GM/Y 5005-2024

密码功能服务安全要求及评估标准研究

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

2024 年 12 月

摘要

在信息技术迅猛发展的时代大背景下，密码技术由产品向服务的升级转型成为了密码产业的一大趋势。密码功能以服务方式提供，能够提升密码资源供给效率和专业化能力，促进密码在各个领域的业务中更广泛的使用，为各种信息系统提供强有力的安全保障能力。密码功能以服务方式提供，意味着密码能力供给者和使用者分离，因此更加需要保证密码功能服务的安全性和规范性。

本项目研究了国内外密码服务的产业发展状况和标准化状况，对目前典型的密码功能服务如电子签名服务、密钥管理服务、身份认证服务进行了分析，归纳了密码功能服务的技术框架和服务模式，提出密码功能服务安全要求和安全评估相关的标准化建议。

关键词：密码功能服务，服务模式，安全评估

目次

前言

《密码功能服务安全要求及评估标准研究》是由密码行业标准化技术委员会根据国家密码管理局批准的《2017 年密码行业标准制/修订计划（商用密码领域）》下达的 2017 年密码行业标准研究编制工作任务。北京数字认证股份有限公司作为牵头单位，成立相应的编制工作组，组织完成该标准研究报告的编制工作。

本报告起草单位：北京数字认证股份有限公司、国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、上海市数字证书认证中心有限公司、数安时代科技股份有限公司、三未信安科技股份有限公司、北京江南天安科技有限公司、格尔软件股份有限公司。

本报告主要起草人：李向锋、夏鲁宁、傅大鹏、高志权、郑强、钱文飞、韩玮。

密码功能服务安全要求及评估标准研究

1. 概述

经济学中的服务通常有两种涵义。其一，是劳动意义上使用的服务概念，称为“服务劳动”，是指第三产业中的非物质生产劳动；其二，是产品意义上使用的服务概念，称为“服务产品”，即以非实物形态存在的劳动成果。

产品和服务都是过程的结果——输出，但产品是有形的，服务是无形的。产品是服务的载体，服务是产品的本质。产品所体现的是一种服务关系，它只有被当作一项服务的形式时，才有意义。ISO9001-2015 标准中已将原来的“产品”统一修订为“产品和服务”，在大多数情况下，产品和服务一起使用。经济学中老的产品与服务的二分法，已经升级为服务—产品统一体。

1.1. 研究背景和意义

在信息技术迅猛发展的时代大背景下，密码技术由产品向服务的升级转型成为了密码产业的一大趋势。密码功能以服务方式提供，能够提升密码资源供给效率和专业化能力，促进密码在各个领域的业务中更广泛的使用，为各种信息系统提供强有力的安全保障能力。

提供和使用商用密码服务，必须保证商用密码服务的安全性和规范性。在 2020 年开始实施的《中华人民共和国密码法》（以下简称“《密码法》”）中，明确规定“商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格”。

目前，我国商用密码产品的认证体系基本成熟，对于电子认证服务也已经存在成熟的管理体制，但对于商用密码服务整体上的认证体系还有待完善。为贯彻落实《密码法》的要求对商用密码服务进行认证，有必要对商用密码服务认证的技术框架、管理机制以及所需标准体系如安全要求、评估准则等进行研究，以此作为设计商用密码服务认证体系的基础。通过对商用密码服务进行认证，能够对商用密码服务质量和安全性进行技术把控，从而建立规范的商用密码服务市场准入机制，促进密码产业的有序发展，为信息产业的发展提供更好的密码支撑能力。

1.2. 密码服务遇到的挑战

1） 新技术与应用模式提出对传统密码的挑战

云计算中心化的部署模式完全改变了以往那种服务器直连密码设备的部署模式，密码设备不能再处于绝对封闭受控的环境中，只能通过开放网络与应用系统连接，必须直接面对互联网的各种安全威胁。

云计算除了部署模式的改变外，支撑技术也发生了改变，密码服务需要适应云服务以虚拟化为基础、以可信计算为信任保障、以微服务为发展方向的云计算平台演进趋势，并解决云服务模式下的密钥隔离、安全接入、访问控制等问题。

以大数据、区块链等新应用对密码技术的创新需求，使得密码技术面临很多新的挑战，如何解决密文检索等问题，迫切需要同态加密、多方计算、基于属性的加密等技术的成熟；如何解决云计算中对密码服务的易用性需求，需要更加易用的身份认证机制，如开放授权、零知识证明等新的密码技术来支撑密码服务。

2) 密码服务尚处初级阶段

虽然各类云计算服务提供商都尝试提供密码服务，但由于这类服务对安全性要求比较高，技术复杂度较大，导致密码服务水平参差不齐，用户是否选择密码服务很大程度上依赖云服务商的促销力度；一方面用户安全意识不足，认为云服务的安全性应由云计算服务提供商来保障，没有认识到密码技术的重要性；另一方面，对密码技术比较了解的用户更愿意接受传统的密码使用方式，还不能完全接受这种密钥被托管的交付方式，这些方面充分显示出密码服务尚处于发展的初级阶段，有很大的发展前景。

1.3.研究目标

通过调研当前国内外现有的与密码服务相关的技术、产业、标准发展现状与趋势，诸如国外电子认证服务、WebTrust 审计标准、欧盟 eIDAS 技术与标准、加密云服务等方面的技术与标准，按照我国《网络安全法》、《密码法》等有关规定，结合我国在商用密码服务领域的实际发展情况及应用需求，分析密码功能服务安全的标准化需求，形成密码功能服务安全要求及评估标准研究报告，明确密码功能服务的内涵、范围、安全要求、安全评估准则等，并提出密码功能服务安全要求与评估标准化建议。

2. 密码服务的概念

由于信息世界的复杂多变，在信息技术领域，“服务”这一概念本身就具有涵盖范围宽广、难以简单概况的特点，即便“服务”这一名词冠以“密码”这一领域限定词时，同样还是难以给它一个简单明确的定义以及清晰的范围限定。

从本质上看，“密码服务”是供与求双方之间一种密码相关的交付模式。这种模式下，所交付的内容可以是密码基础设施，那密码系统的建设和集成自然是一种密码服务；所交付的可以是密码方面的知识，那密码相关的咨询自然也是一种密码服务；所交付的还可以是密码相关的运营管理、运行维护等保障活动，那密码相关的运营自然也是一种密码服务。

同理，如果我们将一个系统内各个密码子系统、密码模块为其它部分之间提供密码支撑也视为一种“交付”，也可以称呼这些密码支撑活动为“密码服务”。例如 GM/T0019《通用密码服务接口 规范》就描述了密码系统、密码产品向典型密码应用支撑和上层应用提供加解密、签名验签等通用密码功能。

随着信息技术的发展，云计算、大数据、移动终端等新技术层出不穷，推动者业务模式的不断演变和创新，越来越多的场景需要密码功能以“网络服务”的方式来提供。在这种场景下，密码功能的使用者通常并不方便或没有足够的能力独立建设自己的密码基础设施、进行密码系统的运营管理和运行维护，因而迫切需要独立与业务的第三方实体完成这些基础性工作并通过网络以不同的形式提供给业务应用，业务应用仅需要按照约定使用这些密码功能。典型的场景如云服务商为云上业务系统提供虚拟的密码资源，接入到业务的虚拟私有网络中使用；如第三方提供电子签名服务、电子合同服务，支持

集成到用户云或非云的业务系统。目前，这种“以服务方式提供密码功能”的活动渐渐成为密码服务的重要内容。

《密码法》中明确提出“商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格”。 这里“商用密码服务”，在《密码法释义》（以下简称“《释义》”）中，指向了 “基于密码专业技术、技能和设施”，为其它实体提供集成、运营、监理等商用密码支持和保障的活动”。

从对密码服务进行认证的角度来看，《释义》中所指出的密码相关的咨询、运营、监理等服务，通常都是对提供服务的主体单位进行认证，依托于现有的信息安全服务资质、计算机信息系统集成资质、信息系统安全运维服务资质认证等体系，围绕产业单位整体是否具备提供安全集成、安全运维等服务能力，通过对提供密码系统集成、运维服务的机构进行认证来保证其密码相关服务的服务质量、服务水平。

而系统内的密码功能支撑，如同一密码设备各层次之间、同一密码系统中设备对外提供的功能、同一组织机构内密码系统提供的功能，通常是设备、密码系统、信息系统内部问题，通常采用产品检测认证方式来确认安全性。

而那些“能够独立承担责任”的组织机构对外“以第三方的形式”提供的“基于网络服务的密码功能”，这也正是作为本文主要研究对象的“密码功能服务”。由于涉及实体间的责任问题，则更加迫切需要通过外部的认证机制保障服务安全合规，而这类服务的认证也正是上述两种认证机制所无法包含的。

“能够独立承担责任”的“第三方”形式，使密码功能的提供者与使用者相分离，服务提供者需要建设基础设施、提供服务，因而需要对密码基础设施的建设、服务的设计、密码功能的正确性、密钥的安全性等内容负责，而服务使用者需要选择服务水平、服务能力合适的服务提供者，并在自己的业务系统进行集成和使用。这也意味着密码功能的使用者不再物理上掌握密码基础设施、密码设备、密码系统以及各种密钥，而密码功能提供者需要掌握并不属于自己的基础设施、设备、系统以及各种密钥。因而，为保证密码应用安全合规，针对这一类密码服务，需要设计与传统模式不同的技术框架和标准体系。在本报告第 4 章介绍了适用于密码功能服务的技术框架和服务模式，在第 6 章给出了密码功能服务安全要求和评估标准的建议。

