ICS 35.040
L 80
备案号：

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0003-2023

密码服务平台建设、运营及监管基本要求

Basic requirements for password service platform construction operation and supervision

天津市商用密码行业协会 发布

目　　录

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。

本文件由天津市商用密码行业协会提出并归口。

本文件起草单位：天津光电安辰信息技术股份有限公司、天津赢达信科技有限公司、南开大学、北京数字认证有限公司、曙光云计算集团有限公司、天津市大数据管理中心、天翼安全科技有限公司、天津光电通信技术有限公司、中汽研软件测评（天津）有限公司 、中汽数据（天津）有限公司、中国电信集团有限公司天津分公司、天津灵创智恒软件技术有限公司、恒银金融科技股份有限公司、天津云安科技发展有限公司、天津市中环认证服务有限公司、道普信息技术有限公司、北京海泰方圆科技股份有限公司、北京国泰网信科技有限公司。

本文件主要起草人：胡双喜、张秋璞、刘哲理、张俊辉、李忠献、汪定、刘婷、李冰冰、赵小锐、李亮、冯建媛、邵学彬、李岩、王健、高博、吕前进、李戈、王艳荣、徐士元、崔悦、刘越喆、姜洋。

密码服务平台建设、运营及监管基本要求

1 范围

本文件规定了密码服务平台的基本架构、技术体系建设要求、运营体系要求、运维体系保障要求、监管体系要求和测评体系实施要求等内容。

本文件适用于指导密码服务平台的研制、建设和检测，规范天津市密码服务及相关安全技术的应用。

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 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GB/T 31168 信息安全技术 云计算服务安全能力要求

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0022 IPSec VPN技术规范

GM/T 0024 SSL VPN技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0088 云服务器密码机管理接口规范

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GM/Z 0001 密码术语

3 术语和定义

密码服务平台 cryptographic service platform

一种提供密码功能服务和密码资源管理的系统，一般由密码服务管理平台和密码资源池组成，可以为用户提供集中的密码资源管理、密码服务管理、应用接入管理、平台管理功能，为业务系统提供统一的密码功能服务。

密码服务管理平台 cryptographic service management platform

具备平台管理功能、密码资源管理功能、密码服务功能的密码模块。

密码资源 cryptography resources

密码物理资源或虚拟资源的集合，为平台提供各种基础密码能力供密码服务使用。

密码资源池 cryptography resources pool

由多个或多组密码资源组成。

密码资源分组 cryptography resources group

两个或以上密码资源组成的逻辑分组。

密码设备 cryptographic device

为密钥等秘密信息提供安全存储，并基于这些秘密信息提供密码安全服务的设备。本标准中指智能密码钥匙、云服务器密码机、签名验签服务器、时间戳服务器等。

身份鉴别 authentication

确认一个实体所声称身份的过程。

密码提供商 password service provide

为用户单位提供密码应用系统中商用密码设备部署、系统集成总体解决方案的服务提供商。

商用密码应用安全性测评机构 commercial cryptographic application security evaluation institution

具备商用密码应用安全性测评机构管理办法规定的基本条件，通过审核评定，在商用密码应用安全性评估体系中从事测评服务的机构。

商用密码应用安全性评估人员 commercial cryptography application security evaluation staff

商用密码应用安全性评估机构中从事商用密码应用安全性评估的人员，简称“密评人员”。

信息系统责任单位 information system responsible unit

信息系统责任单位是信息系统建设、使用、管理单位，是商用密码应用安全性评估的责任单位。

4 缩略语

TLCP:传输层密码协议（Transport Layer Cryptography Protocol）
IPSec:IP 安全协议(Internet Protocol Security)
SSL:安全套接层协议（Secure Sockets Layer）

