ICS 35.040
L 80
备案号：

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0002-2022

云密码支撑服务基本要求

Basic requirements for cloud cryptographic support services

2022-9-19发布

天津市商用密码行业协会 发布

目 次

前　言

本文件按照GB/T1.1-2020《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。本文件由天津市商用密码行业协会提出并组织实施。

本文件由天津市信息安全标准化技术委员会归口。

本文件起草单位：天津光电通信技术有限公司，标准的参与单位为天津灵创智恒软件技术有限公司、南开大学、天津赢达信科技有限公司、天津光电安辰信息技术股份有限公司、天津国芯科技有限公司、恒银金融科技股份有限公司、麒麟软件有限公司、飞腾信息技术有限公司、天津中网基业智能系统工程有限公司、天津市中环认证服务有限公司、中国电信集团有限公司天津分公司、天津云安科技发展有限公司、中互金认证有限公司、天津恒御科技有限公司、安云印（天津）大数据科技有限公司、北京数字认证有限公司天津分公司、江西智慧云测安全检测中心股份有限公司。

本文件主要起草人：李忠献、汪定、张俊辉、张秋璞、胡双喜、张斌、张云峰、刘博、冯彦朝、牛昱、崔悦、王健、徐士元、李文宝、修凤洲、毛乃峥、高博、王泽。

云密码支撑服务基本要求

1.范围

本文件规定了云密码支撑服务的基本要求，从服务能力建设、安全要求、应用规范、管理运营、测评五个层面提出了云上密码支撑服务的技术要求。

本文件适用于指导、规范云上密码支撑服务的规划、建设及运行，也可供第三方评估机构对云上密码支撑服务进行安全测评时参考。在本文件基础上，各领域与行业可结合本领域与行业的密码应用需求来指导、规范相关云上密码支撑服务。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 39786 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

GB/T 39786 和 GM/Z 0001 界定的以及下列术语和定义适用于本文件。

云计算 cloud computing：通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并可按需自助获取和管理资源的模式。

云服务商 cloud service provider：云计算服务的供应方。

云服务客户 cloud service customer:为使用云计算服务同云服务商建立业务关系的参与方。

云计算基础设施 cloud computing infrastructure: 由硬件资源和资源抽象组件构成的支撑云计算的基础设施。

云计算平台 cloud computing platform staff: 云服务商提供的云基础设施及其上的服务软件的集合。

Restful API Restful application programming interface: 符合 REST 网络服务架构形式的应用程序接口。

第三方评估机构 Third party assessment organization: 独立于云计算服务相关方的专业评估机构。

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”。

核查 examine: 密评人员对测评对象进行观察、查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

4.缩略语

下列缩略语适用于本文件：

API：应用程序接口（application programming interface）

CA：证书认证机构（certificate authority）

Caas：密码即服务（cryptography as a service）

IaaS：基础设施即服务（Infrastructure as a service）

JSON：JavaScript 对象表示法（JavaScript object notation）

PaaS：平台即服务（platform as a service）

PQA：后量子密码算法（post-quantum cryptographic algorithm）

PKI：公钥基础设施（public key infrastructure）

REST：表述状态转移（representational state transfer）

SaaS：软件即服务（software as a service）

SDK：软件开发包（software development kit）

SLA：服务水平协议（service Level agreement）

SM2：SM2 椭圆曲线密码算法（SM2 elliptic curve algorithm）

SM3：SM3 密码杂凑算法（SM3 hash algorithm）

SM4：SM4 对称密码算法（SM4 symmetric cryptographic algorithm）

VPC：虚通路连接（virtual path connection）

VPN：虚拟专用网（virtual private network）

5.密码资源建设

5.1 建设目标

云计算中心的密码资源建设目标是将密码计算服务能力进行池化、虚拟化、SaaS 化，体现集约化的建设理念，符合碳中和的国家方针政策。

云计算中心的密码资源建设是通过统筹云平台自身和用户密码资源应用的规划、建设，提供统一的密码能力和密码服务的输出、统一的密码服务质量的输出、统一的密码运营管理的输出，从而实现CaaS的目标。

