ICS 35.080
CCS L 07

DB36

江 西 省 地 方 标 准

DB36/T 1585—2022

基于政务云平台密码服务技术规范

Technical specification for cryptographic service based on the government cloud platform

2022－05－30 发布　　2022－12－01 实施

江西省市场监督管理局　　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这些专利的责任。

本文件由江西省发展和改革委员会提出并归口。

本文件起草单位：江西省信息中心。

本文件起草人：杜军龙、曹成立、温小雨、龙映辉、何黎明、周剑涛、袁小乐、姜林海、刘曙、潘志安、刘芳芳、张彤、胡章敏、占晓华、熊玲珍、许正义、陈海俊。

引　言

为规范和统一全省政务云平台密码服务系统的体系建设，依据《关于印发江西省政务信息化项目建设管理办法的通知》（赣府厅字〔2020〕68号）、《关于规范省级网络和信息系统商用密码应用与安全性评估工作的通知》（赣国密局字〔2020〕12号）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786）等要求，特制定本规范。

基于政务云平台密码服务技术规范

1 范围

本文件规定了基于政务云平台密码服务总体技术架构,政务云平台密码服务系统资源池和密码服务接口的技术要求。

本文件适用于指导政务云平台密码服务系统建设和政务云平台中云租户的用户终端、网络接入、应用系统、应用数据对密码服务的应用。

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，仅所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。

GB/T 37033 信息安全技术 射频识别系统密码应用技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

GM/T 0062 密码产品随机数检测要求

3 术语和定义

GB/T 39786界定的以及下列术语和定义适用于本文件。

3.1

密码 cryptogram

对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的技术和产品。

3.2

电子政务外网 E-government extranet

电子政务重要基础设施，服务于各级党委、人大、政府、政协、纪委监委、法院和检察院等政务部门，满足其社会管理、公共服务、经济调节和市场监管等方面需要的政务公用网络。电子政务外网支持跨地区、跨部门的业务应用、信息共享和业务协同，以及不需在政务内网上运行的业务。电子政务外网与互联网逻辑隔离。

3.3

政务云 government cloud

用于承载各级政务部门开展公共服务、社会管理等电子政务业务信息系统和数据，及政务门户网站的云计算基础设施，可根据不同业务和需求提供基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。

3.4

政务信息系统 government information system

由政务部门建设、运行或使用的，用于直接支持政务部门工作或履行其职能的各类信息系统。

[来源:GB/T 40692—2021，定义4]

3.5

密码服务系统 cryptographic service system

将云计算技术与身份认证、授权访问、传输加密、存储加密等密码技术深度融合，实现对外提供密码服务的应用系统。

3.6

虚拟化 virtualization

一种资源管理技术，将计算机的各种实体资源（处理器、内存、磁盘空间、网络适配器等），予以抽象、转换后呈现出来并可供分割、组合为一个或多个电脑配置环境。

3.7

密钥 key

控制密码算法运算的关键信息或参数。

[来源:GB/T 39786—2021，定义3.6]

3.8

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

[来源:GB/T 39786—2021，定义3.7]

3.9

租户 tenant

对一个物理和虚拟资源进行共享访问的一个或多个云服务用户。

3.10

资源池化 resource pooling

将云服务提供者的物理或虚拟资源集成起来服务于一个或多个云服务客户的方式。

3.11

保护密钥 protection key

非对称密钥，用于对分发的密钥进行加密保护。

4 缩略语

下列缩略语适用于本文件。

TCP：传输控制协议（Transmission Control Protocol）

IP：互联网协议(Internet Protocol)

SSL：安全套接字协议（Secure Sockets Layer）

IPSEC:互联网安全协议（Internet Protocol Security）

5 密码服务系统

5.1 总体架构

密码服务系统包含密码应用层、中间件层、管理服务层、密码资源层，依托密码安全技术，利用云计算技术，为云平台承载的政务信息系统提供密码应用服务。密码服务系统总体架构如图1所示。