5 建设框架

密码服务平台建设框架如图 1 所示。

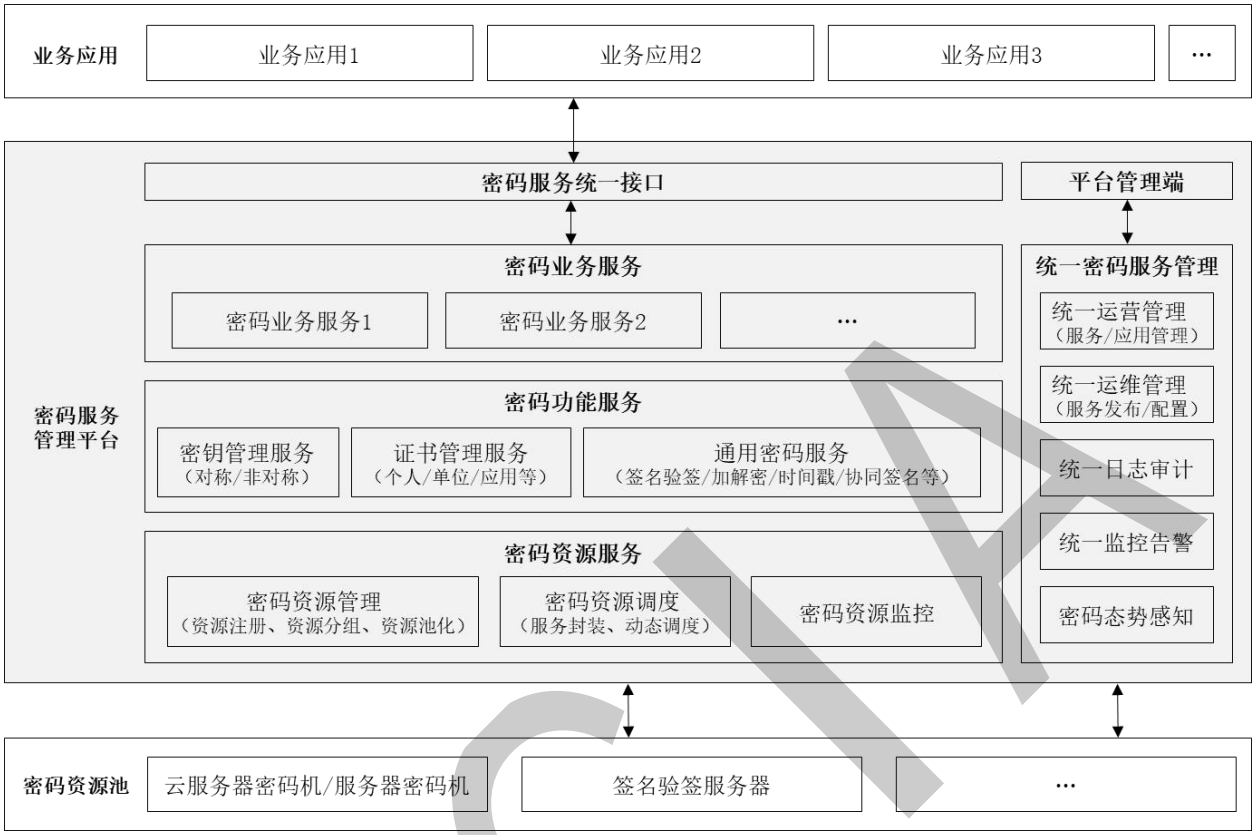

图 1　密码服务平台参考模型

密码服务平台参考模型划分为密码服务管理平台、密码资源池两部分。其功能划分如下：

a)　密码服务管理平台

密码服务管理平台的核心功能及服务模块包括：

密码服务接口：作为后台服务的对外载体，能够将密码服务进行能力封装，对外提供统一的接入网关访问入口，实现密码服务能力的共享。

密码资源服务：基于云容器技术，将密码资源进行虚拟化，能够实现对不同厂商、不同类型密码设备的统一纳管，将密码设备作为密码资源，以池化方式进行统一调度，有效屏蔽密码资源差异性。

