北京商用密码行业协会
Beijing Commercial Cryptography Industry Association

云密码服务技术白皮书（2019）

北京商用密码行业协会

2019 年 9 月

前言

网络安全离不开密码，密码创新促进网络发展。构建普遍安全的网络空间命运共同体，要树立以总体国家安全观为统领，以密码为核心技术和基础支撑的网络信息安全观，通过密码实现网络的可信互联、安全互通，推动建设网络新安全机制、新安全环境、新安全文明。

当前，大数据、人工智能、移动互联网、物联网等技术蓬勃发展，这些新型网络技术或产业都离不开云计算的支撑。云计算作为一种新的信息系统构建模式，正深刻影响着网信行业，它的一个核心特征就是走向平台化、服务化。这个特征对传统的信息技术和产品提出了新的要求，那就是无论从产品形态、部署方式、还是商业模式都要适应云计算中的服务化需求。密码技术也不例外，必须与时俱进，适应云计算的服务化需求，云密码服务的概念就是在这种大环境、大背景下提出的。从传统的密码应用方式转型为云密码服务，面临技术上的、产品上的、部署上的、运维上的、监管上的诸多变化，适应这些变化需要一个过程，这对密码服务供给侧和需求侧都是一个挑战。

北京商用密码行业协会（简称“北京商密协会”）是中国最大的商用密码行业协会，汇集了国内近一半的商密领域企业，近几年协会成员单位积极拥抱云计算，围绕云密码服务积极攻关，对云密码服务的体系框架和关键技术开展深入研究，并在云密码服务领域积累了一些应用经验。为了推动我国云密码服务产业更健康地发展，协会组织有关企业，集思广益、深入研讨，编写了该《云密码服务技术白皮书》（以下简称白皮书）。本白皮书对云密码服务的发展现状和应用需求进行了调研和分析，总结出云密码服务的技术体系框架，从基础设施、服务模式和管理运营等方面阐述了云密码服务的内容和特点。希望本白皮书能够为密码服务的提供商、密码服务的用户提供帮助。

《云密码服务技术白皮书》的编写得到了国家密码管理局和北京市密码管理局领导的支持和指导，得到了北京商用密码行业协会技术专家委员会各位专家的指导和帮助，是北京商用密码行业协会集体智慧的结晶，在此向指导和参与工作的领导、专家和同行表示感谢。

由于编者能力所限，有些观点不一定准确，错误也在所难免，欢迎批评指正。希望本白皮书起到抛砖引玉的效果，推动我国云密码服务产业的健康发展。

顾问指导：

詹榜华　刘　平　荆继武　王建华　郭宝安　季庆光　楠亚丁

于　佳　杨恒亮　孔凡玉　何德彪　张大伟　贾　嘉　秦小龙

指导单位：

北京市密码管理局

参与编写单位：

北京三未信安科技发展有限公司

北京数字认证股份有限公司

兴唐通信科技有限公司

北京信安世纪科技股份有限公司

航天信息股份有限公司

北京天融信网络安全技术有限公司

北京海泰方圆科技股份有限公司

北京网御星云信息技术有限公司

北京中金国信科技有限公司

北京天威诚信电子商务服务有限公司

北京集联网络技术有限公司

北京永新视博数字电视技术有限公司

北京炼石网络技术有限公司

北京江南天安科技有限公司

北京紫光同芯微电子有限公司

编写人员：

张岳公	高志权	邵　淼	魏常辉	李向锋	汪宗斌
全代勇	刘尚焱	傅大鹏	吴　迎	张　妍	孙　燕
王明阳	刘会议	高　嵩	姜晓新	汪　海	刘　岸
宁红宙	蒋红宇	林剑远	张　晶	白小勇	钱　晶
尹　刚	耿　方	胡　伟	刘　婷	赖华添	

目录

第 1 章　导论

1.1 背景

作为新型的信息系统构建架构，云计算自诞生以来发展迅速，它提供的大规模计算、大容量存储、弹性部署、按需提供资源的能力，为用户的业务创新提供了便利，推动了大数据、人工智能、物联网等技术的发展，开始带来一场人类社会的数字化革命。

云计算给整个信息产业带来改变。首先，它促进了一些技术的发展，如虚拟化技术、软件定义网络技术（SDN）、高速网络技术、超大规模数据中心技术，这些技术使得传统的信息系统构建架构发生了变化，软硬件资源标准化、模块化、组件化，更容易复用、集成、管理、动态扩展。其次，它改变了一些产品的形态，过去一些以独立硬件形态存在的设备如路由器、交换机、防火墙、密码机、VPN 网关、入侵检测、堡垒机等开始软件化，以软件模块的形态部署在云服务器上，云服务器成了统一的底层硬件基础设施。最后，也是最大的改变，云计算在改变信息产业的商业模式。过去用户购买硬件、软件，现在是用户租用或购买云平台上的服务，用户像使用自来水、电一样使用云计算平台提供的信息设施服务。云计算服务通常分为 IaaS（Infrastructure as a Service，基础设施即服务）、PaaS（Platform as a Service，平台即服务）、SaaS（Software as a Service，软件即服务）三类，传统的信息产品和技术公司迫切需要按照平台化、服务化的思路，进行产品到服务的转型。

《中华人民共和国密码法（草案征求意见稿）》中对密码的定义：密码是指使用特定变换对数据等信息进行加密保护或者安全认证的物项和技术。密码技术是保障网络安全的核心技术，通过保护数据的机密性、完整性和可用性来保护信息、传递信任。在传统的信息系统架构中，密码技术主要是以独立的软、硬件产品的形态提供密码功能，商业模式也大都是软、硬件的销售模式。但是，云计算推动密码技术从产品形态、商业模式都需要进行向云密码服务转型。

正是在云计算发展形势的推动下，2013 年的美国 RSA 大会议上提出了

“Cryptography as a Service（CaaS，密码即服务）”的概念，探索了密码功能以服务方式来交付的可能性，并设想了相关的应用场景。随后，学术界对这一概念进行了不断的丰富和拓展，并发展出了加密即服务（EaaS）、密钥管理即服务（KMaaS）等新的概念。产业界也进行了更多密码产品和功能的服务化探索，出现了 Amazon Cloud HSM、CoSign 电子签名服务等云密码服务。在我国从 2014 年开始，不少密码厂商就开始了以云服务方式提供密码功能的产品的研发工作，出现了云密码机、云签名系统、云密钥管理等产品，同时一些企业开始推出了云密钥管理服务、云数据加密服务、云身份认证服务、云电子签名服务和云电子合同服务等。

总之，产业界已经认识到密码技术和产品向云密码服务转型的趋势，并正在实践探索中，但云密码服务的应用处于初期阶段，无论从技术上还是商务模式上，还缺乏经验，密码技术的供给侧和需求侧都面临许多需要解决的问题。

1.2 密码技术对云计算的重要性

当前云计算的发展中，安全成为最大的制约因素。随着社会网络化、信息化的程度越来越高，数据资产的价值越来越高，即使在传统的网络信息系统中网络安全问题也是道高一尺魔高一丈，总是面临新的问题。到了云计算环境中，因为云中的网络环境更加复杂，网络安全面临更严峻的挑战。首先，云计算强调信息资源的共享和按需使用，采用虚拟化、分布式存储等技术实现计算资源、存储资源的共享和按需分配，甚至云计算中的网络也通过 NFV（网络功能虚拟化）、SDN（软件定义网络）等技术实现了虚拟化和动态分配。共享提高了资源的利用率，但增加了管理的复杂性，特别是模糊了不同信息系统之间的边界。边界的模糊使得过去许多基于边界防护的网络安全技术面临窘境，如传统的防火墙技术、入侵检测技术等，虽然有 VLAN 等简单的隔离技术，但安全强度不够，使得用户对自己在云上信息的安全管控难以实现。其次，云计算的平台化运营使得信息系统的运营者和使用者可能分离，特别是在公有云中，用户租用公有云运营商的信息资源服务，这时用户的数据和信息系统运行在运营商的公有云上，自己失去了对信息基础设施的控制权，用户怎样相信云运营商能保证用户的信息安全？云运营

商提供什么技术和服务承诺才能让用户放心？这是需要回答的问题。

面对云计算的网络安全挑战，安全产业界认识到传统的网络安全方法和技术的不足，正进行技术升级和创新。普遍的共识是，传统的基于网络边界的安全防护策略和技术在云计算中面临挑战，不能再作为主要的防护思想，而应该基于云中数据的流动、存储、使用等场景定义基于数据的纵深防御体系。我们认为目前在云中有两类安全技术受到重视：

（一）身份认证和授权管理技术。面对日益复杂的网络环境，约翰·金德维格（John Kindervag）于 2010 年提出了“零信任网络”（模型亦称零信任架构），它的基本思想是不再区分内外网，不自动信任内部或外部网络的任何设备和人，应在授权前对任何试图接入企业系统的设备和人进行验证。基于这个思想，谷歌在 2013 年提出了 BeyondCorp 模型，CSA（Cloud Security Allian：云安全联盟）组织于 2014 年提出了 SDP（Software Defined Perimeter：软件定义边界）安全模型，这些模型和实践不依赖基于网络边界的防护策略，采用身份验证、IAM（Identity and Access Management：身份识别与访问管理）和权限管理等技术，做到随时随地的安全访问。

（二）数据加密技术。大数据、人工智能、物联网等技术的发展使人类开始进入数据时代，数据会越来越多、越来越重要，这些数据大都会存放在云中。由于数据的易复制性，数据的安全问题成为云中要解决的急迫问题。所以现在提出数据的全生命周期加密保护思想，在数据从产生、传输、存放等各个环节进行加密保护。

无论身份认证、授权管理、数据存储加密、数据传输加密等，都离不开密码技术，密码技术通过基于数学原理的密码算法来对数据本身进行变换处理，保护数据的私密性、完整性和可用性。不同于基于网络边界的被动安全防护技术，密码技术可以和数据紧密结合，在网络的各个层次部署，实现信息数据的主动安全保护。被加密的不同信息系统的数据在共享的云网络中各自独立，各行其道，只有拥有权限的用户才能使用。CSA 提出的“软件定义边界”在云中要依靠密码技术来完成，有人称之“密码定义边界”。密码技术不仅提供身份验证、授权管理、

全生命周期数据加密保护，还为云中的电子交易提供了业务防抵赖（电子签名）、数据防止篡改（完整性保护）等功能，同态加密、多方计算等新兴密码技术在未来的大数据应用中还能实现隐私保护下的数据共享应用。

由于密码算法是基于坚实的数学基础的，因此密码技术达到的安全强度是可被证明的。如果云运营商采用了合适的密码技术体系来保障用户的信息安全，他是可以向用户证明其服务承诺的。

因此密码技术是保障云安全的重要技术，云密码服务把密码能力变成云中的一种资源服务，在云服务体系中具有十分重要的地位和作用。

1.3 云密码服务的概念

信息资源的平台化、服务化是云计算带给用户最大的好处。用户可以不用关心信息平台建设的细节，按照自己的需求，从云计算平台随时地获得信息资源，而且这些资源是可灵活配置的、动态扩展的。

云密码服务是一种全新的密码功能交付模式，是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的深度融合。密码服务提供商按照云计算技术架构的要求整合密码产品、密码使用策略、密码服务接口和服务流程，将密码系统设计、部署、运维、管理、计费等组合成一种服务，来解决用户的密码应用需求。用户不再“购买”密码硬件或密码系统等密码产品，而是以“租用”的方式使用云中提供的各种密码功能，因此，云密码服务也是一种新的商业模式，云密码服务给传统密码产业带来革命性的影响，具有以下优势：

（1） 按需服务

云密码服务的类别越来越丰富，可以满足多种密码应用需求，用户可以根据自己的功能和性能需要选择合适的密码服务，并且计费方式也越来越精细化。

（2） 快速集成

随着标准化工作的不断推进，云密码服务会变得插件化和标准化，可以像搭积木一样方便快速的集成到密码应用中。

（3） 可伸缩性

和“云”一样，云密码服务也可以动态伸缩，用户不用加大硬件设备投资就能快速满足应用和用户规模增长的需要。

（4） 易于使用

用户不需要掌握专业的密码学知识即可安全的使用云密码服务提供的密码功能，降低了用户的使用门槛。

（5） 成本更低

选用云密码服务由“购买”变为“租用”，不用采购密码设备或密码系统，节约了密码基础设施的建设成本；密码资源的共享有效减少密码应用的使用成本。

（6） 使用更规范

精细化的云密码服务可以帮助用户正确的使用密码技术，也有助于建设安全合规的密码应用系统。

（7） 适用性更强

密码功能以云服务的方式提供，不仅可以解决许多传统密码应用的需求，也适用云计算、大数据等更多应用场景。

1.4 云密码服务的市场前景

当前在全世界范围内云计算发展迅猛，现在安全是掣肘云计算发展的最主要问题，作为网络安全核心技术和基础支撑的密码技术在云计算中将越来越重要。我国高度重视密码技术在保障网络安全中的作用，把密码作为国家的重要战略资源，在金融和重要应用领域全面推广国产密码算法应用，并即将颁布《密码法》。国家已经颁布的《网络安全法》和网络安全等级保护制度 2.0，对云计算环境的安全建设提出了明确的要求，并明确三级及以上的系统需要进行密码应用安全性测评。这些应用需求和政策要求必将给云密码服务带来巨大的市场需求，因此密码产业界应该抓紧进行云密码服务需求的研究、技术和产品的开发、应用的推广部署，为我国的云计算健康发展保驾护航。

第 2 章　云密码服务现状和挑战

随着公有云、私有云、混合云的蓬勃发展，越来越多的重要业务系统迁入云中，使得云计算的安全保障越来越重要，从而推动了密码技术在云安全保障中的应用。一方面不少云平台本身采用密码技术加强自身的安全，另一方面，一些对云用户的云密码服务开始出现，并在一些应用中已经取得较好的成果。但总体情况是尚处于初级阶段，有待发展和完善。本章分析云密码服务发展现状及面临的技术挑战。

2.1　云密码服务应用现状

云密码服务的发展是伴随着云计算应用的不断推进而不断发展。在公有云发展和逐步成熟的进程中，公有云运营商首先提供了密钥管理、数据加密等云密码服务；随着 SaaS 服务的兴起，一些面向公众的以密码技术为安全基础的 SaaS 服务被推出，如身份认证服务、电子合同服务等；另外，传统的密码产品厂商也顺应产品云服务化的需要，推出了一些适合云中部署的产品和服务，为云运营商或云用户提供密码技术解决方案，如密码资源池、云安全访问代理（CASB）服务等。下面我们总结当前出现的主要云密码服务。

（1）　云密钥管理服务

云中的用户身份认证、设备认证、安全通信、数据加密都需要密钥，因此云中存在大量的密钥管理需求。由于密钥的重要性，不但要保证生成、存储、销毁的安全，还要能够方便地获取、使用，因此需要专门的密钥管理系统来保证密钥全生命周期的安全。出于对密钥安全性的考虑，用户可以建立自己的密钥管理系统，但由于用户在密钥管理方面的不专业，更多的是使用云运营商提供的密钥管理服务，或第三方提供的云密钥管理服务。使用云运营商提供的密钥管理服务，方便、快捷，但存在数据和密钥都被云运营商掌握的风险；使用第三方密钥管理服务，数据和密钥分离，可以有更高的安全性。

为了实现密钥管理的互通性和方便性，OASIS 组织制定了密钥管理互联协议（KMIP），KMIP 支持加密应用系统和密钥管理系统之间的可互操作通信，实

现对密码元素进行密钥管理操作。这些元素包括对称密钥和非对称密钥、证书，以及用于创建这些密钥和证书所使用的模板。KMIP 简化了管理密钥的方式，避免了对冗余、不兼容密钥的管理过程，使密钥生命周期管理，包括密钥的生成、提交、更新和删除，都可以得到标准化支持。大多数的关系型数据库、半结构化数据库、大数据系统软件都已经支持 KMIP 协议。我国的密码行业标准《密钥管理互联协议及应用技术规范》也已经进入公开征求意见阶段，支持 KMIP 的密钥管理系统也越来越丰富。

大部分公有云，如国外的亚马逊云、谷歌云、微软云，我国的阿里云、华为云、腾讯云等，都推出了密钥管理服务，用户可以以此为基础对云中的数据进行加密。

（2） 云身份认证服务

IAM 是一套全面的建立和维护数字身份，并提供有效地、安全地 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计的系统。云认证服务主要采用 IAM 构架，认证授权协议主要有 SAML、OAuth、OpenID。这些协议标准可以提供互通的身份认证、跨域授权登录、属性控制等服务。其中，SAML 标准已被我国采纳为国家标准，并且已经发布。

目前，云平台内部多采用 SAML 协议实现用户身份鉴别与授权，如阿里云、华为云等；而对于第三方认证支持，则多采用 OAuth2.0，如微信、QQ、新浪等。凭借 Android 系统的广泛应用，Google authenticator 在国内也获得了较好的发展，微信、阿里云等主流云服务平台都对其提供支持。同时，国内也有类似的应用模式，如网易的将军令，只是其应用范围主要集中在网易内部。

（3） 电子合同服务

电子合同服务的出现一方面解决了传统的纸质合同签署流程繁琐、易出错等问题，另一方面解决了合同电子化过程中身份难以鉴别、数据安全性差、发生纠纷时难以鉴定等问题，从而为用户提供了便捷、安全、合法的在线签约服务。电

子合同一般由合同条款和电子签名组成，电子合同云服务平台以《电子签名法》、《合同法》为法律基础，以密码技术为基础核心技术，以云的方式通过公众平台网站、API/SDK 等方式提供电子签名、电子合同签署和管理等服务。

近年来，电子合同在国内外应用广泛，电子合同服务的厂家百花齐放，已经形成相对稳定的产业生态圈，近两年第三方电子签名市场规模增长势头明显，发展潜力巨大。

（4） 云电子签名服务

云签名是云端参与或代表用户进行电子签名的一种服务，服务端在鉴权之后，使用协同签名方式或调用托管在云端的用户私钥进行签名。云电子签名服务常用于对电子文件的数字签名，有些云签名服务已经能够兼容主流的文档格式（Microsoft 的 Word、Excel 和 Outlook，Adobe 的 PDF，AutoCAD，Bentley 的 Micro Station、TIFF 等）。国外云签名服务开展较早，应用基础广泛，商业模式和技术都比较成熟，并且有很好的法律支撑，而我国的云签名服务近几年才刚刚起步，未来会有很大的发展空间。

（5） 云访问安全代理（CASB）服务

云访问安全代理近几年有了较大发展，成为管理云端及现场系统身份验证及加密的有效方式。可以将 CASB 想象为企业所有云端服务及现场系统的中央数据身份验证及加密中心，并可被所有终端访问，包括私人智能手机和电脑。CASB 时代以前，企业安全经理无法看到公司所有数据的受保护情况，随着云计算的兴起，企业也需要找到跨多个云交付一致安全的方法，保护所有使用企业数据的用户。CASB 帮助企业更好更深入地观察云及 SaaS 使用情况——细致到单个文件名和数据元素的程度。

（6） 云加密存储服务

云计算环境中，在密钥管理服务的支撑下已经实现了丰富的数据加密方案，比如块存储加密、对象存储加密、数据库加密、磁盘加密、文件加密等。用户在选择存储服务时，可选择支持加密的模式，轻松的实现数据存储加密功能。加密

即服务（EaaS，Encryption as a Service，Cryptography/Crypto as a Service）是一种订阅式的服务，云服务客户使用加密技术提供的安全性，而无需额外的安装部署操作。

（7） 云密码资源池服务

出于安全性的考虑，在重要的应用系统中，密码运算、密钥管理要求使用硬件密码模块。由于在云服务器中部署硬件密码模块比较困难，现在一般采用单独部署云密码资源池的方案，云平台通过网络连接使用密码资源池的安全密码功能。密码资源池是密码硬件的集群，也使用云计算的硬件虚拟化技术，将密码硬件资源虚拟成各个相互独立的虚拟密码设备，通过密码资源调度系统进行密码资源的分配、管理和统一调度，并对外提供统一的按需分配、弹性扩展的密码功能服务。

2.2 云密码服务标准化现状

由于云密码服务是个新生事物，目前还缺乏体系化的专门针对云密码服务的标准或技术规范，有些出现在云安全的标准中，本节总结应用于云密码服务的国内外标准或技术规范情况。

2.2.1 国外标准化情况

国际上，与信息安全标准化有关的国际组织很多，但在云计算安全领域涉及密码技术的成果不多，我们主要介绍比较有借鉴意义的美国的 NIST（美国国家标准技术研究所）、CSA（云安全联盟）、OASIS（结构化信息标准促进组织）的相关工作。