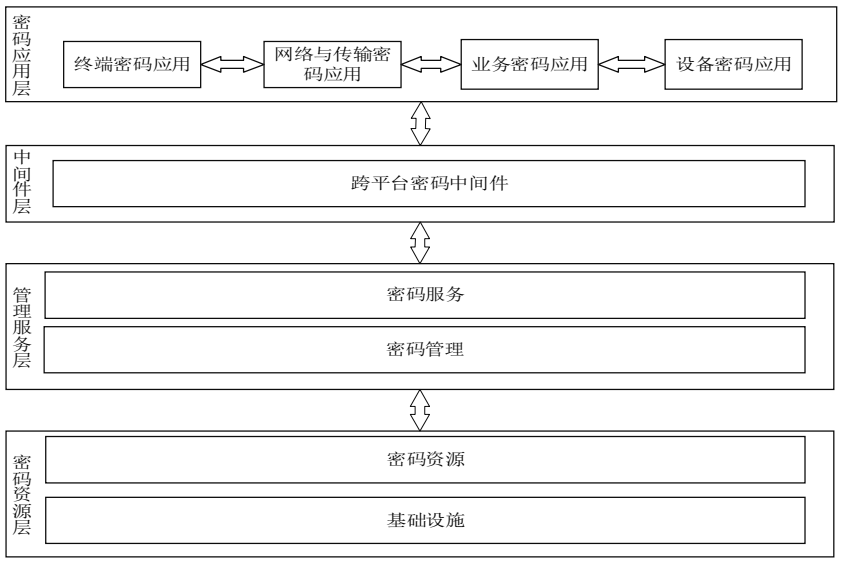

图1 密码服务系统总体架构

5.2 系统层级

5.2.1 密码应用层

密码应用层是密码服务应用范围的统称，密码应用层包括终端密码应用、网络与传输密码应用、业务密码应用和设备密码应用四个方面。

a) 终端密码应用：实现终端用户身份鉴别、终端数据传输和存储安全等；

b) 网络与传输密码应用：实现对应用系统与外部实体之间网络通信的安全防护，例如通信双方身份鉴别、传输安全防护等，确保网络可信接入和安全访问控制；

c) 业务密码应用：实现云平台承载的政务信息系统的身份鉴别、访问控制、数据安全、数据收发行为不可否认性防护；

d) 设备密码应用：通过身份鉴别、权限控制、数据传输保护、操作行为不可否认等技术实现运维管理安全。

5.2.2 中间件层

中间件层提供跨平台密码应用，基于底层密码服务，封装各类通用密码服务接口，制定相应的规范，满足业务应用调用密码服务需求；中间件应支持多种操作系统运行环境。

5.2.3 管理服务层

对云平台承载的政务信息系统提供密码服务，对密码资源层提供密码管理。

5.2.4 密码资源层

密码资源基于密码软硬件设施，主要为密码服务系统提供密钥资源；基础设施由密码软硬件设备构成，为密码资源提供密码应用所需的算力支撑和物理安全保护服务。

5.3 建设要求

5.3.1 总体要求

总体要求如下：

a) 密码服务系统在规划阶段、建设阶段和运行阶段，需根据《商用密码应用安全性评估管理办法（试行）》等相关要求，按照 GB/T 39786 执行，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面采用密码技术措施，建立安全管理制度，采取有效的安全管理措施；
b) 密码服务系统建设完成后，投入运行前应进行密码应用安全性评估，并达到 GB/T 39786 第三级密码应用要求；
c) 政务信息系统建设完成后，建设单位委托国家密码管理部门认定的商用密码应用安全性评估机构对系统开展商用密码应用安全性评估。系统通过商用密码应用安全性评估是项目验收的必要条件；
d) 网络安全等级保护第三级及以上的信息系统、关键信息基础设施、政务信息系统，以及密码相关法律法规和国家有关规定提出明确要求的其他网络和信息系统每年至少开展商用密码应用安全性评估一次。

5.3.2 通用要求

密码服务系统建设应符合以下通用要求：

a) 密码服务系统的基础设施须经过国家密码管理部门核准的商用密码产品；
b) 随机数安全性需满足 GM/T 0062 中的 E 类产品要求，具备出厂检测、上电检测、周期检测、单次检测等随机数检测项目；
c) 密码服务系统中凡涉及对称算法、非对称算法、杂凑算法时，需采用满足国家密码主管部门批准的商用密码算法；
d) 密钥的分发支持物理和在线两种方式。支持密钥数据传输时保护密钥的协商协议，密钥分发机制可提供多种密钥分发策略；
e) 根据不同的安全需求,密码服务系统需提供多种不同安全等级的密钥隔离机制。针对高安全等级场景，能够支持基于硬件虚拟化技术实现的密钥隔离，保证各政务信息系统独享安全密码服

务。

5.3.3 安全要求

5.3.3.1 物理和环境安全

实现对密码服务系统所在机房等重要区域的物理防护，应具备的密码功能包括：

a) 确认进入各重要区域人员的身份，防止无关和假冒人员进入；
b) 保护电子门禁系统进出记录和视频监控音像记录的完整性，防止被非授权篡改。

应结合政务信息系统的网络安全等级选用以下密码应用措施：

a) 部署基于密码技术的电子门禁系统（参考 GB/T 37033、GM/T 0036），对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，并对电子门禁系统进出记录等数据进行完整性保护，数据保留不少于 180 天；
b) 部署基于密码技术的视频监控系统，对视频监控音像记录等数据进行完整性保护，数据保留不少于 180 天。

5.3.3.2 网络和通信安全

实现对密码服务系统与外部实体之间网络通信的安全防护，应具备的密码功能包括：

a) 确保通信实体的身份，防止与假冒实体进行通信；
b) 保护通信过程中的数据，防止数据被非授权篡改，防止敏感数据泄露。

在非安全网络信道中传输敏感数据时，应结合政务信息系统的网络安全等级保护要求部署具有商密型号认证的安全网关类产品，实现通信实体的身份鉴别，通信过程中敏感数据的机密性、完整性保护，网络边界访问控制信息的完整性保护。

