

SZSD

数 字 山 东 工 程 标 准

SZSD 0028—2024

省统建系统密码中心密码服务建设指南

Guidelines for the construction of cryptographic services of provincial unified
construction system cryptographic center

2024 - 04 - 15 发布

2024 - 06 - 01 实施

山东省大数据局 发 布

目 次

前 言 II

1 范围 3

2 规范性引用文件 3

3 术语和定义 3

4 缩略语 4

5 密码中心 5

6 密码服务 7

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。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

本文件由山东省大数据局提出并归口。

本文件起草单位：山东省大数据中心、智慧齐鲁（山东）大数据科技有限公司。

本文件主要起草人：王伟、李德生、马金钊、沈政。

省统建系统密码中心密码服务建设指南

1 范围

本文件规定了省统建系统密码中心的体系结构、主要功能和密码服务类型等相关信息。
本文件适用于省统建系统密码中心的设计建设和服务管理。

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 25069-2010 信息安全技术术语
GB/T 31167-2014 信息安全技术云计算服务安全指南
GB/T 31168-2014 信息安全技术云计算服务安全能力要求
GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
GM/T 0054-2018 国密信息系统密码应用基本要求
GM/Z 0001 密码术语
GM/T 0018 密码设备应用接口规范
GM/T 0019 通用密码服务接口规范
GM/T 0094 公钥密码应用技术体系框架规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

对称密码算法 `symmetric cryptographic algorithm`

加密和解密使用相同密钥的密码算法。

3.2

非对称密码算法/公钥密码算法 `asymmetric cryptographic algorithm/public key cryptographic algorithm`

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.3

带密钥的杂凑算法 `keyed-hash message authentication code (HMAC)`

一种密码杂凑算法，密钥作为其输入参数参与运算。

3.4

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

3.5

SM3 算法 SM3 algorithm

一种密码杂凑算法，其中输出位256比特。

3.6

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

3.7

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.8

数据完整性 data integrity

数据没有遭受一非授权方式所作的篡改或被破坏的性质。

3.9

抗抵赖性 non-repudiation

也称不可否认性，证明一个已经发生的操作行为无法否认的性质。

3.10

密钥管理 key management

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

3.11

密码系统 cryptosystem

采用密码算法、密码协议、密码设备及相关技术，实现密码功能（加密传输、加密存储、鉴别认证、密钥管理等）的系统。

4 缩略语

下列缩略语适用于本文件。

CHSM：云服务器密码机（Cloud-hosted Hardware Security Module）

MAC：消息鉴别码（message authentication code）

HMAC：带密钥的杂凑算法（Keyed-hash Message Authentication Code）
SLB：服务器负载均衡（Server Load Balance）
VSM：虚拟密码机（Virtual Secure Module）

5 密码中心

5.1 总体架构

密码中心总体架构采用松耦合体系结构，使用云计算技术结合密码技术，为省统建系统提供安全可靠的密码服务。密码中心主要系统包括密码服务系统、密码运维系统、密码资源管理系统和密码资源池。总体架构如图1所示。

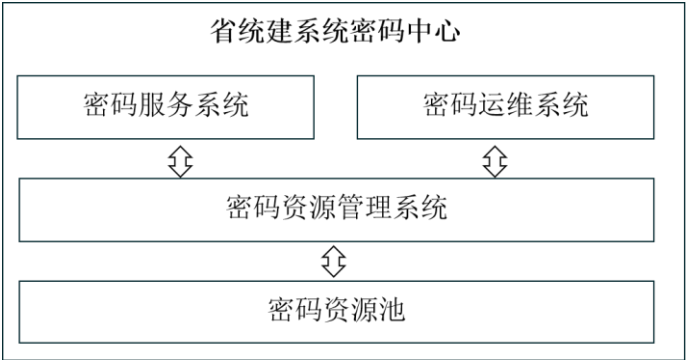


图1 密码中心总体架构图

5.2 密码服务系统

5.2.1 体系结构

密码服务系统具备自助密码服务的能力，为用户提供密码申请、自动开通等服务。密码服务系统包括用户管理、认证管理、服务管理、计量管理、台账管理和应用管理等模块，体系结构如图2所示。

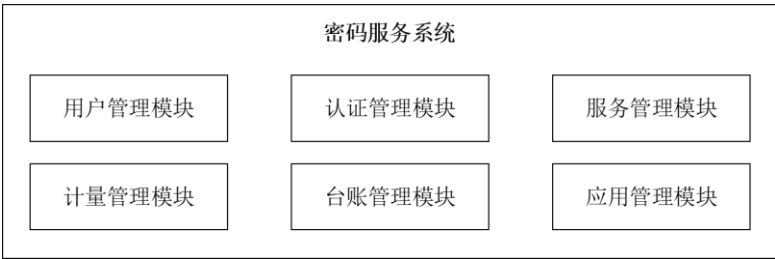


图2 密码服务系统体系结构图

5.2.2 基本功能

密码服务系统基本功能包括密码审批功能、密码服务功能等。

- a) 密码审批功能：提供线上申请开通的密码服务。用户按需向密码中心申请密码服务，经审核批准后，自动开通密码服务。
- b) 密码服务功能：提供按需配置的密码服务。密码服务类别包括机密性服务、完整性服务、抗抵赖性服务、时间戳服务等。

