GM/Y 5015-2024

政务云密码应用安全性测评研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘要

本研究报告，对国内政务云密码应用发展现状以及相关课题和标准研究情况进行调研和分析总结，对政务云密码应用技术进行提炼，给出了政务云密码应用模型和云密码资源池设计要求。

对国内外主流云服务提供商的政务云密码服务解决方案等进行了分析与总结，提炼出了云密码应用、云密钥管理等政务云密码服务；给出了IaaS层典型密码应用、PaaS层典型密码应用、SaaS层典型密码应用模型，为政务云密码应用领域的技术发展及标准研制规划提供参考与指导。

关键词：政务云、云计算、密钥管理、密码测评

目录

前言

本研究报告基于2022年的政务云密码应用情况进行编制，由于2022年政务云的密码应用从标准、建设到测评实施尚不成熟，如本研究报告任何与当前或后续发布的密码国家标准和行业标准不一致之处，以相关密码国家标准和行业标准为准。

本项目参与起草单位有：商用密码检测认证中心、北京信安世纪科技股份有限公司、兴唐通信科技有限公司、北京三未信安科技发展有限公司、山东省计算中心、阿里云计算有限公司、腾讯云计算（北京）有限责任公司、华为技术有限公司、北京数字认证股份有限公司等单位。

项目主要起草人包括：肖秋林、秦体红、汪宗斌、张立花、刘尚焱、杨辰、张晓溪、高志权、张大江、蒋增增、李述胜、魏常辉、何济尘、李自涛、陈萧宇、谢灿、周岩、赵坤等。

政务云密码应用安全性测评研究报告

1 概述

1.1 背景

1.1.1 政策背景

政务云（Government Cloud）是指运用云计算技术，统筹利用已有的机房、计算、存储、网络、安全、应用支撑、信息资源等，发挥云计算虚拟化、高可靠性、高通用性、高可扩展性及快速、按需、弹性服务等特征，为政府行业提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等综合服务平台。

政务云属于行业云的一种，是面向政府行业，由政府主导，企业建设运营的综合服务平台，一方面可以避免重复建设，节约建设资金，另一方面通过统一标准有效促进政府各部门之间的互连互通、业务协同，避免产生“信息孤岛”，同时有利于推动政府大数据开发与利用，是大众创业、万众创新的基础支撑；政务云上运行着大量的政务服务系统，其业务系统安全稳定的运行是社会活动的正常秩序的支柱和保障；政务云汇集了海量的政务数据和公民信息，其信息数据的安全可靠，小至关系个人的隐私数据保护，大到关联国家的信息安全保密。

2018年印发的《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》（厅字〔2018〕36号）把积极推进政务信息系统中的密码应用作为一项重要工作，明确指出要规范电子印章、电子文件、电子证照和移动政务办公中的密码应用，推进安全可靠应用和电子凭证网上报销中的密码应用，加强政务网络、政务云、政务大数据中心、国家基础信息资源库及政务信息资源共享中的密码保护，为推进“三融五跨”，构建全国一体化“互联网+政务服务”提供密码支撑保障。

1.1.2 技术背景

政务云是承载各级政务部门的门户网站、政务业务应用系统和数据的云计算基础设施，用于政务部门公共服务、社会管理、数据共享与交换、跨部门业务协同和应急处置等政务应用。政务云对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务。政务云的建设有利于减少各部门分散建设，提升信息化建设质量，提高资源利用率和减少行政支出等优势。政务云的服务对象是各级政务部门，通过政务外网连接到各单位，使用云计算环境上的计算、网络和存储资源，承载各类信息系统，开展电子政务活动。

密码应用在政务云中身份识别、安全隔离、信息加密、完整性保护和抗抵赖性等方面具有不可替代的重要作用。相对于其他类型的安全手段，如人力保护、设备加固、物理隔离、防火墙、监控技术、生物技术等，正确合理的密码应用是保障政务云安全最有效、最可靠的手段。

云计算中需要借助密码技术应对的安全风险，云计算环境的系统架构较传统的信息系统有很大变化，相应的安全风险及借助密码技术解决的安全风险点需要重新研究，从

多租户环境安全、云访问控制、虚拟化技术安全、数据存储安全等多层级角度进行研究规范。

云计算中与之相应加密服务模式需要研究技术要求，云计算平台具有虚拟化、分布式、资源集中等特点，云环境下相应的密码服务也需要相应调整，如密码服务虚拟化、密码服务动态迁移等，这些都需要进行研究规范。

云计算中新的密码管理需要研究管理规范，云计算平台下的密码资源分发、密码设备部署、密码设备管理等有新需求及新的业务特点，如虚拟化密码设备的管理、虚拟化设备的热迁移等，我国之前已经建设的密钥管理中心等密码服务基础设施提供的服务还比较单一，暂不能适应云计算场景下对密码管理的要求，需要进一步研究规范。

云计算中需要普及国密技术及算法，密码技术是保障信息安全的关键、核心技术，为确保密码算法的自主可控，降低敏感信息泄露和信息系统遭受攻击的风险，国家密码管理局制定并发布了系列的国产加密算法及相关密码行业标准。国家大力倡导信息安全核心产品的国产化、并出台相关政策强制要求在国家信息安全建设过程中使用国产化信息安全密码产品，但在云计算中国密算法及产品的使用需要研究使用规范。

1.1.3 必要性

当前，我国对于信息系统中如何应用密码已经制定了相关的技术标准和管理规定。其中，《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）给出了面向通用信息系统的商用密码应用基本要求，《商用密码安全性评估管理办法（试行）》对重要领域网络和信息系统中如何开展商用密码应用安全性评估工作做出了规定，明确指出在政务信息系统规划阶段，责任单位应当编制密码应用方案，并组织对方案进行评审。

但是，对于政务云中如何落实相关标准要求和管理规定，目前还没有相应的指导性文件。很多单位对于如何编制密码应用方案仍不够了解，密码在政务云建设中的重要作用没有得到充分发挥。针对上述情况，应加快研究云计算密码应用标准、云密码测评标准。

1.2 研究目标

研究政务云密码应用模型、政务云密码资源池、云密码服务等内容，以及结合《信息安全技术信息系统密码应用基本要求》的要求，为后续制定《政务云密码应用安全要求》、《政务云密码应用安全性测评要求》等政务云密码相关的标准和规范提供参考。

2 政务云密码应用典型技术方案

我国主流云服务提供商包括阿里云、华为云、腾讯云等搭建统一密码支撑服务平台，依托该平台可以解决云上信息系统密码服务需求及国产密码算法应用问题，提供统一密码支撑服务。阿里云针对云加解密服务推出基于密钥分层体制的密钥管理服务，可以使用户在服务端和客户端完成加解密以及业务系统的密码应用方案；腾讯云提供解决数据安全问题方案；华为云采用硬件安全模块技术提出基于密钥分层体制的密钥管理方案。

2.1 阿里云技术方案

2.1.1 云产品加密方案

阿里云密钥管理服务（KMS）与多个阿里云产品进行了集成，更大的发挥了KMS的优越性，提供对用户透明的加密服务能力，保障用户的数据安全。在需要数据完整性保护的场景，阿里云政务云通过认证加密模式同时保障数据的机密性和完整性。

KMS与块存储服务（EBS）、云数据库（RDS）、对象存储（OSS）等集成：可以通过KMS主密钥加密控制存储在这些云服务中的数据，同时集成加密解决了其他云产品中原生数据的加密保护问题。

用户在申请相应的云产品加密时，首先通过KMS产生用户主密钥（CMK），或用户密钥管理中心产生用户主密钥（CMK），通过外部导入密钥（BYOK）的形式导入用户主密钥（CMK）。

用户在使用云产品进行数据存储时，云产品会向KMS申请数据密钥（DK）和密态数据密钥（EDK）， 阿里云密钥管理服务（KMS)和云产品之间的通信采用基于SSL的传输保护。云产品得到数据密钥（DK）和密态数据密钥（EDK）后，使用数据密钥加密数据，云产品将加密后的数据和密态数据密钥（EDK）进行存储。

2.1.2 用户业务系统密码应用方案

用户在阿里云上使用云服务器（ECS）搭建自己的业务系统，使用网络存储（NAS）和OSS对象存储服务。用户的业务系统和云存储都有加密保护需求。

用户有自建的密钥管理中心（KMC），可以生成、分发和备份密钥。

用户业务系统使用阿里云加密服务提供密码服务，业务数据密钥由用户密钥管理中心（KMC）分发。

云存储NAS和OSS与阿里云KMS集成提供数据透明加密能力，用户密钥管理中心（KMC）生成用户主密钥（CMK），通过BYOK相关接口导入阿里云密钥管理服务（KMS）。

用户业务系统密码应用方案如下图所示。

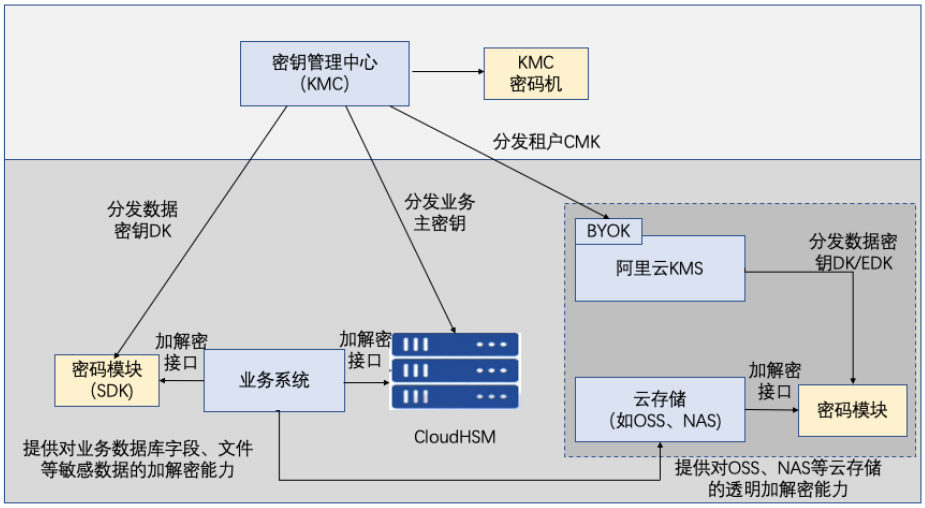

图 2-1 用户业务系统密码应用方案

2.1.3 加密服务应用场景

加密服务适用于阿里云上所有客户，主要使用场景包括云上金融业务系统、政务系统、企业财务系统等敏感数据保护。

（1）敏感数据加密

应用于政务、电商、门户、Web 站点等各类包含大量个人敏感信息的系统应用。杜绝了明文数据被泄露和篡改的风险，提升系统的健壮性和客户价值。阿里云提供的数据加密服务如图2-2所示。阿里云提供的数据加密服务在不同业务系统中的应用如图2-3、图2-4和图2-5所示。

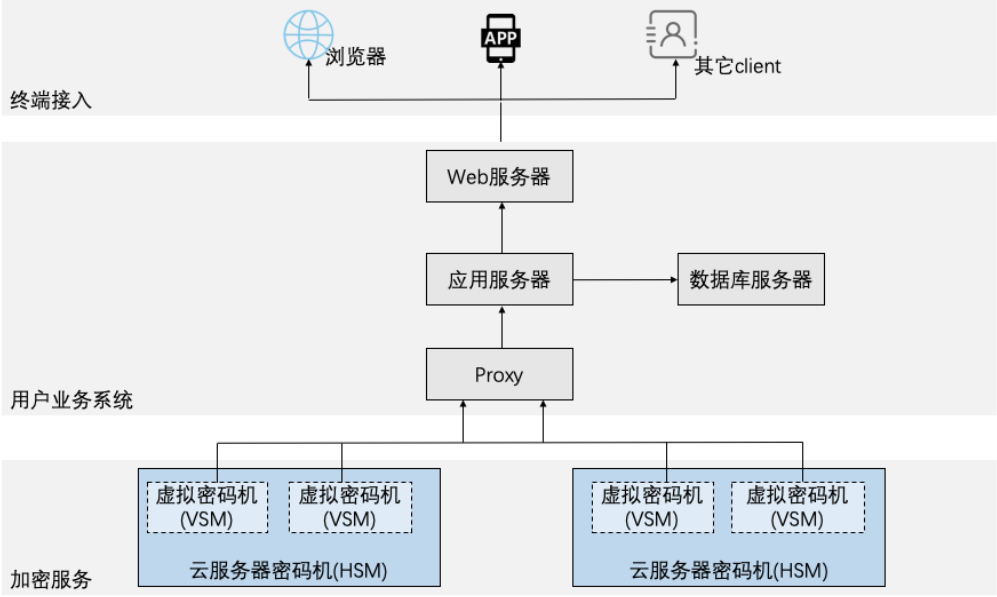

图 2-2 阿里云数据加密示意图

（2）金融支付

应用于POS收单、互联网支付、预付费卡支付、P2P等各类第三方支付应用中，保证支付数据在传输、存储过程中完整性、保密性，支付身份认证和支付过程的不可否认性等，并满足行业监管合规要求。

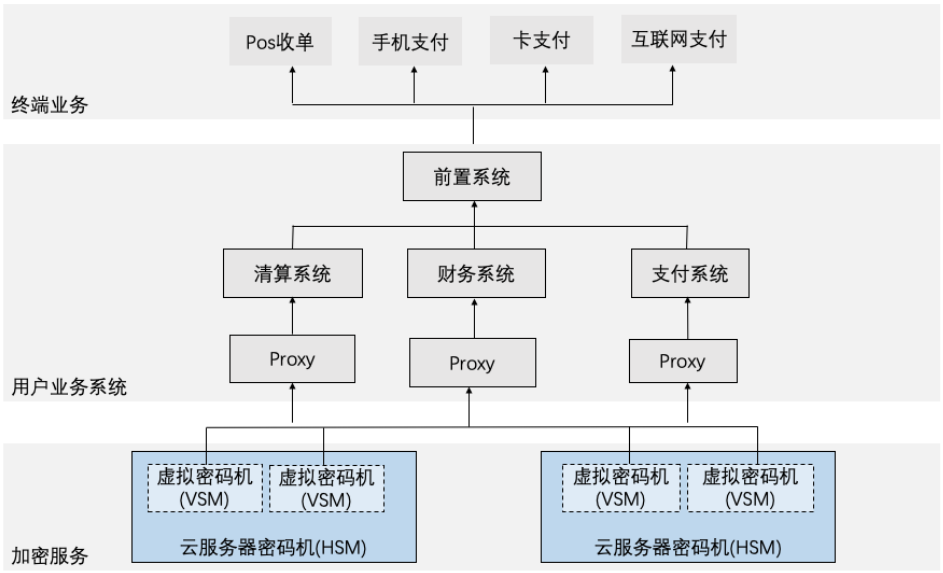

图 2-3 金融支付系统应用示意图

（3）电子政务

应用于电子签章、电子公文、电子政务、CA 系统等各类政务系统中，提供密钥生成与存储、证书签发、数据签名、数据验签、身份认证等服务，符合监管合规要求及等级保护要求，保障政务系统的安全性。