5.3.3.3 设备和计算安全

实现对密码服务系统中各类设备和计算环境的安全防护，应具备的密码功能包括：

a) 对设备的特权用户（含系统管理员、系统操作员、审计管理员）和普通用户的身份进行识别和确认，防止假冒人员登录；
b) 在远程管理时，确保信息传输通道的安全，防止远程传输的信息泄漏；
c) 保护计算机、服务器等设备中的系统资源访问控制信息（如设备配置信息、安全策略、资源访问控制列表等）、重要信息资源安全标记（如数据标签等）、日志记录（如系统日志、数据库日志等）和重要可执行程序（如重要应用程序、关键系统文件等），防止被非授权篡改。

在计算机终端和服务器上，应结合政务信息系统的网络安全保护等级选用以下密码应用措施：

a) 在计算机终端上部署智能密码钥匙、动态口令或其他具有身份鉴别功能的密码产品，对登录的用户进行身份鉴别；
b) 为远程管理搭建安全通信链路（如 SSL 通道），保护信息的机密性；
c) 在服务器端部署具有商密型号认证的签名验签服务器或密码机，实现安全计算能力，建立从系统到应用的信任链，保护重要信息的完整性，保证计算环境的安全可信；
d) 在计算机终端上部署、使用国密安全浏览器。

5.3.3.4 应用和数据安全

实现对政务信息系统中应用及其数据的安全防护，应具备的密码功能包括：

a) 确认信息系统的管理员和普通用户的身份，防止假冒人员登录；
b) 对信息系统的访问控制策略（如安全策略、资源访问控制列表等）、数据库表访问控制信息（如用户身份信息、数据库安全策略、用户权限列表等）、重要信息资源安全标记（如数据标签）等进行保护，防止被非授权篡改；
c) 保护客户端与服务器之间、信息系统之间在非安全网络信道中传输的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息等），防止数据泄露；
d) 保护存储的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息等），防止数据泄露、非授权篡改；
e) 保护可能涉及法律责任认定的信息系统中的数据发送和数据接收操作，确保发送方和接收方对已经发生的操作行为无法否认。

应结合政务信息系统的网络安全保护等级选用以下密码应用措施：

a) 部署证书认证系统或直接采用具有电子政务电子认证服务资质的机构提供的电子认证服务，为用户配置智能密码钥匙、智能集成电路卡、移动智能终端密码模块等具备身份鉴别功能的密码产品，对系统用户身份进行管理；
b) 采用智能密码钥匙或动态口令技术，对访问应用服务器的用户进行身份鉴别；
c) 利用 IPSEC/SSL 技术，对客户端与服务器端、信息系统之间传输的数据进行机密性和完整性保护；
d) 部署存储加密产品、服务器密码机或其他密码模块，对存储的重要数据进行机密性和完整性保护；
e) 部署签名验签服务器、服务器密码机或其他密码模块，对访问控制信息、重要信息资源安全标记进行完整性保护；
f) 根据信息系统的需要，部署签名验签服务器、电子签章系统、时间戳服务器等密码产品，对收发的数据及相关操作记录进行签名，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

6 系统功能分区

6.1 功能分区框架

密码服务系统基于软硬件密码设备资源建设，具有独立部署、高兼容性、低耦合性、可拓展性等特点，针对政务云平台不同的政务信息系统，可采用不同的部署方式提供集中的密码服务，密码服务系统功能分区框架如图 2 所示。