3. 密码相关服务现状

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；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，包括电子签名、安全多方计算、零知识证明等。

随着各领域对密码技术服务需求的涌现，各国对密码服务保障安全重要性的认识也在不断加深，包括美国、英国、欧盟、日本、韩国和我国在内很多国家和组织开始以服务的方式提供密码技术支撑，保护网络信息安全，特别是在电子签名、电子合同等领域进行了密码服务的探索与实践。

近年来，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。国内外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，为密码服务的开展提供了良好的基础设施支撑。

3.1. 国外密码相关服务的现状

在国外，典型的密码服务也大多和云计算有关。其中，典型的是 Amazon 借助其云密码机（CloudHSM）产品，为其云服务提供虚拟密码机。AWS CloudHSM 支持在租户自己的 Amazon Virtual Private Cloud (VPC) 中运行，使租户能够轻松地将 HSM 与运行在 Amazon EC2 实例上的应用程序配合使用。与 Amazon 类似，IBM 通过其 Cloud Hyper Protect 加密服务，使用其基于 FIPS 140-2 4 级认证的硬件提供虚拟环境的密码能力支持。在电子签名和云计算相结合的领域，Adobe 发起组建了基于 PDF 版式文档进行电子签名的 CSC（Cloud Signature Consortium）组织，基于欧洲“合规电子签名”的相关标准和法规，建立了文档电子签名的技术标准和生态体系。

3.1.1. 密钥管理服务 KMaaS

通常，密码功能离不开密钥，因此，密钥管理是密码系统的重中之重。近年来，随着业务的发展，逐渐出现了 KMaaS 这种新的方式，将密钥管理以服务的方式来提供。这方面典型的代表有国外的 Amazon、Sepior，国内的阿里云、三未信安等也提供密钥管理的服务。对这些厂商开展服务的情况我们逐一进行分析。

3.1.1.1. 服务框架

(一) Amazon 的密码服务框架

AWS 为用户提供了一系列安全可靠、可扩展的云计算平台，可进行数据备份与存储、网站托管及游戏开发等，AWS KMS 通过采用硬件安全模块（HSM）的方式实现密钥的生成、安全存储和管理，为云服务和用户提供密钥管理支持。

AWS KMS 可以用来创建和管理用户的主密钥，使用对称加密算法来加密和解密数字数据。AWS KMS 已经和大多数的 AWS 服务集成，即用户可使用自己的密钥来加密 AWS 其它服务中的数据。

AWS 的云密钥管理服务可以通过其密钥管理控制台的 Web 界面来访问，云用户可以按需使用该密钥管理系统创建并管理自己的密钥。每个 HSM 只针对某个既定的用户可用，密钥的所有加密、解密等操作均在 HSM 中完成，虽然 HSM 的使用加强了密钥存储的安全性，但也存在需要创建和维护多个 HSM 组件的问题。

Amazon KMS 架构如图 3-1 所示：

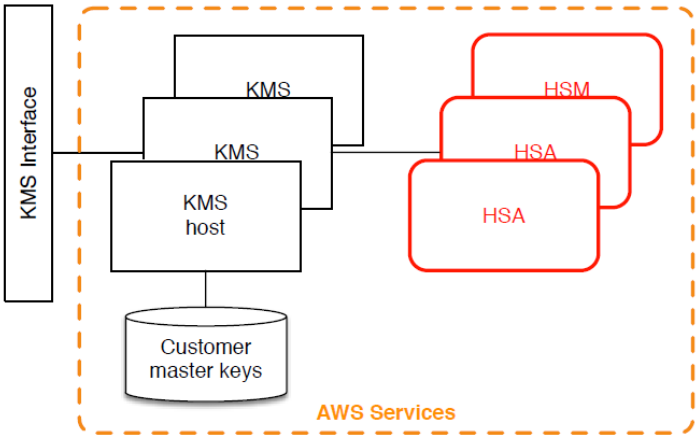

图 3-1 Amazon KMS 架构图

其主要特点是：

（1） 使用满足 FIPS 140-2 的硬件密码模块保护密钥

（2） 与 AWS 其它产品结合，立足于满足 AWS 租户的密钥安全要求

（3） 满足监管审计要求

用户密钥结构从顶层逻辑密钥开始，称为用户主密钥（Customer Master Key，CMK），用户主密钥与能代表用户身份的信息关联，在 AWS 服务空间中被唯一定义，包括一个唯一生成的密钥标识或用户主密钥 ID， AWS KMS 使用 CMK 来生成、加密和解密数据密钥。用户可以创建多个主密钥，即主密钥的不同版本，只有最新版的主密钥才能执行加密操作。

AWS 中的 CMK 有以下 3 种类型：

① 用户托管 CMK

客户托管 CMK 是指用户自己创建的主密钥，用户对这类 CMK 有完全的权限，如启用、禁用、删除、轮换等。在用户 AWS 账户的每个区域（Region）中，最多可以创建 1000 个用户托管 CMK，但是用户可以通过向 AWS 申请提高这个限制。

② AWS 托管 CMK

AWS 托管 CMK 是由与 AWS KMS 集成的服务创建。用户可以查看 AWS 账户中的 AWS 托管 CMK，如果用户使用了 AWS 托管 CMK，也可以在 AWS CloudTrail 中对使用情况进行审核。用户无法管理 AWS 托管 CMK，如进行删除、密钥轮换等操作。

③ AWS 拥有的 CMK

AWS 拥有的 CMK 是 AWS 拥有和管理的在多个 AWS 账户中使用的 CMK 集合的一部分，用户无法查看、管理以及使用 AWS 拥有的 CMK，所以用户也无法在 AWS CloudTrail 中审核使用情况。

用户数据密钥可以通过 SSL 以明文或密文的方式传送给用户，如果是密文方式，则用 CMK 加密。

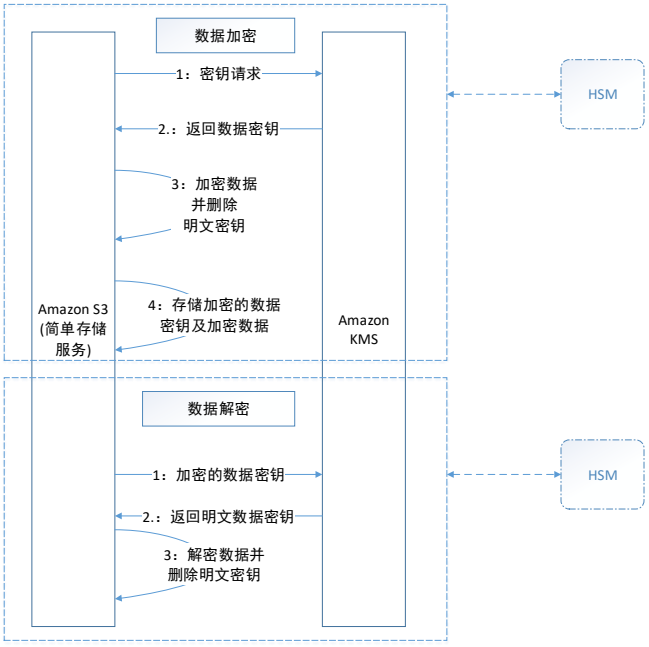

图 3-2 Amazon S3 服务的密钥管理

AWS 简单存储服务（S3）通过其云密钥管理方案实现数据加/解密的应用案例，S3 与 KMS 的所有交互均通过 SSL 建立安全会话，并采用电子认证、数字签名等方式来验证通信双方的身份。

(二)　Sepior 提供基于云的密钥管理系统（KMaaS）

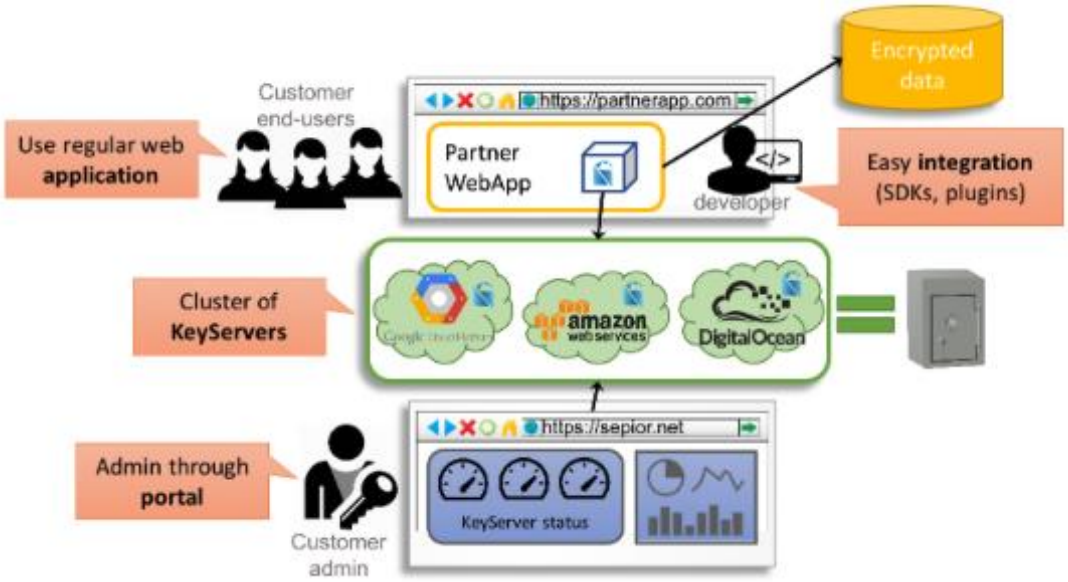

图 3-3 Sepior 的 KMaaS 服务框架

其 KMaaS 服务包括一系列组件：

- 集群的密钥服务器

支持云、容器和虚拟机等多种部署形式，支持部署在谷歌云、亚马逊云、微软 Azure、DigitalOcean 和 Rackspace 中。

Sepior 为用户提供的密钥服务器，采用集群方式部署于多个独立的云平台上，每个密钥服务器均提供密钥管理服务，但各云平台上的每个密钥服务器仅持有用户每个密钥的一份，而单独的一份是无意义的，必须与其他服务器上的几份合成后才能使用。