（一）NIST 组织

NIST 是美国国家标准技术研究所的简称，它制定了一些有影响力的密码技术标准。2010 年 11 月，NIST 云计算正式启动，成立了五个云计算工作组，从参考架构和分类、标准推进、安全、标准路线、业务用例等方面开展了云计算的研究；出版了云计算定义、参考架构、公有云中的安全隐私指南、政府云计算技术

路线图等多份研究成果。在密码技术方面，NIST 发布了《密钥管理建议》（SP 800-57）系列标准、《密钥管理系统设计框架》（SP 800-130）、《美国联邦密钥管理系统配置规范》（SP 800-152）等，其中与云数据加密和密钥管理相关的有《云服务中的密钥管理相关问题和挑战的研究报告》（NIST IR 7956）。下面介绍该报告的内容。

根据云服务商提供的资源类型不同，NIST 将云计算的服务模式分为基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）三类，NIST IR 7956 针对三种云服务模式给出了在各种场景下需要的密码技术，以及对密钥管理的需求，见表 2-1。

表 2- 1 云服务不同模式下密码技术及密钥管理需求对照表

服务层级	安全能力	密码技术	密钥管理需求
IaaS	虚拟机镜像真实性	数字签名	签名私钥的安全
		密码杂凑函数	会话密钥的安全（建立安全会话保证杂凑值和验证结果的传输安全）
		带密钥的消息鉴别码	密钥的传输安全
	虚拟机 API 合法用户的认证	数字签名、SSH 等建立安全会话	签名私钥的安全、会话密钥的安全
	云用户与虚拟机通信安全	安全会话与强鉴别技术，如 TLS/SSH	非对称私钥的安全、会话密钥的安全
	虚拟机之间的通信安全	安全会话与强鉴别技术，如 TLS/SSH	非对称私钥的安全、会话密钥的安全
	数据存储安全	透明数据加密	加密密钥的安全
		数据库/用户级加密	加密密钥的安全
PaaS	服务的真实性与用户身份鉴别	数字签名等技术	签名私钥等的安全
	云用户与开发工具/应用程序通信安全	安全会话与强鉴别技术	非对称私钥的安全、会话密钥的安全

	数据存储安全	透明数据加密	加密密钥的安全
		数据库级/用户级加密	加密密钥的安全
SaaS	服务的真实性与用户身份鉴别	数字签名等技术	签名私钥等的安全
	云用户与应用程序交互安全	安全会话与强鉴别技术	非对称私钥的安全、会话密钥的安全
	数据存储安全	整个数据库加密	加密密钥的安全
		数据库字段选择性加密	加密密钥的安全

（二）OASIS 组织

OASIS 成立于 1993 年，是一个推进电子商务标准发展、融合与采纳的非盈利性国际化组织，它成立了密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）技术委员会，旨在推动企业加密密钥管理的互操作性标准。

OASIS 相继于 2010 年 10 月发布 KMIP V1.0、2013 年 1 月发布 KMIP V1.1、2017 年 2 月发布 KMIP V1.4，同期形成 KMIP V2.0 草案稿。KMIP 是云中协同密钥管理的新标准，主要满足企业密钥管理的标准化需求，针对云中企业级的用户，简化公司管理密钥的方式，消除公司对冗余、不兼容密钥的管理过程，通过对使用密钥进行各种密码活动的客户端与密钥管理系统之间的通信进行标准化，实现对复杂应用环境中的密钥管理。该标准主要面向系统开发和系统框架设计人员，以及使用 KMIP 的应用程序。

KMIP 协议目前已在各大公有云中得到广泛应用。

（三）CSA 组织

云安全联盟（Cloud Security Alliance，CSA）成立于 2009 年，是中立的非盈利世界性行业组织，致力于国际云计算安全的全面发展。

（1）《云计算关键领域安全指南 V4.0》

CSA 于 2011 年 11 月发布了《云计算关键领域安全指南 V3.0》，后又于 2017 年 7 月发布了《云计算关键领域安全指南 V4.0》，其中在数据安全和加密领域提出了如下指导建议：

① 建议 3 种保护云数据传输安全的方法，客户端加密、传输过程中加密和代理加密。

② 对 IaaS、PaaS、SaaS 层服务云数据存储给出了数据加密方法和安全建议。

③ 密钥管理的建议。对密钥管理的载体、方式，管理用户密钥的方式提出建议。

④ 指出安全即服务（SecaaS）是未来发展的重要方向，包括身份、授权和访问管理服务，加密和密钥管理服务等。

（2）《安全服务实现指南 类别 8：加密》

CSA SecaaS（Security as a Service）工作组于 2012 年 9 月发布了《安全服务实现指南 类别 8：加密》（SecaaS Implementation Guidance, Category 8: Encryption），从需求和实施考虑方面，对云计算环境下的密钥管理提出了相关要求和实施建议。

① 密钥管理要求。数据加密密钥应使用安全的方式生成；数据加密密钥应可以被托管；根据职责分离的安全原则，理想情况下，密钥管理应与托管数据的云运营商相分离；需要考虑设计一种远程密钥管理服务用于客户对 KMS 或企业密钥管理（EKM）解决方案的维护；理想情况下，客户端密钥管理模型是被遵循的；关键的撤销策略和相关机制对所有密钥管理模型都至关重要。

② 密钥管理部署建议。在云计算环境中，基于职责分离的安全原则，理想情况下密钥的管理应当与持有数据的云运营商分离开来；在云计算环境中，密钥的管理通常作为一种单独的服务提供，主要包括远程密钥管理服务和客户端密钥管理两种方式，实际应用中云运营商可以根据云服务类型（IaaS、PaaS、SaaS 层

的不同服务）以及特定的需求进行选择。

2.2.2 国内标准化情况

在国内，信息安全标准的制定主要是全国信息安全标准化技术委员会（简称信安标委，委员会编号为 TC260），以及密码行业标准化技术委员会（简称密标委）。信安标委与云密码服务直接相关的国家标准目前还没有。密码行业标准中，密标委正在开展一些云密码相关标准的研制，包括云密码机、云密码资源池、云身份鉴别、云签名技术、云计算密码应用等方面开展了相关标准研究与制度工作，但还未形成体系化的云密码服务标准体系。

表 2-2 云密码服务相关密码行业标准草案或研究课题

序号	技术规范或研究课题	主要内容
1	云服务器密码机技术规范（送审稿）	标准定义了云服务器密码机的相关术语，规定了云服务器密码机功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容。
2	云服务器密码机管理接口规范（送审稿）	规定了云平台管理系统与云服务器密码机之间的设备管理接口和协议。适用于云服务器密码机的研制和检测，也适用于云平台管理系统的开发和使用。
3	云计算密码应用技术体系框架研究	研究云计算中对于密码技术应用的需求，提出云计算中密码技术的应用框架，使得密码技术为云计算提供各种安全保障。
4	云计算密码应用指南（征求意见稿）	分析了云计算服务模式和部署模式，结合我国目前密码应用技术、密码标准、密码产品等现状，提出了云计算密码应用技术框架和云计算密码应用角色框架，为云计算密码相关标准与规范编制、云计算安全保障系统规划设计与安全审查、云计算应用系统与密码产品策划提供参考。
5	云密码资源池技术标准研究	对云密码资源池的实现方案进行研究，从组网、管理、流程等角度提出云密码资源池技

		术方案建议，以满足云计算环境下多租户的数据安全业务需求。
6	云身份鉴别服务密码标准体系研究	主要针对云计算环境中身份鉴别服务进行研究，将身份鉴别作为云服务提供给用户，对云身份鉴别服务中密码应用相关的标准技术为核心展开研究。
7	基于云计算的电子签名服务密码标准体系研究	研究了国内外云签名的发展现状，对国内云签名密码标准化中面临的一些关键问题和难点，结合现有的标准体系，给出了云签名服务标准的框架建议。
8	基于云的电子签名服务技术要求（送审稿）	标准提出了基于云的电子签名服务密码技术要求，包括：传输安全要求、身份鉴别要求、算法要求、密码设备要求、密钥管理要求、证书管理要求、系统建设及运维要求等，本标准可为基于云的电子签名服务的建设、管理和检测提供指导。

2.3 云密码服务面临的挑战

云密码服务会随着云计算的迅速发展给密码产业带来发展机遇，但机遇和挑战总是同时存在的，作为一种新的密码技术服务模式，云密码服务在平台建设、运营管理、应用对接等方面都面临一些新的挑战。

2.3.1 平台建设的挑战

（1） 硬件密码模块的部署问题

密码模块是提供密码算法运算功能的软件模块或硬件设备，由于密码系统特别强调密钥的保护和密码运算的安全，因此在重要的信息系统中要求使用硬件密码模块（HSM），这些设备能提供独立于应用业务主机的密钥保护和密码算法运行的安全环境，在传统的信息系统中，硬件密码模块或以 USB 接口的智能密码钥匙的形态插在 PC 上、或以 PCI-e 接口的密码卡的形态插在主机内、或以网络接口的密码机的形态和主机通过单独的网络通道连接，硬件密码模块需要和所服务的主机通过安全的通道直接连接。但在云中，硬件基础设施是统一的云服务器，

应用服务器运营在虚拟主机上，这时硬件密码模块怎么部署？一种方案是在云服务器中配置支持虚拟化的硬件密码模块（芯片或 PCI-e 接口的密码卡），给每台虚拟服务器分配一个虚拟硬件密码模块，实现虚拟机和虚拟硬件密码模块的绑定，这个方案需要改动云服务器硬件，在已经运营的云中不可行；第二种方案是部署独立的云密码机资源池，云中的虚拟主机通过网络连接云密码资源池中的硬件密码模块。两种方案都面临一些技术上的挑战。第一种方案中，密码模块虚拟化带来的性能降低问题、不同虚拟空间之间的密钥隔离问题等需要解决；第二种方案中，云虚拟机和资源池中密码模块的安全通信问题、相互身份认证问题、密钥隔离问题都需要解决。

（2） 密码产品转变为云密码服务缺乏技术标准

在传统的信息系统架构下，密码产品厂商或集成商把不同应用场景下需要的密码功能定义成了不同的产品，这些产品有硬件设备形态的、有软件系统形态的。如，在 PKI 工程中的 CA 系统、服务器密码机、签名验签服务器；在泛金融 IC 卡业务场景使用的金融数据密码机、支持对称密钥分散的密钥管理系统；实现强身份认证接入的身份认证网关或身份认证系统；保证传输数据安全的、支持 IPSec 协议或 SSL 协议的 VPN 网关设备；专门为文档签名或验签的电子签章服务器或系统；支持不同格式的静态数据加密的硬件设备或软件，如文档加密服务器、数据库加密服务器、大数据加密网关等等。这些设备或软件在云中将服务化，以虚拟机实例、微服务实例的形态存在。这些产品或软件有一些安全性要求，如对硬件密码模块的使用，由于云平台是以 IaaS 方式提供硬件资源使用的，这些产品如何进行软、硬件的逻辑分离？怎样和云平台提供的虚拟硬件密码模块进行安全通信？需要指导性的规范或标准，简单的硬件软件化或不合规的网络连接模式都会破坏产品的安全性。

（3） 用户的密钥安全问题

云计算系统中，用户把信息系统托管给了第三方云运营商或数据中心，信息系统不在自己的掌控之中了，信息系统中保证数据安全的各种密钥怎么管理？公有云有 BYOK（Bring Your own key：用户自己提供密钥）和 HYOK（Hold Your

Own Key：托管运营商管理）两种模式，两种模式各有优缺点，用户在 BYOK 方式下对密钥有更大的掌控权，但使用不方便，也会影响数据加解密的性能；托管方式更方便易用，但云服务商能不能保证用户密钥和数据的安全？有什么技术或措施让用户相信？

（4） 密码算法的合规性问题

由于密码技术对保障国家信息安全的重要性，我国明确要求在重要信息系统中使用符合国家标准的密码算法，但由于云计算的许多基础软件起源于国外的开源软件，其内嵌的密码算法是国外算法，包括在国内主要公有云的许多软件系统中。这些不合规的密码算法需要替换，工作量是巨大的。

（5） 云密码服务需要新技术支撑

云计算的发展推动了大数据等新型信息技术的发展，反过来这些技术又对云计算提出了新的密码技术支撑要求，如密文检索、同态加密、多方计算、基于属性的加密等算法的支持，以及开放授权、零知识证明等新的密码技术。怎样用这些新的密码技术构造完整的新型云密码服务？怎样提升这些技术所使用的密码算法的性能以达到实用性的要求？都面临算法优化、技术实用化的挑战。

2.3.2 运营管理的挑战

云密码服务改变了密码技术的使用方式、部署方式，带来了密码服务的运营管理问题。过去，密码产品提供商提供产品给用户，一般只负责产品的质量保证和售后服务，用户自己运行维护；在云密码服务中，用户不再购买产品，而是购买服务，产品也不再部署在自己的掌控范围内，而是部署在云运营商或云密码服务商的环境中，这时运营管理的问题出现了。

首先是运营管理的责任划分问题。如果云密码服务部署在云运营商的环境中，这时运维涉及云运营商、云密码服务提供商、用户三者的责任划分；如果部署在云密码服务提供商的环境中，是后两者的责任划分问题。若没有明确的责任划分，系统之间的服务配合就没有保证，用户业务系统的运行就没有保障。

其次，云密码服务的服务质量度量问题。云密码服务具有多用户、高并发、安全性要求高等特点，如果缺少对安全保障、服务质量等方面的度量标准和服务承诺，会导致用户在选择密码服务时无所适从、不敢使用的问题。

因此，从产品提供到服务的运营，云密码服务面对诸多运营管理的挑战，从运维管理的责任界面，到服务质量的标准制定、收费价格和计费方式等，不仅需要云密码服务提供商和用户在应用中磨合和积累经验，甚至需要市场监管部门制定服务标准、经营规范。

2.3.3 应用对接的挑战

作为一种标准服务，云密码服务应提供足够的灵活性和丰富的接口形式为各种应用系统提供密码服务。应用系统可能通过不同的接入方式来访问云密码服务，例如：本地化部署的应用系统通过远程网络访问，云端部署的应用通过云内网访问。这些应用系统对响应时间、数据吞吐量、安全性等方面的要求是不一样的，因此需要支持的接入方式、接口形式不同，而且，不同的接入方式和接口方式在计费、运营维护服务等方面存在差异化的要求。另外，不同的接入方式、接口方式需要采用的安全接入技术也不同。在大型的云平台，例如在公有云中，应用系统数量多，对密码的功能需求复杂，对通信安全的要求不一样，这给云密码服务与应用的对接带来挑战，需要积累经验，不断完善。

第 3 章　云密码服务技术体系

作为一种新的密码功能交付方式，云密码服务以云服务的方式为应用系统提供密码功能，从产品形态、部署方式、访问接口到运维管理等方面都与传统密码产品或系统有很大不同，因此云密码服务需要在传统密码技术的基础上结合云计算的环境特点，扩展原有的技术体系。我们根据近年来积累的密码服务产品、密码服务运行及应用的经验，提出了一个云密码服务的技术体系框架。这个框架便于理解云密码服务的类型、对外接口、以及部署和应用方面的问题。

3.1　云密码服务需求分析

密码技术用于保护数据和建立信任，实现网络中的数据加密、身份认证、业务防抵赖等功能，能够被应用于网络的各个层次中。在不同的网络层次中，通过不同的密码协议，保护数据在传输、存储和使用中的安全。云计算是一种新的信息系统部署方式，云计算中各个网络层次的安全需求依然，需要密码技术的支撑保护。但是云计算对信息资源的集中化、共享化、服务化部署需求对密码技术的应用提出了新的要求，密码技术要适应云服务化，传统形式的密码产品或系统要顺应服务化的需求做出改变。

一个传统的基于密码技术的网络安全方案，一般需要公钥密码基础设施、以及相应的软硬件密码产品的支撑。公钥密码基础设施不但通过标准的密码算法、密码协议、数据处理流程定义了数据的加解密机制、数据完整性保护机制、身份的真实性验证机制、业务防止抵赖机制，还定义了网络实体身份和用户公开密钥绑定的机制。基于用户身份和公钥不同的结合形成了不同的技术体系，如基于数字证书的密码体系、基于标识的 IBC 密码体系、以及其他一些无证书密码体系等。目前基于数字证书的 PKI 体制是广泛应用的技术体制。在公钥密码基础设施的框架下，为了应用和部署的方便性，密码厂商把密码算法、密码协议、数据处理流程等实现为不同的密码软硬件产品。密码算法模块是一个基础产品，它提供密码算法功能，出于算法运算环境安全、密钥安全、运算卸载的需要，在高安全需求的信息系统中使用硬件密码模块（HSM）。基础的 HSM 可以是芯片、PCI-e

接口密码卡、密码机等形态。其他的密码硬件类产品是在 HSM 的基础上面向不同应用场景扩展出来的设备，如服务器密码机、金融数据密码机、签名验签服务器、VPN 网关、身份认证网关等。在密码软件产品中，CA 系统、密钥管理系统等是公钥密码基础设施的基础支撑系统，被定义为标准的服务。

前述密码技术和产品要实现云服务化，首先面对的一个问题就是 HSM 在云中的部署问题。由于云中的硬件是集约式部署、共享使用的，因此，HSM 部署到云中要实现密码模块的虚拟化，形成虚拟密码模块，能够被虚拟机实例、微服务实例等共享使用。在一些已经运营的云中，密码模块没有内置在已部署的云服务器中，HSM 只能以外置硬件资源的方式提供服务，为了支持云中按需使用、弹性部署的需求，外置 HSM 需要以集群形式部署，形成云密码资源池，云服务器通过网络和云密码资源池建立安全连接，访问密码服务。

解决了 HSM 的部署问题，其他的密码产品都以软件的形态迁移到云中，以虚拟机实例、微服务实例、软件中间件的形态运行，产品销售模式改变为按需租用的服务模式。除了以密码为核心的服务形式外，有些云服务与密码技术深度融合，最终形成了直接面向最终用户的新型密码服务形态，甚至催生出更多全新的密码服务内容。

3.2 云密码服务分类

根据云计算中的密码应用需求，我们把云密码服务分为三类：云密码资源服务（Cryptography Resource as a Service，CRaaS）、云密码功能服务（Cryptography Function as a Service，CFaaS）、云密码业务服务（Cryptography Business as a Service，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。用户选择哪类的服务取决于他的信息系统部署环境、以及自建的信息系统的边界。

3.2.1 云密码资源服务

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、随机数服务等（图 3-1）。有了这些基础服务，用户就可以建设基于 PKI 技术的各种安全应用或提供更上层的密码服务内容。

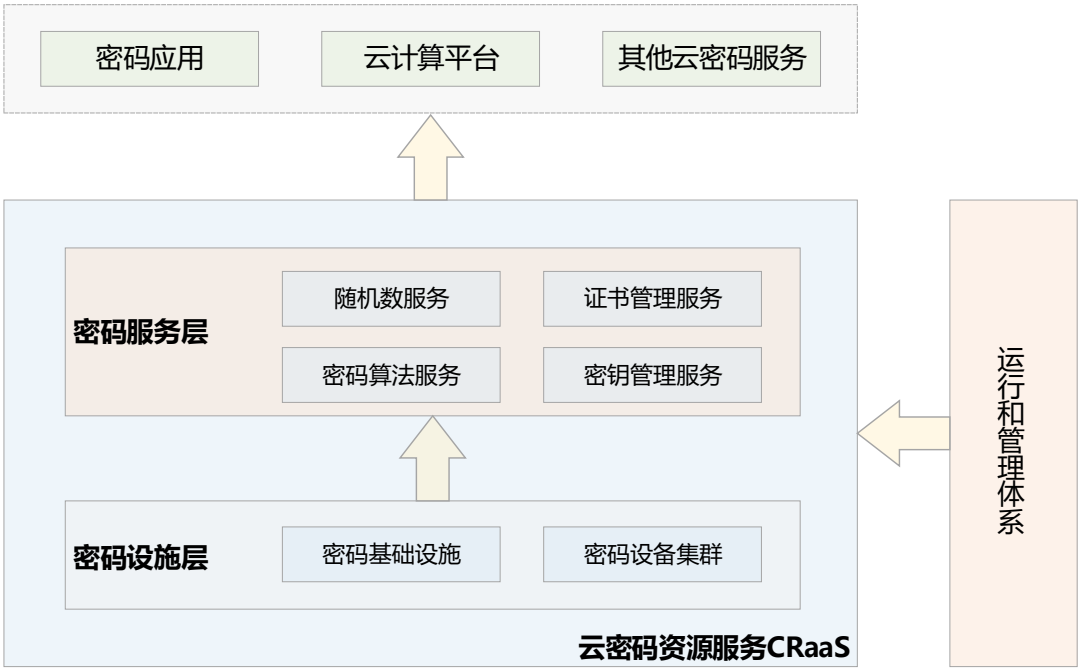

图 3-1 云密码资源服务

密码算法模块服务可以用软件实现，也可以硬件实现，但软件实现的密码模块很难达到较高的安全级别，重要的业务系统中（如等级保护三级以上系统）一般使用硬件密码模块。云密码机或云密码资源池可以实现外置硬件密码模块的虚拟化、弹性部署、按需提供服务。