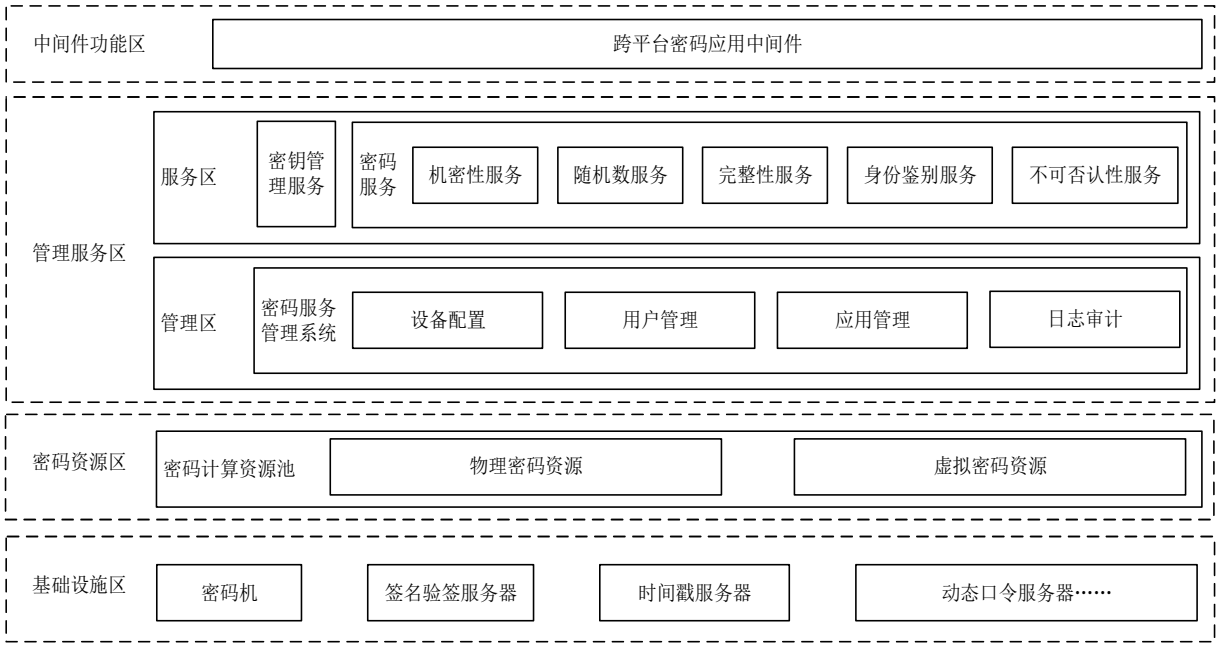

图2　密码服务系统功能分区

6.2　基础设施区

密码服务系统基础设施区由密码设备组成，包括密码机、签名验签服务器、时间戳服务器、动态口令服务器等。密码设备需为国家密码管理局批准型号，相关产品符合国家密码管理局要求。其中，主要密码设备功能如下表所示：

表1　基础设施区功能表

序号	密码设备名称	主要功能
1	密码机	a）密钥产生、存储、使用、备份恢复； b）数据加密、解密； c）数字签名； d）完整性算法。
2	签名验签服务器	a）密钥生成、存储； b）数据签名、验证； c）数字信封功能； d）数据杂凑； e）证书解析； f）证书有效性验证。

表1　基础设施区功能表（续）

序号	密码设备名称	主要功能
3	时间戳服务器	a）密钥生成、存储； b）数据杂凑； c）签发、验证时间戳； d）证书解析； e）证书有效性验证。
4	动态口令服务器	a）动态密码种子生成； b）动态密码验证； c）动态密码管理。

6.3　密码资源区

为支撑云计算环境下的密码应用，密码服务系统应构建密码资源池（包括物理密码资源、虚拟密码资源），通过密码服务管理系统进行密码资源的分配、管理和统一调度，实现按需扩展、灵活配置。密码资源池技术功能包括：

a) 密码资源池的最大服务范围应为一个安全可控区域；
b) 密码资源池应能够根据业务需求进行弹性扩充，并进行统一监控调度和分配，应具有协同处理和容错能力，不因物理安全设备单元的故障或失效影响到整个资源池的正常运行；
c) 通过密码服务管理系统实现对云租户密码服务的管理，包括密码服务需求分解、分配密码资源等；
d) 应保证政务云各租户间密码运算资源及密钥的安全隔离。

6.4　管理服务区

6.4.1　服务区

密码服务系统通过资源池化技术整合底层密码设备资源，提供基于应用程序编程接口、密码中间件等方式的密码资源调用能力。服务包括但不限以下两个方面：

a) 为云租户提供密钥安全管理服务；
b) 为云租户提供数据机密性、随机数、完整性、身份鉴别、不可否认性等密码服务。

6.4.2　管理区

密码服务管理资源提供密码设备、用户、应用、日志审计等管理，充分利用密码设备的运算资源，为密码服务提供密码运算支撑。服务包括但不限以下三个方面：

a) 支持对密码设备、密码资源配置等进行统一管理；
b) 支持对运行的服务进行统一管理；
c) 支持记录并展示重要事件日志。

6.5　中间件功能区

中间件部署在政务信息系统服务端，通过读取配置文件的方式与密码服务系统进行连接，根据不同的连接池配置，提高调用密码服务系统的性能和响应速度；云平台承载的政务信息系统通过中间件调用

密码服务系统的数据签名验签、数据加解密等密码服务接口。

7 服务内容

7.1 密钥管理服务

密钥管理服务需基于密码资源池基础设施，对外提供密钥相关的支撑服务，如密钥托管服务、密钥安全隔离和存储服务、密钥安全访问服务、基于托管密钥的简单加解密服务等，并能够提供统一对外服务接口。应定期跟踪接入政务信息系统数量与密钥使用状态，确保密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等全生命周期的安全。密钥全生命周期管理须符合 GB/T 39786 密钥生存周期管理要求。