云计算中心的密码资源建设目标包含：

a)按需的自助服务：用户可以根据自身的需求在线申请可用的密码能力和服务；

b)动态的可伸缩性：用户可以根据自身业务的发展及时动态调整密码计算能力和服务能力的性能及容量；

c)快速的集成能力：用户可以根据自身的需求选择灵活多样的密码能力的集成和密码服务的使用方式，达到快速密码集成能力；

d)灵活的计费模式：不同的密码能力和密码服务提供合适的计费模式，可以按照租用时间、使用次数、使用量等进行计费；

e)高连续可用性：密码的能力和服务输出不得低于云计算中心高连续可用性设计目标；

f)安全可靠的隔离：用户间密码资源、能力、服务必须严格遵循物理或逻辑隔离；

g)统一的资源调配：云计算中心必须具备整体的密码资源、能力、服务的自动或人工的调配能力；

h)持续的监控能力：云计算中心必须具备密码资源池的资源利用、资源容量的持续监控能力。

5.2 建设框架

云计算中心的密码资源建设涵盖了“密码支撑服务”和“密码应用”这两个层面，通过不同的服务方式为云上用户提供快速便捷、按需自助式的密码资源、能力和服务。

密码应用基础设施：由证书认证系统、密钥管理系统、时间戳系统等构成，对云平台密码应用提供数字证书管理、密钥管理、时间戳管理等密码应用所需的基础支撑。

云计算密码资源：包含密码设备和云密码设备管理工具，池化密码资源，为云用户提供虚拟密码设备租用服务。

云密码支撑服务：在密码基础支撑之上，向云平台自身（含云管理）及云用户信息系统提供通用密码服务、典型密码服务和密钥管理服务。通用密码服务是根据云平台及云平台所承载的业务应用需要，提供按需、弹性的加解密、完整性验证、签名验签等服务；

典型密码服务是基于电子认证基础设施，提供统一认证、单点登录、授权管理、访问控制、电子签章、时间戳、数据库透明加密等服务；密钥管理服务是基于密钥管理基础设施，提供密钥全生命周期的管理服务。密码服务通常由统一的密码服务中间件供上层应用调用。上层应用包括：

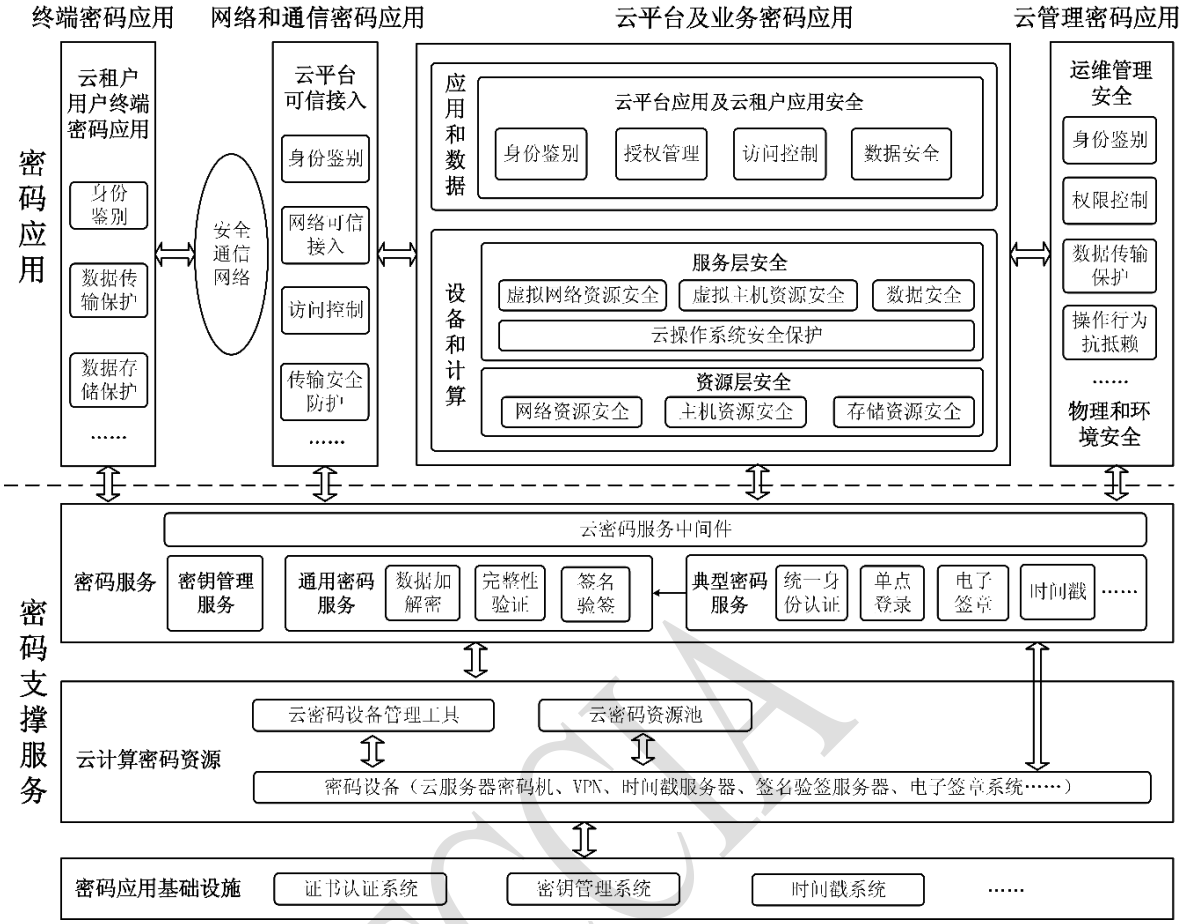
终端密码应用：即云用户用户终端安全密码应用。它是基于云平台提供的密码支撑服务，实现终端用户身份鉴别、终端数据传输和存储安全等。