- 管理门户网站

用户可通过 Sepior 的门户网站，进行所需要的管理操作，包括：

  - ✧ 应用管理
  - ✧ 用户管理
  - ✧ 备份
  - ✧ IDP（Identity Provider）配置
  - ✧ 日志审计

- 服务的使用应用

使用密钥来加密数据的应用，支持通过 SDK 或插件来使用其密钥服务。应用程序能够进行静态数据加密，或进行客户端的加密。

目前，Sepior KMaaS 支持集成 AWS 的 S3 存储服务，支持 S3 的 client-side 加密方案。用户在正确配置插件后，即可方便地调用插件接口完成数据的加密，然后上传到 S3 用户密钥库中。

3.1.1.2. 管理机制

Amazon 提供了完善的管理机制，如提供了 AWS CloudTrail 服务来满足用户的审核、监督和合规性要求，提供了 AWS CloudTrail 来监控和查询密钥使用记录。

3.1.2.数据加密服务

AWS CloudHSM 是基于云的硬件安全模块（HSM），用户能够在 AWS 云上轻松生成和使用自己的加密密钥。并且可以灵活选择使用行业标准的 API 与应用程序集成，这些 API 包括 KCS#11、Java 加密扩展（JCE）和 Microsoft CryptoNG（CNG）库等。此外，CloudHSM 符合标准，用户可以将所有密钥导出到大多数其他商用 HSM。它是一项完全托管的服务，可为用户自动执行耗时的管理任务，例如硬件预置、软件修补、高可用性和备份。借助 CloudHSM 用户还能够通过按需添加和删除 HSM 容量进行快速扩展和收缩，无任何预付费用。

AWS Key Management Service 对用于保护数据的加密密钥提供集中化控制。用户可以创建、导入、轮换、禁用、删除、定义加密数据所用加密密钥的使用策略，并审计这些密钥的使用情况。AWS Key Management Service 可与许多其他 AWS 服务集成，从而让用户可以使用自己控制的加密密钥轻松加密这些服务中存储的数据。AWS KMS 能使开发人员通过在 AWS 管理控制台中进行 1-Click 加密或使用 AWS 软件开发工具包轻松加密数据，从而将加密轻松添加到其应用程序代码中。

AWS Identity and Access Management（IAM）使用户能够安全地管理对 AWS 服务和资源的访问。用户可以使用 IAM 创建和管理 AWS 用户和组，并使用各种权限来允许或拒绝他们对 AWS 资源的访问。

3.1.2.1. 服务框架

CloudHSM 设计安全且高度可用，AWS CloudHSM 在用户自己的 Amazon Virtual Private Cloud（VPC）中运行，使用户能够轻松地将 HSM 与运行在 Amazon EC2 实例上的应用程序配合使用。

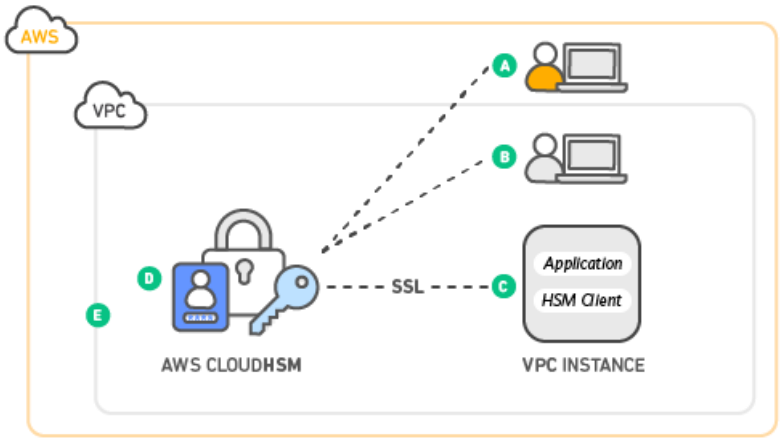

图 3-4 AWS CloudHSM 应用

AWS S3 的数据加密分为服务器端加密和客户端加密两大类：

1)服务器端加密：请求 Amazon S3 在将对象保存到数据中心的磁盘上之前加密对象，并在下载对象时进行解密。服务器端加密不会修改现有的 S3 访问方式。

2)客户端加密：可以在客户端加密数据并将加密的数据上传到 Amazon S3。在这种情况下，用户需要管理加密过程、加密密钥和相关的工具。客户端加密则需要配合各种语言的 AWS 开发工具包来完成访问。

图 3-5 AWS S3 服务端加密文件的流程图

在 AWS S3 中使用 AWS KMS 来加密数据时，AWS S3 会自动完成数据密钥的申请、数据的加密等操作，整个过程对用户来说是透明的，用户无需进行任何的额外操作。

3.1.2.2. 管理机制

AWS CloudHSM 在设计之初就考虑到了责任分离和基于角色的访问控制。AWS 负责监控 HSM 的运行状况和网络可用性，但不参与 HSM 中存储的密钥材料的创建和管理工作。用户负责控制 HSM 以及加密密钥的生成和使用。

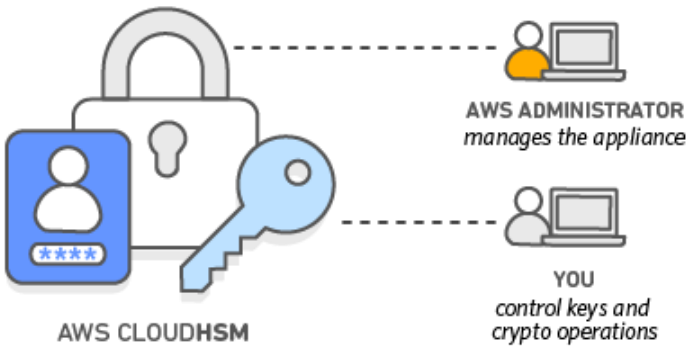

图 3-6 AWS CloudHSM 管理机制

AWS Key Management Service 为用户提供加密密钥的集中化控制。用户可以通过 AWS 管理控制台或者使用 AWS SDK 或 CLI，轻松创建、导入和轮换密钥，以及定义使用策略和审计使用情况。KMS 中的主密钥（无论是由用户导入的还是由 KMS 代表用户

创建的)都以加密格式存储在高持久性的存储中,以帮助确保在需要时可对其进行检索。用户可以选择让 KMS 每年自动轮换一次在 KMS 中创建的主密钥,而无需重新加密已使用主密钥加密过的数据。用户无需记录旧版主密钥，因为 KMS 会保持其可用，以解密以前加密的数据。用户可以创建新的主密钥，并对谁有权访问这些密钥以及它们可用于哪些服务随时加以控制。也可以从自己的密钥管理基础设施导入密钥并在 KMS 中使用。

3.1.3.数字证书服务

3.1.3.1. 服务框架

WebTrust 构建权威认证的网络信任遵循下述的框架和原则：

原则 1：CA 商业活动事项的公布

原则 1 是指：认证中心公布其密钥和证书的生命周期管理情况以及信息保密情况，并且根据公布的内容提供相应的服务。

CA 应必须公布其密钥和证书的生命周期管理情况和信息保密工作情况。涉及到 CA 商务活动情况的信息一般应该放在其网站上,以便所有的注册者和潜在的证书信赖者访问。证书政策（CP）、证书作业准则（CPS）或其他可被用户使用的信息材料中都应包含以上公布的内容。

原则 2：服务的完整性

原则 2 是指：权威认证维持有效控制，以便在以下方面提供合理的保障：

- 适当验证用户信息（ABC-CA的注册活动来完成）；
- CA所管理的密钥和证书的完整性得以确立，并在其生命周期内得到保护；

有效控制和实施密钥管理对于公共密钥基础结构的可信度非常重要。控制和实施加密密钥的管理工作包括了CA密钥的生成活动；CA密钥的保管、备份以及恢复；CA公钥的分配（特别是通过自签“根”证书的形式来完成时）；CA密钥托管（非强制性）；CA密钥的使用；CA密钥的销毁；CA密钥的存档；对CA加密硬件在其生命周期内的管理；以及CA提供的用户密钥管理服务（非强制性）。对密钥生命周期管理进行强有力的控制对于防止密钥泄密事件至关重要，因为密钥泄密可以破坏公钥基础结构的完整性。

用户证书生命周期是CA所提供服务的核心。CA在自己发布的CP和CPS中说明了其服务所依据的标准和操作方法。用户证书生命周期包括下面一些内容：

- 注册（验明身份和鉴别真伪的过程，通过这一过程，个体用户的行为便受到证书的约束）。
- 证书更新（非强制性）
- 用密钥重新为证书加密
- 证书的撤销
- 证书的中止（非强制性）
- 证书状态信息的即时发布（通过证书撤销清单，或是一些形式的网上证书状态协议）
- 在密钥的生命周期内，载有私钥的集成电路卡（ICC）的管理（非强制性）