7.2 机密性服务

需基于密码资源池中密码机等设备，对外提供统一接口的数据机密性服务。机密性实现算法需涵盖国家密码主管部门批准的算法以及常用国际标准算法。

7.3 随机数服务

需基于密码资源池基础设施，对外提供统一接口的随机数服务。随机数的产生需采用由国家密码管理局批准使用的方式，生成随机数的密码产品应符合GM/T 0062的要求。

7.4 完整性服务

需基于密码资源池基础设施，对外提供统一接口的数据完整性服务。完整性实现算法需涵盖国家密码主管部门批准的算法以及常用国际标准算法。

7.5 身份鉴别服务

需基于密码资源池中签名验签服务器等设备，对外提供统一接口的身份鉴别服务。身份鉴别实现算法需涵盖国家密码主管部门批准的算法以及常用国际标准算法。

7.6 不可否认性服务

需基于密码资源池中签名验签服务器、时间戳服务器等设备，对外提供统一接口的不可否认性服务。不可否认性实现算法需涵盖国家密码主管部门批准的算法以及常用国际标准算法。

8 服务管理规范

8.1 设备配置

设备配置要求应包括：

a) 应具备密码设备挂接的配置功能；
b) 应具备密钥资源的增加、删除、修改功能。

8.2 用户管理

密码服务系统应将用户划分为系统管理员、系统操作员、审计管理员三个角色。

各角色职责如下：

a) 系统管理员：定期安全检查，建立变更管理审核和批准制度；
b) 系统操作员：负责密码设备的日常操作维护；
c) 审计管理员：定期对系统管理员、系统操作员等操作行为进行安全审计和监督检查；对系统运行情况进行审计，形成审计报告。

8.3 应用管理

应用管理要求应包括：
a) 应提供政务信息系统绑定密码资源功能；
b) 应提供 IP 地址访问密码资源白名单功能；
c) 应支持密码资源调用开关控制功能；
d) 应支持密钥使用划分功能。

8.4 日志审计

日志审计要求应包括：
a) 应记录密码服务系统访问运行过程日志数据；
b) 应提供日志查询、搜索、过滤、审计等功能；
c) 应具备对审计前后的信息保存、备查等功能；
d) 应具备审计结果展示功能。

9 服务应用规范

9.1 应用接入流程

9.1.1 申请

政务部门向密码服务系统管理单位提出密码服务使用申请，提交密码服务使用申请，申请内容中需明确密码服务类别，类别包含机密性服务、随机数服务、完整性服务、身份鉴别服务、不可否认性服务等。

9.1.2 审核

密码服务系统管理单位对政务部门的申请进行审核，向政务部门反馈审核结果。满足条件的政务信息系统允许实施密码服务接入，不满足条件的需详细说明理由。

9.1.3 开通

密码服务系统管理单位根据密码服务使用申请内容，合理分配所需密码资源。

9.1.4 上线

密码服务系统管理单位向政务部门提供密码服务系统接入相关材料（见9.2.2），协助政务部门完成上线工作。

9.1.5 变更

密码资源变更分为接入前变更和接入后变更。政务部门向密码服务系统管理单位提出密码资源变更申请，密码服务系统管理单位审核变更材料。审核不通过说明理由，审核通过的依据变更类型做出如下操作：

a) 接入前变更资源：密码服务系统管理单位与政务部门确认审核结果，由密码服务系统管理单位执行变更资源操作，将操作结果告知政务部门；
b) 接入后新增资源：密码服务系统管理单位与政务部门确认审核结果，由密码服务系统管理单位执行新增资源操作，将操作结果告知政务部门；
c) 接入后变更资源：政务部门需提前 15 个工作日向密码服务系统建管理单位提交变更申请，执行系统数据还原、备份、更新等操作，执行完毕后，经政务部门确认，由密码服务系统管理单位按操作流程变更密码服务功能，将操作结果告知政务部门。

9.1.6 终止

政务部门向密码服务系统管理单位发起注销接入申请，密码服务系统管理单位审核并提供15个工作日作为过渡期，用于政务部门将系统数据还原、备份、更新等操作。过渡期满后，经政务部门确认，由密码服务系统管理单位按操作流程注销该政务信息系统密码服务功能，将注销结果告知政务部门。

9.2 应用接口规范

密码服务系统通过中间件以接口方式对外提供密码服务，政务信息系统通过添加依赖库的方式引用中间件调用密码服务系统，政务信息系统与密码服务系统之间须网络畅通。

9.2.1 接口说明

为保证密码服务的安全性，密码服务系统提供的接口须符合如下要求：

a) 调用接口必须对中间件做相应属性配置操作；
b) 数据返回类型参考附录 A 具体内容；
c) 中间件基于 TCP/IP 协议与密码服务系统进行通信。

9.2.2 技术手册

密码服务系统管理单位应为接入密码服务的政务部门提供包括但不限于以下技术手册：

a) 密码服务接口规范文档。包含中间件的接入、使用方式，提供详细接口说明；
b) 密码服务系统技术白皮书。包含密码服务系统主要功能、技术特点以及部署方式；
c) 密码服务资源接入中间件。包含密码服务资源接口，提供使用密码服务资源程序；
d) 密码服务资源接入示范程序。包含密码服务资源使用示例，用于软件开发人员快速部署中间件；
e) 密码服务系统安装部署实施计划文档。包含密码服务系统安装部署实施内容（密码服务组成、实施各阶段内容、实施部署、重难点问题及风险应对等）、实施计划（实施路线、进度计划、阶段任务与交付）、保障措施（人员保障措施、经费保障措施、实施质量保障措施、进度保障措施）等内容。