网络和通信密码应用：基于云平台提供的密码支撑服务，实现云平台与经由外部网络连接的实体进行网络通信时的安全防护，例如通信双方身份鉴别、传输安全防护等，并确保网络可信接入和安全访问控制。

云平台及业务密码应用：基于云平台提供的密码支撑服务，实现云平台自身及云用户信息系统网络和通信安全、设备和计算安全、应用和数据安全。设备和计算层面，云平台由资源层和服务层组成。其中，资源层对服务层进行支撑，其密码应用包括了网络资源安全、主机资源安全和存储资源安全等方面；服务层密码应用包括虚拟网络资源安全、虚拟主机资源安全、数据安全和云操作系统安全等方面。应用和数据层面，负责实现云平台应用及云用户应用的身份鉴别、访问控制、数据安全防护等。

云密码管理应用：基于云平台提供的密码支撑服务，实现对云平台运维管理人员、管理操作的身份鉴别、权限控制等方面的安全管理。云平台典型密码应用架构如下图所示：

图 1 云平台典型密码应用构架



5.3 平台能力

平台对外输出的能力和服务包含但不限于以下能力：

a)密码虚拟机：用户独占式使用的密码虚拟机，支撑 SM2、SM3、SM4 等密码计算，密码虚拟机和用户的其他计算资源在同一个 VPC 网络；云服务器密码机宿主机应支持为密码虚拟机分配独立的虚拟密码模块资源，为密码虚拟机提供独立的虚拟密码运算资源和密钥存储空间。

b)密钥管理服务：为用户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、安全存储、更新、销毁、备份和恢复等管理功能，密钥的产生应该使用经过商用密码检测机构检测认证的随机数生成器产生；密钥的存储、备份应该确保机密性和完整性，防止未

授权密钥的泄漏和替换；密钥管理系统和密码虚拟机设备之间通信应确保机密性、完整性和不可否认性，应对操作人员的身份进行验证；

c)CA 服务：为用户提供个人身份证书、设备证书、域名证书等的申请受理和签发；

d)功能化密码服务：为租户提供其他功能化密码服务，该功能化服务是指基于基础密码运算的应用能力，包含但不仅限于数据库透明加密、完整性保护、专用文件加密、安全多方计算、联邦学习等；

e)签名验签服务：为用户提供签名验签服务；

f)时间戳服务：为用户提供时间戳服务；

g)电子签章服务：为用户提供电子签章服务；

h)自助服务申请：用户在线通过平台申请密码资源、能力和服务；

i)统计分析服务：用户可以方便快速查询自己密码资源的申请和使用状况。

5.4 服务形式

根据用户的需求，密码资源、能力和服务以用户独占方式（Exclusive mode）、Saas 化的服务两种服务形式提供服务。用户申请的密码资源、能力、服务可以是这两种服务形式的组合。