5.3 密码运维系统

5.3.1 体系结构

密码运维系统具备密码服务监管和态势分析能力，实时监控密码服务状态，及时发现问题并告警，并为密码资源扩容和密码服务能力提升提供决策支撑。

密码运维系统包括监控管理、交易管理、报表管理、告警管理、事件管理和态势分析等模块，体系结构如图3所示。



图3 密码运维系统体系结构图

5.3.2 基本功能

密码运维系统基本功能包括密码监管功能、态势分析功能和数据呈现功能等。

a) 密码监管功能：基于标准接口和协议可以及时获取密码设备、服务、密码软模块等密码产品的运行状态、密码资源和服务的使用情况等信息，实现与各类密码设备、密码服务、软件密码模块等密码产品间的集中监管。

b) 态势分析功能：基于数据采集、预处理和存储技术，通过前置采集模块对接密码服务、密码设备、密码系统等信息进行采集和分析。

c) 数据呈现功能：对密码服务和密码资源使用状态进行汇集采集，结合密码合规性标准，形成多维度呈现能力。

5.4 资源管理系统

5.4.1 体系结构

资源管理系统具备统筹纳管密码设备形成密码资源池，并具备密码资源管理和编排等能力，实现密码资源在服务组间的负载均衡、密码资源动态调度。

资源管理系统包括密码网关、密码开放平台、密码中间件等模块，体系结构如图4所示。

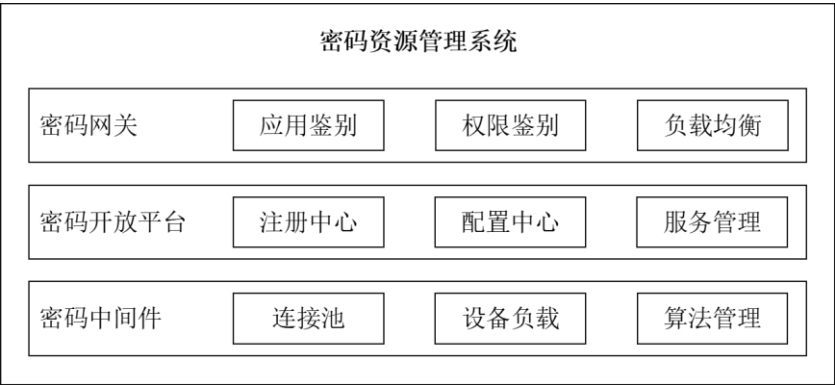


图4 资源管理系统体系结构图

5.4.2 基本功能

资源管理系统基本功能包括密码应用接入功能、密码应用负载功能、密码资源封装功能、密钥管理功能等。

- a) 密码应用接入功能：提供标准的密码应用调用接口，支持多语言环境，使系统可以方便快捷地集成各项密码服务。
- b) 密码应用负载功能：提供应用负载均衡能力，将系统的密码服务请求转发给密码中间件中的密码资源。
- c) 密码资源封装功能：提供纳管密码设备的能力，将密码设备中的密码能力进行封装，对外提供加解密、签名验签、时间戳等密码资源。
- d) 密钥管理功能：提供密钥的全生命周期管理能力，包括密钥生成、存储、分发、启用、禁用、更新、恢复、销毁等。

5.5 密码资源池

5.5.1 体系结构

密码资源池基于虚拟化技术和云管理技术，将密码资源从密码设备中抽离，实现密码资源统一分配、管理和调度，并具有协同处理和容错能力。

密码资源池主要包括服务器密码机、云密码机、签名验签服务器、时间戳服务器等密码设备。密码设备须为国家密码管理局批准型号。体系结构如图5所示。

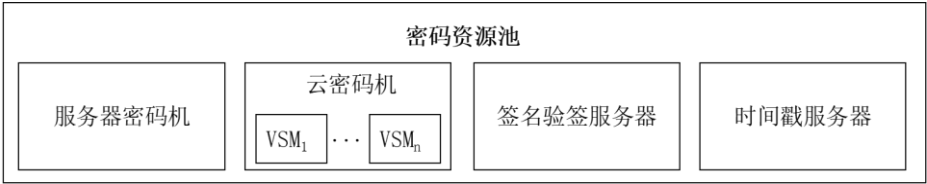


图5 密码资源池体系结构图

5.5.2 基本功能

- 密码资源池具备密码资源配置功能、资源池弹性调度功能和密码资源隔离功能。
- a) 密码资源配置功能：具备定义和划分虚拟密码机不同颗粒度的密码运算能力，实现密码运算能力与虚拟密码机的映射关系。
 - b) 资源池弹性调度功能：具备动态横向扩容密码资源的能力，根据业务需求弹性扩容、灵活配置。
 - c) 密码资源隔离功能：具备各用户间密码运算资源及密钥的安全隔离的能力。

6 密码服务

6.1 机密性服务

机密性服务通过SM4分组对称密码算法，为省统建系统提供应用级数据存储加解密服务，实现重要数据以及文件的机密性保护。

6.2 完整性服务

完整性服务通过SM2算法的数字签名技术、SM3-HMAC技术、SM4-MAC技术，对数据存储和查询过程中进行完整性运算和校验服务，防止数据在存储和使用过程中的非授权篡改，为省统建系统提供数据完整性保护服务。

6.3 抗抵赖性服务

抗抵赖性服务通过使用数字签名、时间戳等密码技术，提供数据原发证据和数据接收证据，实现实体行为的不可否认性，对所需要无法否认的行为进行保护，包括发送、接受、审核、创建、修改、删除、添加、配置等行为。

6.4 时间戳服务

时间戳服务基于时间戳系统，配合签名验签系统或者电子签章服务，为应用系统提供可信安全的时间戳，确保数据的真实性、完整性和可追溯性。

6.5 密钥管理服务

密钥管理服务为省统建系统密钥相关的支撑服务，提供密钥全生命周期管理服务。