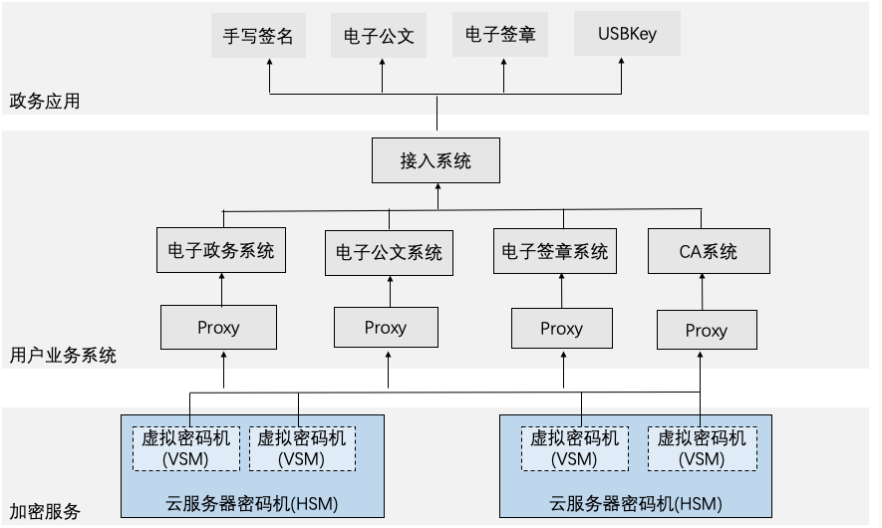

图 2-4 电子政务系统应用示意图

（4）电子票据

应用于电子病例、电子发票、电子合同、电子保单等各类应用，确保电子票据类的应用用户身份的真实性，票据数据的生产、传输、存储过程中的完整性和安全性，符合监管合规要求，保障了电子化安全性，促进电子化业务发展。如图2-5所示。

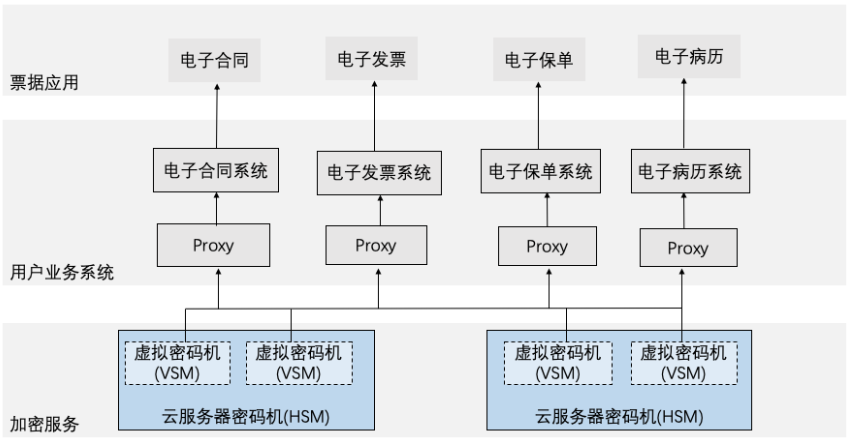

图 2-5 电子票据系统应用示意图

2.2 腾讯云技术方案

为帮助行业客户解决数据安全问题，护航产业安全发展，腾讯安全推出了“云数据安全中台”，实现端到端的云数据全生命周期安全体系，以数据加密软硬件系统（CloudHSM/SEM）、密钥管理系统（KMS）以及凭据管理系统（Secrets Manager）三大能力为核心，将密码运算、密码技术及密码产品以服务化、组件化的方式输出，并集

成至腾讯云产品中，实现从数据获取、事务处理及检索、数据分析与服务，数据访问与消费过程中的安全防护。

依照云计算架构特性以及安全性保障要求，云计算架构密码保障体系包括物理与环境安全、网络和通信安全、访问层安全、云服务层安全、密码应用架构安全、安全管理六个方面，如图2-6所示。

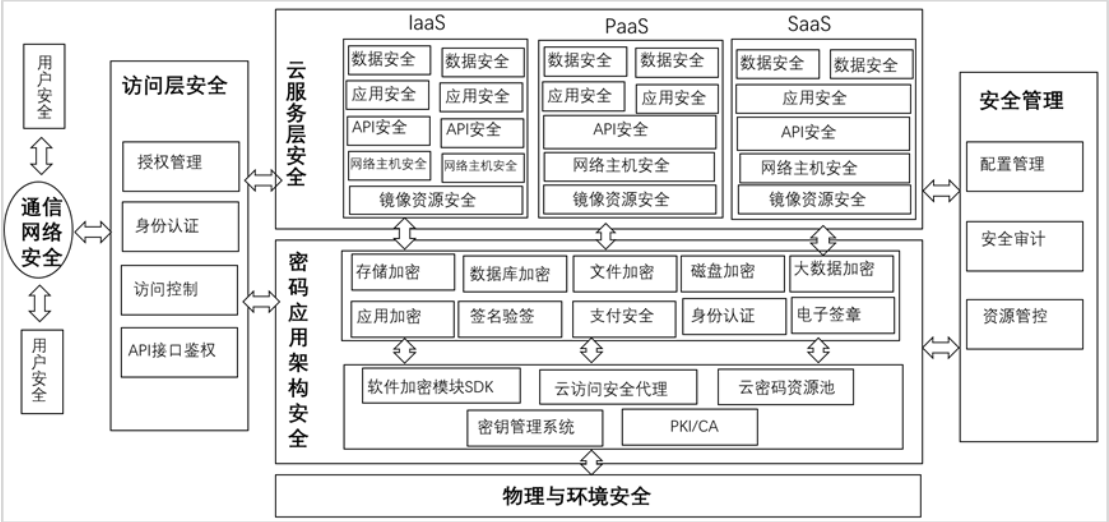

图 2-6 腾讯政务云架构图

（1）物理与环境安全：物理和环境安全主要实现对云平台所在机房等重要区域的物理防护。

（2） 网络和通信安全：主要实现对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，密码应用要求主要涉及云用户与虚拟机、应用与云平台、本地数据中心与云平台等通信过程中实体身份真实性、数据机密性和数据完整性，以及网络边界访问控制和设备接入控制。

（3）访问层安全：主要实现对云平台业务访问的用户身份鉴权及访问控制保护，密码应用要求涉及用户与虚拟机之间、云平台API接口调用访问鉴权等

（4）云服务层安全：包含云计算系统IAAS层、PAAS层、SAAS层安全保障要求，包括虚拟镜像安全保护、应用的用户身份鉴别、访问控制，以及应用相关重要数据的存储安全、传输安全和相关行为的机密性及不可否认性保护等。

（5）密码应用架构安全：基于云计算架构下密码技术应用，构建密码即服务的保障体系，确保云上密码应用的安全性、可靠性、合理性以及可实施性。基于密码即服务层，提供云平台架构，以及IaaS层、PaaS层及SaaS层服务基于密码技术的安全保障。

（6）安全管理: 实现对云计算架构下，密码资源及密码服务的统一动态管控、访问审计以及运维人员的安全管控。

2.3 华为云技术方案

2.3.1 安全服务密码典型技术方案

（1）密钥管理服务

密钥管理服务（KMS）：为平台云服务、租户业务应用提供一种安全可靠、简单易用的密钥托管服务，其密钥安全由硬件安全模块 (HSM) 保护，帮助用户集中管理密钥生命周期安全。解决了云服务加密密钥安全创建、租户密钥统一管理的问题。

用户可登录KMS系统，对租户密钥进行全生命周期管理，包含创建、启用、禁用、删除、轮转、别名、修改用户主密钥等。对于集成了KMS加密的OBS服务，用户登录OBS服务时，可以选择“KMS 加密”加密文件，自动对上传文件加密保存在云端存储，下载时自动解密。

（2）数据加密服务

数据加密服务（DEW），基于经检测认证的云服务器密码机（CloudHSM），构建虚拟化密码资源池，实现IT、密码资源统一调度管控，为用户按需提供虚拟密码机（VSM）的服务，支持政务、金融、公安等行业客户的云上密码服务及国密改造需求。解决了加密机入云、密码及IT资源统一调度、自动化管维的问题。

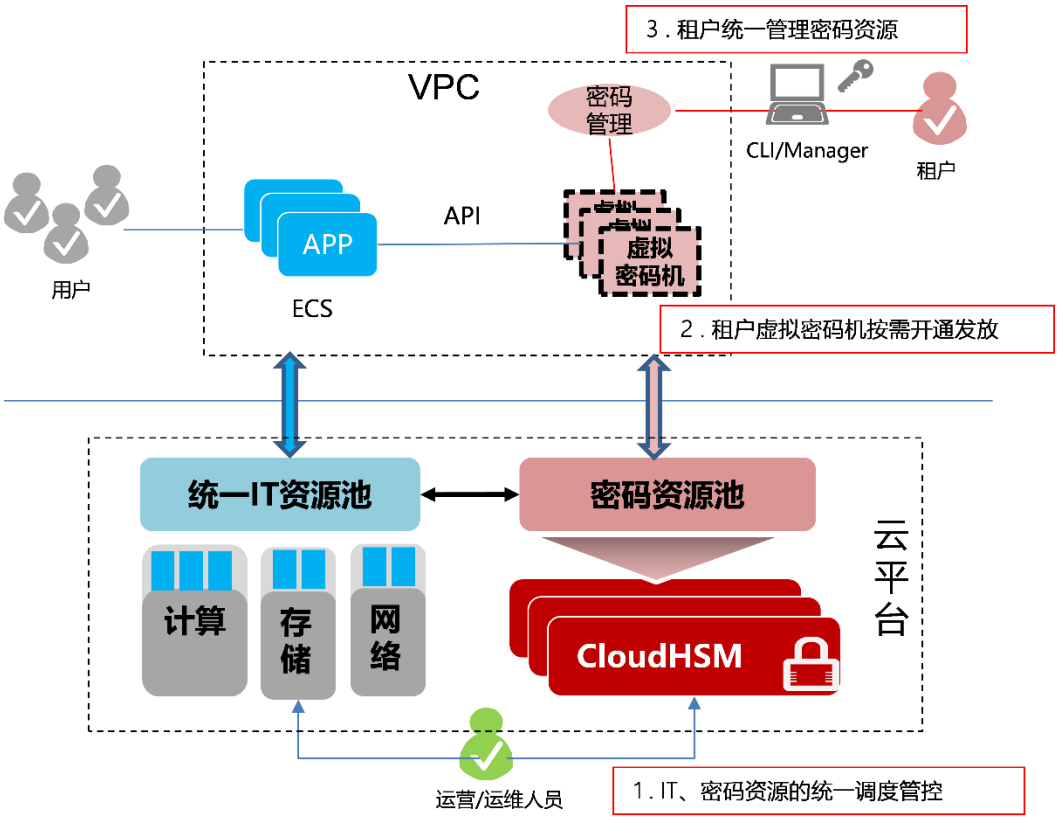

图 2-7 华为云加密服务示意图

数据加密服务基于云加密机在云平台侧实现了虚拟化密码资源池的构建，并可统一调度管理密码资源，实现IT、密码资源的统一调度分配，支持对虚拟密码资源的配置、操作、漂移、升级等。租户在数据加密服务界面，可按需申请相应的VSM资源，服务自动化将VSM设备映射入租户VPC，同时管理员将所需的管理、备份USBKey发放给用户。用户持USBKey登录管理配置工具，远程初始化、配置VSM，并完成应用改造接入，实现应用对加密服务调用。租户可在服务界面进行VSM的申请、维护、关闭等，也可登录管理配置工具对名下所有密码设备、密钥进行统一管理和配置。

2.3.2 PAAS 密码典型技术方案

PAAS系统中涉及对称加密、非对称加密、哈希算法等各种算法。
对称加密中密钥管理的架构如下：

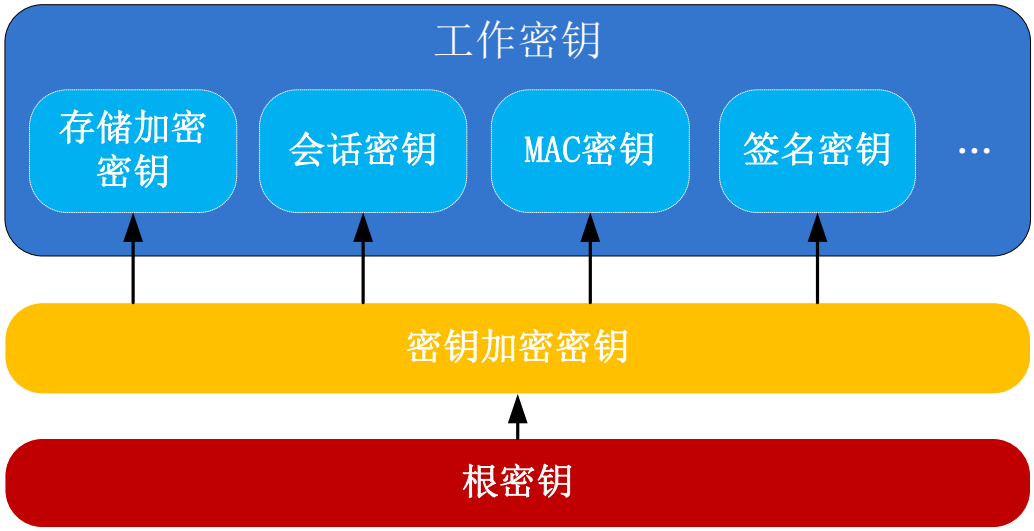

图 2-8 华为云密钥管理服务

在系统中，密钥加密密钥（主密钥）统一由内部的PSM组件管理，每个节点上的密钥加密密钥由PSM生成并分发，不同租户的密钥加密密钥不同。在每个节点上会随机生成根密钥，加密保护密钥加密密钥。