独占式（Exclusive mode）：在密码资源、功能、业务服务层面用户以独占的方式租用和使用密码资源、密码功能、密码业务服务，用户自己负责租用的密码资源、能力、服务的管理和运维，用户租用的密码资源、能力和服务不能以任何形式进行再出租。

SaaS 方式：根据云计算中的密码应用需求，将云密码服务分为三类：云密码资源服务（CRaaS）、云密码功能服务（CFaaS）、云密码业务服务（CBaaS）。按照 CRaaS、CFaaS、CBaaS 的顺序，这三类云密

码服务构成从低到高的层级关系，低层可为上层提供密码服务支撑，并且每一类也可直接为用户提供服务。其中：

a)云密码资源服务（CRaaS）：以密码基础设施、密码设备集群等密码设施为基础，提供了基本的密码服务，包括密码算法服务、证书管理服务、密钥管理服务、随机数生成服务等；

b)云密码功能服务（CFaaS）：基于云密码资源服务或密码基础设施，将面向应用场景的密码功能集合在一起，打包成易部署、易使用的虚拟机模板、微服务模板软件，在云中以虚拟机实例、微服务实例、软件中间件的形态对外提供服务，它们支持面向应用场景的标准接口；

c)云密码业务服务（CBaaS）：是密码技术和特定应用业务的融合，将密码技术的机密性、完整性、可用性的保护机制和应用系统数据处理流程结合形成一个安全的系统，对外提供的类似 SaaS 的服务。

5.5 性能要求

平台的能力随着用户对密码资源、能力、服务的需求的增加可动态进行横向扩展，不同用户根据自身的业务需求动态地进行调整。独占式密码服务基本性能要求如下：

a) 并发数：支持不低于 100 个并发请求；

b) SM2 签名：支持不低于 5000 次每秒；

c) SM2 验签：支持不低于 3000 次每秒；

d) SM3 杂凑：支持不低于 2500Mbps；

e) SM4 加解密：支持不低于 650Mbps。

当以独占方式成倍地申请资源、能力和服务时，最终获得的性能应不低于单项累计之和的 70%。

5.6 管理能力要求

云密码服务是云平台通过资源池化技术整合底层密码设备资源（云计算密码资源和密码应用基础设施），从而提供足够的密码服务支撑能力，云密码服务管理能力不仅能够保障云密码服务的稳定性、可靠性，而且应具备高安全性，具体能力为：

a）建立具有身份鉴别、访问控制和远程安全管理机制的池化密码运算资源，确保各云用户间密码资源安全隔离；

b）管理平台应支持独立管理和统一管理，独立管理是指密码服务应用方独立管理密码资源的能力； 统一管理是指云密码服务的整体运维管理能力；

c）独立管理和统一管理均应提供可视化密码资源应用与统计分析能力；

d）独立管理和统一管理均应满足相应的安全强度。

6.平台安全要求

6.1 总体目标

云平台安全的总体目标是防范数据泄露风险、用户间资源和数据隔离失败风险、API 滥用风险、业务高可用连续性风险、基础设施不可控风险、运营风险和恶意人员破坏风险。

6.2 平台建设安全要求

平台建设使用的密码算法、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。对于密码模块类产品，应满足 GB/T 37092 中二级以上要求。