数字证书管理是 PKI 应用工程中身份认证的一种重要技术，数字证书通过把网络实体在物理世界中的真实身份和数字世界中公钥的绑定实现了网络实体身份的真实性认证机制。提供数字证书服务的运营机构称为“CA 中心”，是数字证书的签发机构，并负责建立和维护用户实体与密钥之间的绑定关系、数字证书全生命周期的管理和维护。CA 中心和数字证书服务早就存在，并已经在社会上

建立起完善的服务体系。公有云或私有云可以使用自建的 CA 系统，也可以使用第三方 CA 的服务。使用第三方的 CA 服务，需要在云中建立数字证书的发放、导入、在线证书状态查询功能的访问接口。云中 CA 的特点是不仅要实现大量云用户的在线审核、在线发证，还要为云中大量的设备或通信实体发证，特别是在物联网应用中，这些证书的数量巨大，因此必须支持自动化、甚至批量的发证机制，这些证书的生命周期管理也必须采用分布式的管理机制。在云中，证书类别会更丰富，各类证书的颁发和管理策略会有很大不同。

密钥管理也是密码技术的重要内容，密钥的安全性是决定密码系统安全性的关键因素，因此无论在密码产品还是在密码应用工程中必须管理和保护好密钥，这包括密钥的生成、获取、使用、销毁等全生命周期的管理等。在云计算中有大量的密钥存在，这不仅是因为云用户数量多、网络实体类型多，还因为云中共享的存储空间使得许多重要的数据需要加密保护，这些数据量巨大、且类型繁多，不同用户的数据、不同类型的数据需要不同的密钥，包括证书公钥、IBC、CLA 等非对称密钥以及多种对称密钥等。大量用户和网络实体的身份密钥、海量的数据加密密钥使得云中的密钥管理必须使用专门的云密钥管理服务。

3.2.2 云密码功能服务

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（图 3-2）。

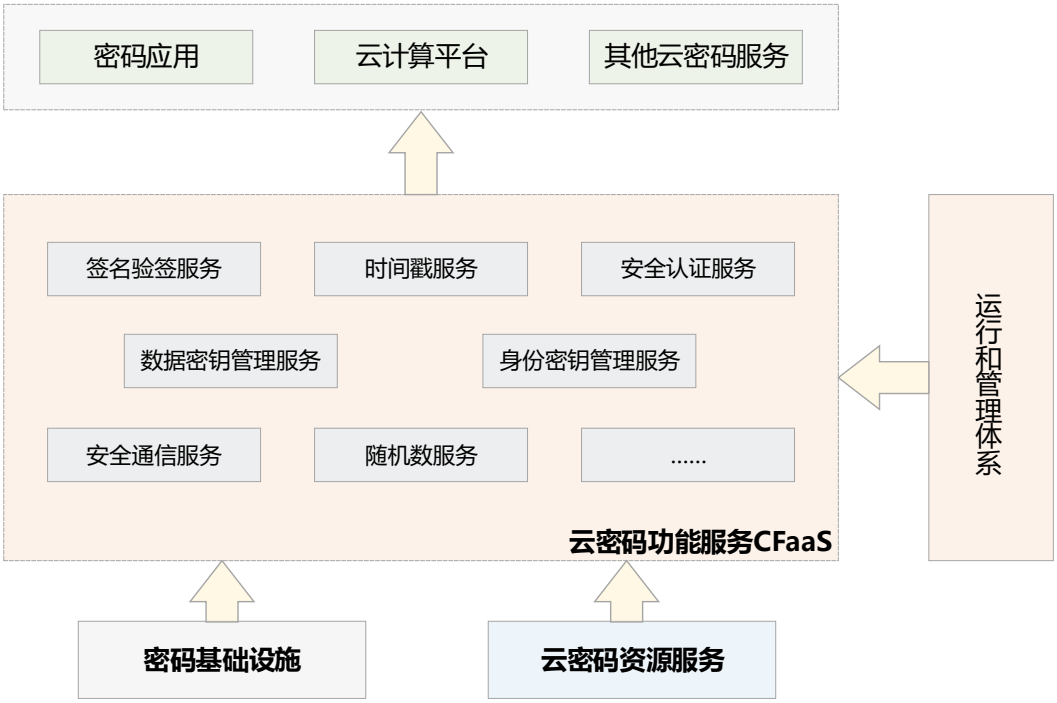

图 3-2 云密码功能服务

一些传统的密码设备，如服务器密码机、签名验签服务器、金融数据密码机、安全认证网关、VPN 等设备，实际上都是面向一定应用场景的密码算法和密码协议结合的产品，它们到了云中必须实现软件功能与硬件模块的分离，硬件模块成为云密码资源服务的一部分，软件功能被重构为虚拟机模板、或微服务模板，成为虚拟的设备。这些虚拟的设备具备部署快速、灵活，可以动态配置，易于水平扩展的特点，适合大并发、弹性部署的需求。

这类的密码功能服务有很多，常用的如：

- 签名验签服务；
- 时间戳服务；
- 安全认证服务；
- 安全通信服务；
- 随机数服务；
- 用户身份密钥管理服务；

- 数据密钥管理服务；
- ……

3.2.3 云密码业务服务

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。从另外一个角度来看，密码业务服务可以认为是经过业务封装的密码功能服务。

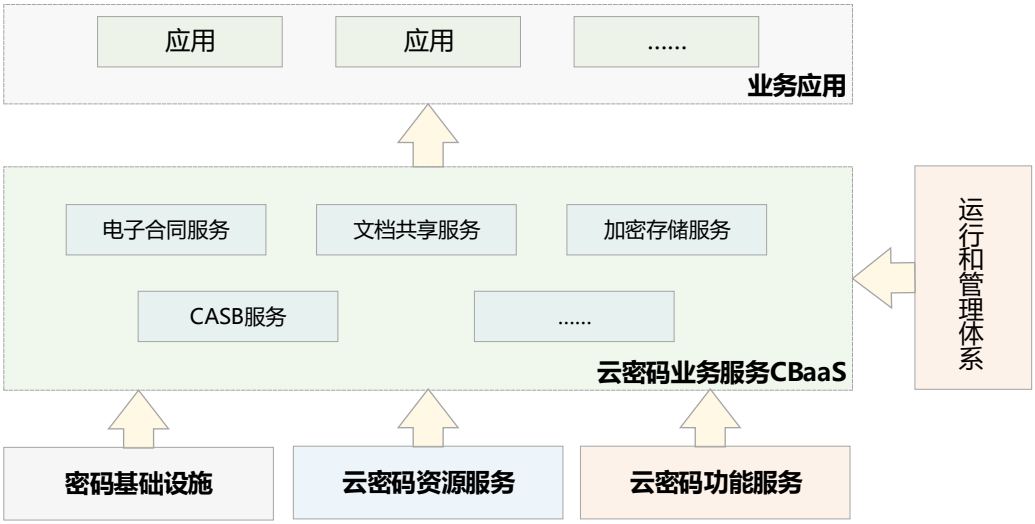

图 3-3 云密码业务服务

云密码业务服务通常更加关注特定业务领域的一个或多个业务过程，致力于解决场景中的业务问题，将这些业务过程组合成用户能够访问和使用的操作流程。云密码业务服务基于云密码资源服务提供的密码设施设施服务、云密码功能服务提供的功能服务接口，保证业务过程的安全，向用户提供基于密码技术的安全业务服务。

常见的云密码业务服务包括但不限于以下类别：

- 电子合同服务；
- 安全文档共享服务；

- 云安全访问代理（CASB）服务；
- 云加密存储服务；
- ……

3.3 云密码服务部署方式

云密码服务可以多种方式部署。典型的部署方式分为以下几种：

（1） 部署在云计算服务提供商的环境中

云密码服务可以和云计算业务服务部署在同一个环境中，通过内置在云服务器中的云密码资源服务，或使用独立的云密码资源服务，云密码功能服务和云密码业务服务以虚拟机或微服务、中间件的形态，利用云计算服务的地域无关性、按需分配的特点，向用户提供各种不同应用模式的云密码服务。如图 3-4 所示。

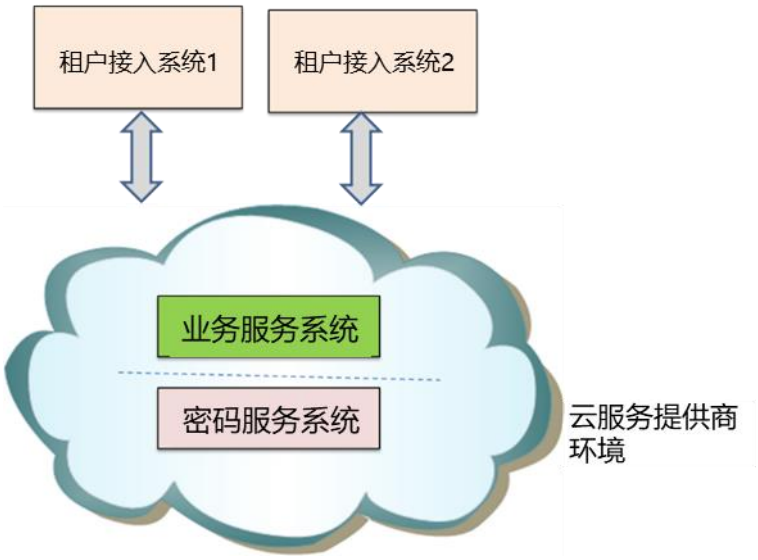

图 3-4 部署在云计算服务提供商环境中

（2） 部署在云密码服务提供商的环境中

云密码服务提供商可以部署独立的云密码服务平台系统，向云计算平台提供密码服务。这时云密码服务平台一般以密码资源池的形态存在，通过安全的网络连接向云平台以及云平台的租户提供服务。云密码服务提供商在自己的平台中实现独立的运维、审计、管理、计费等功能，可以同时为多个云平台提供云密码服

务。云租户使用独立的云密码服务商的服务，可以实现数据存储与密码保护功能的分离，有更高的数据安全性，并摆脱了对云平台的依赖。如图 3-5 所示。

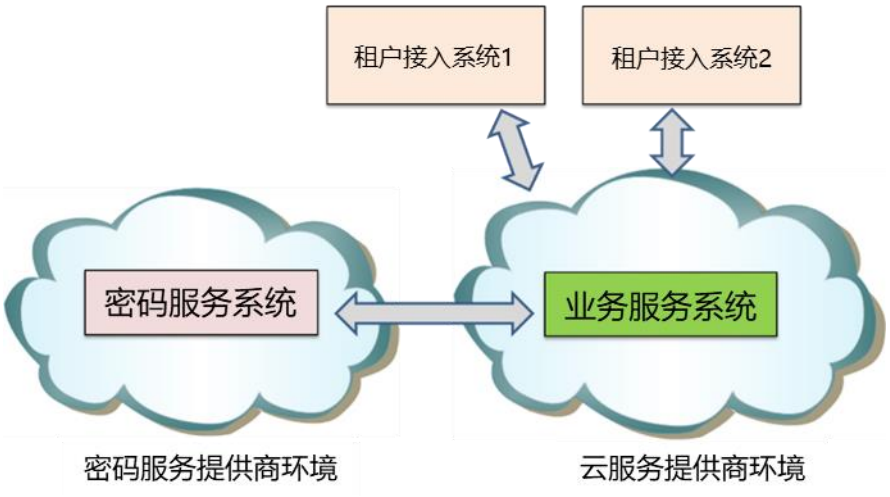

图 3-5 部署在云密码服务提供商环境中

（3） 混合方式部署

云密码服务可以不单纯采用以上的部署模式，而是根据场景需要，采用多种部署模式混合部署。例如一个电子合同服务，可以使用（1）中所描述的部署在云服务商环境中的电子合同流程服务，采用（2）中所描述的电子签名服务、时间戳服务和数字证书服务。如图 3-6 所示，虚线框部分表示密码服务部署的内容。

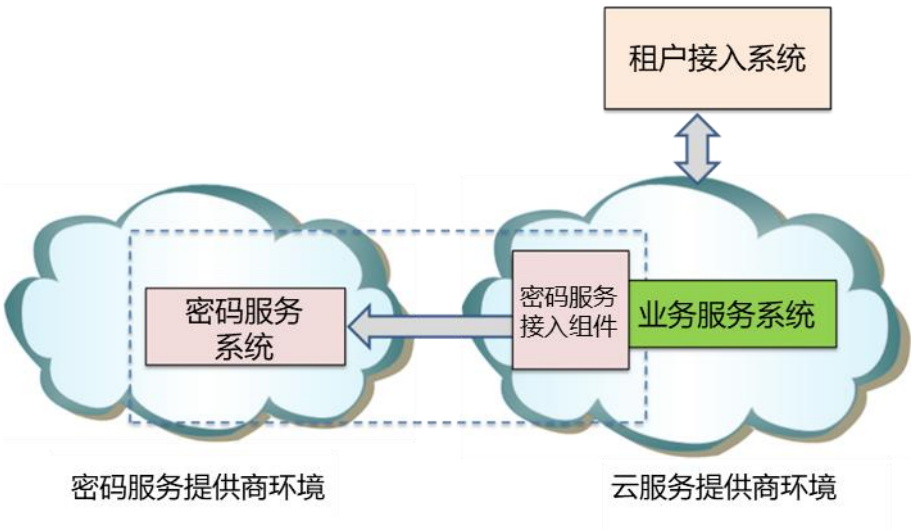

图 3-6 混合方式部署的云密码服务-1

甚至在部署时，可能在云计算服务提供商、云密码服务提供商所部署的密码

服务系统之外还需要在客户环境中部署一定的客户差异化定制逻辑，实现特定客户特有的密码功能需求。如图 3-7、3-8 所示，虚线框部分标识密码服务部署的内容。

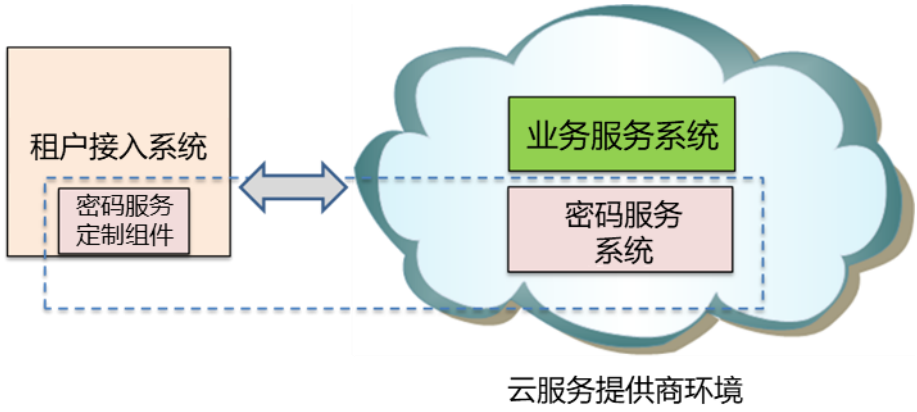

图 3-7 混合方式部署的云密码服务-2

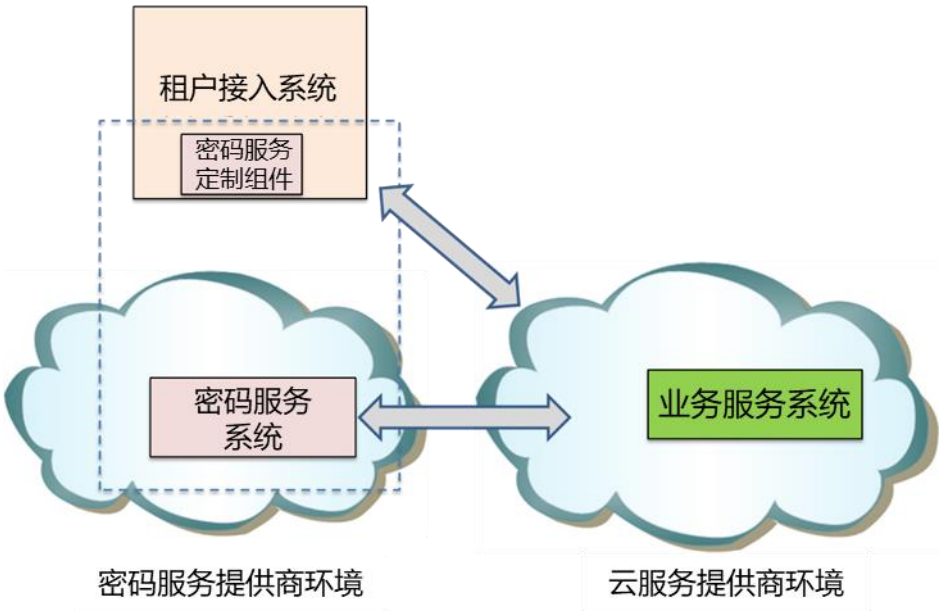

图 3-8 混合方式部署的云密码服务-3

或者在云密码服务提供商部署云密码服务系统，在云计算服务提供商环境部署业务系统和云密码服务接入模块，在租户接入系统部署云密码服务定制组件。如图 3-9 所示，虚线框部分表示云密码服务部署的内容。

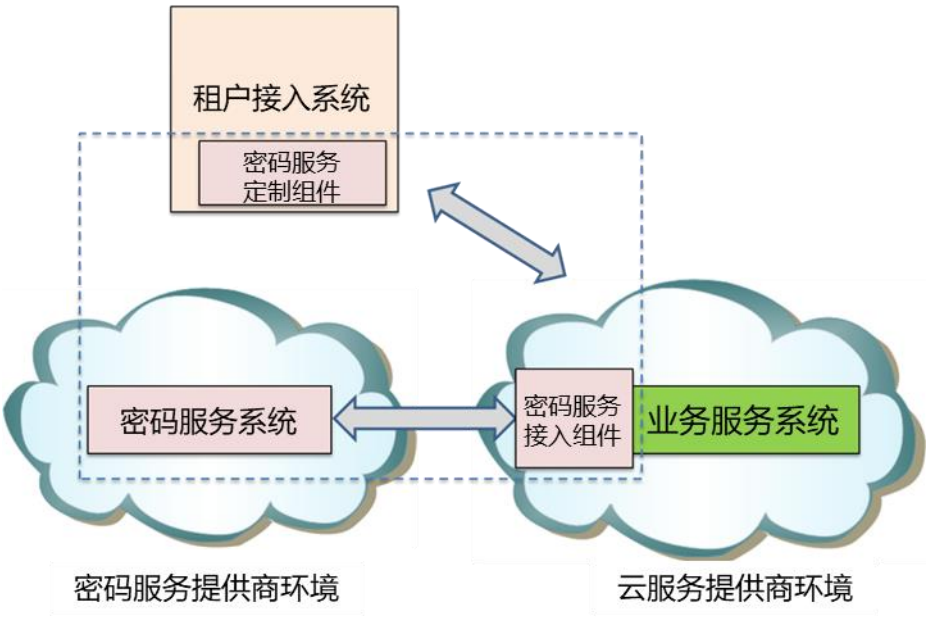

图 3-9 混合方式部署的云密码服务-4

通过上述这些灵活的部署模式，能够以最便捷的方式，向客户提供各种不同应用模式的云密码服务。

3.4 云密码服务访问方式

密码功能要被集成在应用业务系统中，有以下几种典型的访问云密码服务的方式。

（1） 协议方式

很多密码服务通过协议方式向外提供服务。例如，OASIS 的数字签名服务，支持 Digital Signature Services（DSS）规范；密钥管理服务，支持密钥管理互操作协议（KMIP），外围应用通过 KMIP 协议和密钥管理服务进行交互以进行密钥操作；很多身份认证服务支持 OAuth 协议。

密码服务协议，通常以 HTTP 或 HTTPS 协议为基础，采用 XML 或 Json 等数据封装形式，例如证书管理协议 CMP、简单证书下载协议 SCEP 等。

通常，协议运行之前，使用者需要通过密码访问提供商提供的机制进行注册，以获得访问的凭据，然后在协议中，使用此凭据访问，在协议请求报文中要求包含客户端身份认证、数据完整性保护等机制。服务收到请求后，会进行一系列身