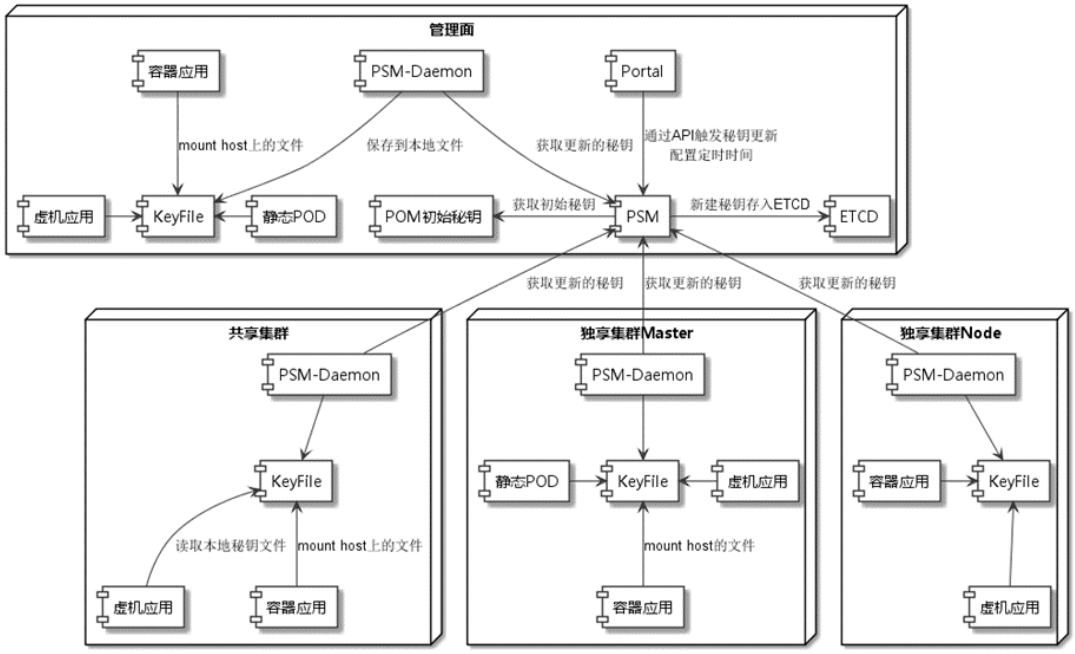

图 2-9 华为云密钥派生示意图

节点上的各服务组件需要做业务敏感数据加密时，直接使用节点上的密钥加密密钥通过PBKDF2派生出工作密钥加密。

2.4 政务云密码应用情况

随着“互联网+政务”融合应用深化，各地省级政务云按照“省市两级、覆盖全省、物理分散、逻辑衔接”的建设原则，构建“1+N+N”的政务云体系，现已进入政务云2.0时代。同时，在密码应用技术方面，国内市场业已日趋成熟，密码厂商纷纷启动了密码服务平台的设计和研发，目前国内多家厂商已经推出了密码服务平台的解决方案，助力于政务云的密码应用建设。

政务云2.0特征是以数据为核心、以IaaS/PaaS深度融合为支撑，以新架构的云应用创新为代表。在2.0阶段，应用对业务连续性和数据安全可靠性保障提出了更高要求。现阶段政务云建设，主要是政务云2.0以IaaS/PaaS深度融合为主，原有的传统密码应用服务方式已经无法与其资源弹性灵活配置的特性相匹配，各省政务云主管单位与各密码厂商一同开始以云的方式去解决云上业务的安全需求，云上统一密码服务平台开始出现。云上统一密码服务平台是政务云上的密码服务云，其在保证自身密码业务安全可信基础上，发挥云架构优势，可以随业务系统弹性动态调配密码资源，保障业务安全需求。

政务云在四川、海南、浙江等省份已有应用。通过调研并结合各省政务云密码应用建设情况分析，当前省政务云密码应用呈现出一些共性特征，情况如下：

（1）平台配套密码基础设施统一建设

受政务云业务大集中模式影响，为满足云上业务安全需求，政务云上密码基础设施作为云上安全基础配套，一般由政务云平台主管部门进行统一规划、统一建设、统一管理。

（2）对业务合规运行情况进行统一监管

在政务云平台业务系统进行过安全测评后，需要对业务运行期间的安全状态进行掌控，对平台及平台各节点的业务安全总体态势有更全面的了解，对平台密码设备或服务及业务调用情况进行统一监管已经得到广泛认同。

（3）业务密码资源集成改造工作量大

由于政务云平台承载业务少则几百多则上千，众多业务安全所需密码设备数量巨大，业务密码应用集成改造工作任务繁重，对政务云密码设备或资源的有效管理，高效有序的实现业务密码应用集成改造是各政务云平台重点关注的问题。

（4）平台具有多网络分区部署

政务云平台由于业务需求，一般同时具有政务外网区及互联网，不同区之间一般由网关或网闸进行安全隔离，政务外网区及互联网区上业务系统均属政务信息系统需要进行安全合规保障。

（5）平台具操作系统及数据库系统多样

各政务云平台由于平台承建方不同，其所用云操作系统，为业务用户所提供的底层系统环境都不同。同时，为满足业务系统的差异化需求，平台所提供的数据库系统也多样，这些差异都需要在进行密码应用系统时进行统筹考虑。

3 政务云密码应用技术要求研究

3.1 政务云的部署模式

政务云是承载各级政务部门的门户网站、政务业务应用系统和数据的云计算基础设施，用于政务部门公共服务、社会管理、数据共享与交换、跨部门业务协同和应急处置等政务应用。政务云对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务。政务云的建设有利于减少各部门分散建设，提升信息化建设质量，提高资源利用率和减少行政支出等优势。政务云的服务对象是各级政务部门，通过政务外网连接到各单位，使用云计算环境上的计算、网络和存储资源，承载各类信息系统，开展电子政务活动。

在云计算的环境中，由云计算服务商提供云计算平台，为租户提供服务。按照服务的形式，一般分为IaaS、PaaS、SaaS三种，其中IaaS、PaaS一般由云平台提供，基于此各应用厂商开发SaaS服务。

图 3-1 政务云应用模型

3.2 密码需求分析

政务云的全面建设和应用，除了面临以病毒、木马、恶意攻击、网络入侵为主的传统安全威胁以外，虚拟化、资源共享、多租户、分布式等核心技术的引入也带来新型安全威胁。针对政务云的安全问题，需要建立以密码为核心的云安全保障体系，保证云基础设施及云管理的安全，同时还应为云租户提供云密码服务，满足云上政务信息系统的安全需求。密码应用需求归纳如下：

（1）身份鉴别需求

身份鉴别需求主要涉及政务云物理和环境安全、网络和通信安全、以及云资源安全访问等方面。一是物理和环境安全方面，云平台应采用密码技术实现其数据中心机房、灾备机房等重要区域的物理访问身份鉴别，从而保证进入人员身份的真实性；二是对于

相互通信的设备实体、API接口、应用程序实例等，应在通信前基于密码技术确认通信双方的身份，保证身份真实性；三是为了保证云平台中各种接入设备的合法性，需要对连接到内部网络的设备进行安全接入认证；四是对于访问云资源的云平台管理员、租户管理员和用户，应基于密码技术进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，从而防止非授权的访问；另外，在虚拟化安全鉴别方面，为了确保虚拟机镜像来源于可信的权威实体，需要对虚拟机镜像模板的真实性进行验证。

（2）关键数据安全存储需求

政务云的关键数据涉及身份鉴别信息、云资源管理信息、云上政务敏感数据、审计数据、密钥等，此外还包括虚拟机镜像文件、快照文件，一方面应采取加密措施，防止云平台和租户关键数据、镜像和快照中可能存在的敏感资源被非法获取，另一方面还应实现完整性保护，防止被恶意篡改。

（3）关键数据安全传输需求

身份鉴别信息、云资源管理信息、云上政务敏感数据、审计数据、密钥等关键数据在传输过程中，同样具有机密性和完整性需求，防止非授权的截获和篡改。

（4）关键操作抗抵赖需求

对于云平台管理员、云租户管理员以及云上政务信息系统用户的关键操作、交易等，应提供数据原发证据和数据接收证据，实现相关行为的不可否认性。

（5）虚拟机迁移安全需求

虚拟机监视器（VMM）在发起和管理虚拟机动态迁移之前，应利用密码技术进行身份鉴别，并对管理数据进行完整性保护，保证虚拟机在迁移过程中的控制平面安全；同时，还应对虚拟机迁移的数据通信信道进行安全加固，来保证虚拟机迁移过程中的数据平面安全。

（6）云密码服务需求

政务云承载着多个政务部门的业务系统，而各部门的业务系统均需要采用密码技术来支撑自身的业务安全。因此，政务云需要将密码作为一种服务为云上系统提供支撑。政务云提供的密码服务，可包括数据加解密、完整性验证、签名验签等通用密码服务，统一身份认证、单点登录、电子签章、时间戳等典型密码服务，以及密钥管理服务。此外，考虑到实际应用中难以为每个租户配置相应的物理密码产品，政务云还需要池化密码资源，为租户提供虚拟化的密码服务，并确保各租户之间密钥隔离、密码运算资源安全隔离、剩余信息清除等。

对标GB/T39786，政务云密码应用需求如下表：

表1：政务云密码应用需求

层面	密码应用需求	
物理和环境安全	云平台	云平台应保证基于密码技术对进入云平台数据中心人员进行身份鉴别;采用数字签名技术或者MAC对电子门禁系统记录进行完整性保护;采用数字签名或MAC技术对视频监控音像记录数据的完整性保护。
	云租户	云租户的物理和环境安全由政务云平台承担。应保证基于密码技术对进入云平台数据中心人员进行身份鉴别;采用数字签名技术或者MAC对电子门禁系统记录进行完整性保护;采用数字签名或MAC技术对视频监控音像记录数据的完整性保护。

网络和通信安全	云平台	政务云平台的运维管理人员（包括云IT资源运维管理、云密码资源运维管理等）应采用SSL/IPSec协议实现对政务云平台的资源进行安全运维管理操作，确保真实可信的云平台管理员才能进入云管理平台；政务云平台不同节点间网络通信，应采用SSL/IPSec协议建立安全信道，确保传输数据的安全；政务云平台的基础设施与密码监管平台之间，通过建立IPSec VPN/SSL VPN安全通道进行密码应用监管数据的安全通信保护。
	云租户	政务云租户的管理人员、业务操作人员应通过SSL/IPSec协议实现对在政务云平台上自己所购买的服务进行安全管理。
设备和计算安全	云平台	对虚拟机镜像文件、快照、云平台管控系统（Hypervisor）与云平台组件之间的管理数据等进行完整性保护；对虚拟机镜像、快照以及云平台鉴别信息等敏感数据进行信源加密，实现敏感信息的机密性保护。对虚拟密码机镜像文件、快照、云密码管理系统与云密码机等各组件之间的管理数据等进行完整性保护。对虚拟机密码机镜像文件、快照以及云密码管理系统鉴别信息等敏感数据进行信源加密，实现敏感信息的机密性保护。
	云租户	对于由政务云租户定制的虚拟机镜像、快照等内容，采用政务云平台提供的通用密码服务实现对虚拟机镜像、快照进行完整性计算，防止虚拟机镜像等被恶意篡改；对于政务云租户保存具体敏感数据的虚拟机镜像、快照等内容，采用政务云平台提供的通用密码服务进行加密保护，防止虚拟机镜像等中的敏感资源被非法访问
应用和数据安全	云平台	应用程序用户使用云服务过程中，确保用于与运行在虚拟机实例之上的应用程序实例的身份鉴别、云租户与部署的应用程序或开发工具实例之间的身份鉴别；政务云存储的云平台自身重要数据包括但不限于网络边界和系统资源访问控制信息、重要信息资源敏感标记、重要程序或文件、日志记录、虚拟机镜像文件、租户镜像文件、租户快照文件等。其中，应采用密码技术保证虚拟机镜像文件、租户镜像文件、租户快照文件在存储过程中的机密性、完整性以及在传输过程中的机密性和完整性；云平台管理应用应采用密码技术实现云平台管理员关键操作行为的抗抵赖性。
	云租户	政务云租户应用系统可通过标准密码服务接口或密码服务中间件直接调用虚拟密码机，实现对敏感数据的保护、签名验签、身份认证等通用密码服务功能，密钥可以保存在虚拟密码机中，也可以使用密码机主密钥加密后保存在业务系统中

3.3 政务云密码应用技术要求

3.3.1 政务云密码应用技术框架

结合云计算功能分层框架和云计算安全特点，提出了政务云密码应用技术框架，包括云用户层、区域边界安全层、服务层、资源层、安全管理中心等。具体如下图所示。

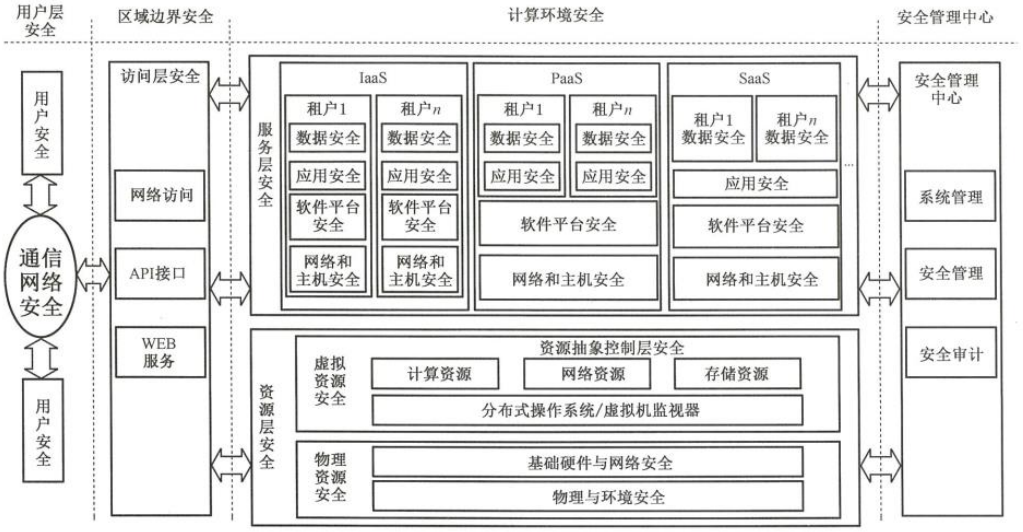

图 3-1 政务云密码应用技术框架

用户通过安全的通信网络以网络直接访问、API接口访问和WEB服务访问等方式安全地访问云服务商提供的安全计算环境，其中用户终端自身的安全保障不在本研究报告研究范畴内。计算环境安全包括资源层安全和服务层安全。其中，资源层分为物理资源和虚拟资源，需要明确物理资源安全设计技术要求和虚拟资源安全设计要求。服务层提出了不同服务模式下云服务商所提供服务的具体实现方式，包含实现服务所需的软件组件。根据服务模式不同，云服务商和云租户承担的安全责任不同。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。基于该技术框架，本章节对政务云各组成部分的密码应用进行了研究，提出了技术要求。