附录 A
（规范性附录）
密码服务系统接口

A.1 数据结构定义

接口中使用的数据结构以用途分类，各类型数据结构定义如下：

A.1.1 接口返回值数据结构定义

接口返回值数据结构定义说明见表A.1。

表A.1 接口返回值数据结构说明

参数名称	数据类型	说明
id	整型	请求序列号
msgType	整型	返回消息类型
errCode	整型	错误码 0 表示成功，其他对应错误码
errMsg	字符串	错误码说明
mData	数据对象	数据实体，可根据不同接口定义不同数据类型

A.1.2 SM4_CBC对称加/解密数据结构定义

SM4_CBC对称加/解密数据结构定义说明见表A.2。

表A.2 SM4_CBC 对称加/解密数据结构说明

参数名称	数据类型	说明
keyNum	整型	密钥号
key	字节数组	密钥数据
iv	字节数组	向量值
inData	字节数组	待加密的原文

A.1.3 SM4_ECB对称加/解密数据结构定义

SM4_ECB对称加/解密数据结构定义说明见表A.3。

表A.3 SM4_ECB 对称加/解密数据结构说明

参数名称	数据类型	说明
keyNum	整型	密钥号
key	字节数组	密钥数据
inData	字节数组	待加密的原文

A.1.4 摘要方法数据结构定义

摘要方法数据结构定义说明见表A.4。

表A.4 摘要方法数据结构说明

参数名称	数据类型	说明
keyNum	整型	密钥号
Key	字节数组	密钥数据
inData	字节数组	待摘要的原文
algo	整型	算法标识,可设置默认值

A.1.5 SM2 非对称密钥数据结构定义

SM2非对称密钥数据结构定义说明见表A.5。

表A.5 SM2 非对称密钥数据结构说明

参数名称	数据类型	说明
key	字节数组	密钥（用于解密时，此参数值传 null）
keyNum	整型	密钥号
inData	字节数组	输入

A.1.6 HMAC_SM3 带标识的摘要方法数据结构定义

HMAC_SM3带标识的摘要方法数据结构定义说明见表A.6。

表A.6 HMAC_SM3 带标识的摘要方法数据结构说明

参数名称	数据类型	说明
keyNum	整型	密钥号
key	字节数组	密钥数据,用于解密时，此值可为空
inData	字节数组	待摘要的原文

A.1.7 裸签名（带时间戳）返回值数据结构定义

裸签名（带时间戳）返回值数据结构定义说明见表A.7。

表A.7 裸签名（带时间戳）返回值数据结构说明

参数名称	数据类型	说明
signData	字节数组	签名值
dataLength	整型	签名值长度
time	字节数组	时间值
timeLength	整型	时间值长度

A.2 密码服务接口说明

A.2.1 获取公钥（加密公钥）接口

获取公钥（加密公钥）接口说明见表A.8。

表A.8 获取公钥（加密公钥）接口说明

接口功能描述	输入要获取的密钥号，并获得加密公钥值		
接口名称	getEncPubkey		
参数	参数名称	数据类型	说明
	keyNum	整型	密钥号
返回值	通用返回值数据结构		属性数据实体为加密公钥，类型为字节数组

A.2.2 获取签名公钥接口

获取签名公钥接口说明见表A.9。

表A.9 获取签名公钥接口说明

接口功能描述	获取签名公钥		
接口名称	getPubkey		
参数	参数名称	数据类型	说明
	keyNum	整型	密钥号
返回值	通用返回值数据结构		属性数据实体为签名公钥，类型为字节数组

A.2.3 获取摘要接口

获取摘要接口说明见表A.10。

表A.10 获取摘要接口说明

接口功能描述	对数据进行摘要运算		
接口名称	getMsgDigestWithAppWithPid		
参数	参数名称	数据类型	说明
	摘要方法数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为摘要计算结果，类型为字节数组

A.2.4 SM2 签名接口

SM2签名接口说明见表A.11。

表A.11　SM2 签名接口说明

接口功能描述	对数据摘要值进行签名		
接口名称	getSM2Sign		
参数	参数名称	数据类型	说明
	keyNum	整型	密钥号
	msgDigest	字节数组	待签名的原文摘要值
返回值	通用返回值数据结构		属性数据实体签名计算结果，类型为字节数组

A.2.5　SM2 验证签名接口

SM2验证签名接口说明见表A.12。

表A.12　SM2 验证签名接口说明

接口功能描述	对数据签名值进行验证		
接口名称	getSM2Verify		
参数	参数名称	数据类型	说明
	keyNum	整型	密钥号
	key	字节数组	公钥值 密钥号 != 0 时，为空； 密钥号==0 时，为公钥值
	msgDigest	字节数组	签名的原文摘要值
	inData	字节数组	签名值
返回值	通用返回值数据结构		属性错误码值==0 表示验签通过,否则验证不通过