平台通用安全要求部分应满足 GB/T 31168 中的增强要求。

平台通用安全要求部分应符合 GB/T 22239 中的三级要求。

平台通用安全要求部分应符合 GB/T 39786 中的三级要求。

6.3 身份鉴别安全要求

应采用密码技术对登录物理、虚拟设备的云平台管理用户、云平台租户进行身份鉴别，保证其身份的真实性。

应采用密码技术对访问云平台应用或开发实例的用户、调用云平台的服务的应用进行身份鉴别，保证其身份的真实性。

应采用密码技术对传输过程中身份鉴别数据进行机密性和完整性保护。

6.4 资源访问安全要求

平台提供应提供以下至少一种访问控制机制：基于角色的访问控制（RBAC）、基于属性的访问控制

（ABAC）或者零信任（Zero-Trust）访问控制。

在创建新用户后，应要求新用户在首次登录时修改系统生成的默认口令，随后才能进行系统功能的正常访问或 API 调用。

系统应禁止共享账户的存在。

系统应具备限制措施，使得一个用户只能从一个地址（IP）登录并访问系统，并施加会话次数限制。应只授予用户所需的最小权限，对于管理用户应遵循角色的权限分离。

访问控制策略规定了主体对客体的访问规则应由授权主体配置访问控制策略。

对于访问控制的粒度限制，应达到主体为用户级或进程级，客体为文件、数据库表级甚至字段级和记录级。

宜对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

6.5 网络通信安全要求

网络和通信安全保护对象包括但不限于云平台主数据中心与灾备中心之间的网络通信信道、云用户，本地数据中心与云平台之间的网络通信信道、外部运维管理网络与云平台之间的网络通信信道、网络边界访问控制信息、内部网络等。云平台网络和通信的安全要求包括：

a）应明确网络边界范围，应清晰明确地划分云平台内各个区域之间的网络边界、虚拟化层网络边界、VPC 用户网络和特殊网络边界；

b）云平台与网络边界外进行远程通信时，应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性；

c）云平台与网络边界外进行远程通信时，采用密码技术保证通信过程中重要数据的完整性；

d）云平台与网络边界外进行远程通信时，应采用密码技术保证通信过程中重要数据的机密性；

e）应采用密码技术来保证云平台网络边界、网络区域边界、虚拟化网络边界访问控制信息的完整性；

f）应采用密码技术对从外部接入到云平台内部网络的设备进行接入认证，确保接入设备的身份真实性（对于第四级云平台）；

g）以上若采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码检测认证机构认证为合格；

h）以上采用的密码模块产品，应至少达到 GB/T 37092 二级（对于第三级云平台）/三级（对于第四级云平台）安全要求。

6.6 用户隔离安全要求

系统允许其用户通过一个登录流程（enrollment process）进入该系统，并获取访问系统及其资源的权限。用户可以分为几类，包括管理员用户、普通用户等。用户在管理粒度上被分到若干组内，

每组称为一个“租户”（tenant）。在一个简单的层级中一个用户只属于一个租户。特殊情况下，一个租户还可以有子租户。

多租户（multi-tenancy）是指一个建立在共同的底层资源上的环境被多个用户共同使用的情形，应满足以下要求：

a)每个不同的用户应当属于不同的责任主体，责任边界和可访问资源边界需清晰明确；

b)不同用户之间的内部资源应当相互隔离，不允许互相访问和相互资源占用；

c)应当使用密码技术保证用户资源隔离权限的完整性；

d)应当保证不同用户之间的基础密码服务能力相互独立、不可相互使用；

e)应当使用密码技术保证不同用户之间的访问权限完整性。

6.7 数据安全要求

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。

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。

重要程序的来源真实性要求：对于系统和应用的重要程序需要保证程序来源的真实性。

提供数据的本地备份和恢复功能：至少每周做一次完全数据备份，备份介质应在场外存放。每个用户可以查询到自己数据的备份信息。应提供合理、适当的环境对备份数据进行恢复测试。

