化的方式实现。

4.4 典型密码应用支撑层

典型密码应用支撑层由电子证据、身份鉴别、访问控制、时间戳和电子签章等服务组成，为应用层提供对应的应用支撑。典型密码应用支撑层需要的密码功能通过调用通用密码应用支撑接口实现。

电子证据通过标准接口为应用层提供证据采集服务，提供可信证据，实现证据的存储、归档、查询和使用审计等管理功能。

身份鉴别通过标准接口为应用层提供身份查询、身份解析、身份验证等身份鉴别服务。

访问控制通过标准接口为应用层提供系统资源的访问控制，实现用户管理、资源管理、访问控制策略管理和用户授权等功能。

时间戳通过标准接口为应用层和典型密码服务层其他组成部分提供与时间戳系统无关的时间戳加盖、验证等时间认证服务。

电子签章通过标准接口为应用层和典型密码服务层其他组成部分提供电子签章生成与验证服务。

典型密码应用支撑层属于中间件，可以单独实现；也可以在保证密钥安全的前提下，采用虚拟化的方式实现密码设备功能。

4.5 基础设施安全支撑平台

基础设施安全支撑平台由证书认证系统、属性管理系统、时间戳系统、密码设备管理和密码资源管理器等组成。

证书认证系统、属性管理系统和时间戳系统等基础设施安全支撑平台为应用技术体系提供证书管理、密钥管理和时间戳管理等基础服务。

密码设备管理向上层管理应用提供统一的设备管理应用接口，为实现远程密钥管理、设备维护、设备监控等上层管理应用提供设备管理功能，将上层管理应用的管理请求转换为标准的消息调用，通过安

全通道实现管理应用与密码设备间的消息传递。

云计算环境下，基础设施安全支撑平台中的密码资源管理对密码资源进行统一管理，包括对密码资源的隔离、协同、整合和调配等。

4.6 框架内的系列规范

框架内各部分间的逻辑关系见图 2。

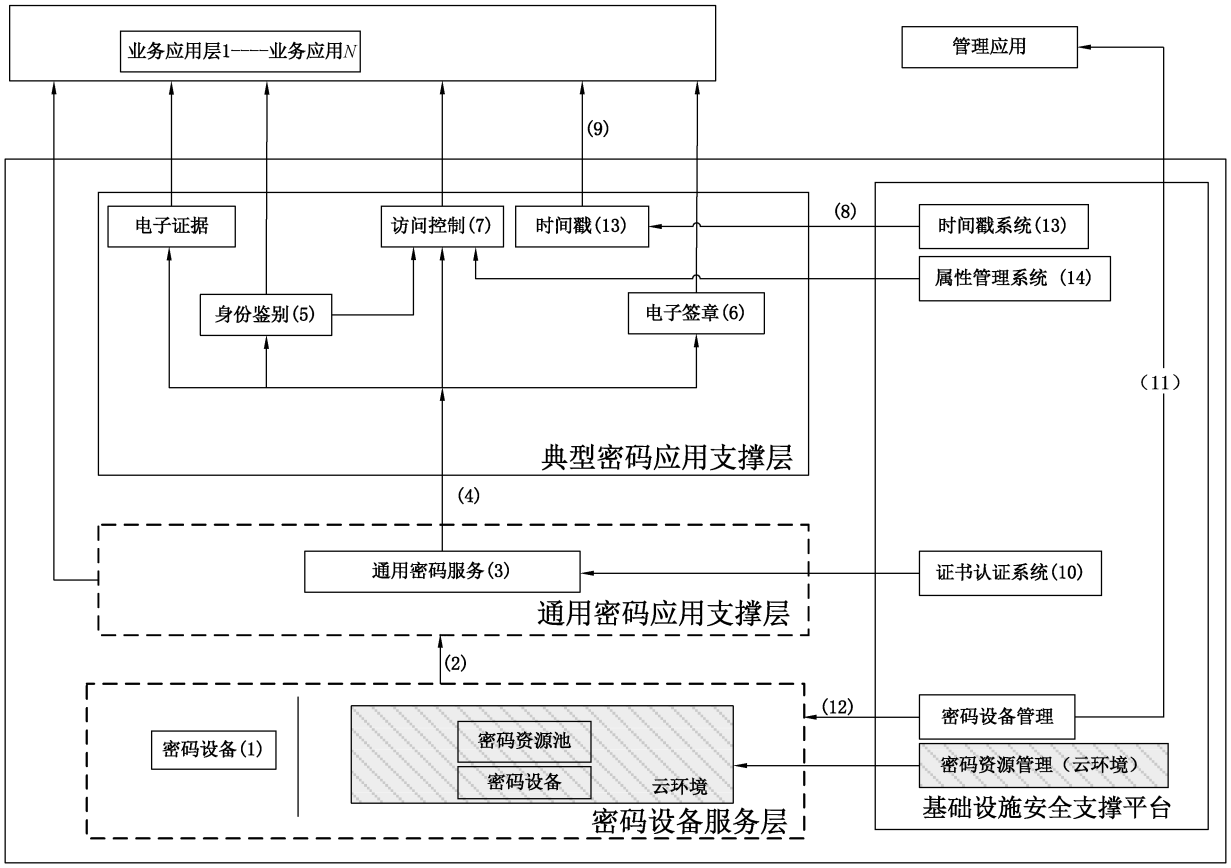

图 2 公钥密码应用技术体系框架逻辑图

4.7 框架内系列标准

本框架内的系列标准包括但不限于：

a) 密码设备（1）：

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0022 IPSec VPN 技术规范

GM/T 0024 SSL VPN 技术规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0029 签名验签服务器技术规范