份认证、访问控制、状态判断等等，判断无误后向客户端返回密码功能处理结果或执行所请求的操作。如图 3-10 所示。

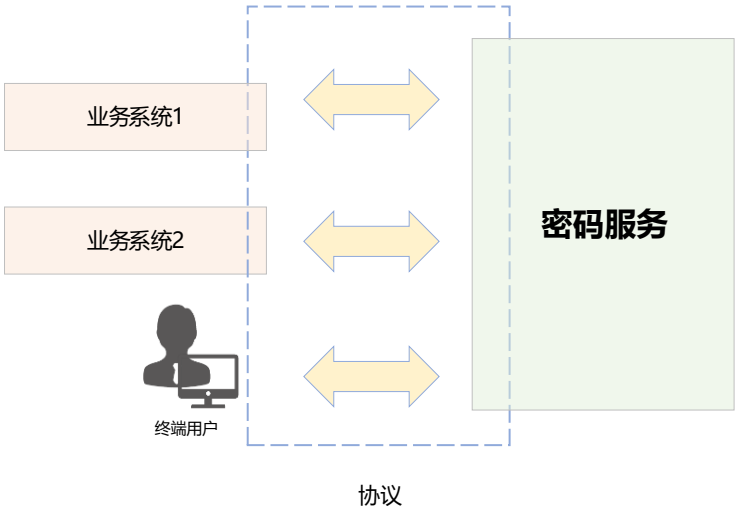

图 3-10 协议方式集成示意图

通过协议方式集成的优势是灵活方便、易于集成和维护，在多种异构的运行环境中集成时，业务各方仅需遵循同样的协议规范实现业务过程和密码过程即可。

（2） 接口库方式

在很多场景下，密码服务向业务请求或应用程序以客户端 SDK 的方式封装了客户端和密码服务之间的交互协议、通信协议，提供 API 接口。例如 AWS 的云密码机向外提供 PKCS#11 的接口，在国内云密码设备向外提供符合 GB/T 36322—2018《信息安全技术 密码设备应用接口规范》（原 GM/T 0018）或 GM/T 0019—2012 《通用密码服务接口规范》的接口库。

API 接口可以根据场景需求有多种形式。例如 Java 的 JCE 接口、Linux 下的动态链接库.so、静态库.a 等等，甚至还可能有 Java script 代码包、go 语言 SDK、python 语言 SDK 等等。API 接口适用于客户端逻辑较为复杂的情况下，用以隐藏协议复杂性，简化客户业务系统的调用逻辑。如图 3-11 所示。

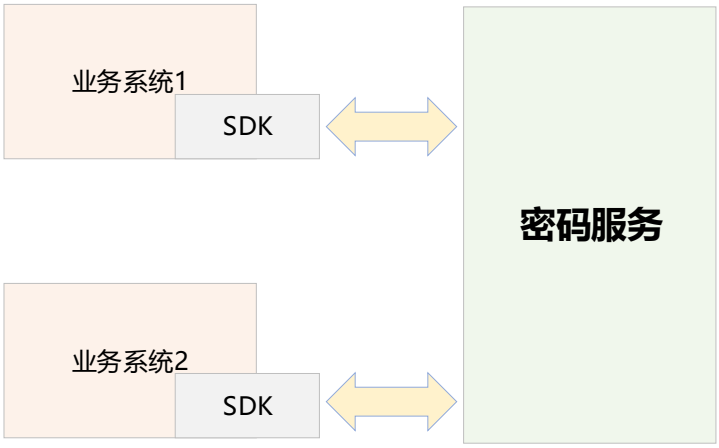

图 3-11 客户端 SDK 方式集成示意图

由于传统基于密码设备产品的应用系统，很多都是使用接口方式来调用密码设备完成密码功能，因此，密码服务所提供的 SDK 接口，与之前的设备接口，通常保持一致。这样，能够最大限度减少业务系统的设计、开发和迁移的工作量。

（3） 代理方式

在某些场景下，例如用户端有很多应用需要访问远程的密码服务，客户端可能存在网络限制问题、客户端访问凭据安全性问题等，这种情况下，可以采用代理模式来集成密码服务。

在使用代理方式集成时，代理通常是一个单独的密码产品，可以表现为一个单独的硬件产品，也可以表现为一个软件系统。代理部署在用户网络域中，其功能是作为安全连接密码服务的桥梁，包括接受业务系统的密码服务请求、访问外网的密码服务、与远程密码服务安全通信，以及安全管理密码服务的访问凭据等能力。在特定的场景下，可以提高业务系统调用密码服务的效率和隐私保护能力。如图 3-12 所示。

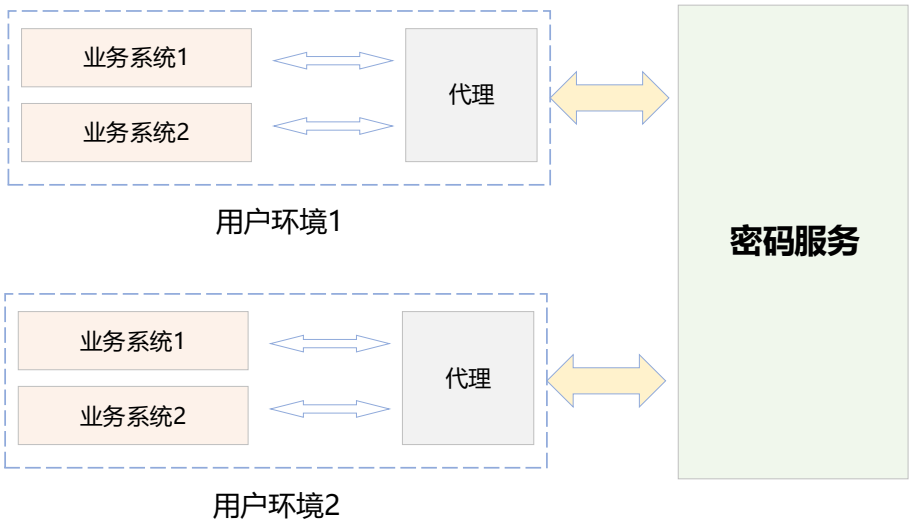

图 3-12 代理方式集成示意图

随着 SaaS 服务的逐步成熟和对安全的更高要求，云访问安全代理 CASB（Cloud Access Security Broker）技术越来越受到关注，并且 CASB 也可作为一种云密码业务服务提供给用户，为用户使用云服务提供身份认证、访问控制、数据加密、威胁防护等丰富的安全能力。如图 3-13 所示。

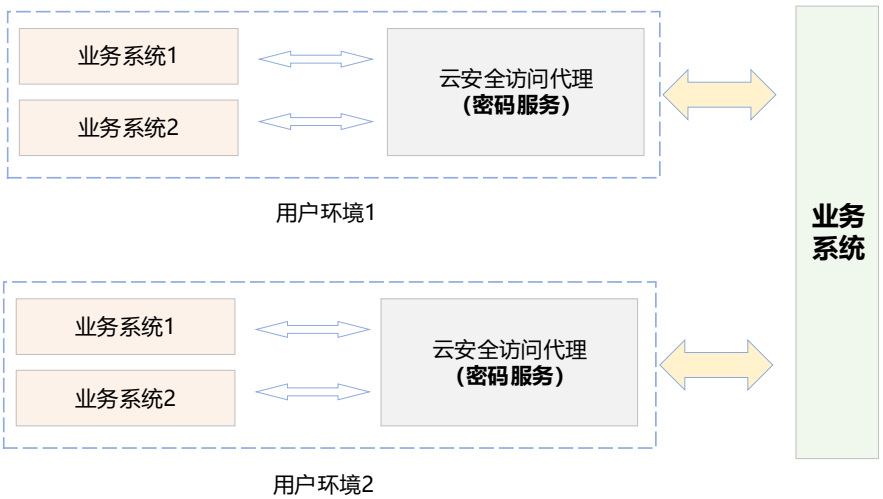

图 3-13 云安全访问代理方式示意图

代理方式集成，尤其适用于用户业务系统存在多个业务应用系统访问密码服务的场景，这种情况下，通过将密码服务访问凭据集中安全管理，增强了业务系统的安全性，也提升了用户的 IT 系统可管理性。用户通过代理，能够便捷地管理其租用的密码服务的各种策略，例如密钥、密码算法等等，这为用户提高了更

大的便利性。

3.5 云密码服务运营与管理

3.5.1 责任划分

云密码服务的所有参与者都应承担相应的安全职责，即在某一云密码服务中服务提供商（包括云密码服务提供商和云计算服务提供商）和用户要分别承担不同的安全职责。参考 CSA《云计算关键领域安全指南 4.0》D1：云计算概念和体系架构中提出的共享责任模型，建立云密码服务不同服务模式下的责任划分，如图 3-14 所示。

图 3-14 云密码服务安全责任划分

云密码业务服务 CBaaS：云密码服务提供商负责所有的云密码服务安全性，因为云密码用户仅适用密码相关应用和业务程序。例如，CBaaS 提供商负责安全策略、日志审计，而用户只能管理和使用。

云密码功能服务 CFaaS：云密码服务商提供功能服务的安全性，而用户负责在他们的功能服务平台上部署应用，建设密码业务，并提供业务所有的安全配置。

云密码资源服务 CRaaS：云计算服务提供商负责基本网络配置、云计算基础环境和云密码服务所依赖的技术安全，不同于 CFaaS、CBaaS，用户要承担更多的安全责任。例如 CRaaS 可监视其密码服务所遭受的信息攻击，但用户在服务商提供的基础上，全权负责如何定义其密钥生命周期管理、接口调用安全等。

3.5.2 运维管理

运维管理是云密码服务的重要工作，需要用户、云计算服务提供商、云密码服务提供商共同完成，并且运维本身也是服务内容的一部分。根据用户运维安全能力，划分三个阶段，用户可根据需要选择不同的运维服务内容，如图 3-15 所示。

图 3-15 用户运维矩阵

3.5.3 服务质量

云密码服务作为一种新兴技术和产业，如何衡量其服务效果，促进云密码服务产业可持续发展，需要相应的建立服务质量管理制度和标准，制定服务质量评价体系。

目前，信息技术服务的质量评价体系还不成熟，云密码服务又明显区别于其他信息技术服务，所以云密码服务的质量评价体系还仅在研究阶段。对云计算等相关信息技术服务的质量评价体系进行了研究，结合云密码服务的特点，从服务的准确性、有效性、响应性、安全性、可靠性等方面提出了适用于云密码服务的质量评价体系，详细指标可参考附录 B。

3.5.4 安全要求

密码技术是网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，所以云密码服务自身的安全性尤为重要。云密码服务需要依赖密码产品及密码应用系统，云密码服务的安全性也取决于密码产品和密码应用系统的安全性。

通用安全要求部分应满足 GB/T 31168—2014 《信息安全技术 云计算服务安全能力要求》的增强要求。

云密码服务的密码基础设施部分及采用的其他密码产品必须是经过国家密码管理部门核准的商用密码产品，且满足 GB/T 37092—2018 《信息安全技术 密码模块安全要求》（原 GM/T 0028）的三级以上要求。

云密码服务系统除密码产品外，需要依据商用密码应用的安全要求，即需满足 GM/T 0054—2018《信息系统密码应用基本要求》的三级以上要求。

随机数安全性需满足 GM/T 0062—2018《密码产品随机数检测要求》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。

3.5.5 计费模式

云密码服务的计费模式通常可根据用户需要分为按时计费和按量计费两种，按时计费是指根据用户选定密码服务内容和性能参数后根据使用时长计算费用，按量计费是指根据用户使用密码功能的次数、流量、空间等数量计算费用。表 3-1 中是几种常见的云密码服务计费方式，即使是同一种密码服务也可选择不同的计费方式。

表 3-1 典型密码服务计费方式

服务名称	计费方式	计费单位
云密码资源池服务	使用时间	自然月/自然年
数字证书服务	证书数量	个
云密钥管理系统	密钥数量	个

云签名服务	签名次数	次
	使用时间	自然月/自然年
云加密存储	存储空间	GB
	累计流量	GB

第 4 章　云密码服务的关键技术

云计算环境对密码技术提出了新的需求，密码技术必须与时俱进适应云中服务化的要求。本章讨论了密码技术云服务化涉及的关键技术。

4.1　一些重要的密码算法相关技术

（1）　密码算法的高性能实现技术

密码算法是密码技术的基础，即使在传统的信息系统中，密码算法的性能也是很重要的，在对性能要求比较高的数据处理场合，加解密会成为系统的处理瓶颈，甚至影响到密码技术的使用。我国已经标准化的常用的密码算法有 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 算法等，这些算法已经在我国广泛应用，对它们的实现优化一直在进行，性能也一直在提升。但云计算还是对算法的性能提出了挑战，因为云中面临海量的数据量，而且数据量的增长呈指数增长，密码算法将一直面临性能提升的实现压力。解决密码算法的性能问题，必须把云中的应用场景细化，有针对性地对各种场景下的密码算法的应用方式进行优化，ASIC 技术是实现高性能密码算法的关键技术。近年来我国在集成电路领域不断加大投入，和发达国家在高端芯片制造领域的差距在缩小，密码行业应该利用国内最新的芯片技术成果，提供高性能的 ASIC 密码算法芯片。

（2）　保留格式加密技术

保留格式加密是一类特殊的对称加密机制，它最主要的特点就是保证密文的格式与加密前的明文格式完全相同。保留格式加密应用于数据库加密，即不需要改动应用系统，也不需要改动数据库结构，此外保留格式加密可以用于数据的脱敏，并可通过调节加密的位数来实现不同的访问控制粒度等。除了可以保证加密前后数据格式保持不变外，保留格式加密算法还具备加密前后数据长度不变等特点。

（3）　同态加密技术

同态加密主要用于密文信息处理。同态加密是指对其加密数据进行处理得到

一个输出，将此输出进行解密，其结果与用同一方法处理未加密原始数据得到的结果一致。与普通加密算法只关注数据存储安全不同，同态加密算法关注的是数据处理安全，提供对加密数据进行加法和乘法处理的功能，使用同态加密算法，不持有解密私钥的用户也可以对加密数据进行处理，处理过程不会泄露任何原始数据信息，同时，持有私钥的用户对处理过的数据进行解密后，可得到正确的处理结果。

（4） 基于属性加密技术

基于属性加密可用于访问授权服务，是保障云存储安全的重要技术之一。ABE 是基于身份的加密体制的进一步演变，ABE 可以构造一个访问控制结构，该结构保证了 ABE 的密文能够被多个不同的用户私钥去解密。

（5） 可搜索加密技术

可搜索加密技术是能够实现合法用户搜索关键词密文，并且保证敌手无法通过关键词密文或者搜索凭证获得用户查询的关键词信息的一种特殊加密技术。

（6） 代理重加密技术

代理重加密是允许一个拥有一些额外信息的半可信代理者把授权者公钥下的密文变换成受理人公钥下的密文，但是代理者以及没有代理人合作的受理人都得不到任何明文信息的一种密码系统。

（7） 协同数字签名技术

协同数字签名是指两个参与方在不泄露各自部分签名密钥的情况下，协同完成数字签名，在签名过程中不出现完整签名密钥恢复的情况，既能保证签名的正确性，又能保证签名密钥的安全性。一般情况下，协同数字签名通过将部分签名委托给数字签名服务器端完成，来简化在移动智能终端上进行数字签名的操作，使用户能够在确保网络签名高度安全的环境下使用相关业务。

（8） 安全多方计算技术

安全多方计算可用于访问授权服务和密文处理服务。安全多方计算的研究主

要针对无可信第三方情况下，安全地进行多方协同计算问题，即在一个分布式网络中，多个参与实体各自持有秘密输入，各方希望共同完成对某函数的计算，而要求每个参与实体除计算结果外均不能得到其他用户的任何输入信息。

（9） 安全外包计算技术

安全外包计算可以让用户将复杂的运算安全的外包给运算能力强的云服务器，并使用户的隐私数据不会泄露给云服务器，用户可以检验云服务器返回结果是否正确。此外，在安全外包计算中，用户本地消耗的资源要明显小于直接完成此项计算任务所消耗的资源，因此需要满足隐私性、可验证性、高效性三点要求。

（10） 可证明数据持有技术

可证明数据持有技术是即使用户删除本地数据，仍然可在无需下载数据的条件下，不泄露数据内容地验证不可信的存储服务器是否正确地持有（保存）数据，避免存储服务提供者删除、篡改数据的一种技术，其主要目的是使用户能在不可信的存储服务器上获得可信的存储服务。

（11） 零知识证明技术

零知识证明可用于身份认证、数字签名、抗选择密文攻击的加密等。零知识证明的基本概念是：假设证明者 P 拥有某秘密信息，通过一系列协议过程，P 可以向验证者 V 证明他知道这个信息，但同时不会将任何与之相关的信息泄露给 V。

4.2 硬件虚拟化技术

4.2.1 密码芯片或密码卡的虚拟化

虚拟化技术是重要的云计算技术，虚拟化实现硬件资源的共享使用、动态分配、灵活调度，提高了 IT 资源利用率。密码模块是一种硬件资源，在云计算平台中也要实现虚拟化。主机内的硬件密码模块一般以 PCI-e 接口密码芯片或 PCI-e 接口密码卡的形态存在，目前 PCI-e 接口设备的虚拟化有以下三种方式：

（1） 基于软件的虚拟化

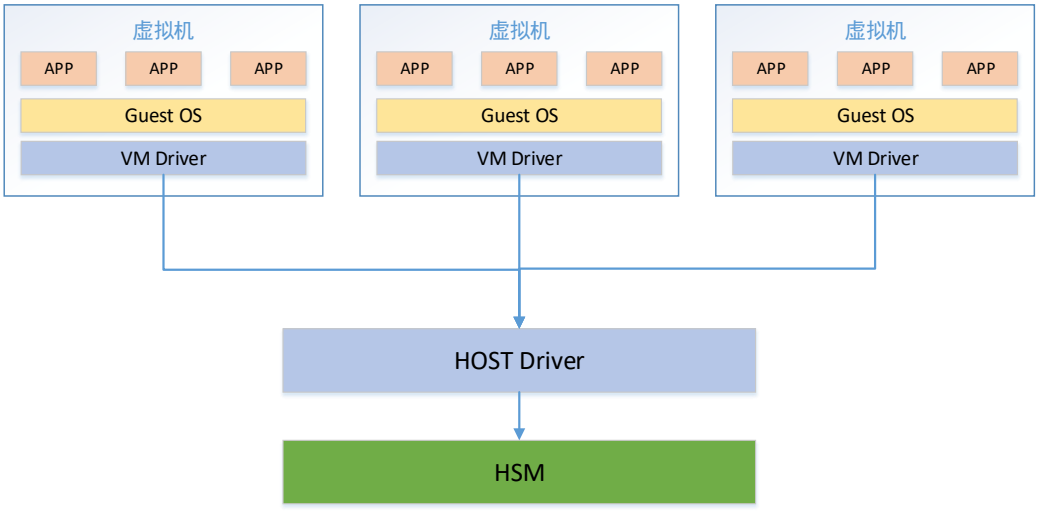

图 4-1 软件虚拟化技术

如上图 4-1 所示，传统的 PCI-e 接口硬件板卡本身是不支持虚拟化技术的。对于这种硬件，如果要在多个虚拟机中进行访问，需要在软件层做工作，软件虚拟化层必须能够截获应用程序对物理板卡的直接访问，并将其重新定向和协调，从软件层面实现分时的或协作的多任务共享，来达到虚拟化的效果。这种虚拟化的方式，优点是对硬件要求低，不需要硬件有特殊的改动；但缺点是效率低，软件截获并重定向对硬件的访问，对服务器 CPU 的开销较大，硬件板卡的性能损耗也很多，另一个缺点是板卡内部的软件隔离性差。

（2） IO 通道辅助的虚拟化

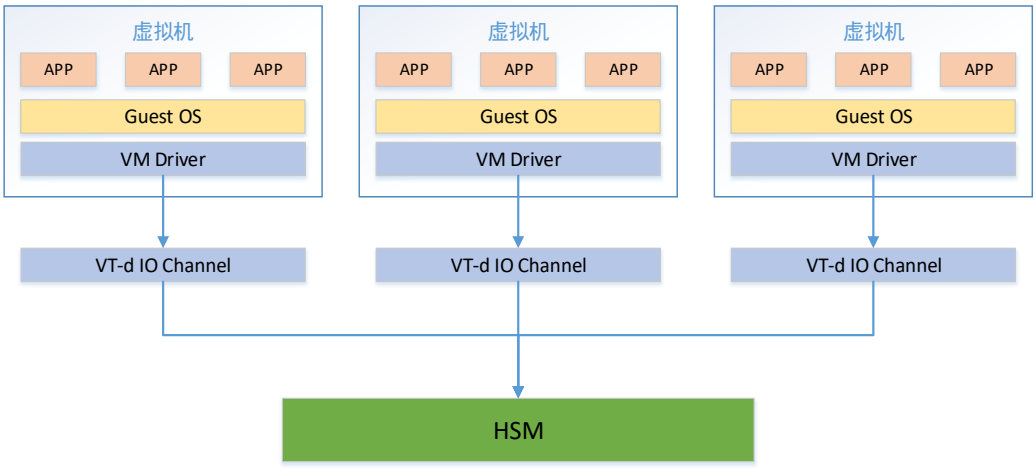

图 4-2 IO 通道辅助的虚拟化技术

如图 4-2 所示，由于软件虚拟化的方式有前述效率低的问题，所以 Intel 提出了 VT 虚拟化技术。该技术由一系列技术组成， 其中 Intel VT-d 技术是一种基于北桥芯片的外设硬件辅助虚拟化技术。这种虚拟化技术的特点是，在 I/O 通道的级别，实现了硬件支持的虚拟化，相比软件虚拟化的方式，大大提高了性能，降低了 CPU 的开销。在隔离程度方面也比软件有所提高，至少在 I/O 通道的级别实现了硬件隔离。但是在板卡内部，仍然和软件虚拟化方式相同。