密码功能服务：通过开放服务的方式提供标准密码服务，涵盖绝大多数的密码及泛密码服务，能够面向业务应用以及上层密码业务服务提供标准、可靠的密码服务，有效屏蔽密码上云的底层复杂度。

密码业务服务：通过将密码功能的业务化服务封装，形成若干业务逻辑上相互独立的业务单元，提供数字信任和数据安全服务的完整交付，满足不同的场景化密码需求。

统一密码服务管理：面向平台各层服务提供实时自动化、智能化的管理能力支撑，为平台高效、安全、灵活的运营工作提供平台化赋能。

b)　密码资源池

密码资源池由多个或多组物理的或虚拟的密码资源组成，为平台提供各种基础密码能力供密码服务使用。

6 密码服务平台技术体系建设要求

6.1 密码资源管理要求

6.1.1 密码资源管理

密码服务平台应满足：

a） 接入的各种密码资源应是经商用密码检测认证合格的密码产品；
b） 接入的密码机设备应符合 GM/T 0018，云服务器密码机应符合 GM/T 0088，其他密码设备应符合相应的标准要求；
c） 应支持不同厂商、不同类型密码资源的接入与删除；
d） 密码资源接入时应进行设备标识、设备型号录入、设备可用性校验，并获取设备厂商、设备类型等相关基础信息进行维护；
e） 密码资源管理应符合 GM/T 0050 和 GM/T 0051。

6.1.2 密码资源分组

密码服务平台应满足：

a） 应支持对密码资源分组进行新增、删除等管理；
b） 应支持分组内密码资源的添加与移除；
c） 不同分组间密钥及其他敏感安全参数应隔离；
d） 应支持分组间密钥及其他敏感安全参数的同步，同步过程中应采用密码技术手段保证数据的机密性和完整性。

6.1.3 密码资源调度

密码服务平台接入的密码设备可以根据业务系统密码服务需求，通过组合调度构成虚拟机集群，并通过统一的密码设备接口为业务系统提供密码服务，具体应满足：

a） 应支持密码资源动态调度，包括但不限于密码机调度服务、签名验签服务器调度服务和时间戳服务器调度服务，对密码资源进行统一的调度和分配，提高密码资源利用率；
b） 应支持基于密码服务请求的压力情况进行密码资源动态扩展；
c） 应支持为接入业务系统划分独立使用的密码资源。
d） 应支持对调度服务的版本管理，并支持灰度发布能力。

6.1.4 密码资源监控

密码服务平台应满足：

a） 应支持对密码资源进行健康检测，发现资源异常时，能够停止对该资源的调度并采取处置措施；
b） 应支持对密码资源进行全局密码资源使用监控，包括密码资源监控、应用使用情况等。

6.2 密码功能服务要求

密码服务平台提供密码服务时，应满足：

a） 至少支持一类密码服务：加解密、签名验签、时间戳、协同签名、身份鉴别等；
b） 应基于密码技术实现对接入密码服务平台的业务系统的认证，包括但不限于对称、证书、哈希运算消息认证码（HMAC），记录必要的业务系统信息，产生并分配该业务系统访问密码服务平台的唯一认证凭据；
c） 应支持提供密钥全生命周期的管理能力，涵盖对称和非对称密钥的产生、分发、存储、导入导出、使用、更新、轮转、归档、备份和恢复、销毁等管理功能，密钥的产生应该使用经过商用密码检测机构检测认证的密码产品产生；
d） 应支持用户证书和设备证书的签发、全生命周期管理以及证书查询服务；

e） 应支持对密码服务的管理，包括启动、停止、创建、删除和修改；
f） 密码服务平台与接入业务系统间应建立安全通道保障数据传输安全；
g） 应支持对系统内存储的业务系统认证凭据等重要数据和敏感信息进行机密性和完整性保护；
h） 应通过密码服务接口向业务应用提供密码服务，密码服务接口可支持不同的实现形式。