3.3.2 物理资源安全密码技术要求

物理和环境安全是信息系统安全的基础层面。如果信息系统的物理和环境安全得不到保障，则设备、数据、应用等都将直接暴露在威胁之下，信息系统的安全就无从谈起。利用密码技术确保信息系统的物理和环境安全，可以有效阻断外界对信息系统各类重要场所、监控设备的直接入侵，并确保监控记录信息不被恶意篡改。对于物理和环境安全性的要求主要有两方面:一是对于物理和环境的访问控制,即未授权人员无法访问重要场所、重要设备和监控设备;二是对各类物理和环境的监控信息的完整性保护，包括人员进入记录、监控记录等，实现事前威慑、事中监控、事后追责。

由于政务云计算特点，云平台应保证基于密码技术对进入云平台数据中心人员进行身份鉴别；采用数字签名技术或者MAC对电子门禁系统记录进行完整性保护；采用数字

签名或MAC技术对视频监控音像记录数据的完整性保护。对于政务云物理和环境安全而言，应保证云计算基础设施位于中国境内，包含密钥和管理系统。对于云租户，云租户的物理和环境安全由政务云平台承担。

3.3.3 虚拟资源安全密码技术要求

由于云计算中大量应用到虚拟化技术，所以对虚拟化的安全防护研究变得尤为重要。虚拟化安全及密码技术要求如下：

（1）虚拟机镜像安全密码应用要求

虚拟机的镜像可能存储相关敏感数据，需要对镜像及所涉及到的私密信息以加密手段进行保护，保护环节需要覆盖虚拟机镜像在产生、存储、使用、流转的各个环节。同时为了保证虚拟机镜像的完整性和可认证性，可对虚拟机的校验值进行数字签名，并针对镜像资源设置访问控制策略。

（2）虚拟机访问安全密码应用要求

虚拟机访问包括用户对虚拟机的访问、应用对虚拟机的访问、不同虚拟机之间的访问以及虚拟机镜像访问。为了确保虚拟机的访问安全，需要对虚拟机的访问对象与访问请求发起者进行双向认证，并确保认证密钥或凭证的安全。

（3）虚拟机隔离安全密码应用要求

在虚拟机隔离方面，虚拟机在本质上是运行于Hypervisor的进程，虚拟机共享着计算、网络和存储资源，在多租户环境下，用户的程序和数据被加载在同一内存之上，用户的程序也可能使用同一物理网卡进行通信，因此需要采用虚拟机隔离技术保证用户的数据不被同一物理机器上的其他用户的虚拟机访问。隔离中使用身份鉴别来确保只有合法的用户或应用程序或虚拟机才能使用资源。采用访问控制技术，如基于角色的访问控制，基于属性的访问控制来确保合法用户的合法访问。采用加密、数字签名技术来确保用户数据在计算过程、传输过程和存储过程中的机密性和完整性。因此，需要确保身份鉴别凭证、加密密钥、签名密钥等的安全。

（4）虚拟机迁移安全密码应用要求

在虚拟机迁移方面，虚拟机迁移的时候，一个虚拟机从一个物理服务器迁移到另一台物理机，需要对传输的网络通道、传输的数据进行加密保护。另外，服务提供商还需要确保没有数据残留在原先的硬盘上，从而防止其他使用原物理机的用户恢复出这些数据，可以通过存储时对所有的数据进行加密来解决。对于加密密钥，应该存储在原虚拟环境中的基于策略的密钥服务器上，密钥服务器应该是高度安全的。

（5）桌面虚拟化安全密码应用要求

在桌面虚拟化方面，桌面虚拟化模式下，用户的所有运行的进程、数据均保留在云端服务器上，在采用加密技术保证用户桌面数据的存储机密性同时，还应通过用户和云端设备、资源的双向认证、访问控制来保证数据的安全访问；通过对传输数据、传输通道的加密保护实现终端和服务端的通信安全；同时，因为虚拟化实质是多用户对云端资源的共享，所以应采用用户隔离、数据隔离等技术手段，从物理上、逻辑上对用户数据进行保护。

（6）虚拟机监控安全密码应用要求

由于云环境的大量用户资源共享，给虚拟机监控提出了两个新的要求：由于资源共享，不同的用户能够监控的资源范围必须得以隔离和区分；由于所有的监控数据都是在云端，用户若想获得监控数据查看状态，必须通过网络从云端将监控数据传输到客户端，所以传输过程中的监控数据安全也必须得到保障。因此，利用身份鉴别和访问控制技术

可以实现监控数据的隔离以防止非法用户访问其他用户的虚拟机实例或应用程序的运行情况等监控数据，利用加密、数字签名等技术来保证监控数据在传输过程中的机密性和完整性。

3.3.4 IaaS 密码应用要求

在IaaS层，主要是把物理资源以服务形式提供给租户使用。云计算服务商为了便于系统管理，提高服务质量，往往会使用集中部署的管理系统来管理分布式部署的资源，在每个节点使用独立的控制器来接受控制指令并分配资源。

IaaS密码应用要求如下：

政务云IaaS接入安全：在云环境中，为了确保访问双方的合法身份，应对所有的访问请求发起者（用户、设备、资源、服务等）和访问对象（用户、设备、资源、服务等）进行双向认证。认证方式可以采用单点登录、多因素认证、身份联合、匿名认证等认证机制，为了确保认证过程中认证双方的身份凭证（如用户名/口令、多因素认证码、令牌等）的安全性，需采用加密、数字签名等密码技术对身份凭证、认证协议等进行安全保护，因此要保障加密密钥、认证密钥等的存储和访问安全。

政务云IaaS交互安全：IaaS层的交互安全主要为虚拟化安全以及网络安全，虚拟化安全参考3.3.3节虚拟资源安全；

政务云通信安全：在网络传输数据的机密性保护方面，应采用数据传输通道加密的方法保障信息在网络传输过程的完整性、机密性和可靠性。例如，通过采用SSL、IPSec等数据通信加密技术实现从用户终端到云端传输通道的安全，或采用HTTPS等安全通信协议进行通信。

政务云IaaS数据安全方面：IaaS服务模式下的数据安全主要包括：静态应用程序支撑数据的安全，结构化的应用程序数据存储的安全，非结构化的应用程序数据存储安全。静态应用程序支撑数据，包括源代码、应用程序使用的参考数据、虚拟机镜像、归档数据和日志记录等，该类数据不同于直接由应用程序生成、处理和存储的数据。这类数据可以在上传给云服务提供商之前先由云租户进行加密。结构化的应用程序数据为运行在虚拟机实例之上的应用程序产生的结构化数据，该类数据的安全可以采用安全的数据库管理系统来保障，数据库管理系统实例需对存储的结构化数据的机密性进行保护。非结构化的应用程序数据存储安全应采用类似于透明加密的存储级加密的方式实现。

3.3.5 PaaS 密码应用要求

在PaaS服务中，PaaS服务通过通用密码服务使用密码资源池提供的密码服务，而PaaS服务本身成为一类特殊的典型密码服务。在PaaS应用中，密码服务管理员分为两类，一类是PaaS服务本身的密码服务管理员，这一类人员一般是云平台的内部业务运维人员；另一类是租户/应用系统管理员，他们可以配置自身的认证密钥、数据加密密钥。

在网络身份鉴别和访问控制方面，为了避免来自网络的非法访问，需要对用户、目标资源进行双向的身份鉴别，并结合访问控制技术防止对资源的非法访问，如单点登录、数据源鉴别等技术手段。

PaaS密码应用要求如下：

政务云PaaS接入安全：在云环境中，为了确保访问双方的合法身份，应对所有的访问请求发起者（用户、设备、资源、服务等）和访问对象（用户、设备、资源、服务等）进行双向认证。认证方式可以采用单点登录、多因素认证、身份联合、匿名认证等认证机制，为了确保认证过程中认证双方的身份凭证（如用户名/口令、多因素认证码、令牌

等）的安全性，需采用加密、数字签名等密码技术对身份凭证、认证协议等进行安全保护，因此要保障加密密钥、认证密钥等的存储和访问安全。

政务云PaaS层的交互安全包括开发者应用调用API、开发者用户访问平台以及应用之间的相互访问，因此需要对访问请求者与访问对象进行双向认证。同时，需采用数字签名、验签和传输通道加密保护技术（如，SSL、SSH技术）与PaaS层部署的应用程序和/或开发工具实例建立安全的交互，确保通信数据机密性和完整性保护。

政务云PaaS层API接口与中间件安全：大部分的API会牵涉到对用户敏感资源的访问，如提取用户信息、查看用户状态等。为了抵御对云平台提供的敏感API的非授权访问，调用此类API时需要进行身份鉴别。

政务云PaaS层平台迁移安全：为了确保平台迁移过程中数据、应用程序等内容的机密性，并防止非授权用户的非法访问，需要采取加密技术对迁移过程中平台数据的机密性进行保护，同时采取身份鉴别与访问控制技术对访问用户的身份和权限进行管理。

政务云PaaS数据安全：PaaS服务模式下的数据安全主要包括静态应用程序支撑数据的安全、结构化的应用程序数据存储的安全、非结构化的应用程序数据存储安全，数据安全存储与IaaS服务模式下的相似。

3.3.6 SaaS 密码应用要求

SaaS层典型密码应用是将密码服务与SaaS层典型应用进行集成与整合，由政务云平台为政务云租户提供具有密码功能的SaaS应用，集成与整合的密码服务功能包括身份认证、传输加密、存储加密等典型密码服务，实现用户安全接入、用户身份认证、应用关键业务防抵赖和应用系统敏感数据安全存储等功能。

在基于云平台构建的密码应用系统中，主要包括应用安全域和管理安全域，其中应用安全域是在资源开通完成后，由密码服务管理员对自己的密码安全系统和密钥进行管理，确保配置完成后的应用系统用户能够安全的访问业务应用系统；管理安全域为云平台用户的应用管理员通过云平台提供的系统与功能，完成云端资源的购买、开通、基础配置等操作。

SaaS密码应用要求如下：

政务云SaaS接入密码应用要求：在云环境中，为了确保访问双方的合法身份，应对所有的访问请求发起者（用户、设备、资源、服务等）和访问对象（用户、设备、资源、服务等）进行双向认证。认证方式可以采用单点登录、多因素认证、身份联合、匿名认证等认证机制，为了确保认证过程中认证双方的身份凭证（如用户名/口令、多因素认证码、令牌等）的安全性，需采用加密、数字签名等密码技术对身份凭证、认证协议等进行安全保护，因此要保障加密密钥、认证密钥等的存储和访问安全。

SaaS交互安全包括内外部用户访问云服务、内部云服务之间的交互、内部云服务与外部云服务之间的交互安全。在云租户与云服务之间进行交互前，需要对交互双方进行双向认证，以确保访问对象与被访问对象的身份的合法性，如采用单点登录、多因素认证、跨域认证等身份鉴别技术，因此需要采取加密等密码技术确保身份鉴别凭证的安全，如访问密钥、用户名/口令等。

SaaS通信安全包括云用户与云服务或云服务之间的传输信道的安全，可使用安全传输协议或直接对传输内容进行加密的方式保障数据传输的安全性。通道加密的方式常采用IPSEC VPN和SSLVPN等数据加密技术，通信双方建立SSL VPN 或IPSEC VPN安全隧道，实现传输通道的安全。

SaaS数据 ：SaaS服务模式下的云租户使用的服务主要是应用软件，这些应用软件通常以托管服务的形式发布，用户通过与云服务提供商之间的网络连接接入服务。因此，SaaS层数据安全主要为应用程序数据安全，包括结构化数据和非结构化数据。SaaS层的内容安全包括数据传输、存储加密以及数据完整性。在SaaS服务中，大量使用瘦客户端、桌面虚拟化等技术，应用和数据都集中存放在“云”上，因此应用数据传输要求采用端到端的数据加密技术来保证重要信息不被截取、监听、篡改，通常在网络协议栈各个层次应用加密技术实现，如利用IPSec、SSL等加密协议进行传输加密。在数据加密的同时，结合利用完整性保护以及签发相应的数字签名等技术，实现数据完整性保护。数据存储和隔离方面：运用存储加密技术实现用户与其所拥有的资源绑定，解决用户之间数据隔离的问题，同时解决了云管理员等获得用户隐私数据的问题。数据加密可采用磁盘加密、字段加密等方式，磁盘加密针对整个数据库进行加密，字段加密对特定数据进行选择性加密，通过选择不同的加密方式达到保护敏感数据安全的目的。多租户环境下，常常需要实现数据隔离，通常有三种方式：独立数据库、共享数据库而数据库模式(schema)分开、共享数据库和数据库模式(schema)，采用磁盘加密或者字段加密等不同加密手段可以这种满足多租户环境应用下的需求。

3.3.7 云租户密码应用技术要求

政务云租户的管理人员、业务操作人员应通过SSL协议实现对在政务云平台上自己所购买的服务进行安全管理，包括对计算、存储等IT资源配置管理和对密码密钥等资源配置管理；

政务云业务服务系统与政务云租户业务服务系统之间应通过SSL协议实现业务数据的安全通信；

对于由政务云租户定制的虚拟机镜像、快照等内容，采用政务云平台提供的通用密码服务实现对虚拟机镜像、快照进行完整性计算，防止虚拟机镜像等被恶意篡改；

对于政务云租户保存具体敏感数据的虚拟机镜像、快照等内容，采用政务云平台提供的通用密码服务进行加密保护，防止虚拟机镜像等中的敏感资源被非法访问；

政务云租户应用系统可通过标准密码服务接口或密码服务中间件直接调用虚拟密码机，实现对敏感数据的保护、签名验签、身份认证等通用密码服务功能，密钥可以保存在虚拟密码机中，也可以使用密码机主密钥加密后保存在业务系统中。

3.3.8 安全管理密码应用要求

在系统管理方面的要求包括:

采用密码技术对系统管理员进行身份鉴别，确保系统管理员身份的真实性；采用密码技术保证系统管理员的访问控制信息的完整性。

在审计管理方面的要求包括:

采用密码技术对审计管理员进行身份鉴别，确保系统管理员身份的真实性；采用密码技术保证审计管理员的访问控制信息的完整性。

3.3.9 密钥管理

与密码技术息息相关的密钥管理技术是提供云计算环境机密性、数据源认证、实体认证、数据完整性和数字签名等安全密码技术的基础，包括密钥从生成到销毁的全生命周期。一旦密钥泄露或者密钥管理系统沦陷，传输通道安全、虚拟化安全、云中数据访

问及其数据本身的安全等都将无法得到保障。由于云计算环境相对于传统的计算环境具有虚拟化、多用户、分层次、集约化的特征，现有密钥管理体系架构已无法适应其需求。

云计算环境中的用户密钥管理包括对称密钥管理和非对称密钥管理。其中对称密钥主要应用于大量数据的加解密，如虚拟网络加密、镜像加密、对象存储加密、云应用数据加密等；非对称密钥主要应用于用户身份认证、数据签名验签和少量的数据加解密保护，如云计算用户身份认证、数据源认证和抗抵赖等。

云服务的各个层面涉及到的密钥以及对密钥管理的要求也各不相同，具体如下：

（1）IaaS层的密钥管理

IaaS层安全主要为虚拟化安全以及网络安全，虚拟化安全包括虚拟机镜像安全、虚拟机访问安全、虚拟机隔离安全、虚拟机迁移安全、虚拟机监控安全、桌面虚拟机化安全；网络安全主要为网络传输安全以及网络通信实体可信。

（2）PaaS层的密钥管理

PaaS服务模式下的交互安全包括访问安全、API接口与中间件安全、平台迁移安全。

（3）SaaS层的密钥管理

SaaS层的交互安全包括交互访问安全以及应用程序安全。

密钥的生命周期管理包括密钥生成、密钥分发与使用、密钥存储、密钥挂起、密钥更新、密钥归档、密钥撤销、密钥销毁、密钥备份与恢复等。从密钥的整个生命周期看，安全措施要渗透到每一个过程中。在创建的过程中要进行用户分类和鉴权，存储的过程中要考虑加密、访问控制，调取给外部使用的过程中要考虑权限管理、获取过程需要日志审计等，归档过程要考虑时间戳管理和加密，最后销毁过程要考虑防止数据恢复等。

3.3.10 密码资源池

政务云密码服务资源池基于云服务器密码机硬件集群构建密码设施层，为政务云为平台及业务应用提供密码资源的按需自助服务、弹性伸缩扩展和服务可计量等能力。

云平台密码服务由云服务器密码机（硬件）和云密码服务管理系统（软件）构成，云密码服务管理系统可以对密码资源池进行统一管理，如下图所示。

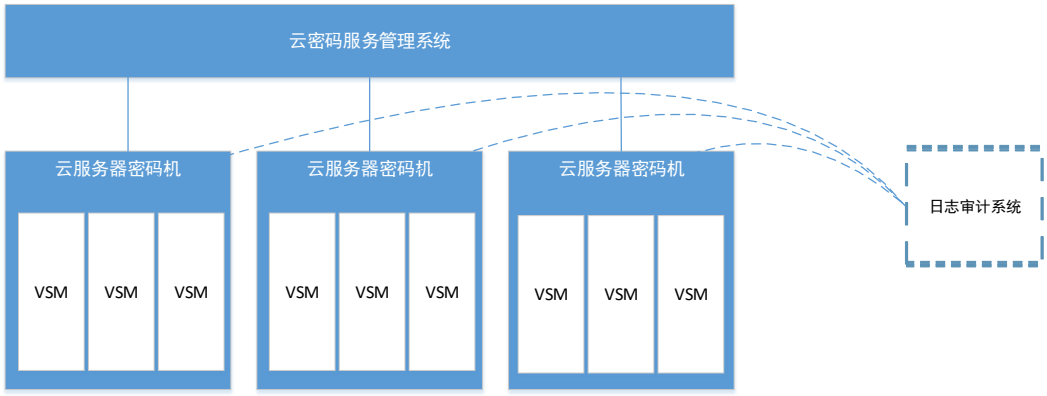

图 3-3 密码资源池示意图

密码资源池主要要求包括：

（1）物理资源可靠性

a) 专用硬件级安全，系统采用硬件云服务器密码机搭建，底层采用专用密码芯片，切实保护平台或租户密钥安全;

b)云密码资源池基础设施应与其他云资源物理隔离，不能共用服务器、交换机，以保障云密码资源池基础设施的高可用性；

c) 云密码资源池管理、业务、存储平面各分配独立的物理网口，进行物理链路隔离；

（2）虚拟密码机可靠性

a) 在宿主密码服务器发生故障时，应能通过集群或者热迁移的方式，不中断提供服务;

b) 应支持冷备方式，即在宿主密码服务器或密码虚拟机发生故障时，受影响的密码虚拟机在其它宿主密码服务器上的备份能手动重启;

c) 为保障安全性，云密码资源池与其他租户资源池应物理隔离;

d) 应支持对密码虚拟机所在物理机范围进行指定或限定的能力，保证密码虚拟机仅能迁移至指定资源池。

（3）接口要求

a) 云密码资源池应支持标准的密码管理接口和密码调度接口，以供上层应用系统调用，完成密码资源池的管理和能力调用功能;

b) 管理接口用于上层应用系统对设备进行各种管理操作，操作可分为以下几大类：设备管理类、权限管理类、密钥管理类、设备状态查询类等。

c) 密码调度接口用于上层应用系统调用密码服务能力，进行租户业务数据的处理;

d) 强制审计，云服务器密码机把收到的管理类指令和操作自动发送到独立审计系统；

e) 安全通讯：调用系统与密码机通讯采用标准密钥协商机制每次获取协商会话密钥，对通讯加密。

3.3.11 云身份鉴别密码技术要求

为了保证云中数据的安全性，云端的服务应鉴别访问者的身份。由于政务云计算环境具有其特有的特性以及云计算客户新的需求，对身份鉴别技术有了不同的需求，身份鉴别技术也面临不同的挑战。另外，尽管国内外各标准组织在身份鉴别方面出台了一系列的标准，但是难以满足云计算环境身份鉴别服务对身份鉴别技术的新需求。首先，云环境中的用户身份凭据的管理面临的安全威胁比传统的应用场景中更加严峻，安全性要求更高；其次，对于云中高度敏感的数据，需要更加安全的、用户可控的身份鉴别机制，可以使用一次性口令、基于生物特征（指纹、人脸、虹膜、生物行为等）的鉴别技术以及基于USB接口等智能卡识别的技术等强鉴别机制；最后，云环境下需要方便快捷的技术来解决联合身份鉴别（跨安全域或跨服务）。

政务云身份鉴别服务作为其他云服务和应用的基础服务，面临着不同的安全鉴别需求，为了保障云环境下身份鉴别服务的身份凭证管理安全、访问通信以及鉴别协议的安全，应采取相应的密码技术应对可能存在的网络攻击和安全漏洞带来的安全威胁：

（1）终端登录认证密码应用要求

在系统登录时，应对登录实体进行身份认证，确保系统使用者的合法性。传统的用户名+口令的认证方式较为简单，若能结合多因子身份认证（如key+pin码），生物特征识别技术等进行登录强认证，则能较好规避终端非法使用的安全风险。

（2）云服务客户端程序认证密码应用要求

云服务客户端提供商可对其提供的客户端程序进行签名，保障其提供的程序能被终端用户进行认证。

（3）接入认证密码要求

接入包括客户端到云服务的接入，也包括了IaaS、PaaS、SaaS三种云服务模式下各种服务对服务、对设备、对数据资源的访问接入请求。在政务云中，应对所有的访问请求发起者（用户、设备、资源、服务等）和访问对象（用户、设备、资源、服务等）进行双向的认证，以保证双方均能确定对方的合法身份。

传统的基于用户名/口令方式过于简单，因此为提高安全性，需要采用强认证方式，强认证通过使用多因素验证方式或加密技术实现，常见的如基于数字证书或PKI技术、Kerberos和令牌或智能卡等进行身份识别。

同时考虑到云计算环境下云用户的便利性，使用单点登录技术和跨域认证技术。目前常用的一些云计算中身份认证方法有开放式身份认证协议OAuth（用于不披露凭证的情况下进行第三方授权访问），OpenID技术（用于联合身份认证、单点登录）。总之，针对云接入，采用强认证、单点登录认证、跨域认证，以及代理、协同认证、资源认证等多种认证技术，安全、便捷地满足云接入的认证密码需求。

3.3.12 政务云应用数据安全密码技术要求

由于政务信息的高敏感度，国家对政务云的安全越来越重视。政务云中数据安全密码技术要求如下：（1）数据完整性密码应用要求

对云端数据的完整性保护验证按照执行实体可以分为两类，即用户与云服务提供商交互来完成验证，以及用户授权可信第三方进行数据完整性验证。无论哪种方式都需遵循尽量减小客户端的存储、计算和通信开销，以尽量减轻云端负担的原则，以便能够得到更好的服务质量。完整性保护验证应由云计算服务商按照用户要求在云端进行，一方面需要检查数据的完整性，为用户返回完整性检查结果；另一方面需要检查数据副本的完整性，并向用户出示副本检查结果。对于加密后的数据，可直接提供密文检查结果。

数据的完整性保护在IaaS云服务模式侧重于对虚拟化中的完整性保护（如虚拟机镜像模板的完整性保护）、存储数据的完整性检测以及传输数据的完整性检测。

数据的完整性保护在PaaS云服务模式侧重于对传输数据的完整性检测。

数据的完整性保护在SaaS云服务模式侧重于对处理数据的完整性检测，一般结合访问控制策略对处理的数据进行完整检测操作。

（2）数据隔离密码应用要求

政务云计算中用户数据隔离主要是对多租户的数据隔离，多租户架构下不同租户数据的存储有三种模式，对应着三种隔离的级别和实现的复杂度：

a）专用数据库模式：每个租户使用该租户专用的数据库。该模式下，资源共享率最低，但数据隔离复杂度最低。

b)共享数据库模式:多个租户共享同一个数据库,但是分不同的表或模式(Schema)进行存储。

c）共享数据库表模式：多租户的资源共享达到了数据库表的级别，同一个数据库表中可能存放多个租户的数据。该模式下,资源共享率最高,但数据隔离复杂度也最高。

从密码应用角度而言，可以采用为用户分配不同的密钥加密用户数据，形成逻辑隔离。

在政务云中，所有租户共享云计算资源，隔离的要点在于多租户之间的隔离。包括虚拟机隔离、存储隔离等；对于私有云，则是面向用户的更细粒度的隔离，除了虚拟机隔离、存储隔离，还需要对信息流的控制。

（3）数据残留处理密码应用要求

对云计算数据残留处理的密码应用主要是通过密码技术实现在云服务商完全不可信的情况下保证对数据的安全删除。

密码学保护技术的核心思想是对上传到云存储中的数据进行多次加密，并由一个（或多个）密钥管理者来管理密钥，当数据需要删除时，密钥管理者删除该数据对应的解密密钥，因此即使云服务提供商保留了该文件的某些拷贝也无法解密该文件。

数据残留处理主要是对IaaS云服务模式下存储残留数据的安全删除，包括云计算租户退出服务释放虚拟机磁盘空间后，虚拟机的安全删除。还包括对数据备份的安全删除。

（4）隐私保护密码应用要求

云环境中用户隐私保护通过集中信息流控制和差分隐私保护技术实现，防止非授权的隐私数据泄露，并支持对计算结果的自动除密。在数据存储和使用阶段，可使用一种基于客户端的隐私管理工具，提供以用户为中心的信任模型，帮助用户控制自己的敏感信息的存储和使用。基于现有的隐私处理技术，包括K匿名、图匿名以及数据预处理等可以处理大规模待发布数据时所面临的问题。匿名数据搜索引擎可以使得交互双方搜索对方的数据，获取自己所需要的部分，同时保证搜索询问的内容不被对方知道，搜索时与请求不相关的内容不会被获取。

隐私保护在IaaS服务模式下主要是对存储数据的隐私保护，基于隐私处理技术，对用户的隐私信息进行处理，保证存储在云端的隐私信息不被违规的获取。

隐私保护在SaaS服务模式下主要是对数据使用时的隐私保护，基于隐私处理技术，在数据使用时保护用户的隐私信息。

（5）数据加密应用要求

云计算中的数据加密主要有三种实现方法：硬件加密、软件加密和网络加密。硬件加密指通过专用加密芯片或独立的处理芯片等实现密码运算，包括加密卡、单片机加密锁和智能卡加密锁等。软件加密指使用相应的加解密软件实现加解密操作，包括密码表加密、软件校验方式、序列号加密、许可证管理方式、钥匙盘方式和光盘加密等。网络加密指不使用本地的软硬件进行加密，而基于网络的其他计算机或设备来完成加解密或验证工作，网络设备和客户端之间通过安全通道进行通信。

IaaS云服务用户使用云服务提供商提供的各种基础计算资源，例如虚拟机、存储器、网络架构等。故IaaS云服务的数据加密侧重于对虚拟化的安全保护（如虚拟机镜像的加密保护、虚拟机迁移的加密保护等）、对存储数据的加密保护、对网络通信的数据的加密传输。

PaaS云服务用户使用云服务提供商提供的开发工具和运行资源。PaaS云服务数据加密的侧重于对容器的加密，以保护云计算用户开发环境的安全。

在SaaS云服务中，用户使用的服务主要是应用软件，这些应用软件通常以托管服务的形式发布，用户通过与云提供商之间的网络连接接入服务。SaaS云服务的数据加密主要侧重于是对数据内容的保护，如对浏览器的XML加密、cookies加密等。

（6）数据检索密码应用要求

云计算的数据检索主要是对IaaS云服务存储数据的密文检索，应通过密文搜索算法对云端的密文状态的数据进行检索。

4 政务云密码应用测评研究

4.1 政务云密码应用测评的主要依据

随着云计算被广泛应用。为降低系统成本，打通数据融合，越来越多的企业事业单位的系统选择部署在云上。云计算技术融合了软硬件资源，采用了虚拟化技术，主机边界和网络边界相对于传统数据中心而言变得非常模糊，因此部署在云平台上的系统，其安全风险也随之增加。实际测评中，经常会碰到云平台和云租户业务应用系统密码应用的密评，其相对于传统的信息系统，云密码应用测评有所不同。