（3） 硬件级的虚拟化

为进一步提高虚拟化的功能和效率，PCI-Special Interest Group 提出了 Single-Root I/O Virtualization（SR-IOV）虚拟化技术。通过 SR-IOV，一个 PCI-e 设备不仅在 I/O 通道层面实现了硬件虚拟化，还在设备内部实现了硬件虚拟化。一个设备可以包含多个 PCI 物理功能，或者包含共享设备内资源的多个虚拟功能。在 SR-IOV 模型中，不需要任何中间软件的转换，因为虚拟化是在 PCI 设备内部实现的。虚拟机管理程序只要简单地将虚拟功能映射到 VM 上就可以实现本机设备的虚拟化，保证了虚拟化的性能和安全。这种虚拟化技术具有最高的性能和效率。隔离性也是由硬件来保证的，具有和分离的多个设备相同的安全程度。如图 4-3 所示。SR-IOV 虚拟化技术是 PCI-e 设备最先进的技术，但实现的难度比较大，目前国内只有很少的厂商产品支持。

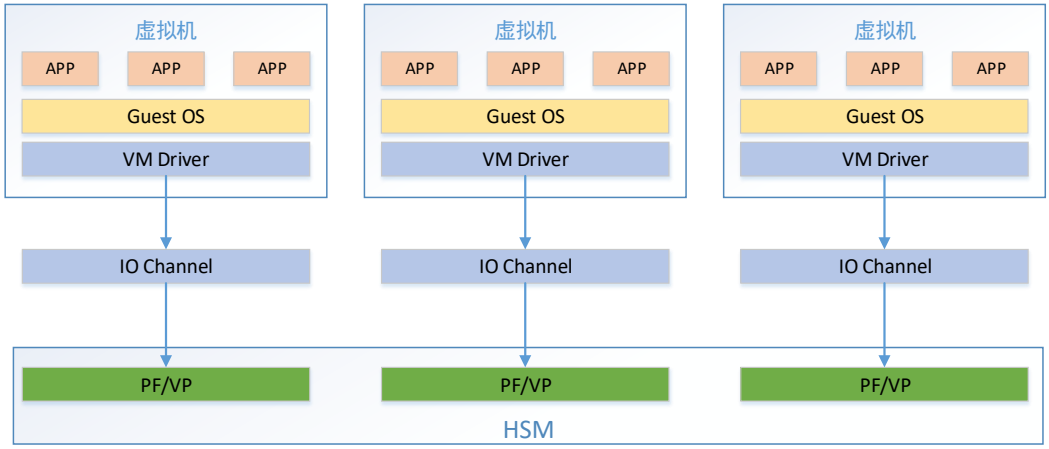

图 4-3 基于 SR-IOV 的硬件虚拟化技术

4.2.2 云密码资源池

云密码资源池是一种创新性的产品，为了适应云平台动态扩展、弹性扩容的

需求，密码设备厂商，把虚拟化技术和云管理技术应用在密码设备集群，把密码设备集群组织成“密码设备云”，形成集成化的云密码服务资源池。

如图 4-4，是云密码资源池中单台服务器的逻辑组成图，物理服务器内置了支持硬件虚拟化的密码芯片或密码卡，密码卡被虚拟成多个虚拟密码卡，为每个虚拟机或微服务实例提供密码模块功能，在虚拟机或微服务实例中实现密码逻辑功能服务。

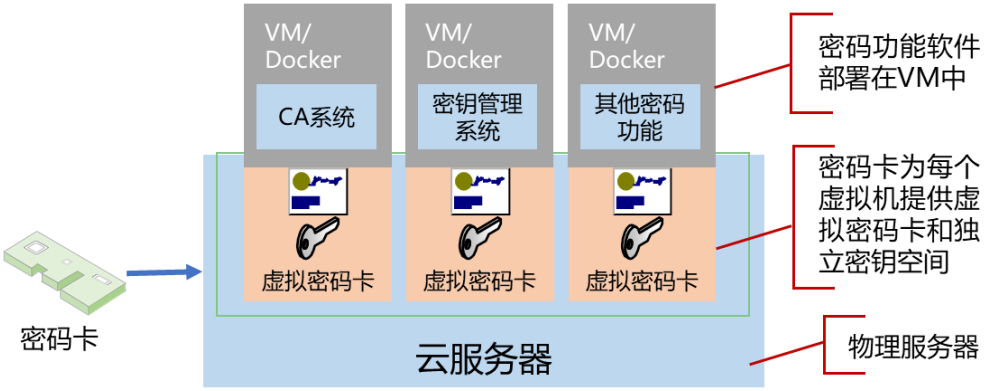

图 4-4 单台云密码资源池服务器

密码资源池是这种设备的集群，多台设备由统一的云操作系统和管理软件管理，通过网络对外提供各种密码服务。密码资源池一般单独部署，通过安全的网络通道和云平台连接，在云平台中，部署密码设备的访问代理，访问代理可以是虚拟机实例、微服务实例、或接口软件包。密码资源池部署如图 4-5。

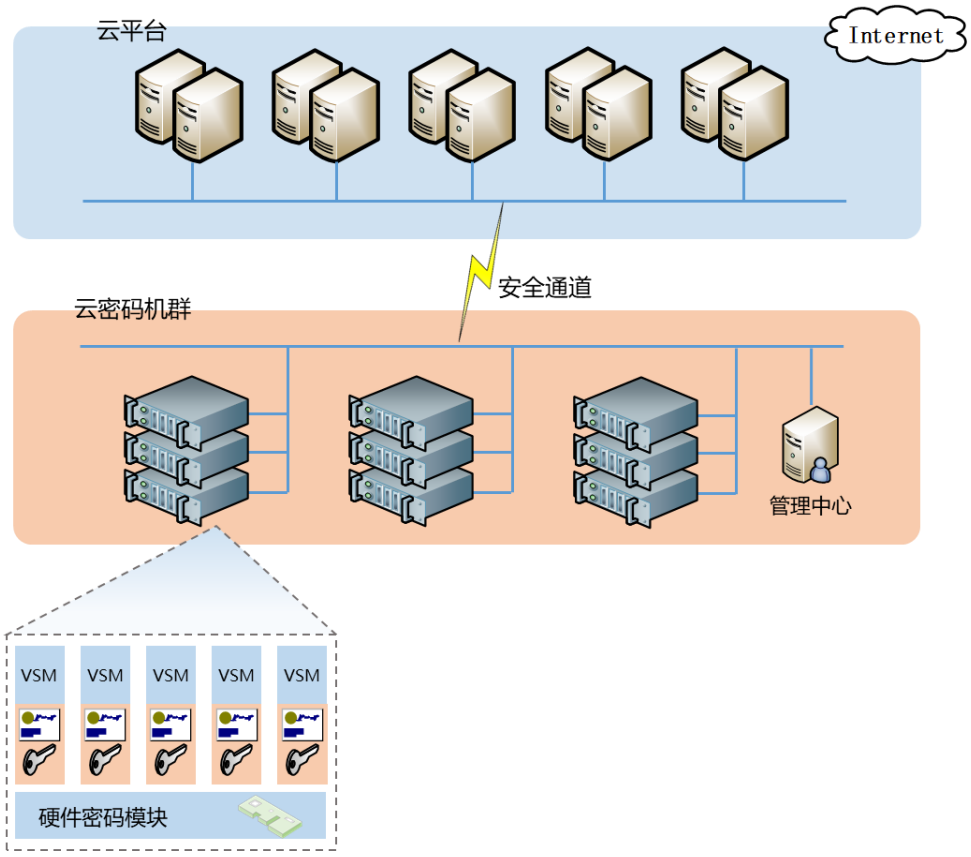

图 4-5 云密码资源池

云服务器密码机（简称“云密码机”）是国密局批准的一种新的产品型号种类，是云密码资源池的一个应用案列，云服务器密码机实现了传统服务器密码机的功能，但可以集群部署，实现了虚拟密码机的动态创建、远程管理、按需部署、弹性扩容，满足云计算平台中对密码机的需求。目前，已有多家厂商获得了商密型号证书。

4.3 云密钥管理技术

（1） 密钥隔离

云密码服务面向不同的安全等级要求，需要提供多层次的密钥隔离机制。对于核心领域及关键行业需要提供高安全等级的密钥隔离，建议直接采用云密码资源池提供硬件密钥隔离安全。对于常规业务应用需提供基于主密钥隔离的安全密钥管理服务。对于多用户的应用场景，在以上密钥隔离技术的基础上提供用户级的密钥隔离。

（2） 远程管理

由于云密码服务系统位于云计算服务商或云密码服务提供商的硬件环境中，用户对云密码服务的运维管理只能远程进行，并且需要云密码服务商的配合，用户需要根据实际需要与云密码服务商分配运维责任。通常情况下，建议密码硬件基础设施和基础网络的运维管理由云密码服务商或云计算服务提供商提供，用户更应关注密钥管理、安全策略配置及安全审计等方面的运维管理。使用 PKI 或其他身份认证技术、SSL/TLS 安全通信技术等保证远程管理的安全性。密码服务开通时，可由服务提供商设置初始管理员后，将身份认证凭证（如智能密码钥匙等）交给用户，用户即可远程登录到云密码服务管理界面。

（3） 访问控制

云密码服务不同于传统的密码设备单一、可控的安全部署模式，其灵活性、远程性、迁移性都会带来更高的风险。访问控制作为云密码服务中接入服务的关键一环，应基于角色、服务、身份等采用多种认证模式的对云密码服务进行访问授权控制，云密码服务通过集成证书认证、OAuth 认证、SMAL 认证、OpenID 等认证形态提供多种模式的访问控制。对于不同的业务服务模式，采取最合适的访问控制机制，可以极大的提高云密码服务的安全性，同时，借助访问控制机制，为云中密码服务的全链审计提供有效的技术支撑。

4.4 云密码服务安全访问技术

云密码服务的用户可能通过物理设备（PC、服务器、手机终端等）访问服务，也可能通过云中的虚拟主机访问服务，因此云密码服务的访问主体最终落实到物理设备，或云中的虚拟主机、微服务实例、或应用程序等实体。这些实体通过云密码服务提供的访问接口使用密码服务，它们和云密码服务实体之间要建立安全的通信链路，同时要保证通信实体身份的真实性。

通信安全的协议主要有 IPSec 协议、SSL/TLS 协议等。IPSec 协议部署在网络层，对通信节点之间所有的 IP 包加密，分为网络层的 IP 包安全处理（ESP、AH 协议）、应用层的密钥协商（IKE 协议）两部分，实施难度较大，不太适合云

中多样化实体的安全通信需求。SSL/TLS 协议（我国密标委制定了和此协议类似的被称为 TLCP 的协议）是基于会话层的安全通信协议，它的密钥协商和数据安全处理在一个网络连接会话中，只是把通信过程分为密钥协商阶段和数据安全通信两个阶段，比较轻型，多数情况下更适合云中各种通信实体之间的安全通信。

无论使用哪种安全协议，都需要进行通信实体的身份认证和数据的加密处理。数据的加密处理一般使用对称密码技术，而身份认证使用非对称密码技术，非对称密码技术可以采用基于数字证书的公钥体制、IBC（基于标识的公钥体系）或者其他无证书公钥技术体制，其中基于数字证书的身份标识与认证方式是最成熟、并被广泛应用的，被 IPSec 协议、SSL/TLS 协议支持。因此云中首先要建立网络实体的数字证书生命周期管理机制，支持物联网证书发放的 CA 系统应该有适合物联网的特殊特点；其次，访问端需要解决密码运算和密钥的安全存储问题。如果是物理的终端可以采用硬件密码模块，如在 PC 上使用 USB 接口的智能密码钥匙，在服务器上使用密码卡，但在云中的服务器或一些手机终端上无法增加硬件密码模块，不得不使用软件密码模块，而软件密码模块中的密钥安全又成为了一个防护点。目前常用软件密码模块的安全防护技术如下：

（1）白盒密码技术：将密钥与密码软件程序代码相融合，不直接存储密钥，提高密钥存储的安全性。

（2）软件逆向工程防护技术：通过代码混淆、增加冗余代码等技术，实现对密码软件模块的防护，提高软件逆向工程的难度。

（3）基于寄存器和 cache 缓存的密钥安全技术：在密码运算过程中，将密钥限定在寄存器和 cache 缓存中，防止密钥在内存中被非法读取和泄露。

（4）基于 TEE 等执行环境的安全技术：利用 CPU 提供的 SGX、Trustzone 等隔离计算执行环境，保障密码软件运算时的密钥和敏感参数的安全性。

第 5 章　云密码服务发展趋势

5.1　云密码服务应用发展趋势

5.1.1　应用场景更加丰富

当前云计算、大数据、物联网、人工智能等技术和应用飞速发展，互联网、物联网、工业互联网各种网络融合发展，过去相对独立分散的网络和系统已经融合为深度关联、相互依赖的整体，形成了人机交互、天地一体、万物互联的网络空间，这就催生了融合环境下可根据用户需求弹性、按需配置、安全共享定制等高度灵活的云密码服务广阔应用场景。

云密码服务不仅可面向具有高安全性和高性能需求的电子商务、电子政务领域应用，而且随着 IT 系统云化，还可应用于各种智慧系统领域。在智慧城市、智慧交通、智慧医疗等各种新的应用场景中，通过它可以解决数据的存储、网络传输、身份认证、数据完整性等安全问题。

5.1.2　服务内容更加多样化

随着数字资产的价值不断提高以及个人隐私保护意识的不断增强，信息安全的重要程度也在不断提升，以密码技术为安全支撑的应用服务越来越多。回顾密码技术的演变我们可以发现，随着数字化进程的不断提升，日渐丰富的业务应用系统已经将 IT 系统从规模程度、复杂度、颗粒度提升到新的高度，产生与之匹配的安全控制能力需求，从而推动密码产品和密码服务面向业务场景，呈现出更多的多样化。

5.1.3　向业务端演化

随着应用场景的丰富和服务形式的多样化，不同的业务端应用对密码技术提出了更多差异化的需求，如：不同的部署环境要求、不同的算法以及应用模式、不同的性能要求等。只有贴近业务端需求，密码技术才能发挥出更好的安全支撑

作用。因此，密码产品和密码服务将呈现向业务端演化的趋势。同时，在融合环境下，攻击者的多元攻击将倒逼安全防护能力的进化，这也将推动密码产品和密码服务向业务级演化，并呈现出向更细粒度演进的发展趋势。

5.2 云密码服务技术发展趋势

5.2.1 密码技术持续创新

近年来，在密码技术自身发展和新兴应用的促进下，密码技术不断创新，在密码理论、关键技术、密码产品等方面进展显著。

云计算与大数据等“互联网+”新技术的普及应用，对密码技术提出虚拟化、保留数据格式加密、同态加密、安全隔离等方面的要求；在物联网、工业控制领域中，需要更轻量级的密码算法；区块链和数字货币的发展需要密码技术提供基础支撑，多方计算、零知识证明等密码技术研究成果丰硕。

国内密码芯片在制造工艺、综合性能、存储容量、接口类型、安全性等方面已经取得了长足的进步，并得到了广泛应用。密码模块与密码机的种类不断丰富，与应用的契合度也越来越高，伴随着云计算与物联网的发展，不断有新的高速密码模块与密码机产品诞生。这些密码产品方面的进步，为云密码服务的开展提供了良好的基础设施支撑。

5.2.2 密码技术与新技术深度融合

密码服务需要面向更新的使用场景，部署在全新的应用环境，提供创新的密码服务内容，这些方面的改变不仅对密码技术本身提出挑战，更离不开其他新技术的支撑。

云计算安全离不开密码技术的支撑，但传统的密码产品难以适用于云计算的应用场景，尤其是在公有云环境中更为突出。以密码机为例，传统网络环境中密码机和应用服务器“背靠背”部署方式的模式在云环境下已不再适用，为适应云计算环境的密码应用和部署，亟需密码机具备资源共享、远程管理、高可用等新

特性，加速了密码技术和虚拟化技术的融合，衍生出云密码资源池这一产物。

以安全大数据为基础，结合人工智能技术，建立基于环境、动态、整体的密码服务和密码应用感知系统，全天候、全方位感知密码应用安全态势，从全局视角提升对密码应用安全威胁的发现识别、精确分析和应急处理，增强云密码服务的防御能力和威慑能力。

5.2.3 云密码服务标准体系化

任何一种技术的大规模应用都需要标准化工作的支持，同时标准化工作开展的时机非常重要，如果开展得过早，没有足够的技术积累和试点应用经验的支持，形成的标准就会指导性不强、带来工作的浪费，而如果标准化工作开展的过晚，会造成产业发展的无序，对产业的健康发展带来影响。当前，无论从国际、国内，都缺乏针对云密码服务的标准和技术规范，一些云密码服务系统的建设只能参考已有的针对传统密码系统建设的标准，但是由于应用部署环境不同，这些旧的标准难以适用于云计算环境。比如对密码机的使用，传统的系统中要求应用主机和密码机通过专用的网络通道“背靠背”连接，但在云中，已无法建立物理的专用网络通道；对密码模块的使用配置要求直接在主机上进行，但在云计算中，用户接触不到云服务器，只能远程配置。这些应用环境的变化，需要系统地考虑新的方式方法及其安全性与标准化。安全符合“木桶原理”，即系统的安全性取决于最短的板子，只有通过标准化，才能让所有的木板一样整齐，避免云密码服务系统安全设计的漏洞出现。

我国密码行业标准化技术委员会已经开始制定云密码服务相关的标准，我们认为应该加快速度，因为我国云计算发展迅速，国家重视商用密码的应用，云密码服务系统已经越来越多，业界已经出现在云计算平台中应用密码技术的困惑。我国的互联网应用、移动互联网发展走在世界的前列，在云密码服务标准体系制定方面我国也可以走在世界的前面。

5.3 云密码服务产业发展趋势

5.3.1 基础产业迅速发展

除了云密码相关技术不断创新外，云密码服务所需要的基础支撑产业也在不断进步，如密码芯片、密码模块、基础平台等。密码芯片处于密码产业的最上游，同样也是云密码服务产业的基础之一。云密码服务对密码芯片的运算性能、安全性、虚拟化支持等方面要求更高。性能方面，SM2、SM3、SM4 等密码算法的性能都在不断刷新记录。安全性方面，部分芯片产品可达到国密局密码芯片安全等级二级认证，个别达到三级水平。制造工艺方面，密码芯片技术在向更高工艺上发展。密码模块与密码机的种类不断丰富，与应用的契合度也越来越高。

云计算与物联网的发展催生出新的高速密码模块与密码机产品。GM/T 0028—2014 《密码模块安全技术要求》赋予了密码模块更广的概念，并规定了四个递增的、定性的安全要求等级，提高了用户对密码产品安全性的认知，能够更好地帮助用户在不同应用和工作环境中正确的选择密码产品。

5.3.2 云密码服务催生新生态

云密码服务是新型的密码服务模式，不仅涉及密码技术的创新发展，还涉及服务模式、商务模式的创新和发展。传统的密码产品厂商要顺应时代的需求，向云计算服务方式转变，云运营商要使用云密码服务，并向云用户提供密码保障服务。云运营商、密码产品和密码服务提供商、用户，要重新思考自己的定位、以及和其他方的关系，构建云密码服务的新生态。

附录 A

典型云密码服务

A.1 云密码资源池服务

密码资源池服务提供者构建密码资源池，可根据负载动态调整云密码机的规模，实现密码运算资源的动态调整和灵活调度。密码资源池服务为用户提供按需高效、弹性可扩展的密码服务。