6.3 密码业务服务要求

密码服务平台应满足:
a） 应支持至少一类密码业务服务的接入：电子签章服务、身份核验服务、电子认证服务、电子合同服务等。

6.4 平台管理功能要求

密码服务平台应满足：
a） 应支持对接入业务系统信息进行维护、变更；
b） 应支持配置访问控制策略，并根据访问控制策略控制接入业务应用对密码服务平台的访问；
c） 平台管理端与密码服务平台间应建立安全通道保障数据传输安全；
d） 应对系统内存储的用户认证凭据等重要数据和敏感信息进行机密性和完整性保护；
e） 应支持密码资源运维管理能力，提供可视化密码资源运维监控与统计分析；
f） 应提供完整的密码服务统一接口全生命周期管理能力，包括但不限于添加、发布、版本迭代、废弃；
g） 应支持基于密码服务统一接口进行认证授权，严格控制访问数据权限，避免越权访问造成数据泄露；
h） 应支持对密码服务接口进行监控，包括密码服务接口可用性、接口使用情况等。

6.5 平台安全要求

6.5.1 密码算法

密码服务平台中使用的密码算法，应采用符合国家密码管理部门要求的密码算法。

6.5.2 密码技术、密码产品和密码服务

平台建设使用的密码技术、密码设备、密码服务应为通过商用密码检测认证机构认证的商用密码产品及服务，且满足GB/T 39786中规定的对应等级要求。

6.5.3 密钥管理

密码服务平台应支持密钥全生命周期安全管理，包括密钥的产生、分发、存储、导入导出、使用、更新、轮转、归档、备份与恢复、销毁等环节，应满足如下要求：

a） 密钥产生

密钥产生管理应按照密码管理部门统一规划实施,应在经商用密码检测认证合格的密码部件或模块内部产生；密钥产生及协商应使用符合 GM/T 0005 要求的随机数。

b） 密钥分发

密钥分发应采取安全措施，防止在分发过程中泄露、修改和替换。

c） 密钥存储

密钥应以安全形式或密文形式存储。

d） 密钥导入导出

密钥应采取加密或知识拆分等安全方式进行导入导出。

e） 密钥使用

密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用私钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换。