云平台系统的密码应用较为复杂，云平台系统的密码应用分为两个层面，一是云平台系统为满足自身安全需求所采用的密码技术，二是云租户通过调用云平台提供的密码服务为自身业务应用提供密码保障。因此，对运行在云平台上的云上应用进行密评时原则上需要完成云平台自身密码应用的测评和对云上应用系统密码应用的测评。云平台测评与一般信息系统基本一致，但由于云平台还需要为云上应用提供计算、存储、网络、密码等资源，还应关注云平台自身的密码应用以及对云租户提供的密码服务。云上应用测评则与一般信息系统测评略有不同，其部分测评结论依赖于云平台测评的结果。

目前，政务云密码应用测评的依据标准包括《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码应用测评要求》（GM/T 0115-2021）、《信息系统密码应用测评过程指南》（GM/T 0116-2021）、《商用密码应用安全性评估办法（试行）》、《商用密码应用安全性评估测评过程指南（试行）》和《商用密码应用安全性评估测评作业指导书（试行）》，同时参考《政务云密码支撑方案及应用方案设计要点（试行）》以及通过评估的密码应用方案。

4.2 政务云密码应用测评的主要内容和方法

针对政务云自身的特点并结合GM/T 0115、GM/T 0116等标准进行测评，现阶段的主要测评方法包括访谈、文档审查、现场查看、配置核查和工具测试，以下主要举例介绍现场查看、配置核查和工具测试方法，供测评人员开展现场测评工作参考。

4.2.1 云平台密码应用测评

政务云密码支撑设计首先需要满足云平台自身的密码应用需求，保障云平台物理与环境、网络与边界、云基础设施的安全性。云平台自身的密码应用测评应包括但不限于身份鉴别、重要数据的安全存储、重要数据的安全传输、虚拟机迁移安全和密钥管理五个方面，结合GB/T39786等标准的密码应用要求的四个层面和云平台密钥管理进行描述。GB/T 39786各个层面分别对应四个不同的安全等级，每一个安全等级对密码技术要求均不相同，本报告根据《信息安全技术信息系统密码应用基本要求》中密码技术要求在政务云中应用而进行测评研究。

4.2.1.1 物理和环境安全

a) 采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
b) 采用密码技术保证电子门禁系统进出记录数据的存储完整性；
c) 采用密码技术保证视频监控音像记录数据的存储完整性。

政务云主要采用密码技术，保证其数据中心机房、灾备机房等重要区域进入人员身份的真实性。测评时应验证重要区域是否采用密码技术进行物理访问身份鉴别，以及物理访问身份鉴别机制实现的合规性、正确性和有效性。

测评方法：

a) 通过查看电子门禁系统后台配置、实地查看(如使用错误、未授权的门禁卡尝试

打开门禁)等方式，检测和评估电子门禁系统身份鉴别机制的正确性和有效性；

b) 在条件允许的情况下，可使用通信协议分析工具捕获电子门禁系统后台与门禁系统的通信数据，分析鉴别过程，验证身份鉴别机制是否正确实现。

4.2.1.2 网络和通信安全

a) 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
b) 采用密码技术保证通信过程中数据的完整性；
c) 采用密码技术保证通信过程中重要数据的机密性；
d) 采用密码技术保证网络边界访问控制信息的完整性；

系统需要在该层面进行设备认证，则：

采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。

（1）身份鉴别

在虚拟化环境下，客户虚拟机通过虚拟网络实现虚拟网络对物理网络设备的复用，因此政务云的通信实体应在通信前基于密码技术对通信双方首先进行虚拟网络设备身份鉴别，可采用 IPSec/SSL VPN 技术方式实现。测评时应验证实体标识与鉴别数据的绑定方式是否合规、安全，鉴别机制是否符合相关标准要求，以及密码产品的合规性、使用的正确性和有效性。

测评方法：

a) 检查密码产品配置（算法、协议、双证书）是否正确；
b) 在两台 IPSec VPN 之间、客户端和 IPSec/SSL VPN 之间接入 IPSec/SSL 协议检测工具，分析密码协议是否符合密码相关国家标准、行业标准的有关要求；接入通信协议分析工具，捕获 IPSec 协议 IKE 阶段、SSL 协议握手阶段数据报文，分析密码算法标识或密码套件标识，验证身份鉴别采用的密码算法的合规性；
c) 使用数字证书格式合规性检测工具，验证 VPN 证书是否合规，并验证证书签名结果是否正确。

（2）通信安全：

云平台管理员与云平台管理应用之间的通信应建立安全传输通道，如采用SSL协议，保证云管理数据传输的安全性。测评时应验证远程通信安全机制实现的合规性、正确性和有效性。

测评方法：

a）在云平台管理终端与云平台管理应用服务器之间接入通信协议分析工具，分析云平台管理数据传输机密性和完整性保护措施是否有效、以及所采用的密码算法合规性；
b）如果云平台管理数据经机密性或完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能、MAC运算功能或签名验签功能是否被有效调用。

（3）设备接入认证：

对于第四级政务云，应采用密码技术对连接到内部网络的设备进行身份鉴别，以确保接入云的设备真实可信。对于设备从网络边界外接入云平台内部网络的情况，可通过IPSec/SSL VPN或安全认证网关对设备进行接入控制；对于设备从网络边界内连接内部网络的情况，可在网络边界内配备身份鉴别设备（如统一身份认证系统），并建立访问

控制机制，对接入设备进行接入控制。测评时应验证设备接入认证机制实现的合规性、正确性和有效性。

测评方法：

a）核查密码产品配置，验证身份鉴别协议、密码算法的合规性；

b）在接入设备与认证网关之间接入通信协议分析工具，捕获认证过程数据包，分析接入认证机制实现的正确性和有效性；

c）在条件允许的情况下，尝试将未授权设备接入内部网络，核实设备接入认证机制的有效性。

4.2.1.3 设备和计算安全

a）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

b）远程管理设备时，采用密码技术建立安全的信息传输通道；

c）采用密码技术保证系统资源访问控制信息的完整性；

d）采用密码技术保证设备中的重要信息资源安全标记的完整性；

e）采用密码技术保证日志记录的完整性；

f）采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

（1）身份鉴别

当用户登录从政务云服务提供商处租用虚拟机时，由于虚拟机镜像可能会被非法篡改或者被恶意者攻击，云用户首先关注虚拟机镜像模版的安全性，可以通过检查虚拟机镜像模版的真实性实现。使用数字签名、杂凑函数、带密钥的消息鉴别码和使用云服务提供商部署的自主访问控制来鉴别虚拟机镜像模版的真实性。政务云应采用密码技术对访问云平台计算资源和存储资源的用户进行身份标识和鉴别，使用智能密码钥匙（用于产生“挑战-响应”中的SM2数字签名）作为身份鉴别因素之一可满足该条款要求。测评时应验证设备本地登录身份鉴别机制是否符合相关标准要求，实现是否正确、有效。

测评方法：

a）使用数字证书格式合规性检测工具，验证设备证书是否合规，并验证证书签名结果是否正确；

b）条件允许情况下，使用总线监听工具对智能密码钥匙APDU指令进行抓取分析，验证身份鉴别机制实现的正确性。

（2）远程通信安全

云平台管理员与云平台管理应用之间的通信应建立安全传输通道，如采用SSL协议，保证云管理数据传输的安全性。测评时应验证远程通信安全机制实现的合规性、正确性和有效性。

测评方法：

a）在云平台管理终端与云平台管理应用服务器之间接入通信协议分析工具，分析云平台管理数据传输机密性和完整性保护措施是否有效、以及所采用的密码算法合规性；

b）如果云平台管理数据经机密性或完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能、MAC运算功能或签名验签功能是否被有效调用。

（3）虚拟机迁移

虚拟机迁移的过程中，需要控制平面和数据平面同时工作，方可完成一次成功的迁移。控制平面上，虚拟机监控器（VMM）之间的用来发起和管理虚拟机动态迁移的通

信机制需要加入身份鉴别和防篡改机制；数据层面上，虚拟机迁移的数据通信信道要进行安全加固，以防止可能的监听攻击和篡改攻击。测评时应验证虚拟机迁移安全保护措施的合规性、正确性、有效性。

测评方法：

a）对于同一物理机内的虚拟机迁移，在物理机虚拟交换机上使用数据包捕获工具，分析迁移前是否进行了VMM双向身份鉴别，迁移过程中的重要数据是否进行了机密性和完整性保护，使用的密码协议、密码算法是否合规；

b）对于跨物理机的虚拟机迁移，设定迁移的源主机和目的主机，在两台物理机之间的交换机上接入通信协议分析工具捕获通信数据，分析迁移前是否进行了VMM双向身份鉴别，迁移过程中的重要数据是否进行了机密性和完整性保护，使用的密码协议、密码算法是否合规；

在虚拟机迁移前的源主机上尝试修改虚拟机数据（或对应的MAC值），在目的主机上查看虚拟机数据完整性保护机制的有效性。

（4）重要可执行程序进行完整性保护

重要可执行程序进行完整性保护以及来源的真实性验证基于可信计算的完整信任链，信任链可基于PKI技术实现，根证书应存放在可信的安全单元内。

测评方法：

a） 核查是否采用密码技术对重要可执行程序进行完整性保护并实现其来源的真实性保护，并验证重要可执行程序完整性保护机制和其来源真实性实现机制是否正确和有效。

4.2.1.4 应用和数据安全

a）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

b）采用密码技术保证信息系统应用的访问控制信息的完整性；

c）采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

d）采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

e）采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

f）采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

g）采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

对于四级信息系统：

h）在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，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。

（1）身份鉴别

应用程序用户使用云服务过程中，确保用于与运行在虚拟机实例之上的应用程序实例的身份鉴别、云用户与部署的应用程序或开发工具实例之间的身份鉴别。通常使用SSL协议或SSH协议，实现服务实例和客户端之间的相互鉴别，也用来设置用于加解密和生成消息鉴别码的安全会话密钥。

测评方法：

a）使用数字证书格式合规性检测工具，验证设备证书是否合规，并验证证书签名结果是否正确；

b）工具检查云用户与验证引擎之间是否建立安全的通信信道，所采取的通信协议是否合规、协议实现是否正确、有效。

（2）传输机密性

政务云传输的云平台自身重要数据包括但不限于云平台资源访问者的身份鉴别信息、虚拟机镜像文件、租户镜像文件、租户快照文件等，应采用密码技术保证重要数据在传输过程中的机密性，可使用网络和通信层面搭建的安全传输通道或对待传输的数据进行加密运算后传输来实现。测评时应验证机密性保护机制实现的合规性、正确性和有效性。

测评方法：

a）在数据交互双方之间接入通信协议分析工具，分析是否进行了密钥协商、传输的重要数据是否非明文、数据格式（如分组长度等）是否符合预期、以及所采用的密码算法合规性；

b）如果重要数据加密后传输，在云服务器密码机等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能是否被有效调用。

（3）存储机密性

政务云存储的云平台自身重要数据包括但不限于网络边界和系统资源访问控制信息、重要信息资源敏感标记、重要程序或文件、日志记录、虚拟机镜像文件、租户镜像文件、租户快照文件等。其中，应采用密码技术保证虚拟机镜像文件、租户镜像文件、租户快照文件在存储过程中的机密性，测评时应验证机密性保护机制实现的合规性、正确性和有效性。

测评方法：

a）查看存储的重要数据，判断存储的数据是否非明文，数据格式是否符合预期，从而验证机密性保护措施的有效性；

b）检查相关密码产品算法配置是否正确；

c）在重要数据存储设备和密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能是否被有效调用。

（4）传输完整性

政务云传输的云平台自身重要数据包括但不限于云平台资源访问者的身份鉴别信息、虚拟机镜像文件、租户镜像文件、租户快照文件等，应采用密码技术保证重要数据在传输过程中的完整性，可使用网络和通信层面搭建的安全传输通道或对待传输的数据进行完整性保护后传输来实现。测评时应验证完整性保护机制实现的合规性、正确性和有效性。

测评方法：

a）在数据交互双方之间接入通信协议分析工具，分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）是否符合预期；如果是使用数字签名技术进行完整性保护的，可使用公钥对抓取的签名结果进行验证；

b）如果重要数据经完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析签名验签功能或MAC运算功能是否被有效调用。

（5）存储完整性

政务云存储的云平台自身重要数据包括但不限于电子门禁系统进出记录、视频监控音像记录、网络边界和系统资源访问控制信息、重要信息资源敏感标记、重要程序或文件、日志记录、虚拟机镜像文件、租户镜像文件、租户快照文件等。政务云应采用密码技术保证云平台自身重要数据在存储过程中的完整性，测评时应验证完整性保护机制实现的合规性、正确性和有效性。

测评方法：

a）查看存储的重要数据，判断受完整性保护的数据在存储时的数据格式（如签名长度、MAC长度）是否符合预期；
b）使用数字签名技术进行完整性保护的，可使用公钥对存储的签名结果进行验证；
c）在重要数据存储设备和密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析签名验签功能或MAC运算功能是否被有效调用；
d）在条件允许的情况下，尝试修改存储的重要数据（或对应的签名值、MAC值），查看完整性保护机制的有效性。

（6）关键行为抗抵赖

云平台管理应用应采用密码技术实现云平台管理员关键操作行为的抗抵赖，可通过使用智能密码钥匙中的签名私钥对云管理用户的关键操作信息进行签名、云平台管理应用调用服务器密码机或签名验签服务器进行验签来实现；可采用时间戳服务，对审计记录提供统一的时间标记。测评时应验证抗抵赖功能实现的合规性、正确性和有效性。

测评方法：

a）如果使用了第三方电子认证服务，则对密码服务进行核查；
b）使用相应的公钥对作为不可否认性证据的签名结果进行验证；
c）检查密码产品算法配置；
d）在云平台管理应用服务器和相关密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析验签功能、时间戳服务是否被有效调用。

4.2.1.5 密钥管理

云环境下的密钥管理，根据具体的应用需求，大量存在密钥半托管或全托管的形式。无论传统密码还是云密码，都要求密钥产生、存储、分发、使用、备份、销毁的全生命周期可管可控，而云环境下特有的虚拟化、分布性特点对密钥的全程管控提出了更高的要求。云平台自身密码应用涉及的密钥包括IPSec/SSL VPN身份鉴别签名密钥对、IPSec/SSL VPN加密密钥对、IPSec/SSL VPN会话密钥/工作密钥、云平台关键数据完整性保护密钥、云平台关键数据加密密钥、虚拟机迁移密钥等。政务云应保证密钥全生命周期（生成、存储、分发、导入与导出、使用、备份与恢复、归档与销毁等环节）的安全性，保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，保证公钥不被非授权的修改和替换。测评时应通过实际操作、查看记录、采集数据等方式验证密钥管理功能的正确性。