GM/T 0030 服务器密码机技术规范

b) 密码设备服务层到通用密码应用支撑层(2)：

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0018 密码设备应用接口规范

接口规范中所涉及的接口命名和错误代码区间划分按照附录 A 和附录 B 进行。

c) 通用密码服务(3)：

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

d) 通用密码应用支撑到上层(4)：

GM/T 0019 通用密码服务接口规范

GM/T 0020 证书应用综合服务接口规范

e) 身份鉴别(5)：

GM/T 0026 安全认证网关产品规范

f) 电子签章(6)：

GM/T 0031 安全电子签章密码技术规范

g) 访问控制(7)：

GM/T 0032 基于角色的授权管理与访问控制技术规范

h) 时间戳系统到时间戳(8)：

GM/T 0033 时间戳接口规范

接口规范中所涉及的接口命名和错误代码区间划分按照附录 A 和附录 B 进行。

i) 时间戳到应用层(9)：

GM/T 0033 时间戳接口规范

接口规范中所涉及的接口命名和错误代码区间划分按照附录 A 和附录 B 进行。

j) 证书认证系统(10)：

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

k) 密码设备管理到管理应用(11)：

GM/T 0050 密码设备管理 设备管理技术规范

GM T 0051 密码设备管理 对称密钥管理技术规范

GM/T 0052 密码设备管理 VPN 设备监察管理规范

l) 密码设备管理到密码设备服务层(12)：

GM/T 0052 密码设备管理 VPN 设备监察管理规范

GM/T 0053 密码设备管理 远程监控与合规性检验接口数据规范

接口规范中所涉及的接口命名和错误代码区间划分按照附录 A 和附录 B 进行。

m) 时间戳(13)

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

n) 属性管理系统(14)

GB/T 16264.8 信息枝术 开放系统互连 目录 第 8 部分：公钥和属性证书框架

以上密码行业标准中已有部分标准转化为国家标准，见附录 C。

附 录 A
（规范性）
接 口 命 名

本框架内各规范的接口命名如下：

密码设备应用接口：SDF_XXXXXX；

通用密码服务接口：SAF_XXXXXX；

密码设备管理接口：SMF_XXXXXX；

证据采集与管理接口：SCF_XXXXXX；

身份鉴别接口：SIF_XXXXXX；

授权管理与访问控制接口：SPF_XXXXXX；

时间戳服务接口：STF_XXXXXX；

智能密码钥匙接口：SKF_XXXXXX；

证书应用综合服务接口：SOF_XXXXXX；

电子签章服务接口：SEF_XXXXXX。

附 录 B
（规范性）
错误代码区间划分

本框架内各规范接口分配的错误代码区间为：

密码设备应用接口：0x01000000～0x01FFFFFF；

通用密码服务接口：0x02000000～0x02FFFFFF；

密码设备管理接口：0x03000000～0x03FFFFFF；

证据采集与管理接口：0x04000000～0x04FFFFFF；

身份鉴别接口：0x05000000～0x05FFFFFF；

授权管理与访问控制接口：0x07000000～0x07FFFFFF；

时间戳服务接口：0x08000000～0x08FFFFFF；

智能密码钥匙接口：0x0A000000～0x0AFFFFFF；

证书应用综合服务接口：0x0B000000～0x0BFFFFFF；

电子签章服务接口：0x0C000000～0x0CFFFFFF；

保留将来使用接口：0x0D000000～0xFFFFFFFF。

附 录 C
（资料性）
框架中密码行业标准已转化为国家标准清单

框架中密码行业标准已转化为国家标准清单如下：

a） GM/T 0022《IPSec VPN 技术规范》对应国家标准 GB/T 36968—2018《信息安全技术 IPSec VPN 技术规范》；

b） GM/T 0028《密码模块安全要求》对应国家标准 GB/T 37092—2018《信息安全技术 密码模块安全要求》；

c） GM/T 0016《智能密码钥匙密码应用接口规范》对应国家标准 GB/T 35291—2017《信息安全技术 智能密码钥匙应用接口规范》；

d） GM/T 0009《SM2 密码算法使用规范》对应国家标准 GB/T 35276—2017《信息安全技术 SM2 密码算法使用规范》；

e） GM/T 0010《SM2 密码算法加密签名消息语法规范》对应国家标准 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》；

f） GM/T 0015《基于 SM2 密码算法的数字证书格式规范》对应国家标准 GB/T 20518—2018《信息安全技术 公钥基础设施 数字证书格式》；

g） GM/T 0034《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》对应国家标准 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》。

参 考 文 献

[1] RFC 2560 X.509 互联网公开密钥基础设施在线证书状态协议—OCSP

[2] RFC 2459 X.509 互联网公开密钥基础设施证书和 CRL 轮廓

[3] RSA Security：Public-Key Cryptography Standards (PKCS)

[4] RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[5] RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol

[6] RFC 1777 Lightweight Directory Access Protocol

[7] RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema

[8] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

中华人民共和国密码
行业标准
公钥密码应用技术体系框架规范
GM/T 0094—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 1 字数 25 千字
2021年4月第一版 2021年4月第一次印刷
*
书号:155066·2-35901 定价 18.00 元

GM/T 0094-2020

码上扫一扫 正版服务到