f） 密钥更新

应按照密钥更新周期要求更新密钥，并采取有效的安全措施，保证密钥更新时的安全性。

g） 密钥轮转

应提供密钥自动轮转能力，支持密钥轮转策略配置。

h） 密钥归档

支持通过界面方式对即将归档与已归档的密钥进行管理，并对归档的密钥提供长期的安全存储。

i） 密钥备份与恢复

若支持密钥备份与恢复，应以知识拆分或密文形式备份到安全存储介质中，应支持以安全形式恢复备份的密钥；密钥备份或恢复应进行记录并生成审计信息。

j） 司法密钥恢复

应支持司法密钥恢复审核，可对密钥的申请人、密钥持有人、申请人联系方式、密钥标识等进行审核。

k） 密钥销毁

应具备在正常情况和紧急情况下的销毁密钥措施；密钥销毁应进行记录，并生成审计信息。

6.5.4 通信安全

密码服务平台与平台管理端或业务应用之间应建立安全通道;密码服务平台需要远程调用或管理密码资源时，密码服务平台与密码资源之间应建立安全通道。安全通道应满足：

a） 采用 IPSec 协议时，应符合 GM/T 0022；

b） 采用 TLCP 或 SSL 协议时，应符合 GB/T 38636 或 GM/T 0024；

6.5.5 软件安全

密码服务平台应满足：

a） 应支持对密码服务平台自身的软件完整性和重要配置完整性进行验证；

b） 所有的安全协议及管理软件应自主实现。

6.5.6 身份鉴别

密码服务平台应满足：

a） 应具备身份鉴别机制，鉴别机制应符合 GB/T 15843；

b） 应采用具备密码二级资质及以上的产品，实现管理员身份的鉴别，并满足双因子身份鉴别。

6.5.7 安全审计

密码服务平台应满足：

a） 应对日志记录进行保护，避免受到未授权的访问和未预期的删除、修改或覆盖等；

b） 应使用密码技术保证日志记录的完整性；

c） 应提供安全审计功能，对系统自身运行状态和涉及系统安全的行为、人员、时间的日志记录进行跟踪、统计和分析。

6.5.8 隔离安全

密码服务平台应满足：

a） 应使用密码技术保证接入业务系统对统一密码服务接口和密码资源访问控制信息的完整性；

b） 应使用密码技术保证密码服务平台用户访问控制信息的完整性；

c） 应保证接入业务系统的密钥数据相互独立、不可相互使用。

6.5.9 数据安全

密码服务平台应满足：

a） 应保证重要数据传输和存储机密性要求：用户身份鉴别信息、用户隐私敏感信息、虚拟资源镜像文件、虚拟资源快照、重要业务数据等需要保证在传输过程中以及存储时的机密性保护要求；

b） 重要数据传输和存储完整性要求：进行机密性保护的重要数据以及授权信息、应用配置信息、资源配置信息、重要程序、重要标识数据、日志数据、审计数据在数据传输和存储过程中的完整性保护要求。

6.5.10 监管要求

密码服务平台应满足：

a） 应提供安全分析数据上报接口，并实现与监管平台的集成；
b） 应构建安全的数据传输链路，确保安全分析数据的传输机密性和完整性。

6.6 密码应用合规性要求

密码服务平台应符合以下合规性要求：

a） 使用的密码算法应符合国家法律、法规的规定及密码相关国家标准、密码行业标准的有关要求；
b） 使用的密码技术应符合密码相关国家标准、行业标准或经国家密码管理部门审查认定；
c） 使用的密码产品应经商用密码检测认证合格；
d） 使用的密码服务应经国家密码管理部门审查认定；
e） 应通过商用密码产品检测，并获得商用密码产品认证证书；
f） 应对密码服务平台进行商用密码应用安全性评估，检测评估执行方应具备相关的测评资质。测评应每年进行一次，测评分值应达到商用密码安全性评估阈值。

7 密码服务平台运营体系运行要求

7.1 平台运营服务要求

密码服务平台应面向平台建设方的提供运营服务，包括但不限于：

a） 平台业务运营服务：应驻场于平台建设方，替代平台建设方完成面向租户的服务开通、变更等运营工作，并定期向平台建设方进行汇报；
b） 平台方案规划服务：应驻场于平台建设方，根据租户使用情况、租户业务需求、平台运行情况进行平台功能、部署等优化升级方案编写；
c） 平台开发支持服务：应驻场于平台建设方，根据平台优化升级方案完成平台功能开发工作；
d） 培训服务：应根据平台建设方需求提供运营培训、开发培训；
e） 平台运维服务：应提供密码服务平台及相关密码设备的运维工作；
f） 技术巡检服务：应提供平台实时监控工具，基于监控数据定期对平台软件、服务器、网络设备、密码设备进行技术巡检，并出具巡检报告。

7.2 租户运营服务要求

密码服务平台应面向租户提供运营服务，包括但不限于标准服务和增值服务。其中，标准服务应根据租户要求进行服务，包括但不限于：

a） 租户方案规划服务：应面向租户进行调研，提供业务系统接入密码服务平台的技术方案；
b） 业务开通指导服务：应指导租户运营人员进行账户开通及业务开通；
c） 应用接入指导服务：应指导租户开发人员按照技术文档对接密码服务平台；
d） 租户开发支持服务：应对租户开发人员进行密服平台对接技术指导或替代租户开发人员完成对接；
e） 培训服务：应根据租户需求提供运营培训、开发培训；
f） 租户业务运营服务：应替代租户运营人员完成运营工作，并定期对租户进行汇报。