密码服务资源池设计划分为密码设施层、密码服务层和密码管理层。密码服务资源池技术架构如图 A-1 所示。

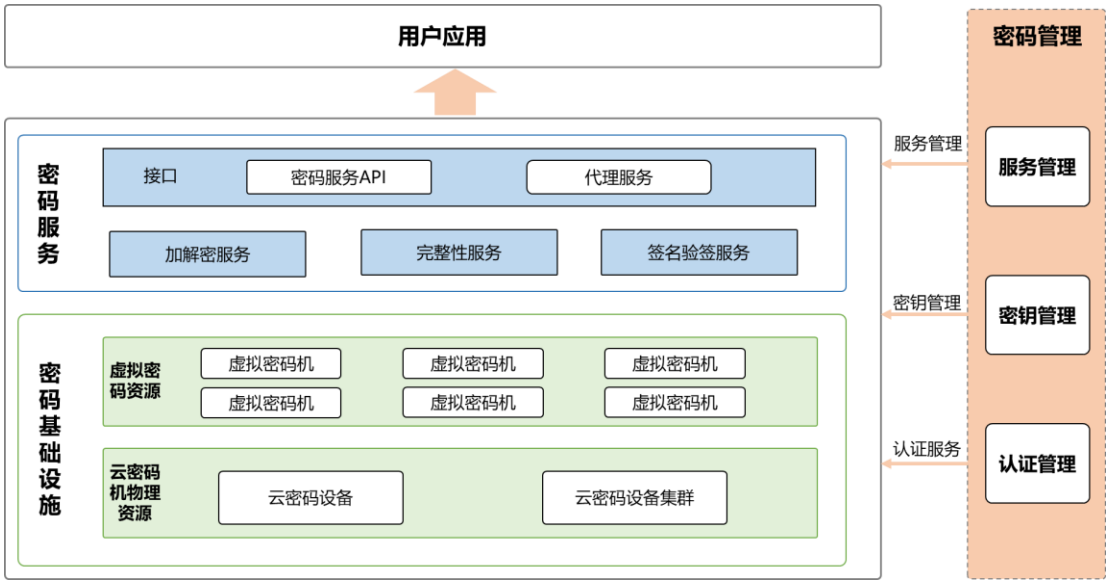

图 A-1 密码服务资源池技术架构

- 密码设施层

密码服务资源池设施层是利用云密码设备建设的密码硬件资源池。云密码设备是密码服务资源池的重要密码硬件设施。云密码设备基于高性能的硬件加密平台，采用虚拟化技术在硬件平台上同时运行多个虚拟化密码机，在提供密码设备基本功能的基础上，支持虚拟化部署，达到保证功能服务不变的同时降低总体成本及提高服务资源利用率的目的。云密码设备应符合国家密码管理部门的相关标准要求及经过检测审批。

- 密码服务层

密码服务资源池服务层是由密码服务 API 及密码应用代理等组成的密码服务资源池。密码服务 API 技术要求应符合商用密码行业标准 GM/T 0018—2012《密码设备应用接口规范》。代理服务技术要求应符合商用密码行业标准 GM/T 0024—2014《SSL VPN 技术规范》。

- 密码管理层

密码服务资源池管理层是密码服务资源池的支撑与运维平台。其中管理层的密钥管理与认证管理为密码服务资源池提供密钥与证书的管理服务支撑；管理层的密码服务监管负责密码服务资源池的运维保障，包括监控云密码设备、密码资源池服务、密码应用及其运行状况，同时结合云平台的运维、安全等要求，对密码服务资源池数据进行统一存储、备份和恢复。

应用场景：密码资源池服务支持租户的密码服务应用，支持云租户到云平台的传输密码保护，支持平台内部不同节点之间的传输保护，支持云平台数据存储密码保护、支持管理员的登录认证和数据传输保护，支持租户的登录认证。

A.2 CA 云服务

证书认证系统（简称 CA）是 PKI 密码应用体系中的核心基础设施，是对生命周期内的数字证书进行全过程管理的安全系统。证书认证系统从逻辑上分为核心层、管理层和服务层，其中，核心层由密钥管理中心、证书/CRL 生成与签发系统、证书/CRL 存储发布系统构成；管理层由证书管理系统和安全管理系统构成；服务层由证书注册管理系统（包括远程用户注册管理系统和本地用户注册管理系统）和证书查询系统构成。

CA 系统是密码应用系统的安全基础，CA 系统的建设和运行必须遵守相应的安全规范，包括系统安全、通信安全、证书管理安全、安全审计、物理安全、人员安全等多个方面，以及系统运行的可靠性。

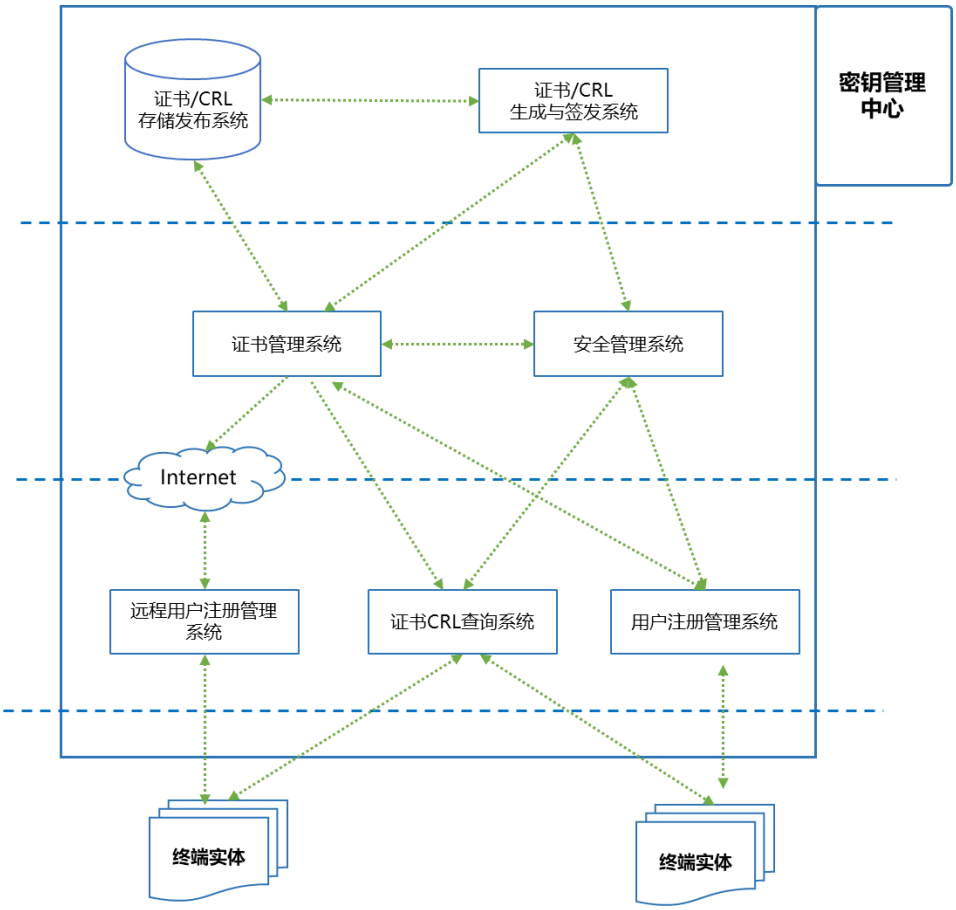

图 A-2 证书认证系统逻辑结构

移动互联网、物联网等发展迅速，对安全的要求越来越强，密码技术的应用越来越广泛和深入。其中终端证书的需求量越来越大，应用接入数量也在逐渐增多，给 CA 的服务能力带来巨大的挑战。基于云计算的弹性计算特点，可提高 CA 的突发处理能力，以应对特殊场景的高并发服务要求。根据 CA 系统的特点，把包括远程用户注册管理系统、OCSP 及 CRL 证书状态查询服务、LDAP 证书发布系统等服务层的子系统迁移到云上，可有效提升 CA 的服务性能，并能满足安全管理要求。

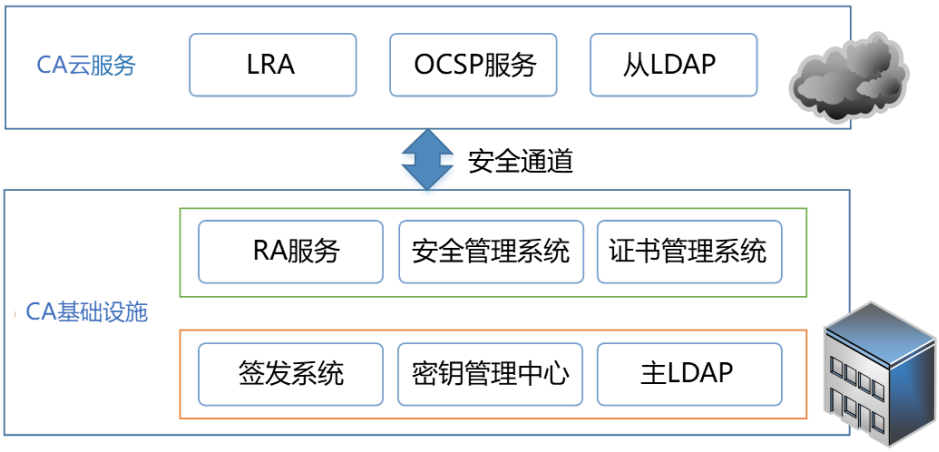

图 A-3 CA 云部署

A.3 云密钥管理服务

云密钥管理服务是指基于密码资源池基础设施，为平台服务商、密码租用单位/个人等用户提供密钥托管相关的支持活动，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、密钥的策略控制服务、基于托管密钥的简单加解密服务、密钥使用的日志记录服务、密钥高可用服务等。

- 密钥托管服务

用户可通过云密钥管理服务，进行密钥的生命周期管理，包括密钥的生成存储、密钥的查看、密钥的别名和描述、密钥的启用和禁用、密钥的销毁、密钥材料的导入以及定时轮换等功能。云密钥管理服务借助密码资源池生成密钥，密钥不得以明文形式出现在云密钥管理服务之外，确保密钥安全。

- 密钥安全隔离和存储服务

云密钥管理服务应采用严格的隔离措施，对不同用户的密钥进行有效的存储隔离和访问隔离，防止非法用户/未授权用户获取和访问密钥。云密钥管理服务采用经过国家密码主管部门技术检测的密钥管理系统，对密钥采取严格的保护措施后再存储，防止密钥被非法获取。

- 密钥的安全访问服务

云密钥管理服务应结合身份认证服务（IAM），采用身份鉴别、数据完整性、

数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

- 密钥的策略控制服务

云密钥管理服务采用策略控制，可实现对密钥的更细粒度的授权，比如限制用户能访问的 API/SDK，限制密钥的使用时间、跨用户授权密钥的访问权限等。

- 基于托管密钥的简单加解密服务

用户可借助云密钥管理服务，使用托管的密钥或已被授权的密钥，进行简单的加解密运算，比如小数据量的加密解密、产生外部的数据加密密钥、产生随机数等。

- 密钥使用的日志记录服务

云密钥管理服务应将用户对密钥的访问记录在日志中，借助这些日志，用户可以对托管密钥的使用情况进行监控和审计，确保密钥的使用合法性和可控。日志应存储在可靠的位置，便于用户查看和审计。

- 密钥高可用服务

云密钥管理服务应采取可靠的技术架构，比如前端负载均衡、备份恢复、集群与数据同步等，给出服务可用性承诺，确保服务可用性不低于承诺值。

云密钥管理服务的逻辑框图如图 A-4 所示：

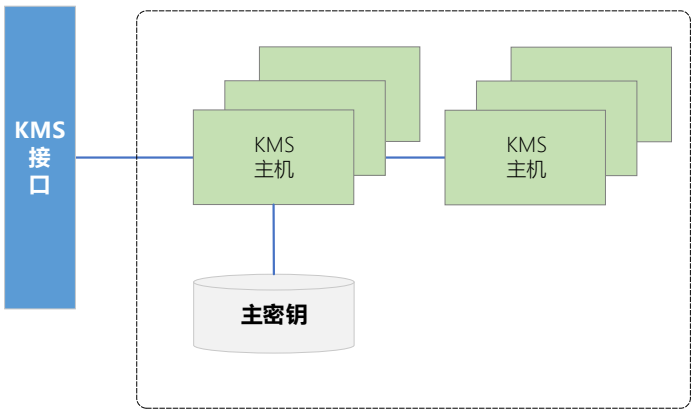

图 A-4 云密钥管理服务逻辑框图

云密钥管理服务一般由四个部分组成：

- HSM

即底层密码设备或云密码资源池，提供密钥保护和运算能力。

- KMS Host

云密钥管理服务的运行主机，提供云密钥管理服务的核心功能。

- 数据库

数据库用来存储实际的密钥值，密钥值经过严格的保护措施后再存储，防止密钥泄露。不同用户的密钥存储有一定的的隔离措施，防止密钥的非法访问。

- 应用接口

云密钥管理服务对外提供统一的、易用的 API/SDK，采用标准协议，方便不同用户和应用系统的使用。

云密钥管理服务典型的应用场景主要有两个：

- 少量数据的加解密

用户的数据通过安全信道传输到云密钥管理服务，服务端完成加密、解密后，操作结果通过安全信道返回给用户，如图 A-5 所示。

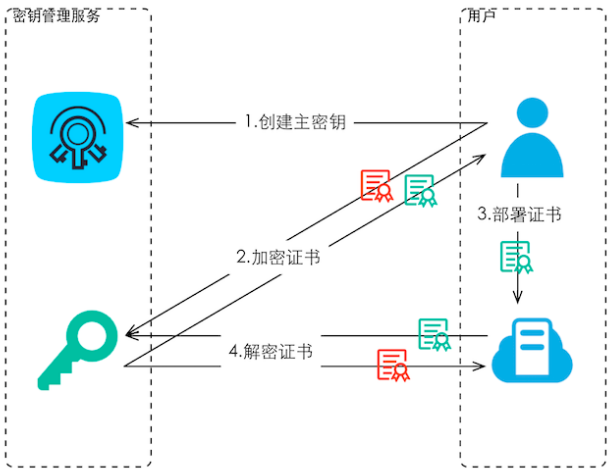

图 A-5 加密、解密证书

- 使用信封加密在本地加密、解密数据

使用云密钥管理服务创建一个主密钥，使用主密钥生成一个数据密钥，再使用数据密钥在本地加解密数据，如图 A-6 所示。这种场景适用于大量数据的加解密。数据无须通过网络传输即可实现加解密，从而在保证安全性的同时降低了成本。

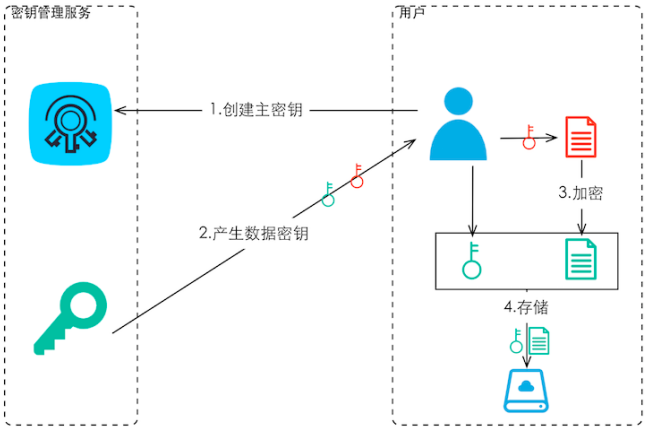

图 A-6 加密本地文件

A.4 云电子签名服务

云电子签名服务是指基于密码基础设施，为平台服务商、密码租用单位/个人等用户开展电子印章、电子证据、时间戳、电子文件、应用程序等数据电文所需的可靠电子签名功能，如签章服务、安全日志审计服务、安全电子文件验证服务、可信时间戳服务、安全电子证据管理服务等。

电子签名服务的典型框架如图 A-7 所示：

图 A-7 电子签名服务典型框架

云电子签名服务典型架构由云签名服务、签名方和依赖方组成。CA认证中心作为系统外部服务用于向签名者提供数字证书以及相关服务。各部分的功能介绍如下：

- **依赖方**

  依赖方是指需要使用电子签名来进行后续业务操作的相关方。

- **签名方**

  签名方指进行电子签名的主体。签名方通常需要使用应用程序对电子签名过程进行控制和确认。在某些业务场景中，签名方和依赖方可能为同一实体。

- **云签名服务**

  云签名服务是基于云的电子签名服务的最主要部分。云签名服务通过技术和管理等手段，以云服务的方式，为签名方和依赖方提供用户管理、密钥管理和数字签名服务。云签名服务具备云服务按需服务、泛在接入、资源池化、快速伸缩性、服务可计量等特性。

云电子签名服务一般支持多种签名模式，包括客户端签名模式、协同签名模式和服务端签名模式等。

- **客户端签名模式**

客户端签名模式下，密钥存放在客户端的密码模块中。需要进行电子签名时，在云签名服务端配合下，由签名方确认完成签名。客户端签名模式用于向个人提供签名服务的业务场景。这种场景下，用户终端例如个人计算机、平板电脑、智能手机通常应当有硬件密码设备可供使用。

- **协同签名模式**

  协同签名模式下，密钥分为服务端因子与客户端因子，客户端因子保存在用户终端，服务端密钥因子加密保存在云签名服务的密钥库中。在电子签名过程中，在签名方确认下，由客户端和云签名服务共同完成签名。

  协同签名模式用于向个人提供签名服务的业务场景。尤其适用于面向多种异构终端例如智能手机、平板设备的移动互联网业务场景中。

- **服务端签名模式**

  密钥加密保存在云签名服务的密钥库中。在电子签名过程中，签名方通过密码技术进行身份确认和授权，在云签名服务完成签名。服务端签名模式用于向业务应用提供签名服务。

通常，云电子签名服务为 CFaaS 模式（密码功能即服务），集成方通过在业务系统或终端中通过交互协议或 SDK 来使用云签名服务，完成业务所需的电子签名。

A.5 云身份鉴别服务

云身份认证服务是构建在 SaaS 层的云服务，为不同计算模式的云服务提供身份鉴别。当组织机构将应用部署到云环境时，将遇到身份认证的新需求和挑战，以云服务的方式提供身份认证是一种合适的解决方案。云安全联盟（CSA）指出，将应用部署到云计算环境中将面临凭据管理、强身份鉴别、委托身份鉴别（跨越不同的域或跨越不同的服务进行身份鉴别）等挑战。IAM 是云计算环境中一种典型的云身份认证服务，见图 A-8。

- 用户的创建和管理

用户可以通过管理控制台、命令行界面或 API 创建。如果用户需要访问管理控制台，那么需要为用户创建用户名/口令作为登录凭证。如果用户需要通过 CLI 或 API 访问云服务，那么需要为用户创建 API 访问密钥作为访问凭证。

- 用户安全凭证及管理

为了访问账户资源，用户必须提供相关凭证；使用管理控制台，用户必须提供正确的口令；使用 CLI 或 API 调用，用户必须提供正确的访问密钥。如果用户仅通过 API 或 CLI 访问资源则不需要口令，拥有访问密钥即可。

- 用户名/口令

账号口令管理：可以通过注册账号时的邮件地址和口令，以及管理控制台来更改账号口令。可以对口令设置安全策略，如口令长度、口令字符组成限制、口令更改周期、口令过期无效等。

用户口令管理：可以通过管理控制台、CLI 或 API 三种方式对用户的口令进行创建、更改、删除等操作。

- 访问密钥

当用户创建完访问密钥后，返回给用户一个访问密钥 ID 和秘密的访问密钥。默认情况下，创建完的访问密钥状态为激活状态，意味着用户可以使用该密钥发起 API 调用请求，该访问密钥可以被执行禁用、启用、撤销、更改、删除操作。