对整个注册过程实施有效控制是非常重要的，因为如果没能很好的控制校验工作，用户和证书信赖者就无法有效利用CA颁发的证书。有效的证书撤销程序以及即时发布证书状态信息也非常重要，因为用户和证书信赖者据此能知道什么时候他们便不能再利用CA颁发的证书。

原则3：CA的环境控制

第三个原则——CA维持保持有效控制，以便合理保障以下几点：

- 注册者和证书信赖者的信息仅限于获得授权的个人使用，如果不属于公布的 CA 商业活动事项，不得使用这些信息；
- 保障密钥和证书在其生命周期管理的连续性；
- 授权并实行 CA 系统的发展、维护和运行工作，以保证 CA 系统的完整性。

建立和维护一个可靠的CA环境对于保障CA商业活动的可信度至关重要。如果未有力的控制CA环境，对密钥和证书生命周期管理的控制力度便会大打折扣。CA环境控制包括CP和CPS管理、安全管理、资产分类和管理、人员安全、CA设施的物理安全和环境安全、运行管理、系统访问管理、系统发展和维护、业务连续性管理、监督和合规性管理，以及事件日志的制作。

3.1.3.2. 管理机制

密钥生命周期管理控制：1. CA 密钥的生成，CA 维持有效控制，以合理保障 CA 密钥对的生成符合工业标准；2.CA 密钥保管、备份和恢复，CA 维持有效控制，以合理保障 CA 私钥的保密性和完整性；3. CA 公钥分配，CA 维持有效控制，以合理保障在首次及随后的分配中，CA 公钥的完整性和真实性，以及相关参数得到了保护。4.CA 密钥托管（非强制性），CA 维持有效控制，以合理保障被托管的 CA 签名私钥的保密性；5. CA 密钥的使用，CA 维持有效控制，以合理保障 CA 密钥只在预定地方发挥预定的功能。6. CA 密钥的销毁，CA 维持有效控制，以合理保障 CA 密钥在密钥对生命周期结束之时已经被完全销毁；7. CA 密钥存档，CA 维持有效控制，以合理保障已经存档的 CA 密钥的保密性，永远不再生成该密钥。8.CA 加密硬件生命周期管理，CA 维持有效控制，以合理保障只有合适的获得授权的人才能使用加密硬件；CA 维持有效控制，以合理保障 CA 加密硬件的正常运行。

证书生命周期管理控制：1.注册者注册，CA 维持有效控制，以合理保障注册者的身份已经被合理验明；CA 维持有效控制，以合理保障注册者申请证书的信息的准确性、权威性和完整性；2. 证书更新（非强制性），CA 维持有效控制，以合理保障证书更新请求的准确性、权威性和完整性；3. 证书密钥更新，CA 维持有效控制，以合理保障证书密钥更新请求的准确性、权威性和完整性；CA 维持控制，以合理保障证书撤销或到期之后的证书密钥更新请求的准确性、权威性和完整性。4. 证书签发，CA 维持控制，以合理保障新证书、更新的证书，以及密钥更新了的证书的生成和发放符合公布的 CA 商业活动事项。5. 证书分配，CA 维持控制，以合理保障证书一旦发放，根据发布的 CA 商业活动事项，注册者和证书信赖者都能够利用完整准确的证书；6. 证书撤销，CA 维持控制，以合理保障证书撤销基于获得批准的有效证书撤销请求。7. 证书中止（非强制性），CA 维持控制，以合理保障证书基于被批准的有效证书中止请求上被中止。8. 证书状态的信息处理，CA 维持控制，以合理保障注册者和证书信赖者能够利用即时、完整以及准确的证书状态信息（包括 CRL 和其他证书状态查询机制）。9.集成电路卡（ICC）的生命周期管理（非强制性），CA 维持控制，以合理保障 CA（或 RA）安全的控制了 ICC 的准备工作；CA 维持控制，以合理保障 CA（或 RA）安全控制 ICC 应用数据文件的准备情况；CA 维持控制，以合理保障在发放 ICC 前 CA 准许赋予 ICC 以可用性；CA 维持控制，以合理保障 CA（或 RA）安全保管和分配 ICC；CA 维持控制，以合理保障 CA 安全控制 ICC 的失活和重新激活工作；CA 维持控制，以合理保障在 ICC 交还给 CA（或 RA）之后，CA 安全停止了它的使用。

证书作业准则（CPS）和证书政策(CP)管理：CA 维持有效控制，以合理保障有效管理和控制 CPS 和 CP。

安全管理：CA 维持有效控制，以适当保障信息安全工作在正确的管理指导和支持下进行；CA 维持有效控制，以适当保障组织内部的信息安全得到了妥善管理；CA 维持有效控制，以适当保障第三方使用 CA 的设备、系统和信息资源的安全；CA 维持有效控制，以适当保障当其他组织或实体代行 CA 的某些职能时，信息安全得到了有效控制。

资产分类及管理：CA 维持有效控制，以合理保障 CA 的资产和信息得到适当级别的保护。

系统访问管理：CA 维持控制，以适当保障只有获得授权的人才有权访问 CA 系统。

商业活动连续性管理：CA 维持控制，以合理保障发生灾难事件时运行的连续性；CA 维持控制，以合理保障出现 CA 签名私钥泄密情况时，商业活动运行保持连续性；CA 维持控制，以合理保障在 CA 停止提供服务时注册者和证书信赖者受到的影响能够最小化。

3.1.4.云访问安全代理服务 CASB

3.1.4.1. 服务现状

CASB 是帮助企业在云端实现安全策略的系统，位于云服务提供商和消费云服务的企业之间，可以看作是和“Shadow IT”、未授权的云服务对抗的专用武器。CASB 部署在网络边界并使用多种代理类型，可以识别对云服务的每次响应或从云服务进行的连接。在 CASB 创建之初，它们经常作为物理设备部署在客户数据中心。现在，更多地以“安全即服务”（SaaS）模型部署为云服务本身，实现了从产品向服务的转变。

通常，下一代防火墙、Web 应用程序防火墙和其他安全工具被认为很复杂，无法发挥最大优势。相对来说，CASB 是便捷的配置和部署工具，对经验不足的安全团队比较友好。

Figure 1. Magic Quadrant for Cloud Access Security Brokers

Source: Gartner (October 2019)

图 3-7 2020 年 CASB 魔力象限

1) Microsoft

微软被评估为魔力象限的领导者，其提供的 Microsoft Cloud App Security（MCAS）一种云访问安全代理 (CASB)，可提供多功能可见性、控制数据传输以及进行复杂分析，通过它可以识别和防御用户的所有云服务中的网络威胁，主要侧重于核心功能领域，并且在与其他 Microsoft 安全产品一起补充时效果最佳。微软已将完全不同的分类机制合并为一种，可在 MCAS，Office 365，Azure 信息保护（AIP），本地权限管理服务（RMS）和终端的 Windows Information Protection（WIP）之间共享。微软的产品管理机制比较复杂，将自身提供的多个软件混乱地捆绑，安全性相互依赖，典型的 Microsoft 云安全策略需要多个 Microsoft 产品共同完成，而不仅仅是 CASB，查看企业许可信息时就可以发现，通常会访问超过用户所需的微软的安全产品和协议。

2) Bitglass

Bitglass 的 CASB 产品广泛适用于有效的 SaaS 服务安全和治理的几乎全部要求，并在所有核心功能和大多数可选功能领域提供了完善的服务。Bitglass 的业务主要在北美和欧洲，客户往往是许多行业的大型企业，但总体市场影响力不如其他同等级厂商。2020 年，Bitglass 发布了功能强大的终结点代理，该代理增加了零信任网络访问（ZTNA）和 SWG 的功能，再加上 RDP 和 SSH 的浏览器内的 JavaScript 实现，可实现超过传统 CASB 的用例，提供安全的互联网访问和威胁防护（SWG）、高级威胁防护、来自控制台管理的供应商私有应用程序处理和高水平的 SaaS 控制。该产品的缺点是管理界面显示以应用程序为中心，而不是以功能为中心，这可能会导致想要在多个 SaaS 应用程序上执行等效操作的策略之间存在不一致。

3) Symantec

Symantec 的 CASB 产品 Cloud SOC 主要专注于核心功能领域，并通过大多数产品配置中包含的单独控制台，在 CASB、SWG、安全电子邮件网关（SEG）、ZTNA 和端点之间实现 DLP 协调。Cloud SOC 可以包括各种基于常见数据格式和类型、字典、文件类型检测、指纹识别和相似性匹配的预定义 DLP 选择器，可以从正负内容的集合中进行训练，可以从一系列可选检测器构建自适应访问控制，包括阈值、威胁、行为、设备、用户位置和序列等。不足之处是，Cloud SOC 的管理界面有点过时，有时为了配置一个策略需要在多个区域协调完成，配置 DLP 策略时这一点尤其明显。

2019 年，几乎没有软件开发或集成经验的硬件供应商 Broadcom 收购了 Symantec 的企业安全软件产品线。收购之后，产品开发速度有所放缓，服务支持也受到了影响。

4) Forcepoint

Forcepoint 在魔力象限中被评估为有远见的厂商，其 CASB 主要致力于为现有产品组合提供更强的 SaaS 可见性和控制力。2020 年，Forcepoint 将其 CASB DLP 与基于云的数据保护服务相集成，Forcepoint SWG 的客户可以结合使用 SWG 和 CASB 策略来阻止对高风险的云服务的访问。Forcepoint 的云 DLP 提供了跨多个产品的单个策略引擎，这种组合可有效减少策略的重复。从 2020 年 4 月开始，Forcepoint 适用于 FedRAMP ATO（联邦授权和管理项目）的 CASB 动态云解决方案已跻身中等影响水平。2020 年 10 月，Forcepoint 被 Francisco Partners 收购。