A.2.6　SM4_CBC加密接口

SM4_CBC加密接口说明见表A.13。

表A.13　SM4_CBC 加密接口说明

接口功能描述	SM4_CBC 加密运算		
接口名称	getSM4CBCEnc		
参数	参数名称	数据类型	说明
	SM4_CBC 对称加/解密数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM4_CBC 模式加密计算结果，类型为字节数组

A.2.7　SM4_CBC解密接口

SM4_CBC解密接口说明见表A.14。

表A.14　SM4_CBC 解密接口说明

接口功能描述	SM4_CBC 解密运算		
接口名称	getSM4CBCDec		
参数	参数名称	数据类型	说明
	SM4_CBC 对称加/解密数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM4_CBC 模式解密计算结果，类型为字节数组

A.2.8　SM4_ECB加密接口

SM4_ECB加密接口说明见表A.15。

表A.15　SM4_ECB 加密接口说明

接口功能描述	SM4_ECB 加密运算		
接口名称	getSM4ECBEnc		
参数	参数名称	数据类型	说明
	SM4_ECB 对称加/解密数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM4_ECB 模式加密计算结果，类型为字节数组

A.2.9　SM4_ECB解密接口

SM4_ECB解密接口说明见表A.16。

表A.16　SM4_ECB 解密接口说明

接口功能描述	SM4_ECB 解密运算		
接口名称	getSM4ECBDec		
参数	参数名称	数据类型	说明
	SM4_ECB 对称加/解密数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM4_ECB 模式解密计算结果，类型为字节数组

A.2.10　SM2 公钥加密接口

SM2公钥加密接口说明见表A.17。

表A.17　SM2 公钥加密接口说明

接口功能描述	SM2 公钥加密运算		
接口名称	getSM2PubKeyEnc		
参数	参数名称	数据类型	说明
	SM2 非对称密钥数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM2 公钥加密计算结果，类型为字节数组

A.2.11　SM2 私钥解密接口

SM2私钥解密接口说明见表A.18。

表A.18　SM2 私钥解密接口说明

接口功能描述	SM2 私钥解密		
接口名称	getSM2PrivateDec		
参数	参数名称	数据类型	说明
	SM2 非对称密钥数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 SM2 私钥解密计算结果，类型为字节数组

A.2.12　HMAC_SM3 摘要接口

HMAC_SM3摘要接口说明见表A.19。

表A.19　HMAC_SM3 摘要接口说明

接口功能描述	HMAC_SM3 摘要运算		
接口名称	getHMacSM3		
参数	参数名称	数据类型	说明
	HMAC_SM3 带标识的摘要方法数据结构	数据结构	
返回值	通用返回值数据结构		属性数据实体为 HMAC_SM3 摘要计算结果，类型为字节数组

A.2.13　Detach签名接口

Detach签名接口说明见表A.20。

表A.20 Detach 签名接口说明

接口功能描述	Detach 方式签名		
接口名称	detachedSign		
参数	参数名称	数据类型	说明
	plainText	字节数组	待签名的原文
	subject	字节数组	用于签名的私钥对应的公钥证书的主题
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性数据实体为 Detach 方式签名结果， 类型为字节数组

A.2.14 Detach验签接口

Detach验签接口说明见表A.21。

表A.21 Detach 验签接口说明

接口功能描述	Detach 方式验签		
接口名称	detachedVerify		
参数	参数名称	数据类型	说明
	plainText	字节数组	签名原文
	signData	字节数组	签名值
	needCert	整型	标明是否返回用于验证签名的公钥证书
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.15 不校验证书Detach验签接口

不校验证书Detach验签接口说明见表A.22。

表A.22 不校验证书 Detach 验签接口说明

接口功能描述	不校验证书 Detach 方式验签		
接口名称	detachedVerifyNoCheckCert		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文
	signData	字节数组	签名值
	needCert	整型	标明是否返回用于验证签名的公钥证书
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.16 Attached方式签名接口

Attached方式签名接口说明见表A.23。

表A.23 Attached 方式签名接口说明

接口功能描述	Attached 方式签名		
接口名称	attachedSign		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文
	subject	字节数组	证书主题
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性数据实体为 Attached 方式签名结果， 类型为字节数组

A.2.17 Attached方式验签接口

Attached方式验签接口说明见表A.24。

表A.24 Attached 方式验签接口说明

接口功能描述	Attached 方式验签		
接口名称	attachedVerify		
参数	参数名称	数据类型	说明
	signData	字节数组	签名值
	needCert	整型	标明是否返回用于验证签名的公钥证书
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.18 裸签名（无摘要标识）接口