用户访问密钥管理主要包括通过管理控制台完成对访问密钥的创建、更改和查看操作，或者通过 CLI 和 API 完成对访问密钥的创建、更改、查看以及轮换操作。

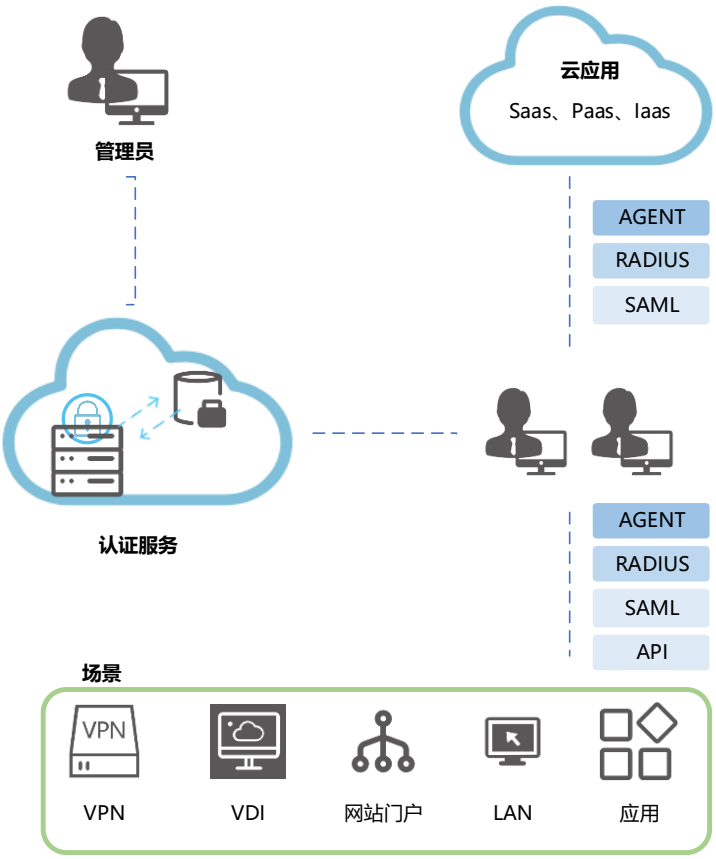

图 A-8 云计算中的 IAM 服务

身份鉴别技术的安全依赖于密码技术的采用。在云平台中有专门的密钥管理机制来管理其云服务中所用到的密钥。在云服务的身份鉴别技术中，无论是身份账户的存储、使用，还是 SAML、OpenID 等协议的使用，都需要采用密码技术来保障安全，如采用对称加密技术来加密敏感的身份信息和传输中的身份凭证等敏感信息，采用数字签名技术来防止协议消息被篡改等。

A.6 云加密存储服务

数据加密服务是指基于云密码资源池和云密钥管理服务基础设施，为平台服务商、密码租用单位/个人等用户提供基于场景的数据加密支持活动，如敏感字段加解密服务、文件/对象加解密服务、数据库加密服务、文件系统加密服务、磁盘加密服务、大数据加密服务等。

- 敏感字段加解密服务

借助云密码资源池和云密钥管理服务的接口，加密系统中的敏感字段，实现数据的加密脱敏，同时加密密钥被安全存储和安全调用，确保密钥安全。

- 文件/对象加解密服务

基于云密码资源池和云密钥管理服务的接口或客户端工具，实现对文件或自定义对象的加密，同时加密密钥被安全存储和安全调用，确保密钥安全。

- 数据库加密服务

用户可通过数据加密服务，进行数据库数据的透明加密。数据库透明加密的主密钥通过云密钥管理服务托管和保护，实际加密数据的是数据密钥，数据密钥通过主密钥保护。数据密钥严禁以明文形式出现在数据加密服务和云密钥管理服务之外，密文的数据加密密钥与加密后的数据一块存储。

- 文件系统加密服务

用户可通过数据加密服务，进行文件系统的加密。文件系统加密的主密钥通过云密钥管理服务托管和保护，实际加密数据的是数据密钥，数据密钥通过主密钥保护。数据密钥严禁以明文形式出现在数据加密服务和云密钥管理服务之外，密文的数据加密密钥与加密后的数据一块存储。

- 磁盘加密服务

用户可通过数据加密服务，进行磁盘数据的加密。磁盘数据加密的主密钥通过云密钥管理服务托管和保护，实际加密数据的是数据密钥，数据密钥通过主密钥保护。数据密钥严禁以明文形式出现在数据加密服务和云密钥管理服务之外，密文的数据加密密钥与加密后的数据一块存储。

- 大数据加密服务

用户可通过数据加密服务，对接大数据框架中的密钥管理，对大数据框架提供主密钥托管、数据密钥的生成和保护、通过访问控制限制用户权限等功能。主密钥通过云密钥管理服务托管和保护，数据密钥通过主密钥保护。数据密钥严禁

以明文形式出现在数据加密服务和云密钥管理服务之外，确保数据安全。

数据加密服务的逻辑框图如下：

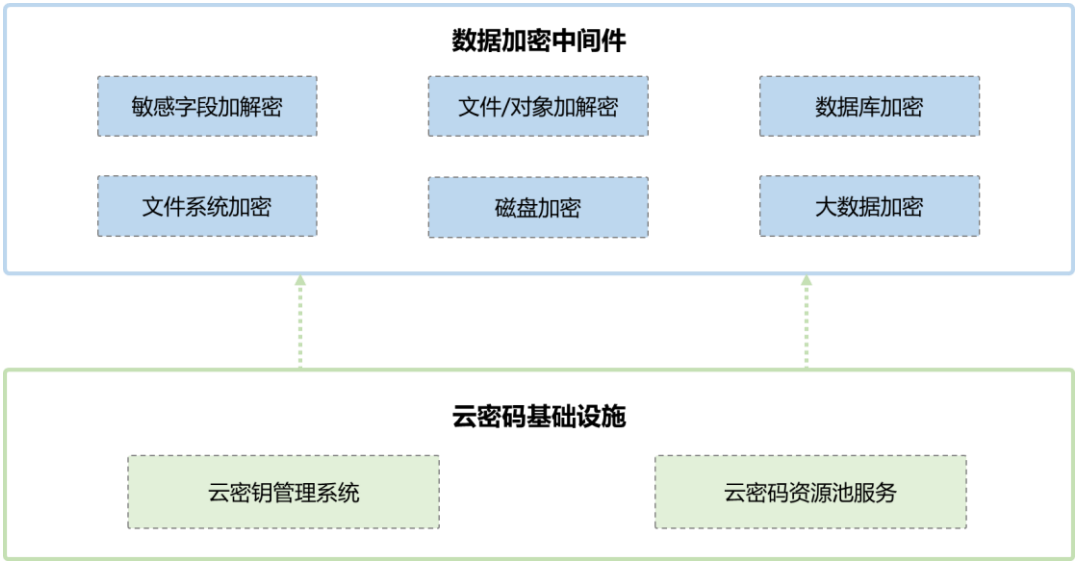

图 A-9 数据加密服务逻辑框图

数据加密服务的应用场景举例如下：

- 数据库 TDE 加密

某些数据库软件提供了一种称为透明数据加密（TDE）的功能。使用 TDE，数据库软件在将数据存储在磁盘上之前对数据进行加密。数据库的表列或表空间中的数据使用表密钥或表空间密钥进行加密。这些密钥使用 TDE 主加密密钥加密。可以将 TDE 主加密密钥存储在云密钥管理服务上，从而提供额外的安全性。

图 A-10 TDE 加密

- 磁盘加密

磁盘加密中间件使用云密钥管理服务管理磁盘加密的主密钥，对应每个磁盘阵列产生一个数据加密密钥。磁盘加密中间件使用安全合规的算法调用数据加密密钥加密应用程序写入磁盘的数据，并在应用程序读取时自动解密。

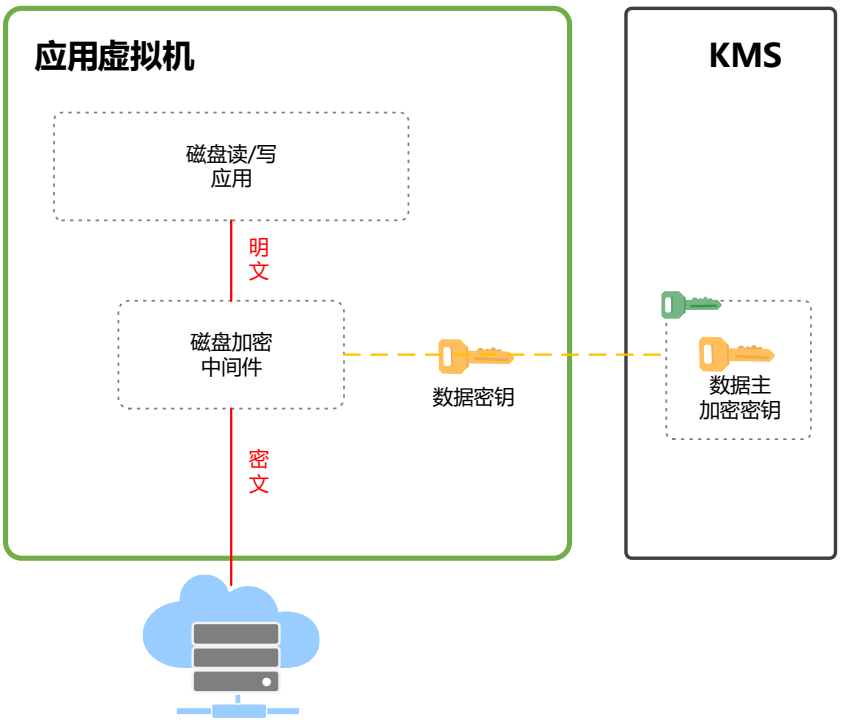

图 A-11 磁盘加密

A.7 云电子合同服务

云电子合同服务，主要目标是提升合同签署效率，解决不必要的资源消耗及用户应用便利性问题，同时利用互联网和移动终端的特性，通过引入电子合同签署服务，实现电子合同签署全流程电子化，同时保证电子化签署后的电子合同具备与纸质合同同样的法律效力，提高业务效率，提升用户体验。

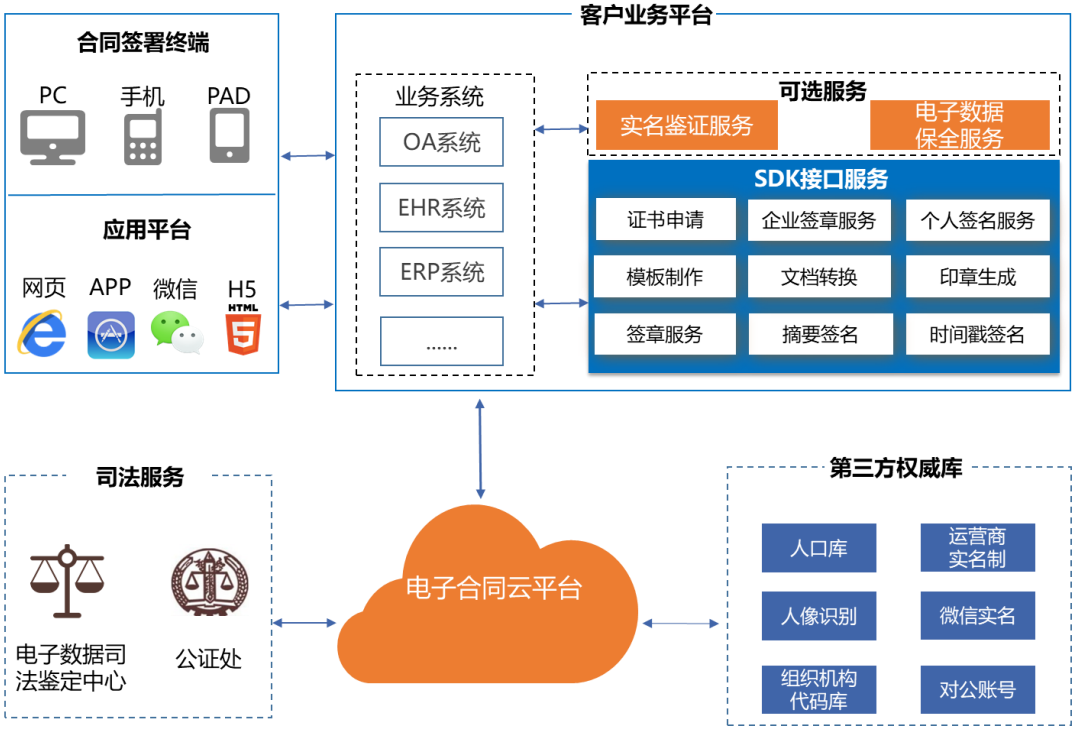

图 A-12 云电子合同服务

云电子合同服务为客户提供 SDK 接口服务，包括证书申请、企业签章服务、个人签名服务、模板制作、文档转换、印章生成、签章服务、摘要签名和时间戳签名，与客户业务系统集成；合同原文不出本地，哈希摘要上传至云电子合同服务完成电子签名。用户可使用任何一个终端都能签署协议，包括：PC、手机以及 PAD；支持全平台签署：网页、应用 APP、微信小程序、公众号，以及 H5 页面。

云电子合同服务在提供服务时，对接权威第三方服务，包括自然人信息验证服务和法人信息验证服务，实现合同签署主体的身份识别；数字证书服务和云签名服务，以及可信时间源服务，实现签署人的数字证书的签发，以及电子签名数据处理；第三方电子数据保全服务，实现电子合同数据的第三方证据保全；以及

包括签名验证证明、公证、司法鉴定等电子合同司法举证和证明服务。

云电子合同服务所提供的服务，主要包括：

（1） 身份鉴证服务

云电子合同服务多种维度的身份在线鉴证方式，鉴证个人和企业身份，支持对合同相关各方的网络身份进行核实验证，从而确保电子合同签署和操作用户的网络身份真实有效。从用户类型上，身份识别服务支持对自然人的身份识别、组织机构（法人）的身份识别。

（2） 合同签署服务

通过云电子合同服务进行合同签署时，云电子签名服务的服务过程包括：

（a） 业务系统发起合同签署，上传文档信息、签名图片和签章位置等信息，通过接口的方式，在本地计算文档摘要，并将摘要信息发送至数字认证电子合同云平台；

（b） 数字认证电子合同云平台进行签名计算，返回签名信息至客户业务平台，包括：数字证书、摘要签名和时间戳签名；

（c） 客户平台通过接口的方式进行文档合并；

（3） 电子数据保全服务

电子数据保全服务，旨在为任何形式的电子证据进行安全存证。实现在证据产生源头直接采集，确保证据的真实性；实现在采集完成后立即固化和加密，通过安全传输通道直接发送至保全系统；保全系统将接收到的电子证据采用先进的国产密码算法进行加密并加盖时间戳，采用分布式和多节点方式进行保存，保存的期限可灵活配置，最终实现电子证据的长效和安全的存储；保全后的电子证据在保全系统鉴定客户身份和所对应权限后，提供查询和下载服务；在事后出现纠纷时，可提供对应的司法服务。

云电子合同服务能够满足签约各方便捷签约的需求，同时也节约了签约成本，进一步提升客户的信息化程度和客户的品牌形象。

A.8 CASB 数据加密服务

CASB 全称是 Cloud Access Security Broker，云访问安全代理，可以提供数据加密服务。通过 CASB 数据加密云服务管控平台，为已经存在的各种缺乏足够内生安全机制的云服务应用系统提供补充的、增强的数据加密保护措施。

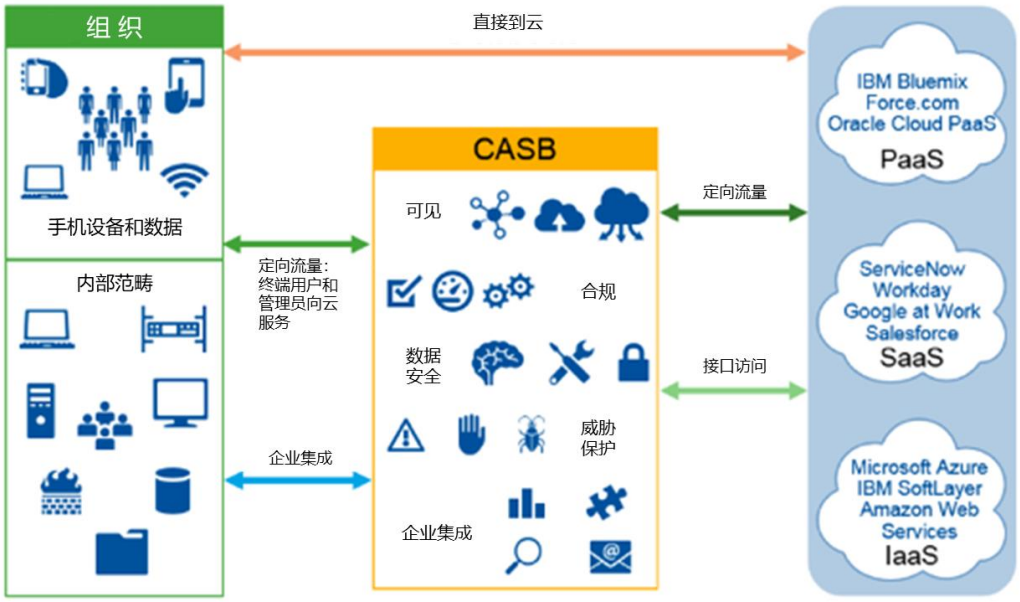

图 A-13 CASB 模式防护云端威胁

CASB 分为代理模式和 API 模式，部署模式和技术本质分别如下：

方案	CASB 代理模式（串网关）	CASB API 模式之插件版（切面插件）
技术本质	网关侧分析和代理应用请求 以适配方式增强数据安全与业务安全	应用内识别用户数据操作 以配置方式增强数据安全
优缺分析	实施成本中，应用免改造但需适配 云访问安全代理（SaaS）、关键应用安全代理（应用云迁移、私有应用）	实施成本低，仅需配置安全策略 关键应用安全代理（应用云迁移、私有应用）

大量的云服务应用系统在其规划和建设阶段都是首先着眼于业务，而对于安全，尤其是数据安全，缺乏基于应用自身考虑的、内建的安全手段，仍沿袭传统

思想将安全依赖于外部手段，如网络安全和主机安全。但是随着系统安全问题的复杂化，外部安全手段已不足以为云应用系统提供足够的安全保障，使得云应用系统暴露在极大的风险中。此时对云应用系统进行改造以加强数据安全保护机制通常是不可接受的，代价高周期长风险大。CASB 数据加密服务为风险中的云应用系统提供了很好的后补的数据安全防护。

在 CASB 代理模式（Proxy）下，采用如下图：

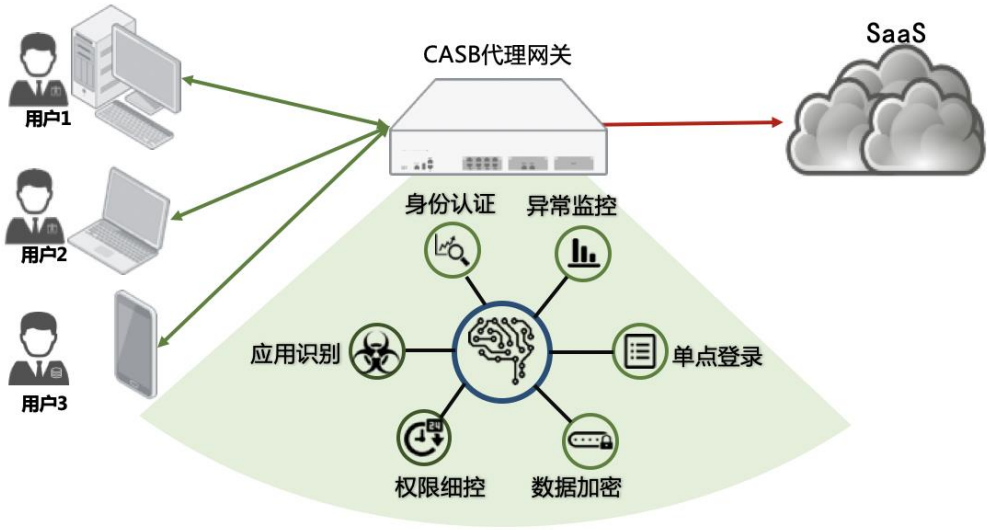

图 A-14 CASB 代理模式

在 Proxy 模式中，CASB 串联入用户端与云服务端，对用户端上传到云服务端的上行流量做预处理，对云服务端下载到用户端的下行流量做后处理。CASB 在用户端与服务端之间既扮演正向代理又扮演反向代理来完成工作。CASB 服务商有公有部署，也有私有部署，还有一少部分二者都支持。

CASB 作为部署在客户和云服务商之间的安全控制点。通过嵌入身份认证、设备识别、单点登录、异常监控、加密等企业安全策略，来监控和防护企业用户对云上资源的连接访问。Proxy 模式下，CASB 要处理企业上传到云应用的全部流量，重要数据采用加密等安全策略处理后在上传到云服务商。API 模式中，企业数据直接传给云服务商，CASB 通过利用云应用的 API，对用户进行访问控制以及执行企业的安全策略。

核心功能：

- 可见性：目前 SaaS 和很多其他的公有云服务缺乏企业级的活动监控，CASB 可以提供企业内使用云服务的数据、使用人员、客户端设备以及使用情况，提供集中化视图，对异常行为进行检测、阻断和记录，可以识别哪些云应用被哪些员工使用了，从而避免了 Shadow IT 的存在。

- 合规性：企业 IT 系统往云上迁移后，仍然能满足外部法律以及内部标准等合规性要求，并对云服务商进行信任评级、提供内容监控、审计日志等功能。CASB 的特性可以很好地弥补多云应用以及基础设施的合规缺口，不论访问云服务的用户与设备是在网络边界的内部或者外部。