增值服务需由租户单独提交服务开通申请，包括但不限于：

a） 电子签章服务：可对接密码服务平台，提供电子签章服务；
b） 电子合同服务：可对接密码服务平台，提供电子合同服务；
c） 数字证书服务：可对接密码服务平台，提供数字证书服务；
d） 密码咨询和培训服务：可根据租户需求提供密码咨询和培训服务。

7.3 服务流程规范要求

密码服务平台的运营服务流程应符合：

a） 应建立运营服务中心，保障密码方案完整落地和有效应用；
b） 应编制密码服务平台密码服务运营流程规范，包括但不限于：账户开通流程、服务开通流程、方案支持流程、技术支持流程、应急处理流程。

7.4 运营管理规范要求

密码服务平台运营规范的建设应符合：

a） 应制定密码服务平台运营体系建设相关监管规范，包括但不限于：应用集成指南、应用接口规范、应用管理办法、人员管理办法、运营考核制度；
b） 应制定密码服务平台运营体系建设相关服务汇报、服务考核制度。

8 密码服务平台运维体系保障要求

8.1 运维服务内容要求

应提供密码服务平台运维体系建设服务，服务内容包含但不限于：
a） 系统日常运维支持：应驻场于平台建设方，提供密码服务平台日常运行维护工作，包含但不限于：系统运行监控、日常数据调整、运维流程的设定与标准化；
b） 软件故障诊断和处理：应驻场于平台建设方，配合平台建设方解决密码服务平台在运行过程中出现的故障及问题，根据平台建设方要求及时协调进行分析处理；
c） 软件升级：技术支持服务期内，应负责为密码服务平台安装最新的补丁包和升级补丁；
d） 健康检查：应定期对各节点的密码服务平台运行情况进行健康检查，提供预防性维护服务；
e） 数据维护：应严格按照数据处理流程，对系统运行过程中遇到系统升级、系统异常、业务异常等情况产生的部分异常或错误数据进行调整和恢复；
f） 性能调优：应根据系统监控或健康检查情况，对系统软件进行性能优化；
g） 系统迁移：技术支持服务期内，应对各节点提出的系统迁移需求提供远程或必要的现场技术支持；
h） 备份和恢复：应提供定期对密码服务平台的数据库、中间件、应用系统等的备份与恢复工作，确保系统运行状态和数据的正确性；
i） 应急响应：应根据平台建设方要求，制定应急响应方案，开展应急响应演练等工作；
j） 重点保障：应根据平台建设方要求，在重大节假日以及平台建设方事先告知的关键时间节点，提供现场值守等重点保障服务；
k） 知识库管理：应定期对故障处理报告进行分类、统计、汇总、分析，逐步完善日常运维知识库，并提交平台建设方归档留存。

8.2 运维管理制度要求

密码服务平台运维服务应符合：

a） 应编制密码服务平台运维管理制度，建立长效运行的服务标准；
b） 密码服务平台运维体系建设相关管理制度应包括但不限于：密码应用安全管理制度、密钥管理制度、合规操作章程、应急处置制度、响应支持制度、监管评估制度、团队建设制度、运营考核制度等。

8.3 运维流程规范要求

密码服务平台运维服务应符合：
a） 应编制密码服务平台运维流程规范，保证密码服务的合理性；
b） 应制定密码服务平台运维体系建设的流程规范，包括但不限于：系统建设流程、服务开通流程、工程验收流程、密钥生命周期使用流程、人员管理流程、应用集成流程、系统上线流程、系统升级流程、应急处理流程。

9 市密码应用监管要求

9.1 密码服务建设方监管要求

密码管理部门应对本地区的密码服务建设方进行统一监管，应符合以下要求：
a) 密码服务建设方实行市、区两级属地化管理；
b) 区级密码管理部门应对本地区密码服务建设方进行备案管理，统一报送至市级密码管理部门；
c) 区级密码管理部门应对密码服务建设方建设的密码应用系统阶段状态进行备案，包括密码应用规划、密码应用建设、密码应用运行、密码应用终止四个阶段状态，统一报送至市级密码管理部门。