裸签名（无摘要标识）接口说明见表A.25。

表A.25 裸签名（无摘要标识）接口说明

接口功能描述	裸签名（无摘要标识）		
接口名称	rawSignaturePreHash		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文摘要
	subject	字节数组	证书主题
返回值	通用返回值数据结构		属性数据实体为裸签名（无摘要标识）结果值， 类型为字节数组

A.2.19 裸签名验证（无摘要标识）接口

裸签名验证（无摘要标识）接口说明见表A.26。

表A.26　裸签名验证（无摘要标识）接口说明

接口功能描述	裸签名验证（无摘要标识）		
接口名称	rawVerifyPreHash		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文摘要
	signData	字节数组	证书主题
	cert	整型	用于验签的证书
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.20　裸签名接口

裸签名接口说明见表A.27。

表A.27　裸签名接口说明

接口功能描述	裸签名		
接口名称	rawSignature		
参数	参数名称	数据类型	说明
	plainText	字节数组	待签名原文
	subject	字节数组	证书主题
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性数据实体为裸签名结果值， 类型为字节数组

A.2.21　裸签名验证（传入的参数为证书数据）接口

裸签名验证（传入的参数为证书数据）接口说明见表A.28。

表A.28　裸签名验证（传入的参数为证书数据）接口说明

接口功能描述	裸签名验证（传入的参数为证书数据）		
接口名称	rawVerify		
参数	参数名称	数据类型	说明
	plainText	字节数组	签名原文
	signData	字节数组	签名值
	cert	字节数组	用于验签的证书
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.22　不校验证书裸签名验证（传入的参数为证书数据）接口

不校验证书裸签名验证（传入的参数为证书数据）接口说明见表A.29。

表A.29　不校验证书裸签名验证（传入的参数为证书数据）接口说明

接口功能描述	不校验证书裸签名验证（传入的参数为证书数据）		
接口名称	rawVerifyNoCheckCert		
参数	参数名称	数据类型	说明
	plainText	字节数组	签名原文
	signData	字节数组	签名值
	cert	字节数组	用于验签的证书
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.23　裸签名（带时间戳）接口

裸签名（带时间戳）接口说明见表A.30。

表A.30　裸签名（带时间戳）接口说明

接口功能描述	裸签名（带时间戳）		
接口名称	rawSignatureAddTime		
参数	参数名称	数据类型	说明
	plainText	字节数组	待签名原文
	subject	字节数组	证书主题
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性数据实体为裸签名（带时间戳）的签名结果，数据结构为裸签名（带时间戳）返回值

A.2.24　裸签名验证（带时间戳，传入的参数为证书数据）接口

裸签名验证（带时间戳，传入的参数为证书数据）接口说明见表A.31。

表A.31　裸签名验证（带时间戳，传入的参数为证书数据）接口说明

接口功能描述	裸签名验证（带时间戳，传入的参数为证书数据）		
接口名称	rawVerifyAddTime		
参数	参数名称	数据类型	说明
	plainText	字节数组	签名原文
	signData	字节数组	签名值
	cert	字节数组	用于验签的证书
	time	字符串	时间串，格式“YYYYMMDDhhmmss”

表 A.31 裸签名验证（带时间戳，传入的参数为证书数据）接口说明（续）

接口功能描述	裸签名验证（带时间戳，传入的参数为证书数据）		
参数	参数名称	数据类型	说明
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.25 不校验证书裸签名验证（带时间戳，传入的参数为证书数据）接口

不校验证书裸签名验证（带时间戳，传入的参数为证书数据）接口说明见表A.32。

表A.32 不校验证书裸签名验证（带时间戳，传入的参数为证书数据）接口说明

接口功能描述	不校验证书裸签名验证（带时间戳，传入的参数为证书数据）		
接口名称	rawVerifyAddTimeNocheckCert		
参数	参数名称	数据类型	说明
	plainText	字节数组	签名原文
	signData	字节数组	签名值
	cert	字节数组	用于验签的证书
	time	字符串	时间串，格式“YYYYMMDDhhmmss”
	algoType	整型	摘要算法标识 1:MD2；2:MD5；3:SHA1；5:SHA256；8:SM3
返回值	通用返回值数据结构		属性错误码 =0 表示验签通过

A.2.26 数字信封编码接口

数字信封编码接口说明见表A.33。

表A.33 数字信封编码接口说明

接口功能描述	数字信封编码		
接口名称	evpEncode		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文摘要
	cert	字节数组	用于数字信封编码的证书
返回值	通用返回值数据结构		属性数据实体为数字信封编码结果， 类型为字节数组

A.2.27 数字信封解码接口

数字信封解码接口说明见表A.34。

表A.34　数字信封解码接口说明

接口功能描述	数字信封解码		
接口名称	evpDecode		
参数	参数名称	数据类型	说明
	plainText	字节数组	原文摘要
	cert	字节数组	用于数字信封解码的证书
返回值	通用返回值数据结构		属性数据实体为数字信封解码结果， 类型为字节数组