备份数据占用的存储空间在分配给其他用户时应进行安全擦除。

当检测到数据完整性遭到破坏时，系统应进行告警并提供有效的数据恢复手段。

6.8 高可用安全要求

应使用密码技术保证云平台系统配置信息的完整性，并保证高可用集群配置信息的完整性。应使用密码技术保证云平台配置备份和数据备份的完整性。

应使用密码技术保证云平台配置备份和数据备份的机密性。

应使用密码技术保证云平台配置信息同步过程中的完整性。

应使用密码技术保证云平台配置信息同步过程中的机密性。

应使用密码技术保证云平台异地备份数据的完整性和机密性，及备份传输过程中数据的完整性和机密性。

7.应用规范要求

7.1 总体目标

云中心的所有信息系统应使用云平台提供的密码资源服务能力。各信息系统应按照云平台提供的API或SDK等对接方式改造信息系统，保证密码资源服务能力能够被正确使用，使得信息系统中机密性保护对象、完整性保护对象、真实性保护对象、不可否认性保护对象均在符合国家法律法规的原则下得到有效地保护。

7.2 密钥使用

对于密钥生存周期管理，云平台上的信息系统应满足以下要求：

a)禁止以任何明文形式存储、使用密钥，禁止以明文形式将密钥提供给信息系统访问；

b)密钥生成和存储应利用云平台提供的密钥产生和存储机制来获得相关的密钥；

c)若需要进行密钥分发，应以加密形式在VPC网络内进行传输，并保证传输内容的机密性和完整性，对接收者的身份需要进行鉴别；

d)密钥的使用范围应适当合理，避免多人、多系统使用相同密钥对存储数据进行机密性和完整性保护；

e)信息系统应具备密钥周期性更新机制。确保密钥更新后被保护的数据依然可用。一般性密钥更新周期不长于18个月，被保护的数据应在3个月内变更为由新密钥保护，最长不超过6个月；

f)信息系统应具备密钥泄露后的密钥应急更新机制。在应急期间，应加强对被保护对象的数据访问者的身份鉴别和授权，只有使用新密钥进行重新保护的数据对象才能被授权者访问，所有被保护的数据对象应在1周内由新密钥进行重新保护；

g)在国家法律法规规定的备份、存档数据留存时效失效后，才能销毁信息系统用于保护数据对象的密钥。

7.3 完整性

应使用国家密码管理机构批准的消息认证码或数字签名算法对数据进行完整性保护。

完整性计算不能仅针对需要保护的数据本身，应对需要保护的数据及被保护数据所属的对象主体标识联合进行完整性保护。

信息系统通过系统本身业务流程对保护对象进行访问、修改之前，应进行完整性验证，在验证通过后才能进行业务动作，验证失败次数超过阈值时，应通过发送通知、记录日志等方式对系统管理员进行告警提醒，同时拒绝下一步的任何业务动作，提示用户需联系管理员进行人工干预。

对于完整性保护对象，应制定合理的完整性校验周期，以防保护对象长期不进行完整性校验，失去保护的有效性。不经常被访问到的

数据保护对象根据数据分级分类的要求，至少每周进行一次完整性校验。

对于重要数据的传输，信息系统应对重要数据本身或者整个报文进行完整性保护。完整性校验应利用云平台提供的基础密码资源能力完成计算。

7.4 机密性

应使用国家密码管理机构批准的加密算法对数据进行机密性保护。

机密性计算不能仅针对需要保护的数据本身，应对需要保护的数据及被保护的数据所属的对象主体标识联合进行机密性保护。

数据对象在进行机密性保护的同时，应进行完整性保护。

信息系统通过系统对被保护的数据对象进行访问、修改之前，应对访问者进行身份鉴别和授权确认。对于机密性保护对象，应制定合理的解密测试周期，以防保护对象长期不进行校验，失去保护的有效性。不经常被访问到的数据保护对象根据数据分级分类的要求，至少每周进行一次数据解密校验测试。对于重要数据的传输，信息系统应对重要数据本身或者整个报文进行机密性保护。

机密性的计算应利用云平台提供的密码基础服务能力完成。

7.5 抗抵赖

应使用国家密码管理机构批准的数字签名算法实现抗抵赖。

对于基于数字信封的数字签名，其中一次性对称密钥的产生应由云平台提供的密码资源服务提供。抗抵赖使用的签名证书，应由通过国家密码管理部门认证的第三方电子认证服务机构颁发。企业组