5) Netskope

Netskope 是强调云应用发现和 SaaS 安全状态评估的 CASB 提供商之一，作为 CASB 采用的初始案例。它已在管理和非托管 SaaS 应用程序(包括大量用户活动监视和 DLP / DCAP 功能)中深入分析用户操作。这还包括通过互联网内容适配协议(ICAP)与本地 DLP 系统集成。Netskope 的主要实现方式是转发代理和 API。它仅提供对象级加密并支持仅与 Salesforce 的字段级加密。为了提供 CASB 服务，它使用一种全球分布式云基础架构，使用位于北美，欧洲和亚洲 Equinix 数据中心的自己的硬件服务器。它还提供本地虚拟或物理设备部署选项。

6) CipherCloud

CipherCloud 是 CASB 领域的先驱，其产品广泛应用于各大核心领域和细分行业，CipherCloud 的早期 CASB 产品关注于云应用中的数据加密和标记化，并且能够与本地密钥管理、DLP、DCAP 集成，形成解决方案，所以也常用于为客户提供级别较高的数据保护服务。CipherCliud 使用反向代理的方式，实现对 Salesforce 数据保护，同时支持正向代理和 API，支持物理部署和虚拟化部署。2013 年以后，CipherCloud 功能增强，加入内容和用户监控，更新云发现和 SaaS 安全状态评估。2020 年，CipherCloud 开始向周边领域扩展，如内置零信任网络安全模块（ZTNA）和安全 Web 网关（SWG），并与 SD-WAN 和 Web 防火墙进行集成。另外，CipherCloud 的 CSPM 开发完善，遵循多个通用框架，可以替代独立工具，SSPM 产品比大多数竞争对手更先进，并且在某些情况下可以自动修复有风险的配置。在市场影响力和知名度方面，CipherCloud 相对弱势。

提供 CASB 产品和解决方案的公司在关注的业务层面既有交叉，也各有不同，都是在 SaaS 业务的过程中的身份识别、访问权限、操作权限、数据及文件生命周期、数据资产加密、数据迁移、数据备份、以及审查回溯等各个环节提供保护。从技术角度上来看，CASB 的实现并不是什么难题，但是如何实现对大量 SaaS 服务适配，SaaS 业务云端历史数据与新数据的全局发现与整理，对 SaaS 业务过程的无缝干预与用户无感体验，这些工程性问题恰恰是 CASB 产品的真正难点。

3.1.4.2. 服务框架

在 RSA Conference 2017，云访问安全代理(CASB)成为整个行业关注的焦点，Skyhigh、Netskope、360 等全球多家企业都展示了 CASB 产品和方案。

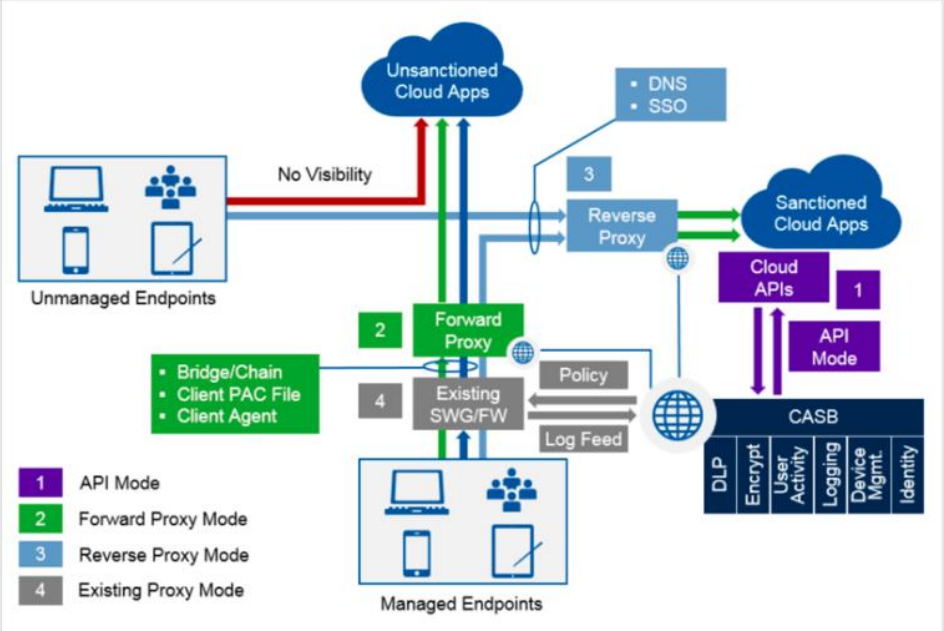

图 3-8 CASB 服务逻辑

CASB 概念在 2012 年由 Gartner 提出，定义了在新的云计算时代，企业或用户掌控云上数据安全的解决方案模型。CASB 可以看作一个安全策略的执行点，有两种服务模式：一种是 Proxy 模式，另一种是 API 模式。在 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再上传到云服务商；在 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。

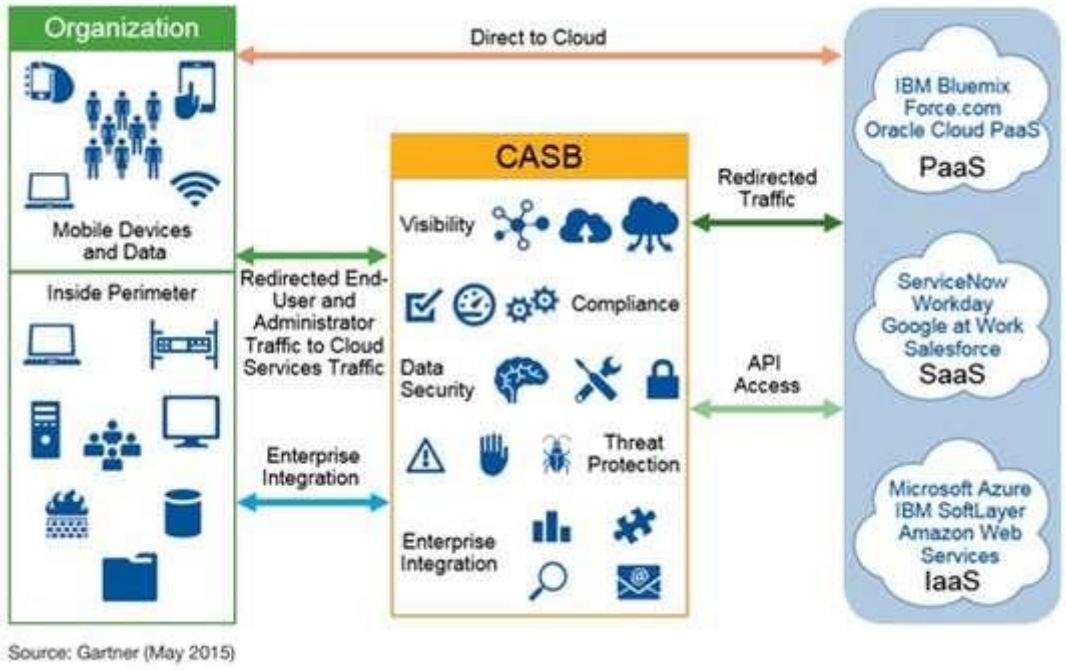

图 3-9 CASB 功能

上图中，Gartner 指出了 CASB 的四大功能，分别是：可视性（Visibility），合规性（Compliance），数据安全（Data Security）以及威胁防护（Threat Protection），以及和企业内部其他的安全技术集成。

- 可视性：CASB 提供对企业内使用云服务的使用人员、客户端设备以及使用情况，是否安全事业，提供集中化视图，查找和监视往返云服务流量的方式，对异常行为进行检测、阻断和记录，帮助企业安全团队保证企业安全措施是遵照安全计划执行的，避免了 Shadow IT 的存在。
- 合规性：企业安全团队通过 CASB 能够查看从一个云传输到另一个云以及在内部部署的基础结构和云之间传输的数据，除了可以更好地了解组织的云基础架构之外，这还可以查看存储在云中以及处理中的数据，清楚地了解云绑定数据的状态，尤其在帮助企业 IT 系统往云上迁移后，仍然能满足合规性要求，并对云服务商进行信任评级、提供内容监控、设计日志等功能。
- 数据安全：CASB 结合了人员、设备、内容和应用多个维度，执行一系列规则，提供 DLP、Encryption、Tokenization、身份验证和访问控制等数据安全保护，防止云端数据泄露。
- 威胁防护：CASB 可以提供针对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特定威胁的防护手段，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。

3.1.5.云签名服务

3.1.5.1.　DocuSign

DocuSign 成立于 2004 年，是电子签名的全球标准（The Global Standard for eSignature），也是电子签名交易管理领域的领导企业。DocuSign 能帮助公司用户在因特网上迅速地获取具有法律效力的签名，免除了用户要通过传真或邮件签名的麻烦。

3.1.5.1.1. 服务框架

DocuSign 的签名步骤可简化为发送、签字、存储三步：

1．发送:选中需要签名的文件，填写收件人的邮件地址，拖动工具栏中的标识到文件的特定位置，提醒收件人在哪里需要签名，或者是其他需要填写的信息，然后点击“Send”即发送。

2. 签字:收件人在收到邮件之后，即便他没有 DocuSign 账号也可以签名，邮件中的链接地址可以让他在 DocuSign 的界面上完成签字，既可以选择推荐的几款签名，也可以自己创建个性签名，点击确认便完成签名。