测评方法：

a）了解并核查各类密钥是否按照密码应用方案，由相应的机构或密码产品生成；
b）核查各类密钥是否按照密码应用方案进行存储，存储的介质或载体是否合规；
c）核查各类密钥是否按照密码应用方案和安全机制进行分发，获得密钥的实体是否为密码应用方案中指定的密钥角色；
d）核查密钥的使用、更新、撤销、归档、备份及恢复是否按照密钥管理策略执行。
e）密钥托管机制应核查设计方法是否采用秘密共享的方式，其他方式是否合理、合规，检查用户不应具有在他们中间分配其他秘密密钥的能力；
f）政务云加密服务中的加密密钥的访问需要进行严格的控制，在云加密服务不可用时，云服务提供商处存储的加密密钥也应当不可用，以使被加密数据的安全访问得到有效控制；

g）密钥的访问控制方面，应对密钥访问者的访问权限进行审核，应避免用户的越权访问，进而确定是否具备访问该密钥的权限，并对其行为进行控制，密钥的访问控制方式应能可靠地支持对多用户的不同级别或类别的信息进行有效隔离和完整性保护；

h）核查不同服务和政务云之间的密钥管理互操作协议是否合规，检查对称和非对称加密密钥、密钥策略等的管理机制。

4.2.2 云密码应用测评

政务云上提供数据加解密、完整性校验、签名验签等通用密码功能为政务云业务系统提供安全服务，政务云密码应用测评与传统架构的信息系统密码应用测评类似，由于云计算的特性，某些方面又存在着差异性，如政务云应用的密钥管理、政务云应用的模式以及政务云应用的数据保护等。结合GB/T 39786标准的密码应用要求的四个层面和云平台密钥管理进行描述。物理和环境安全在政务云应用方面的密码要求及测评方法和政务云平台上的基本相同，其测评结果可以复用，此处不再赘述。

4.2.2.1 网络和通信安全

a）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b）采用密码技术保证通信过程中数据的完整性；

c）采用密码技术保证通信过程中重要数据的机密性；

d）采用密码技术保证网络边界访问控制信息的完整性；

系统需要在该层面进行设备认证，则：

采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。

（1）身份鉴别

政务云的通信实体应在通信前基于密码技术对通信双方首先进行虚拟网络设备身份鉴别，可采用IPSec/SSL VPN技术方式实现。测评时应验证实体标识与鉴别数据的绑定方式是否合规、安全，鉴别机制是否符合相关标准要求，以及密码产品的合规性、使用的正确性和有效性。

测评方法：

a) 检查密码产品配置（算法、协议、双证书）是否正确；

b) 在两台 IPSec VPN 之间、客户端和 IPSec/SSL VPN 之间接入 IPSec/SSL 协议检测工具，分析密码协议是否符合密码相关国家标准、行业标准的有关要求；接入通信协议分析工具，捕获 IPSec 协议 IKE 阶段、SSL 协议握手阶段数据报文，分析密码算法标识或密码套件标识，验证身份鉴别采用的密码算法的合规性；

c) 使用数字证书格式合规性检测工具，验证VPN证书是否合规，并验证证书签名结果是否正确

（2）通信安全：

云平台管理员与云平台管理应用之间的通信应建立安全传输通道，如采用SSL协议，保证云管理数据传输的安全性。测评时应验证远程通信安全机制实现的合规性、正确性和有效性。

测评方法：

a）在云平台管理终端与云平台管理应用服务器之间接入通信协议分析工具，分析云平台管理数据传输机密性和完整性保护措施是否有效、以及所采用的密码算法合规性；
b）如果云平台管理数据经机密性或完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能、MAC运算功能或签名验签功能是否被有效调用。

4.2.2.2 设备和计算安全

a）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
b）远程管理设备时，采用密码技术建立安全的信息传输通道；
c）采用密码技术保证系统资源访问控制信息的完整性；
d）采用密码技术保证设备中的重要信息资源安全标记的完整性；
e）采用密码技术保证日志记录的完整性；
f）采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；

1）身份鉴别

政务云应采用密码技术对访问云平台计算资源和存储资源的用户进行身份标识和鉴别，使用智能密码钥匙（用于产生“挑战-响应”中的SM2数字签名）作为身份鉴别因素之一可满足该条款要求。测评时应验证设备本地登录身份鉴别机制是否符合相关标准要求，实现是否正确、有效。

测评方法：

a）尝试正常登录和异常登录（包括错误的口令、不插入智能密码钥匙或插入未授权的智能密码钥匙等情况）情况下，是否按照预期结果完成身份鉴别；
b）使用数字证书格式合规性检测工具，验证设备证书是否合规，并验证证书签名结果是否正确；
c）条件允许情况下，使用总线监听工具对智能密码钥匙APDU指令进行抓取分析，验证身份鉴别机制实现的正确性。

（2）远程通信安全

云平台管理员与云平台管理应用之间的通信应建立安全传输通道，如采用SSL协议，保证云管理数据传输的安全性。测评时应验证远程通信安全机制实现的合规性、正确性和有效性。

测评方法：

a）在云平台管理终端与云平台管理应用服务器之间接入通信协议分析工具，分析云平台管理数据传输机密性和完整性保护措施是否有效、以及所采用的密码算法合规性；
b）如果云平台管理数据经机密性或完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能、MAC运算功能或签名验签功能是否被有效调用。

（3）重要可执行程序进行完整性保护

重要可执行程序进行完整性保护以及来源的真实性验证基于可信计算的完整信任链，信任链可基于PKI技术实现，根证书应存放在可信的安全单元内。

测评方法：

a）核查是否采用密码技术对重要可执行程序进行完整性保护并实现其来源的真实性保护，并验证重要可执行程序完整性保护机制和其来源真实性实现机制是否正确和有效。

4.2.2.3 应用和数据安全

a）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；
b）采用密码技术保证信息系统应用的访问控制信息的完整性；
c）采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
d）采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
e）采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
f）采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
g）采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
对于四级信息系统：
h）在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，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；

（1）身份鉴别

应用程序用户使用云服务过程中，确保用于与运行在虚拟机实例之上的应用程序实例的身份鉴别。通常使用用户名+口令或者智能密码钥匙、移动终端密码模块的双因素身份鉴别，实现服务实例和客户端之间的相互鉴别。

测评方法：

a）使用数字证书格式合规性检测工具，验证设备证书是否合规，并验证证书签名结果是否正确；
b）工具检查云用户与验证引擎之间是否建立安全的通信信道，所采取的通信协议是否合规、协议实现是否正确、有效。

（2）传输机密性

政务云传输的云平台自身重要数据包括但不限于云平台资源访问者的身份鉴别信息、虚拟机镜像文件、租户镜像文件、租户快照文件等，应采用密码技术保证重要数据在传输过程中的机密性，可使用网络和通信层面搭建的安全传输通道或对待传输的数据进行加密运算后传输来实现。测评时应验证机密性保护机制实现的合规性、正确性和有效性。

测评方法：

a）在数据交互双方之间接入通信协议分析工具，分析是否进行了密钥协商、传输的重要数据是否非明文、数据格式（如分组长度等）是否符合预期、以及所采用的密码算法合规性；

如果重要数据加密后传输，在云服务器密码机等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能是否被有效调用。

（3）存储机密性

政务云存储的云平台自身重要数据包括但不限于网络边界和系统资源访问控制信息、重要信息资源敏感标记、重要程序或文件、日志记录、虚拟机镜像文件、租户镜像文件、租户快照文件等。其中，应采用密码技术保证虚拟机镜像文件、租户镜像文件、租户快照文件在存储过程中的机密性，测评时应验证机密性保护机制实现的合规性、正确性和有效性。

测评方法：

a）查看存储的重要数据，判断存储的数据是否非明文，数据格式是否符合预期，从而验证机密性保护措施的有效性；
b）检查相关密码产品算法配置是否正确；
c）在重要数据存储设备和密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析加解密运算功能是否被有效调用。

（4）传输完整性

政务云传输的云平台自身重要数据包括但不限于云平台资源访问者的身份鉴别信息、虚拟机镜像文件、租户镜像文件、租户快照文件等，应采用密码技术保证重要数据在传输过程中的完整性，可使用网络和通信层面搭建的安全传输通道或对待传输的数据进行完整性保护后传输来实现。测评时应验证完整性保护机制实现的合规性、正确性和有效性。

测评方法：

a）在数据交互双方之间接入通信协议分析工具，分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）是否符合预期；如果是使用数字签名技术进行完整性保护的，可使用公钥对抓取的签名结果进行验证；
b）如果重要数据经完整性保护后传输，在云服务器密码机、签名验签服务器等密码产品前接入通信协议分析工具，同时配合密码产品日志记录，分析签名验签功能或MAC运算功能是否被有效调用。

（5）存储完整性

政务云存储的云平台自身重要数据包括但不限于网络边界和系统资源访问控制信息、重要信息资源敏感标记、重要程序或文件、日志记录、虚拟机镜像文件、租户镜像文件、租户快照文件等。政务云应采用密码技术保证云平台自身重要数据在存储过程中的完整性，测评时应验证完整性保护机制实现的合规性、正确性和有效性。

测评方法：

a）查看存储的重要数据，判断受完整性保护的数据在存储时的数据格式（如签名长度、MAC长度）是否符合预期；
b）使用数字签名技术进行完整性保护的，可使用公钥对存储的签名结果进行验证；
c）在重要数据存储设备和密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析签名验签功能或MAC运算功能是否被有效调用；
d）在条件允许的情况下，尝试修改存储的重要数据（或对应的签名值、MAC值），查看完整性保护机制的有效性。

（6）关键行为抗抵赖

云平台管理应用应采用密码技术实现云平台管理员关键操作行为的抗抵赖，可通过使用智能密码钥匙中的签名私钥对云管理用户的关键操作信息进行签名、云平台管理应用调用服务器密码机或签名验签服务器进行验签来实现；可采用时间戳服务，对审计记录提供统一的时间标记。测评时应验证抗抵赖功能实现的合规性、正确性和有效性。

测评方法：

a）如果使用了第三方电子认证服务，则对密码服务进行核查；
b）使用相应的公钥对作为不可否认性证据的签名结果进行验证；
c）检查密码产品算法配置；
d）在云平台管理应用服务器和相关密码产品之间的交换机接入通信协议分析工具，同时配合密码产品日志记录，分析验签功能、时间戳服务是否被有效调用。

4.2.2.4 密钥管理

政务云为云上应用提供密码服务涉及的密钥包括物理密码机主密钥、虚拟密码机主密钥、应用主密钥、云上应用密钥对、租户密钥对、云上应用重要数据保护密钥等。政务云应保证密钥全生命周期（生成、存储、分发、导入与导出、使用、备份与恢复、归档与销毁等环节）的安全性，保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，保证公钥不被非授权的修改和替换。另外，政务云为云租户提供密钥托管功能，应采用严格的鉴别机制确保只有使用该服务的用户才能对其应用密钥管理系统进行配置；应确保用户在云平台中使用密钥时，处理独立安全环境中或用户租用的密钥管理系统中；应采用密钥隔离手段，确保云平台使用的密钥和云租户使用的密钥不得分配同一密钥管理系统进行管理。测评时应通过实际操作、查看记录、采集数据等方式验证密钥管理功能的正确性。

测评方法：

a）了解并核查各类密钥是否按照密码应用方案，由相应的机构或密码产品生成；

b）核查各类密钥是否按照密码应用方案进行存储，存储的介质或载体是否合规；

c）核查各类密钥是否按照密码应用方案和安全机制进行分发，获得密钥的实体是否为密码应用方案中指定的密钥角色；

d）核查密钥的使用、更新、撤销、归档、备份及恢复是否按照密钥管理策略执行。

e）密钥托管机制应核查设计方法是否采用秘密共享的方式，对于云租户的签名密钥应采用门限机制实现密钥信息秘密共享，不应采用全托管方式，其他方式（如同态加密、多方计算等）是否合理、合规，检查用户不应具有在他们中间分配其他秘密密钥的能力；是否落实了密码应用方案中的密钥管理方案；

f）政务云加密服务中的加密密钥的访问需要进行严格的控制，在云加密服务不可用时，云服务提供商处存储的加密密钥也应当不可用，以使被加密数据的安全访问得到有效控制；

g）密钥的访问控制方面，应对密钥访问者的访问权限进行审核，应避免用户的越权访问，进而确定是否具备访问该密钥的权限，并对其行为进行控制，密钥的访问控制方式应能可靠地支持对多用户的不同级别或类别的信息进行有效隔离和完整性保护；

h）核查不同服务和政务云之间的密钥管理互操作协议是否合规，检查对称和非对称加密密钥、密钥策略等的管理机制。

4.3 政务云密码应用测评的主要流程和步骤

政务云的密码应用安全性评估过程分为四项基本活动：测评准备活动、测评方案编制活动、现场测评活动、综合测评与报告编制活动。

4.3.1 测评准备活动

测评准备活动的目标是顺利启动测评项目，准备测评所需的相关资料，为编制测评方案打下良好的基础。测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。

4.3.1.1 项目启动

密评机构首先与测评委托单位签订测评委托协议或合同，在项目启动任务中，密评机构根据测评委托协议和被测政务云规模，组建密评项目组，从人员方面做好准备，并

编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等内容。

4.3.1.2 信息收集和分析

密评项目组获取责任单位和被测政务云的基本情况，通过查阅政务云已有资料，了解整个系统的构成和密码应用情况，为编写测评方案并开展现场测评工作奠定基础。

密评项目组收集责任单位提供的基本资料，包括：被测政务云描述文件（包含安全需求分析、安全方案设计、安全保护等级定级情况等相关文件）、安全管理制度文件（包含密码和密钥管理等相关文件）、密码应用方案及评审意见等。如果责任单位提供的基本资料不完善或存在相互矛盾的地方，测评人员可以与政务云相关人员进行进一步沟通，以全面、准确了解政务云的密码应用情况。对于在规划阶段没有专门制定密码应用方案的已建政务云，密评机构应提炼和总统出实际的密码应用方案。

4.3.1.3 工具和表单准备

密评项目组成员在进行现场测评之前，应熟悉与被测政务云相关的各种组件、调试测评工具、准备各种表单等。主要包括以下步骤：

a）测评人员选取并调试本次测评过程中将用到的测评工具；

b）如果具备条件，测评人员可以模拟被测政务云搭建测评环境进行前期准备和验证，为测评方案编制活动、现场测评活动提供必要的基础；

c）准备和打印表单，主要包括：现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表等。

4.3.2 测评方案编制活动

测评方案编制活动的目标是整理测评准备活动中获取的政务云相关资料，为现场测评活动提供最基本的文档和指导方案。测评方案编制活动包括测评对象确定、测评指标确定、测评检查点确定、测评内容确定、以及测评方案撰写和确认五项主要任务。