织内部实现抗抵赖要求时使用的签名证书，可为自签发的数字证书。

接收方和发送方均不能抵赖的数字签名不可抵赖机制，可通过双方直接签名或第三方仲裁提供的不可抵赖机制实现。

抗抵赖的签名及验签应利用云平台提供的密码资源能力完成计算。

7.6 出错处理

信息系统和提供密码资源服务能力的云平台在密码调用出错发生时，双方均应记录错误日志。禁止在错误日志中包含隐私、敏感数据，若需要记录，应进行有效数据脱敏处理。

提供密码资源服务能力的云平台在遭遇密码服务出错时， 应提供清晰、统一、可查的错误代码。信息系统在遭遇密码计算出错时，若影响进一步的业务功能，应在不违反安全性的原则下向用户提供明确清晰的通告信息，并通过邮件、系统通知等手段向系统管理员发送告警通知。

信息系统应按照密码应急处理规范要求建设高可用信息系统，以保障业务的高连续可用性。

7.7 应用接入

信息系统可通过 SDK 或者 RESTful API 这两种方式中的任意一种与云平台进行密码资源服务能力的集成和对接。

信息系统应确保 API 调用使用到的用户、口令的妥善存储，禁止以明文形式进行存储此类数据，应对数据进行机密性和完整性的保护。

信息系统在调用 API 后应及时关闭会话，减少会话被劫持和重放的可能性。

信息系统在长时间使用某次身份鉴别和授权获取的会话令牌进行 API 调用后，应重新对API 调用者进行身份鉴别和授权。

7.8 服务接口

云平台可提供的服务接口形式包括SDK或RESTful API，应至少其中一种为信息系统进行密码资源服务能力的集成和对接。

使用SDK或RESTful API中的任何一种方式进行密码服务能力调用之前，应对调用方进行身份鉴别和授权验证，通过身份鉴别和授权验证后创建一次性会话令牌。

通过用户口令方式实现身份鉴别时，禁止以明文形式将口令存储在SDK配置文件中或以硬编码的方式将口令嵌入SDK包中，禁止以明文方式通过HTTP传输口令。

云平台应提供通过SDK或RESTful API方式进行口令修改，并应提供管理页面，允许用户通过Web页面进行口令变更。

用于身份鉴别的口令应定期更改，更改间隔应不超过3个月。会话令牌应有合理的失效时间，最长静默时长不超过2小时。

通过身份鉴别和授权创建的会话令牌，禁止连续使用超过8个小时。超过8个小时应再次进行调用者身份鉴别和授权。

云平台应具备防范对API调用进行劫持和重放攻击的措施。

云平台应提供支持Linux、Windows平台上信息系统的Java、C、Python等SDK语言包，以进行密码资源服务能力的对接。

RESTful API接口应采用HTTPS POST方式进行服务请求，编码方式统一使用UTF-8编码，请求和响应数据格式均为JSON格式。

只有持有有效会话令牌的API调用者才能进行其他API的调用访问。

7.9 透明的存储加解密服务

云平台应提供透明的存储加解密服务，如数据库透明加解密服务。

数据库透明加解密服务应按数据库实例，为应用按需提供基于表空间或列空间的数据透明加解密服务。

数据库透明加解密服务应满足以下要求：

基于表空间或列空间，实现敏感数据的存储加密；

a)对于有权限的应用、用户，支持敏感数据的透明读写；

b)对于无权限的应用、用户，只能读取敏感数据的密文。

c)无需修改应用和业务逻辑；

d)实现数据库加密密钥的多级管理，不同的表、列使用不同的加密密钥；

e)支持敏感数据的完整性校验；其中计算完整性校验值时应采用基于密钥的报文完整性算法，如HMAC。

8.管理运营要求

8.1 总体目标

运营管理是对运营过程的计划、组织、实施和控制，是与产品生产和服务创造密切相关的各项管理工作的总称。运营应考虑如何对生产运营活动进行计划、组织和控制。运营管理的对象是服务目录、用户、订单、统计报表、计量等。运营管理的活动以客户和业务为中心。

8.2 管理要求

云服务商应严格保护云计算平台的客户数据和用户隐私。在授权信息系统用户及其进程、设备（包括其他信息系统的设备）访问云计算平台之前，应对其进行身份标识及鉴别，并限制授权用户可执行的操作和使用的功能。