3．存储: 电子文件在邮件发送过程中保存在 DocuSign 的云存储系统中。收件人和发件人可以随时随地通过 DocuSign 的账号查阅签署的文件，或者把它们打印出来保存。

3.1.5.1.2. 管理机制

DocuSign 基于云模式提供云签名、云存储和云验证。其应用模式都是基于 WEB（HTML5）、移动终端(iPad、iPhone)等。

DocuSign 云签名：使用 DocuSign 服务器证书保证文档的防篡改性，签名后 PDF 文档通过 Adobe Reader 工具查看的签名证书为 DocuSign 服务器证书，无法查看签名用户的真实信息。

DocuSign 云存储：签名后的文档存储在其云平台，用户通过接收的邮件链接，查看文档。云存储通过 DocuSign 信封 ID（类似文件哈希值）的方式，提供文档唯一存储服务，例如 DocuSign Envelope ID: DE1622AF-9EC4-4853-AE7C-CB38EA56FAB7。通过此信封 ID，用户能在一定的时间范围内，下载预览此签名文件。

DocuSign 云验签：签名后的 PDF 文档需要通过云验签服务才能查看签名用户的信息。其云验签返回结果包括文档信封 ID、文档状态、签名者信息、签名外观、签名时访问机器 IP 及签名时间等。

3.1.5.2. Adobe EchoSign

EchoSign 公司是由 Jason Lemkin 和 Jeffrey Zwelling 成立。而便携文档格式标准的创立者 Adobe 公司在 2011 年收购了 Echo Sign 公司。Adobe EchoSign 是在线数字签名服务软件，致力于数字签名技术，目标是使数字签名成为人们签署文件和合同的标准方式，在被收购后，整体品牌已更新为 AdobeSign，通过 CSC 联盟聚集了大量的 TSP，对外提供服务。

3.1.5.2.1. 服务框架

Adobe EchoSign 为中小型企业提供订制服务并开放应用程序接口(API)，使得企业能够根据自己的工作流程整合签名技术来发送、追踪、签署文件，从而让纸张签名成为

过去式。通过 Adobe EchoSign，可以免费或付费订阅网络上的电子签名服务，在平均不到 1 小时内对档案进行电子签署，而不需要自行追踪签名。Adobe EchoSign 允许用户在 iPad、iPhone 和 iPod 里的文档中添加具有法律效力的电子签名，然后更为安全地发送给目标接受者。文档可通过 Adobe EchoSign 库，相册，电子邮件附件，或从其他应用程序(Box.net 和 Dropbox)发送。用户还可以跟踪实时状态，更新协议的状态，并从应用程序的帐户查看所有签署的协议。在签字过程中，Adobe EchoSign 应用提供与 Adobe EchoSign Web 服务相同发送和签名的保护，包括密钥身份验证、隐私与欺诈保护等等。

3.1.5.2.2. 管理机制

EchoSign 的服务模式与 DocuSign 类似,基于云模式提供云签名、云存储和云验证。不同之处如下。

EchoSign 云签名：用户下载 PDF 前，EchoSign 已在 PDF 进行了一次证明式签名，并设置了文件权限。EchoSign 云签名并不需要用户证书，只是保留了用户签名笔迹等，并且签名在 Reader 并不显示为签名，而是一个类似嵌入手写签名图片信息的超链接。

EchoSign 云验证：（与 DocuSign 类似）通过唯一 ID，连接云验证，验证用户签名的相关信息。通过云验签链接，能查询到此文档在签名相关信息及业务流程所有操作日志记录。

3.1.6.其它形态的密码服务

针对新型信息系统的技术架构例如边缘计算、雾计算所提供的密码服务，除服务能力、效率、时延、功能封装形式等方面有场景的独特要求外，从密码能力供给模式而言，和上述章节的密码服务并没有大的区别。针对其它部署形态的系统，例如基于混合云、私有云的系统，除去服务提供方实体角色带来的管理方面、责任方面不同外，从技术角度，和上述章节描述的密码服务也没有大的区别。因此，就不一一单独展开描述了。

3.1.7.小结

通过本章中所介绍的国外密码服务的发展情况，可以看到，国外的密码服务通常是由大型 IT 公司主导，尤其是云计算巨头如 Amazon、Microsoft 等依靠其在云计算服务方面的巨大优势，构建与自身云服务业务强相关的密码服务，形成事实上的标准，进而影响上下游产业链，形成密码服务产业体系。

此外，国外还依托于商业公司组成的联盟方式，推进密码服务的标准，典型的就是 CAB Forum 建立了 CA 的标准体系，CA 机构围绕该联盟的各种标准，在 WebTrust 审计体系下和浏览器、操作系统、文档阅读器厂商合作开展证书应用。

3.2.我国密码相关服务现状分析

随着信息技术产业的发展，我国产业界对密码服务这一理念的实践和尝试也在逐步推进。与国外不同的是，我国密码服务一开始就基于统筹规划和标准引导，强调服务的认证，并纳入到密码应用安全评估体系，构建密码能力支撑和密码应用供需两侧协同配合的机制。

在我国，电子认证服务（核心是数字证书服务）是发展最早、最成熟的，已广泛应用于各种应用场景。此外，不少密码厂商开展了以云服务方式提供密码功能的服务的尝

试，例如云电子签名服务，通过密码技术与云计算技术的相互融合和支撑，提供易于水平扩展、按需服务、资源共享的密码功能。

同时，近年来一些大型集团化客户，规划和建设了统一密码服务基础设施，为集团内各个应用系统提供密码设备统一部署和统一管理、统一服务入口，将分散的密码资源统一管理起来，便于安全管理和统一业务入口。

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。典型的云密码服务包括云虚拟密码机服务、云电子签名服务等。

3.2.1.基础密码服务

3.2.1.1. 对称密钥服务

随着信息安全越来越受到企业厂商的重视以及相关机构对密码产品监管的逐渐加强，厂商对于高质量密钥的需求也越来越强烈。VoIP、视频监控和车联网等因为涉及到众多敏感重要内容，在传输的过程中必须进行安全加密才可以保证信息的安全性；对于个人用户的安全保证，如果使用个人加密密钥对数据进行加密，由用户设置的密钥在安全性上存在众多问题。因此，密码厂商推出对称密钥服务，主要对用户提供高质量的对称密钥生成、密码运算等服务功能，可以广泛应用于 VoIP、安防、防伪、银行、社保、交通等多个行业的信息系统中。

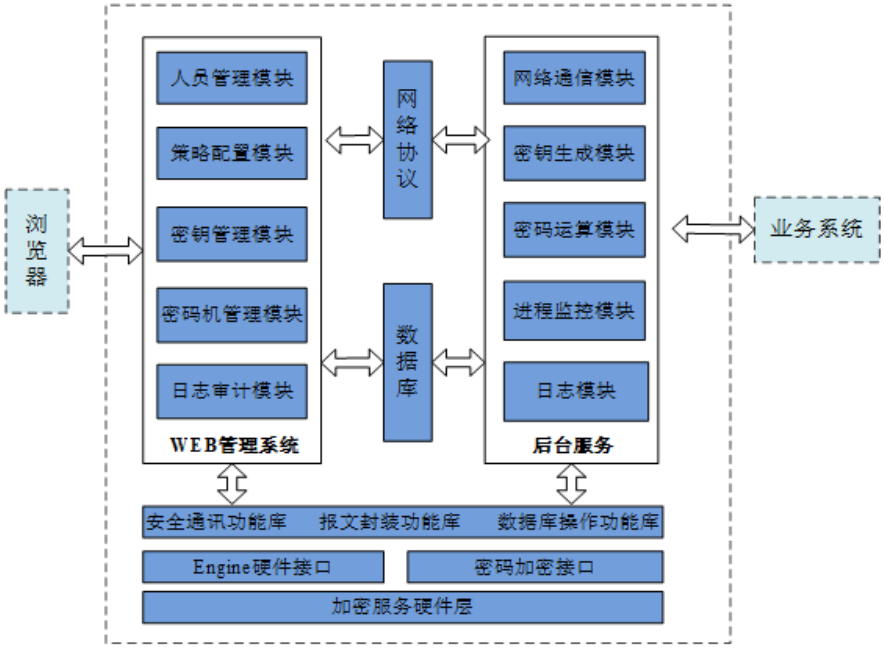

图 3-10 对称密钥服务框架

对称密钥服务通常采用硬件生成高质量的密钥，生成后的密钥保存于硬件密码设备内部或加密存放于系统数据库内，保证了密钥的安全存储。

对称密钥服务包括网络通信、密钥生成、密码运算、进程监控、数据库访问、日志等模块；WEB 管理系统包括人员管理、用户管理、策略配置、密钥管理、密码机管理、日志审计等模块。

对称密钥服务当前主要应用于会话密钥生成，系统密钥分散等主要场景，通过对称密钥服务提供的会话密钥获取，分散密钥获取，用户注册，密码运算等接口为系统提供相应的服务。

KMI 由 KMC(Key Mangement Center,密钥管理中心)提供统一的密钥管理服务，涉及密钥生成服务器，密钥数据库服务器和密钥服务管理器等组成部分。

典型的对称密钥服务包括 KMI 和 KMS。

KMI 由 KMC(Key Mangement Center,密钥管理中心)提供统一的密钥管理服务，涉及密钥生成服务器，密钥数据库服务器和密钥服务管理器等组成部分。