9.2 密码提供商监管要求

密码提供商应对其提供的密码产品及服务在本地密码协会进行登记备案，依法开展密码服务，接受本地密码协会的行业自律管理。

9.3 密码产品及服务监管要求

密码管理部门应对本地区的密码产品和服务进行统一监管，应符合以下要求：
a) 密码产品及服务实行市、区两级属地化管理；
b) 区级密码管理部门应对密码服务商提供的密码产品和服务，按照商密产品认证目录进行分类管理，统一报送至市级密码管理部门。

9.4 密码应用系统监管要求

密码管理部门应对接入密码服务平台的信息系统的密码应用系统进行统一监管，应符合以下要求：
a) 密码应用系统实行市、区两级属地化管理；
b) 区级密码管理部门应对密码应用系统分类管理，包括关键信息基础设施、政务密码应用系统、重要工业控制系统、重要密码应用系统、基础信息网络等类别，统一报送至市级密码管理部门；
c) 区级密码管理部门应对本地区信息化系统密码应用方案开展商用密码应用安全性合规性审查，统一报送至市级密码管理部门；
d) 市级密码管理部门根据工作需要，不定期对本地区重要领域网络与信息系统开展商用密码应用安全性专项检查。

9.5 密码应用态势监管要求

市级密码管理部门应对密码服务平台提供的密码服务态势进行统一监管，应符合以下要求：

a） 应实现对密码算法、密码协议应用合规性的监管；

b） 应实现对数据的密码应用有效性的监管；

c） 应实现对密码资源的服务请求量、资源服务趋势、资源异常的实时监控；

d） 应实现密码资源的智能巡检；

e） 应实现对密码资源使用历史数据进行统计分析汇总。

10 接入密码服务平台的信息系统密码应用测评要求

10.1 测评实施要求

测评机构在开展信息系统测评过程中，应符合以下要求：

a）合规性评估：判断信息系统使用的密码算法、密码协议、密钥管理是否符合法律法规、国家标准、行业标准的相关要求，使用的密码产品和密码服务是否经过国家密码管理部门核准或由具备资格的机构认证；

b）正确性评估：判断密码算法、密码协议、密钥管理、密码产品和服务使用是否正确，即系统中采用的标准密码算法、协议和密钥管理机制是否按照国家和行业标准进行正确的设计和实现，自定义密码协议、密钥管理机制的设计和实现是否正确，安全性是否满足要求，密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确；

c）有效性评估：判定信息系统中实现密码保障系统是否在信息系统运行过程中发挥了实际效用，是否满足了信息系统的安全需求，是否切实解决了信息系统面临的安全问题。

10.2 测评监管要求

10.2.1 测评机构监管

密码管理部门应对本地区的测评机构进行统一监管，应符合以下要求：

a）测评机构应遵循密码法中的市场准入管理制度要求；

b）本地区密码管理部门对符合该要求可进入本地市场并具有相关密码测评资质的单位进行统一备案管理。

c）进入本地市场并具有相关密码测评资质的单位应在本地密码协会进行登记，依法开展密码测评服务，接受本地密码协会的行业自律管理。

10.2.2 测评服务监管

密码管理部门对信息系统测评过程进行监管，应符合以下要求：

a）测评项目实施过程中，测评机构应接受国家密码局、本地区密码管理部门的监督管理；

b）本地区密码管理部门可对测评机构备案资质，测评服务全过程进行监管，可随机对测评服务进行抽查；

c）对于登记备案的密码测评机构开展的密码测评服务应符合制定的相关测评服务标准，接受本地密码协会的行业自律管理。

d）测评机构应当在年底编制商用密码应用安全性评估工作报告，并报送本地区密码管理部门。

10.2.3 整改监管

对于测评报告中责令整改的信息系统，本地区密码管理部门应对信息系统进行整改，并对整个过程进行监管，监管内容包括整改内容、整改周期、整改进度。