云服务商应对云计算平台进行配置管理。在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，并设置和实现云计算平台中各类产品的安全配置参数。

服务商应为云计算平台制定应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务商应建立事件处理计划，包括对事件的预防、检测、分析、控制、恢复等，对事件进行跟踪、记录并向相关人员报告。服务商应具备灾难恢复能力，建立必要的备份设施，确保客户业务可持续。

云服务商应根据安全需求和客户要求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的未授权访问、篡改和删除行为。

云服务商应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。服务商应制定监控目标清单，对目标进行持续安全监控，在异常和非授权情况发生时发出警报。

云服务商应确保能够接触客户信息或业务的各类人员（包括供应商人员）在上岗时具备履行其信息安全责任的素质和能力，应在授予相关人员访问权限之前对其进行审查并定期复查，在人员调动或离职时履行安全程序，对于违反信息安全规定的人员进行处罚，处罚依据相关法律法规及行业规定等。

8.3 运营规范

门户运营：通过单点登录，使资源使用者能够统一地进行密码云资源的开通、监控、调度、分配、计量/计费和业务优化工作，并通过运营门户提供的个性化功能，设置符合个人使用习惯的工作界面。

面向用户根据其权限，提供对应密码资源的服务目录、服务等级管理等策略管理界面，提供用户使用的资源和业务的状态查看界面。

用户管理：完成用户的注册、注销，用户基本信息修改、密码修改、用户基本信息查询等操作。主要包括：

a)用户注册：通过管理员为用户进行注册。当注册完成后，相关帐号、密码信息将通过 Email 方式发送给用户；

b)用户注销：用户注销时，平台应确认该用户已退订所有业务。若该用户存在已开通业务，则提醒用户先退订业务，再进行注销。用户注销后，平台通知用户注销结果；

c)用户基本信息修改：用户登录访问门户入口后，可对其基本信息进行修改。关键信息（如用户名等）可设置为不允许用户修改；

d)密码修改：用户登录访问门户入口后，可对其登录密码进行修改。用户需输入原密码、新密码、确认新密码，在提交平台验证成功后，平台提示用户操作结果；

e)权限管理：权限管理是指对运营平台管理的服务能力提供进行分层和访问控制。应支持权限浏览，支持权限创建、修改、查询和删除，支持权限分级，支持权限审计。

密码服务管理：密码服务由可提供的密码资源服务组成。资源服务一般包括：资源属性、SLA 服务等级、计量方式等。密码服务需经过审核并发布后，在门户展现提供给业务客户选用。

订单管理：对于云运营者，应提供订单查询、浏览、统计等功能。云运营者可在统一门户查看订单的统计信息，包括订单数据，如订单数量、分类、费用、用户数等相应信息。订单管理功能处理用户的业务申请请求。客户的业务申请请求通过审批流程进行审批，审批结果自动通过电子邮件或短信等形式通知客户。在审批通过后申请请

求应通过资源模板进行实例化，生成用户所申请的服务，并通过电子邮件或短信等形式将服务信息（如 IP 地址，管理员口令等）通知用户。

服务等级管理：服务等级作为密码云服务的一个属性，是向客户提供服务的质量承诺。在运营体系中，服务等级管理负责完成 SLA 服务级别的制订、修改、删除、查询。服务等级的主要组成要素包括可用性、可靠性、连续性、性能等。

计量/计费管理：计量/计费管理是实现量化服务的前提和基础，通过计量/计费模型的设定，可帮助云运营者实现云资源的量化服务。计量/计费管理功能通过从平台侧获取资源使用计量/计费信息，根据设定的计量/计费管理规则，对使用计量/计费进行统计。计量/计费管理应包括以下功能：

a)资源使用信息数据采集和展现；

b)资源使用量计算、计量/计费数据查询和计量/计费数据统计。

9.合规测评要求

云密码支撑服务应符合国家法律、法规的规定及信息安全国家标准、密码行业标准的有关要求，应对相关的基础设施、信息系统进行商用密码应用安全性评估，以确保服务的合规性与安全性。

应对云密码支撑服务进行等级保护测评及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 70 分以上。