KMI 的密钥分发机制分为静态分发和动态分发。静态分发分为点对点配置、一对多配置、格状网配置。其中，点对点配置可用单密钥或双密钥实现。单密钥为鉴别提供可靠参数，但不提供不可否认服务，数字签名需要用双钥实现；一对多配置可用单密钥或双密钥实现。只在中心保留所有各端的密钥，各端只保留自己的密钥。是建立秘密通道的主要方法；格状网配置的特点是可使用单密钥或双密钥实现。也称为端端密钥，密钥配置量为全网 n 个终端中选 2 的组合数。

动态分发可分为基于单密钥的单密钥分发和基于单密钥的双密钥分发。基于单密钥的单密钥分发，特点是首先用静态分发方式配置的星状密钥配置，主要解决会话密钥的分发；基于单密钥的双密钥分发特点是公私钥对都当作秘密变量处理。

KMS 密钥管理服务（Key Management Service）与传统密钥管理基础设施 KMI（Key Management Infrastructure）相比具有多集成、易使用、高可靠以及低成本等优势。KMS 借助身份认证与访问控制、密钥操作审计、与云计算服务集成等方式，支持更好的集成到业务系统；通过简化密码运算接口、支持自带密钥、支持密钥轮转等方式提高易用性；通过分布式、多冗余实现高可靠服务。

3.2.1.2. IBC 加密服务

IBC（基于标识的密码系统，Identity-Based Cryptography）是在传统的 PKI 基础上发展而来，主要简化在具体安全应用在大量数字证书的交换问题，使安全应用更加易于部署和使用。

IBC 密码技术使用的是非对称密码体系，加密与解密使用两套不同的密钥，每个人的公钥就是他的身份标识，比如 email 地址，电话号码等。而私钥则以数据的形式由用户自己掌握，密钥管理相当简单，可以很方便地对数据信息进行加解密。

IBC 的基础技术包括数据加密、数字签名、数据完整性机制、数字信封，用户识别，用户认证等。

图 3-11 和图 3-12 给出 IBC 应用的典型服务框架，并给出具体例子：

企业可以使用 IBC 进行安全数据通信，包括终端到终端，终端到应用，应用到应用的情况。在实际的 IBC 系统中，不仅支持使用用户的身份标识作为公钥，而且支持使用包含用户身份的策略信息来做公钥，如下的标识就是结合着状态作为公钥：

Name="" status="成功完成工作 A"

例如，Alice 想发送信息给 Bob,只有 Bob 完成工作 A 才可以解密阅读消息，实际上当 Bob 和密钥服务器连接以获取自己的私钥时，只有他正确地证明自己的身份，并且状态为完成工作 A，密钥服务器才为他分发私钥。

这种简便，易于理解的密钥显示了 IBC 极大的优越性，使得不需数字证书，IBC 技术就可实现加密签名方法。

图 3-11 IBC 密钥服务示例流程图(1)

1.“用户 B”要向“用户 A”发送一封加密邮件，“用户 B”在自己的信任标识域中加入“用户 A”的公钥标识（其 Email 地址），通过 IBC 基于标识的密码体系加密并且使用自己的标识（其 Email 地址）进行签名并发送出去。

2. “用户 A”收到了“用户 B”的信件，如果“用户 A”没有获取私钥，他将向 Key Server 请求获取私钥。

图 3-12　IBC 密钥服务示例流程图(2)

3. 如果“用户 A”本身就拥有本身的私钥，“用户 A”将通过本身的私钥对“用户 B”的信件进行解密验证，在这个解密和验证的过程中，“用户 A”是不需要与 Key Server 进行认证的，因此可以做到离线解密验证。

4.如果用户“用户 A”暂时没有解密邮件的私钥，可以经过身份认证之后，从 Key Server 中获得自己的私钥，然后就可以根据自己的私钥解密“用户 B”发给自己的的邮件，看到邮件内容，同时可以看到“用户 B”对邮件所做的签名，以对该邮件进行准确的身份验证。

在管理方面，IBC 允许用户选择自己的公钥，并通过可信的中央服务器接受到自己的私钥，IBC 的公钥是用户的身份标识，可以用企业代码、身份号码、Email 地址、网络帐号、姓名、职位、时间等，甚至它们的组合作为实体的标识和公钥。这样做极大的方便了公开密码的管理。在安全通信过程不采用数字证书的概念，而直接将安全方案与加密或验证方法联系起来。不需数字证书，IBC 技术就可实现加密签名方法。因而用户无需进行公钥交换、认证。

IBC 密钥管理包含两大主要功能：密钥产生和密钥更新。在 IBC 系统平台上，这些功能是通过中央密钥管理服务器来实现的，它管理企业的安全应用。

密钥产生功能就是产生安全通信过程中需要的公钥和私钥。密钥更新功能确保密钥根据需要进行变化，这样如果密钥如果丢失或被盗，可以对系统和用户进行保护。

IBC 系统通过一个密钥服务器来产生密钥，密钥服务器的主要功能是为用户产生私钥，并使得用户，服务和应用程序能利用 IBC 加密。

3.2.1.3. 电子认证服务

电子认证服务是为电子签名的真实性和可靠性提供证明的活动。在我国，自《电子签名法》2005 年实施以来，电子认证行业发展已经近二十年。截至 2020 年 11 月，获得工业和信息化部“电子认证服务许可证”的机构共 48 家，签发在用有效数字证书超过 7 亿张，广泛应用于电子政务、电子商务、金融交易、移动互联网、医疗卫生等多个领域。在支撑信息化、保障网络安全方面发挥了重要作用，电子认证服务行业已成为国家实施网络可信身份战略的重要组成部分。

在技术层面，电子认证服务机构需要按照现行的技术规范，通过 CA 和 RA 系统向外提高数字证书相关的服务，包括用户注册、证书签发、证书冻结/解冻、证书吊销、证书更新等服务，在服务过程中保证系统安全。机构需要发布证书策略和认证业务声明，声明电子认证服务活动中各方的责任和义务、证书适用范围等各种信息，保证证书服务和证书策略中的声明是一致的。CA 应采用技术和管理手段，保证证书策略中的各种承诺能够得到满足。

在 GB/T25056 中给出典型的 CA 系统逻辑架构如图 3-13 所示：

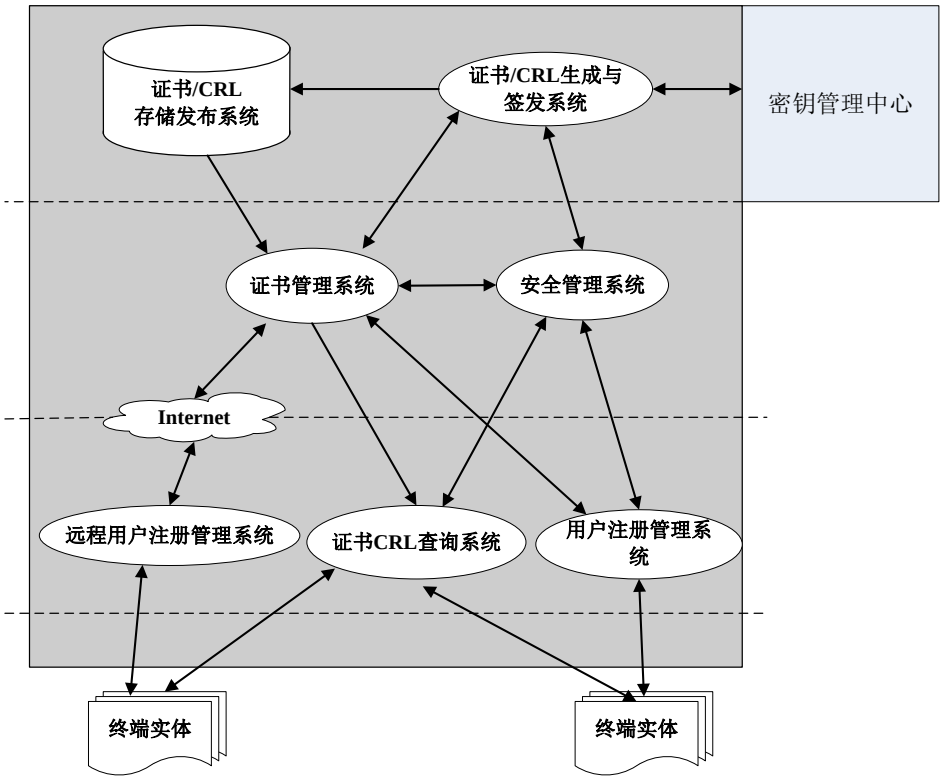

图 3-13 CA 系统逻辑架构

CA 在向用户提供加密证书时，加密密钥通常由密钥管理中心进行管理。密钥管理中心通过向 CA 提供服务，支持为用户提供加密证书所需的密钥，满足各类数据加密应用场景，同时，密钥管理中心还支持提供司法恢复功能。