- 数据安全：企业想要掌控自己的数据，不管这些数据存储和处理是在终端用户的设备上还是在云服务商服务器，CASB 可以实现结合人员、设备、内容和应用多个维度，提供 DLP、Encryption、Tokenization 等多种类型的数据安全保护，防止云端数据泄露。CASB 可以提供基于上下文，感知业务的安全策略下发。

- 威胁防护：CASB 可以提供云服务商基础设施威胁防护之外的一些关乎企业用户自身的特定威胁，诸如账户劫持问题。CASB 可以帮助企业对进出云上的数据、用户访问云服务资源行为进行监控，及时发现威胁并且做出防御。

在 CASB API 模式的插件实现版下：

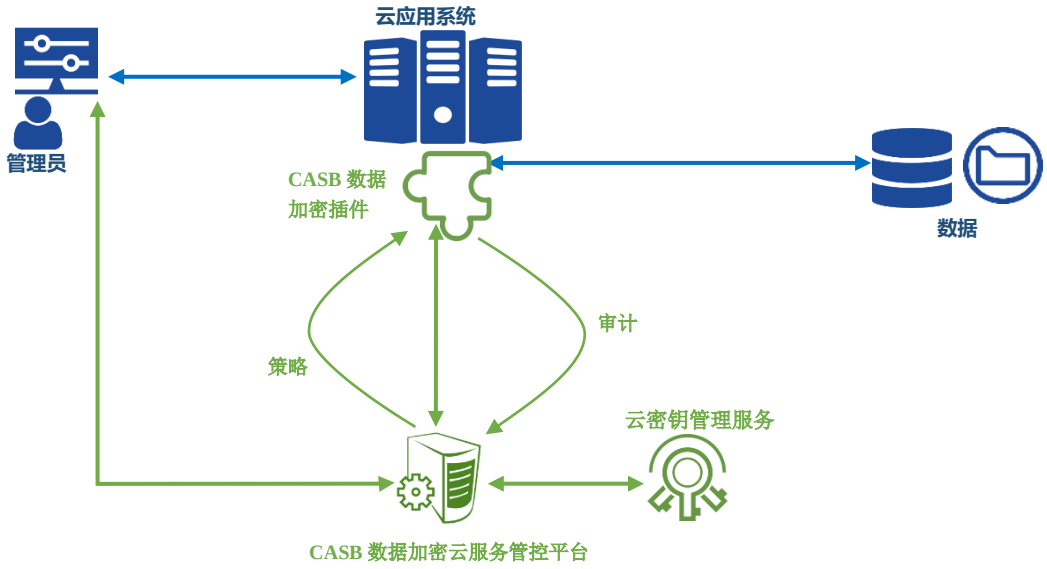

图 A-15 CASB 数据加密服务

如上图所示，CASB 数据加密服务无需对原有云服务系统进行改造。其核心工作机制是：在原有系统中部署 CASB 数据加密插件，并通过 CASB 数据加密云服务管控平台集中管理安全策略，CASB 在这些安全策略的指导下进行数据加密、访问控制及审计操作。

CASB 数据加密插件是数据加解密、脱敏、审计以及访问控制的集中作用点。它运行在目标应用系统中，但是对目标系统的业务不会产生任何影响，对系统透明，也无需对系统进行改造。CASB 数据加密插件支持多种数据库品牌、版本，而且客户无需因其数据库的选型而做额外的部署和调整工作。

CASB 数据加密服务管控平台是一个集中管控平台，通过它进行中心化的管理，可以为多个应用系统、应用系统的多个子系统或模块进行数据安全策略的管理，包括制定和调整数据加解密、脱敏及访问控制策略，以及将策略分发到各个系统中。

这些策略可以对数据安全防护进行极细粒度的定义：防护的数据对象可以到行级、列级、单元级别，主体到具体的用户，并能结合上下文环境、业务动作进行控制，数据保护动作可以是加密、脱敏；数据安全策略从 CASB 管控平台下发到云服务系统中的 CASB 数据加密插件，CASB 插件依据策略中的数据防护定

义，结合云应用系统中发生的具体数据访问，进行相应的数据防护动作。

CASB 数据加密服务与云密钥管理服务配合进行工作。对数据进行加解密所需要的密钥，通过云密钥管理服务进行管理，确保密钥的安全性，以及充分利用云密钥管理服务的各种特性和管理能力。

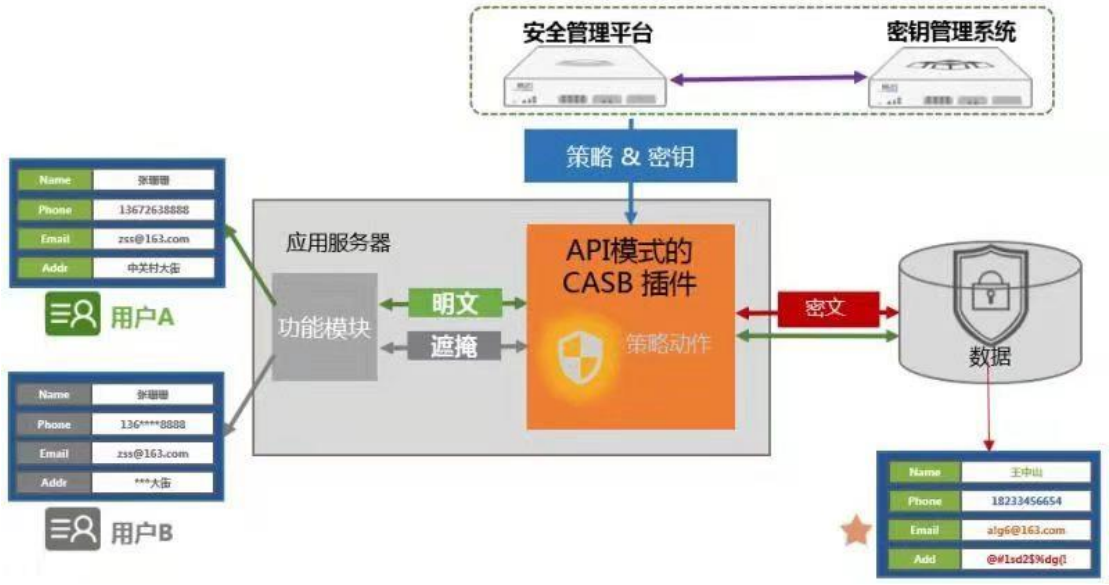

图 A-16 CASB 插件结合策略进行主体到人、客体到字段的处理

所有发生的数据访问事件，以及进行的相应的数据防护处理，都会记录下来，发送给审计系统进行审计。通过审计，能发现数据访问特性、变化趋势，可以帮助分析系统以进行优化，当发生异常访问情况时，可以进行告警；在有必要的情况下，可以进行访问阻断。

CASB 数据加密服务的功能及特性：

- 免改造目标应用系统为其提供数据安全保护能力，对目标系统透明；
- 易于实施和部署，支持多种软硬件平台，支持大多数数据库品牌；
- 集中化管理，分布式加密。通过单一的 CASB 数据加密服务管控平台，将策略分发至各个系统，在各个系统中进行数据安全防护；
- 安全防护机制多样，包括：数据加密、脱敏、访问控制、审计。
- 数据加密及访问控制能做到极细粒度，主体到人，客体到字段级，并能

结合上下文环境进行控制；

- 支持多种加密算法；
- 密钥可结合云密钥管理服务进行管理。

附录 B

云密码服务质量评价指标

表 B-1 云密码服务质量评价指标

一级指标	二级指标	说明
服务准确性	服务完备性	按照 SLA 提供符合要求的所有密码功能服务
	算法正确性	密码算法是否符合相应算法标准
	协议正确性	密码协议是否符合相应技术标准
	密码处理性能	承诺能达到的密码运算性能指标
	数据可迁移性	保证用户启用或启用该服务时，数据和密钥能有效地迁入和迁出
服务有效性	业务弹性	承诺用户动态扩展或缩减业务开展所需资源的时间及最大扩展容量
	业务可用性	按月统计，在合同期内用户业务可用时间的概率
	平台管理可用性	对多设备、多密钥、多应用的统一管理能力
	异地容灾服务可用性	建立异地容灾系统，容灾系统能够实现正常的系统备份和切换功能，灾难恢复能力达到 GB/T 20988—2007《信息安全技术 信息系统灾难恢复规范》3 级以上
	业务容灾可用性	建立业务容灾系统，容灾系统能够实现业务层面的系统备份和切换功能
服务响应性	服务的及时响应性	能按照 SLA 在要求的时间内及时响应用户的服务请求
	服务互动沟通机制	对服务提供机构的互动沟通机制的建立与实施情况

		进行检查
	服务投诉解决率	统计并比较得到有效处理的投诉数量和收到的投诉数量
	资源配置及时性	能够在规定时间内及时响应用户对业务资源的要求
	运维事件响应率及解决率	对于运维事件按照不同的响应级别要求在规定的时间内予以响应并加以解决
	业务开通响应及时性	对于业务开通的请求在规定的时间内予以响应
	定制化服务响应及时性	用户在申请定制化服务后可在规定的时间内获得服务响应
服务安全性	密钥安全性	提供安全的密钥保护机制
	数据保密性	对用户的重要数据进行加密保护
	密钥和数据隔离性	承诺对不同用户的数据和密钥进行有效隔离，保证同一资源池的用户数据和密钥互不可见
	网络隔离和访问控制	承诺在网络中对不同用户设置隔离区域并对访问权限进行限制
	用户接入认证	用户可通过多种方式进行认证，至少要支持基于数字证书的身份认证
	安全审计	提供安全审计相关功能并形成相应的审计记录和报表
	系统告警有效性	为用户提供全面有效的告警信息
服务可靠性	服务可用性	应按照 SLA 要求向用户提供持续的可用的服务的能力，可用性应达到 99.9%以上

	服务的恢复能力	承诺用户在服务不可用时在 SLA 规定时间内恢复服务的能力
	数据存储持久性	承诺在合同期内数据和密钥保存不丢的概率
	数据备份可靠性	承诺在合同期内对密钥及数据进行备份，保证在数据丢失时能够有效找回
	应急情况响应措施	针对出现的应急情况有必备的应对响应措施

附录 C

专业术语

ABE 基于属性的加密（Attribute-based Encryption），可用于访问授权服务。

AD 活动目录（Active Directory），是一种目录服务。

AES 美国加密标准（Advanced Encryption Standard），一种对称密码算法，又称 Rijndael 加密算法。

AWS 亚马逊公司旗下云计算服务平台（Amazon Web Services）。

BYOK/ BYOE 自带密钥加密（Bring our own keys/ Bring your own encryption），一种适用于云加密的密钥管理模式。

CA 证书颁发机构（Certificate Authority），对数字证书进行全生命周期管理的实体，也称为电子认证服务机构。有时也指证书认证系统。

CaaS 密码即服务（Cryptography as a Service），云密码服务初期的概念。

CAPI 加密应用程序接口（Cryptography API），微软提供的加密接口。

CASB 云访问安全代理（Cloud Access Security Broker）。

CBaaS 云密码业务服务（Cryptography Business as a Service）。

CFaaS 云密码功能服务（Cryptography Function as a Service）。

CRaaS 云密码资源服务（Cryptography Resource as a Service）。

CLI 命令行界面（command-line interface）。

CMP 证书管理协议（Certificate Management Protocol）。

CPS 信息物理系统（Cyber Physical System）。

CPU 中央处理器（Central Processing Unit）。

CRL 证书撤销列表（Certificate Revocation List），由证书认证机构（CA）签

发并发布的被撤销证书的列表。

CRM 客户关系管理（Customer Relationship Management）。

CSA 云安全联盟（Cloud Security Alliance），是一个中立的非盈利世界性行业组织，致力于国际云计算安全的全面发展。

DB 数据库（Database）。

DLP 数据泄密（泄露）防护（Data Leakage Prevention）。

DSA 数字签名算法（Digital Signature Algorithm），一种公钥算法。

DSS 数字签名服务规范（Digital Signature Services）。

EaaS 加密即服务（Encryption as a Service）。

EBS 弹性块存储（Elastic Block Store），为虚拟机实例提供的数据块级别的存储卷。

ECC 椭圆曲线密码算法（Elliptic Curve Cryptography），一种公钥密码算法。

ERP 企业资源计划（Enterprise Resource Planning），是一套企业运营管理软件。

FIPS 美国联邦信息处理标准（Federal Information Processing Standards）。

FPE 保留格式加密（Format Preserving Encryption），加密后数据格式和长度不变，适用于敏感信息保护。

HSM 硬件密码模块（Hardware Security Module），如密码机、密码卡等。

HTTP 超文本传输协议（HyperText Transfer Protocol)。

HTTPS 超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer 或 Hypertext Transfer Protocol Secure），即 HTTP 下加入 SSL 层。

IaaS 基础设施即服务（Infrastructure as a Service），云计算的服务模式之一。

IAM 身份识别与访问管理（Identity and Access Management）。

IBC/IBE 基于标识的密码体系（Identity-Based Cryptograph/Encryption）。

IDC 互联网数据中心（Internet Data Center）。

IoT 物联网（Internet of Things）。

IPSec IPSec 协议（Internet Protocol Security），一种网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

ISO 国际标准化组织（International Organization for Standardization）

JCA/JCE Java 加密框架/Java 加密扩展（Java Cryptography Architecture/Java Cryptography Extension），Java 环境中使用密码的框架和实现。

JSON JS 对象表示法（JavaScript Object Notation），是一种轻量级的数据交换格式。

Kerberos 一种计算机网络授权协议。

KMaaS 密钥管理即服务（Key Management as a Service），一种密码服务概念。

KMIP 密钥管理互联协议（Key Management Interoperability Protocol）。

KMC 密钥管理中心（Key Management Center）。

KMS 密钥管理系统（Key Management System）。

LDAP 轻量目录访问协议（Lightweight Directory Access Protocol）。

MFA 多因素身份验证（Multifactor Authentication）。

NFV 网络功能虚拟化（Network Function Virtualization）。

NGFW 下一代防火墙（Next Generation Firewall）。

OASIS 结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards），一个国际开放标准组织。

OAuth 开放认证协议（Open Authorization），一种开放、简单、安全的资源

授权协议。

OCSP 在线证书状态协议（Online Certificate Status Protocol）。

PaaS 平台即服务（Platform as a Service），云计算的服务模式之一。

PDF 便携式文档格式（Portable Document Format），一种电子文件格式。

PKCS#1 公钥密码标准（Public-Key Cryptography Standards (PKCS) #1），RSA 密码规范。

PKI 公钥基础设施（Public Key Infrastructure）。

RA 证书注册机构（Register Authority），受理数字证书的申请、更新、恢复和注销等业务的实体。有时也指 RA 系统，是 CA 系统的一部分。

RSA 一种非对称密码算法。

S3 简单存储服务（Simple Storage Service），AWS 提供的一种网络存储服务。

SaaS 软件即服务（Software as a Service），云计算的服务模式之一。

SAML 安全断言标记语言（Security Assertion Markup Language），是一个基于 XML 的开源标准数据格式，用于在身份提供者和服务提供者之间交换身份验证和授权数据。

SCEP 简单证书注册协议（Simple Certificate Enrollment Protocol）。

SDK 软件开发工具包（Software Development Kit）。

SDN 软件定义网络（Software Defined Network）。

SDP 软件定义边界（Software Defined Perimeter），CSA 提出的一种安全模型。

SHA 安全散列算法（Secure Hash Algorithm），包含一系列密码杂凑算法。

SLA 服务等级协议（Service-Level Agreement）。

SMx 商用密码算法系列，包括 SM1、SM2、SM3、SM4、SM6、SM7、SM9

等密码算法。

SR-IOV 单根 I/O 虚拟化（Single-root I/O Virtualization），一种硬件虚拟化技术。

SSL/TLS 安全套接层/传输层安全（Secure Sockets Layer/Transport Layer Security），为网络通信提供安全及数据完整性的一种安全协议。

TDE 透明数据加密（Transparent Data Encryption）。

TEE 可信执行环境（Trusted Execution Environment）。

TSA 时间戳机构（Time Stamp Authority），用来产生和管理时间戳的可信服务机构。

UEBA 用户和实体行为分析（User and Entity Behavior Analytics）。

vHSM/VSM 虚拟化（硬件）密码模块（virtual Hardware Security Module/Virtual Security Module）。

VLAN 虚拟局域网（Virtual Local Area Network）。

VM 虚拟机（Virtual Machine）。

VPC 虚拟私有云（Virtual Private Cloud）。

VPN 虚拟专用网（Virtual Private Network），如 SSL VPN、IPSec VPN 等。

VXLAN 虚拟扩展局域网（Virtual Extensible LAN），一种网络虚似化技术，是对 VLAN 的一种扩展。

XML 可扩展标记语言（eXtensible Markup Language）。

同态加密，一种加密函数，对明文进行环上的加法和乘法运算再加密，与加密后对密文进行相应的运算，结果是等价的。对加密信息仍能进行分析，而不会影响其保密性。

参考资料

[1] 《中华人民共和国密码法（草案征求意见稿）》

[2] 《中华人民共和国网络安全法》

[3] 《商用密码管理条例》(1999)

[4] 《商用密码知识与政策干部读本》（2017）

[5] 《云（服务器）密码机技术规范》（征求意见稿）（2018）

[6] 《云计算关键领域安全指南 v4.0》CSA

[7] 《电子认证 2.0 白皮书》信安标委(2018)

[8] 《密码行业标准体系研究报告》密标委(2017)

[9] 《基于云计算的电子政务电子认证服务应用指南》（征求意见稿）(2018)

[10] 《云计算密码保障体系研究报告》(2018)

[11] 《基于云计算的电子签名服务密码标准体系研究》(2018)

[12] 《云计算身份鉴别服务密码标准体系研究》(2018)

[13] 《云密钥管理技术研究》(2018)

[14] 《数据流通关键技术白皮书(1.0 版)》中国信通院(2018)

[15] GB/T 37092—2018, 信息安全技术 密码模块安全要求[S]. 2018.

[16] GB/T 36322—2018, 信息安全技术 密码设备应用接口规范[S]. 2018.

[17] GB/T 31168—2014, 信息安全技术 云计算服务安全能力要求[S]. 2014.

[18] GB/T 20988—2007, 信息安全技术 信息系统灾难恢复规范[S]. 2007.

[19] GB/T 36733—2018, 服务质量评价通则[S]. 2018.

[20] GB/T 34077.1—2017, 基于云计算的电子政务公共平台管理规范 第 1 部分：服

务质量评估[S]. 2017.

[21] GM/Z 4001—2013，密码术语[S]. 2013.

[22] GM/T 0062—2018，密码产品随机数检测要求[S]. 2018.

[23] 宋飞，董贵山，邓子健，张岳公. 发挥密码基础支撑作用，整体保障云计算安全[J]. 信息安全与通信保密. 2018(5).

[24] 史欣慧，基于 KMIP 协议的密钥管理系统的设计与实现[D]，山东大学，2018.

[25] 杨小伟，基于属性的加密方案研究[D]，电子科技大学，2017.

[26] 卞超轶，朱少敏，周涛. 一种基于保形加密的大数据脱敏系统实现及评估[J]. 电信科学. 2017(03).

[27] 欧海文，付永亮，于芋，胡馨月. 一种改进的 OAuth 授权机制有效性分析[J]. 计算机应用与软件. 2017(12).

[28] Black J, Rogway P. Ciphers with arbitrary finite domains[M]. Berlin Heidelberg:Springer, 2002.

[29] Hossein Rahmani *, Elankovan Sundararajan, Zulkarnain Md. Ali, Abdullah Mohd Zin. Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud

[30] Vassilev A, Staples R. Entropy-as-a-Service: Unlocking the Full Potential of Cryptography[J]. Computer, 2016, 49(9):98.

[31] Peter Robinson. CRYPTOGRAPHY AS A SERVICE[OL]. The Security Division of EMC.

[32] Archer D W , Bogdanov D , Lindell Y , et al. From Keys to Databases—Real-World Applications of Secure Multi-Party Computation[J]. The Computer Journal, 2018.

[33] Zhang, Hongwen (6 April 2015). Bring your own encryption: New term in the cloud age[J]. Networks Asia. Retrieved 10 April 2015.

[34] 沈志荣， 薛巍， 舒继武，可搜索加密机制研究与进展，软件学

报,25(4):880-895， 2014

[35] 葛春鹏, 代理重加密若干问题研究, 博士论文，南京航空航天大学，2016

[36] 罗富财, 云存储中可证明数据持有方案及相关问题研究, 硕士论文，福建师范大学， 2016