4.3.2.1 测评对象确定

测评人员根据已经了解到的被测政务云信息，分析整个政务云及外部相关系统，确定出测评对象。主要包括以下步骤：

a）描述被测系统。测评人员对政务云资料进行整理，确定被测系统并加以描述。描述时一般以政务云的网络拓扑结构为基础，采用总分式的描述方法，先说明整体结构，然后描述外部边界连接情况的边界主要设备，最后介绍网络区域组成、主要业务功能及相关的设备节点，并着重描述其中的密码应用情况；

b）确定测评对象。测评人员分析政务云的重要程度及其相关资产、设备和组件，根据核心资产在政务云内的流转，确定出与密码相关的测评对象。责任单位需要确定被测政务云需要保护的核心资产。核心资产以及其他需要保护的配套数据（如审计信息、配置信息、访问控制列表等）、敏感安全参数（主要指密钥）的价值由责任单位根据密码应用方案、等级保护定级方案等继承和确定，并与密评机构进行协商确认；

c）资产价值评估。责任单位对于各类核心资产、密钥、控制访问列表信息、配置信息、审计信息等敏感信息，根据资产的重要性和关键性，进行资产价值的认定。资产价值分为高、中、低三个等级，价值越高的资产遭到威胁时将导致更

高的风险。资产价值高低的界定可由责任单位根据密码应用方案、等级保护定级方案等继承和确定，并与密评机构进行协商确认；

d）描述测评对象。测评人员描述测评对象时，一般采用分门别类的方式加以描述，包括机房及物理环境、业务应用软件、主机操作系统、数据库管理系统、网络互联设备、密码设备、安全设备、安全管理人员、安全管理文档等。在对每类测评对象进行描述时则一般采用列表的方式，包括测评对象所属区域、设备名称、用途及涉及的密码技术等内容。

4.3.2.2 测评指标确定

根据已经了解到的被测政务云定级结果，测评人员确定出本次测评的测评指标。

测评指标确定主要包括以下步骤，尤其要注意其中不适用指标的判定：

a）根据被测政务云提供的基本资料，获得被测政务云的定级结果；

b）根据被测政务云等级保护的级别，选择相应等级的安全要求作为测评指标；

c）不适用指标的判定可以遵循以下原则：

通过评审的密码应用方案中未列的密码安全功能指标可列为不适用指标；

政务云无相应安全需求的指标，可列为不适用指标；

应依据政务云的保护边界明确测评边界，由边界外的对象所实现的功能指标可列为不适用指标。

4.3.2.3 测评检查点确定

测评过程中，需要对一些关键安全点进行现场检查确认，比如利用工具抓包测试，查看关键设备的配置，确认密码算法、密码产品、密码服务的使用情况等。这些检查点需要在方案撰写时考虑，并且充分考虑到检查的可行性和风险，最低限度的避免对被测政务云，以及云上业务系统的影响。主要包括以下步骤：

a）根据政务云实际情况，确定进行现场检查的测试点和测试方法；

b）为了防止密码产品未在政务云中实际发挥作用的情况发生，测评人员应重点确认密码产品是否在政务云中被正确、有效的调用；

c）需要使用工具检查时，在尽量保证政务云正常、安全运行的情况下，确定工具接入点，并结合网络拓扑图，采用图示的方式描述测评工具的接入点、测评目的和测评对象等相关内容。

4.3.2.4 测评内容确定

本部分确定现场测评的具体实施内容，即单元测评内容。主要是依据责任单位提供的通过评审的政务云密码应用方案，把各层面上的测评指标结合到具体测评对象上，并说明具体的测评方法，构成可以具体实施的测评单元。涉及到现场测评部分，应根据确定的测试检查点，编制相应的测评内容。

4.3.2.5 测评方案撰写和确认

测评方案是测评工作实施的基础，用于指导测评工作的现场实施活动。测评方案包括但不限于以下内容：项目概述、密码应用情况、测评对象、测评指标、测试检查点以及单元测评实施等。主要包括以下步骤：

a）根据委托测评协议书和责任单位提供的基本资料，描述政务云及其密码应用情况等内容：

b）列出测评活动所依据的标准和规范性文件；
c）依据委托测评协议书和被测政务云情况，估算现场测评工作量。工作量可以根据配置检查的节点数量和工具测试的接入点及测试内容等情况进行估算；
d）根据密评项目组成员和责任单位人员安排，编制工作安排情况。在进行时间计划安排时，应尽量避开被测政务云的业务高峰期，避免给政务云带来影响。同时，在测评计划中应将具体测评所需条件以及测评需要的配合人员也一并给出，便于测评实施之前双方沟通协调、合理安排；
e）密评机构应对撰写完成的测评方案进行审核和确认后方可允许测评人员开展现场测评活动。

4.3.3 现场测评活动

现场测评活动是密评工作中的重点。密评机构依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

4.3.3.1 现场测评准备

本任务启动现场测评，是保证密评机构能够顺利实施测评的前提。主要包括以下步骤：

a）召开测评现场首次会，密评机构介绍测评工作，说明测评过程中具体的实施工作内容，进一步明确测评计划和测评方案，明确测评时间安排以及测评过程中可能存在的安全风险等，以便于后面的测评工作开展；
b）测评双方确认现场测评需要的各种资源，包括责任单位的配合人员和需要提供的测评条件等，确认被测系统已备份相关数据；
c）与责任单位签署现场测评授权书。

4.3.3.2 现场测评和结果记录

密评项目组根据测评方案以及现场测评准备的结果，安排测评人员在约定的测评时间，通过人员访谈、文档审查、实地查看、配置检查以及工具测试的方法开展测评工作。主要包括以下步骤：

a）测评人员检查系统边界内所有实现密码功能的密码算法、密码产品和密码服务是否取得了国家密码主管部门的核准或许可；
b）测评人员根据责任单位提供的密码产品用户手册、密码应用方案等进行密码产品配置检查。对于经检测认证合格的密码产品，测评时不对其本身进行重复检测，主要进行符合性核验和配置检查；
c）测评人员根据现场测评结果填写完成测评结果记录表格。

4.3.3.3 结果确认和资料归还

密评项目组完成现场测评后，测评双方对发现的问题进行确认，并归还相关资料。主要包括以下步骤：

a）测评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对遗漏和需要进一步验证的内容实施补充测评；
b）测评双方对测评过程的主要现场记录和事实进行现场确认；

c）密评机构归还测评过程中借阅的所有文档资料，并由责任单位文档资料提供者签字确认。

4.3.4 综合测评与报告编制活动

现场测评工作结束后，密评项目组对现场测评获得的测评结果进行汇总分析，并编制评估报告。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、综合测评及评估报告编制等主要任务。

4.3.4.1 单项测评结果判定

本任务主要是针对测评指标中的单个测评项，结合具体测评对象，分析测评证据，形成单项测评结果，单项测评结果是形成评估结论的基础。主要包括以下步骤：

a） 针对每个测评项，分析该测评项所对抗的威胁在被测政务云中是否存在，如果不存在，则该测评项应标为不适用项；

b） 针对每个测评项，如果该测评项为适用项，则判定测评结果与预期结果之间的一致性，包括符合、部分符合和不符合三种结论；

c） 形成单项测评结果汇总表。

4.3.4.2 单元测评结果判定

本任务主要是对单项测评结果进行汇总，分别统计所属不同单元的单项测评结果，从而判定各个单元测评结果，并以表格的形式逐一列出。

测评对象在某个测评指标的单元测评结果判别原则如下：

a）测评指标包含的所有测评项的单项测评结果均为符合，则该测评对象对应该测评指标的单元测评结果为符合；

b）测评指标包含的所有测评项的单项测评结果均为不符合，则该测评对象对应该测评指标的单元测评结果为不符合；

c）测评指标包含的所有测评项的单项测评结果不全为符合或不全为不符合，则该测评对象对应该测评指标的单元测评结果为部分符合。

4.3.4.3 综合测评

针对单元测评结果中的部分符合和不符合单元，采取逐条判定的方法，给出综合测评结果。主要包括以下步骤：

a）针对单元测评结果中的部分符合和不符合单元，分析其中的测评项与相关的其他测评项、其他层面的测评对象、其他区域的测评对象是否能发生关联关系，这些关系是否能“弥补”该测评单元的不足，以及该测评单元的不足是否会影响与其有关联的测评单元的测评结果；

b）汇总上述分析结论，形成系统综合测评结果。

4.3.4.4 评估报告编制

评估报告包括但不限于以下内容：评估概述、测评对象、测评指标、测评内容和方法、单项测试、单元测评、综合测评结果等。报告编制主要包括以下步骤：

a）评估概述描述被测政务云的总体情况、测评的主要目的和依据。在编制测评对象、测评指标、测评内容和方法等部分时，应参考测评方案的相关部分内容，并根据实际测评情况进行修改：

b）针对被测政务云存在的安全隐患，从系统安全角度提出改进建议。此外，由于系统现有情况限制所造成的某些不适用指标，也可以给出相应的改进建议；
c）列表给出现场测评的文档清单和单项测评记录，以及单项测评结果判定情况，给出单元测评和综合测评的结果；
d）评估报告编制完成后，密评机构应根据测评委托协议书、责任单位提交的相关文档、测评原始记录和其他辅助信息，对评估报告进行内部审核；
e）评估报告经密评机构内部审核通过后，由授权签字人进行签发，提交测评委托单位；
f）测评委托单位将评估报告提交至政务云项目验收专家组，专家组进行综合评审，给出评审意见，为管理部门给出项目审查或验收决策提供参考。

5 标准化研究

由于云计算自身的特点、部署模式、安全需求、运营管控需求、审计与服务连续性、合规性需求等特殊性，云计算将不是传统的小规模分散式的运作模式，资源集中化和规模化更需要强调系统的规范化建设。密码技术作为支撑云计算应用安全的核心，为适应这种模式的转型，重要的是建立密码应用技术体系规范和建设安全管理基础设施。加强商用密码标准和云计算应用结合度，加大密码标准对云计算的支撑力度，加强云计算环境下的密码基础类标准、应用类标准、检测类标准和管理类标准的研究和制定。

5.1 本研究报告在现在标准体系中的位置

对于政务云中如何落实相关标准要求和管理规定，目前还没有相应的指导性文件，也缺乏相应的标准、技术规范。这将导致密码在政务云中的应用、测评无“法”可依。因此本研究报告帮助责任单位在政务云的规划设计、建设实施和运行维护中合规、正确、有效地运用密码技术，更加充分有效的发挥密码技术在政务云中的安全保障作用。同时，帮助测评人员如何针对政务云进行科学的测评提供指导依据。

5.2 标准化建议

建议完善云计算密码应用技术标准体系，密码技术为实现云计算的技术创新，需要建立云计算密码应用技术标准体系，该标准体系包括基础类标准、应用类标准、检测类标准和管理类标准，如云计算密码应用体系框架规范、数据加密标准、密码接口标准、身份认证管理标准、密钥管理标准等。

建议完善虚拟化密码应用指南/规范/标准：主要研究/制定在虚拟化应用场景中身份认证和访问管理、隐私保护、虚拟化安全、存储安全等领域中密码应用技术规范；以及多租户环境下密码应用相关规范/指南等。

建议完善云计算中密码设备虚拟化标准：制定云计算中密码设备（密码卡、USB_KEY）的虚拟化标准，提供与云计算平台无关的通用接口标准、应用标准、请求标准、设备虚拟化安全标准。

建议完善密码服务虚拟化标准：包括密码服务虚拟化的全过程应用、接口、请求与响应，虚拟化密码服务及安全标准等。

建议加密卡虚拟化研究/指南/规范/标准：主要研究/制定虚拟化环境下加密卡的软硬件技术要求和应用体制要求，使加密卡适用于云计算的基础设施环境。如平台虚拟化、I/O虚拟化等，研究虚拟化环境下的加密卡应用需求模式，加密卡的软件虚拟化研究、加密卡的硬件虚拟化研究。虚拟化环境下加密卡密钥管理需求研究、虚拟化环境下的加密卡密钥管理机制的适应性研究、虚拟化环境下设备迁移过程的密钥管理研究等。

建议云计算身份鉴别技术规范，研究在云计算环境下身份鉴别技术，结合我国云计算在不同云服务中的身份认证需求，提出独立于云服务的开发的身份标示认证框架；在充分考虑OpenID现有的安全问题基础上，定义认证协议主体及流程；深入研究认证协议及认证过程中的互操作性和应用环境，对传输的数据格式、通信类型、通信过程、签名方法等制定具体的实施细则。

建议移动终端平台应用安全技术规范：研究移动终端如移动浏览器、移动APP的安全访问以及安全接入，研究移动证书在移动终端使用中的发放流程与业务规则，研究终端数据安全存储，研究移动设备自身的安全性，研究虚拟化技术为移动终端平台安全提供的应用模式。

建议完善云密钥管理技术标准，我国尚未开展相关工作，但鉴于我国产业界云服务市场的迫切需求以及在云密钥管理方面已有一些初步的实施方案，因此有必要提出一个明确的、清晰的云密钥管理技术及密码技术支撑体系框架，为未来云计算环境下密钥管理相关工作提供参考与指导。

建议完善云平台密码应用测评标准。现行的密码应用安全性评估标准或规范，能够很好地指导传统网络与信息系统的密码应用安全性测评实施，但不能完全体现云计算的特点，缺少云平台密码应用及测评方面的相关标准或指南，导致不同测评机构对标准规范的把握程度不同、对云计算密码应用的理解不同、以及技术能力参差不齐，难以依据现有的测评指导标准或规范全面、有序地开展云平台密码应用安全性评估工作。

6 总结

政务云作为行业云，和一般云计算系统面临的问题几乎一样，现在基于 GB/T 39786 标准做政务云测评，很多要求不好落地，GB/T 39786 要求中很多密码技术在云环境中如何应用，如云密钥管理、云身份鉴别等密码技术，需要针对云计算的制定专门的密码应用规范、测评规范等。

通过政务云密码应用测评研究，可以为后续测评提供支撑，提高测评机构对政务云密码应用测评质量，指导测评机构实施具体测评工作。同时，云服务商在政务云密码应用建设或改造时，可以根据研究报告并结合自身应用特点，开展密码保障系统研发和建设工作。