在我国，各个运营电子认证机构通过国家根 CA，形成严格层次的信任模型以及相应的管理体系，如图 3-14 所示。

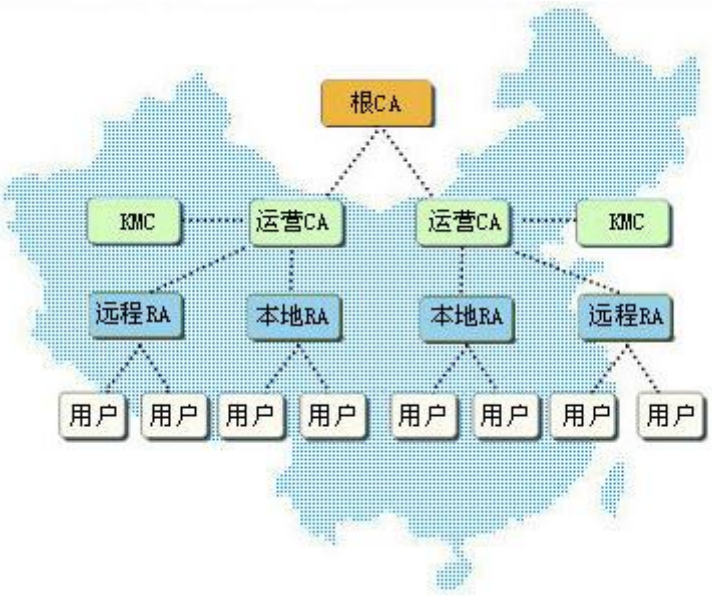

图 3-14 国家电子认证根建设架构

3.2.2.密码功能服务

3.2.2.1. 电子签章服务

a) 发展现状

2005 年 4 月 1 日正式施行的《电子签名法》，确立了可靠电子签名的法律效力，也确立了可靠电子签章与物理盖章行为同等的法律效力，推动电子签章技术从单纯添加印章图片的阶段进入到结合数字证书电子签名的阶段。2014 年，我国密码行业标准化委员会发布了《安全电子签章密码技术规范》，2020 年发布了相应的国家标准，规范了电子印章和电子签章的数据结构、密码应用和处理流程，促使电子签章的密码应用走向标准化、规范化。

早期，电子签章是以产品销售的方式为用户提供电子签章功能，即用户单位直接采购电子印章系统及相关产品，建设部署在企业内部，提供单位部门章和人员章的制作，支持内部办公人员进行文件签章、验章等，电子签章文件也通常仅在单位内部流转和验证，为无纸化办公提供有力支撑。

随着互联网的迅猛发展，电子签章的使用需求已经不仅仅局限于解决单位内部信任关系和无纸化办公问题，跨企业、跨地域、跨行业的业务也急需电子签章技术的支撑，迫切需要更加便捷的电子签章服务，电子商务、电子政务、移动展业等行业的需求尤其明显。因此，一方面，不少省、市公安机关基于法人实物印章备案管理等传统优势以及国家机关公信力，在本省、市范围内开展面向法人单位的电子签章服务，如兴唐通信科技有限公司为部分省、市公安机关建设部署的法人电子签章服务平台；另一方面，面向垂直行业涌现出一批电子签章技术应用服务性企业，以 e 签宝、法大大等电子合同服务平台为代表。

b) 服务框架

云计算环境下的签章服务平台通常基于 PKI 技术提供签名的数字证书支持，在线提供数字证书的申请、存储、使用、吊销及电子印章申请、审核、签发、发布、冻结、解冻、撤销、签章、验章、查询、审计等全生命周期的管理功能。签章服务平台以第三方服务的形式提供服务，用户单位的程序或系统仅需调用服务接口即可完成电子签章，无需独立建设和维护电子签章系统。

基于云的签章服务平台一般由密码厂商支撑建设，基于密码技术建设，符合相关密码应用要求和电子签名相关法律、标准要求。

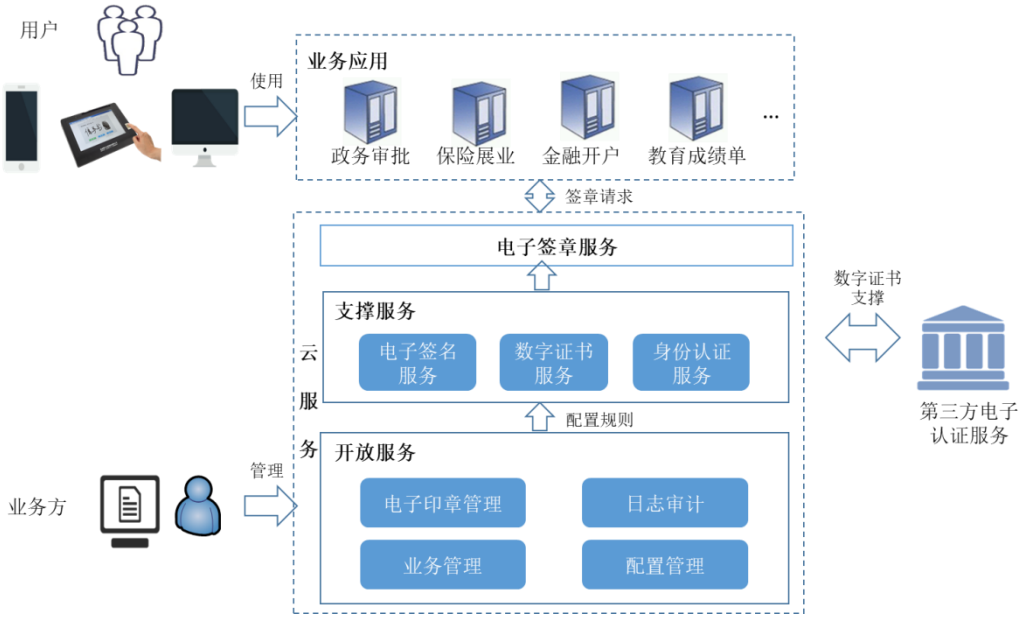

图 3-13 基于云的电子签章服务平台架构

基于云的电子签章服务平台一般依托于第三方电子认证服务提供的数字证书服务作为信任基础，以云服务形式供租户的业务应用调用。同时，为了方便用户管理和配置，通常以租户为单位提供配置管理服务。

基于云的电子签章服务通常为三层结构，包括：

1） 开放服务

印章管理系统：为客户提供印章管理服务，包括租户信息管理、查询、印章策略管理、印章审核管理等

日志审计：印章管理和签章服务的日志审计。

业务管理：为客户提供调用电子签章服务的业务系统及调用规则的管理，如用户管理、签章业务管理、签章文件模板管理、授权管理等，以保证签章业务的安全管理。

2） 支撑服务

电子签名服务：电子签章服务是在电子签名服务的基础上，实现对待签章文件的电子签章。

数字证书服务：为用户或用户单位提供数字证书下载服务，安全密码模块生成密钥并加密存储在云端，云端向 CA 机构请求签发数字证书，完成证书下载。单位证书必须受个人证书或业务系统控制。

身份认证服务：用户调用个人或企业数字证书进行电子签章时，须先进行身份认证，认证通过方可获得相应签章授权。

3） 电子签章服务

直接供客户业务应用调用进行电子签章，通常针对不同文件格式的签章需求业务需集成不同的签章服务接口，如 PDF 文件签章、DOCX 文档签章、网页签章等。

3.2.2.2. 通信加密服务

近年来，全球网络电话（VoIP）发展迅速，其通过使用分组交换技术使数据传送具有灵活性强、可靠性高、经济性好等优点。VoIP 经由传统网络进行语音数据的传递，

必然要考虑到开放的网络环境带来的各种安全问题，要保障数据传递过程不被破坏、不被篡改、不被非法监听。

国内各厂商已经在国家密码相关部门的领导下研发和部署了相应的产品，其主体思路是基于 PKI 机制的网络加密电话体系，该体系在原有 VoIP 的通信框架中加入身份认证、数据加密、数字签名等技术，将网络内语音数据从“生产”到“消费”的环节全周期保证安全性。

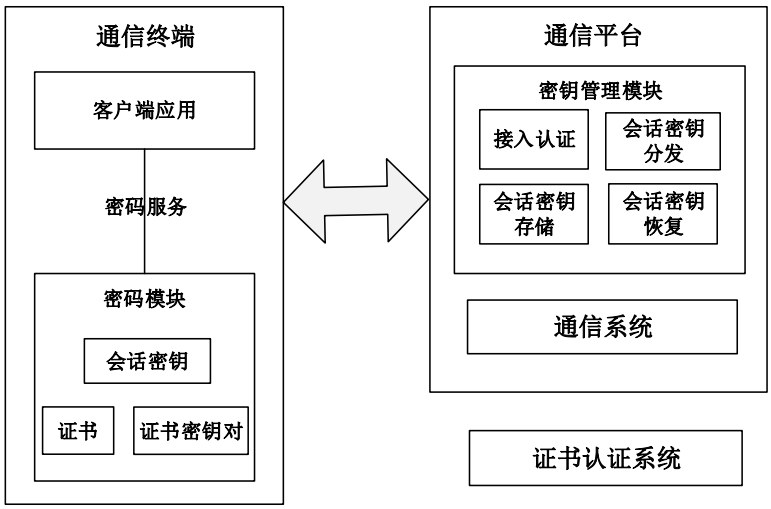

图 3-14 VoIP 通信加密服务框架

网络加密电话系统由通信平台和通信终端两大部分组成，其中通信平台由通信系统和密钥管理模块组成，另可自建证书认证系统或采用第三方证书认证服务。

密钥管理模块提供密钥管理服务，包括会话密钥的生成与管理；与终端通信和交互，完成对终端的身份鉴别和会话密钥的分发，其中的密钥生成和密码运算均由硬件密码设备完成。

终端需要密码模块提供安全的密钥管理和密码运算服务，包括使用密码模块存储证书和密钥，以及提供加密语音、身份认证时用到的密码算法。

证书认证系统为终端和密钥管理系统提供证书的签发、查询、撤销、更新等服务，证书认证系统作为独立的系统提供服务。在即时通讯领域，目前主流即时通讯软件都实现了对数据的加密，加密密钥由服务端生成并下发到客户端，加解密动作在客户端完成。一般加密密钥由即时通讯服务器后台管理。也有即时通讯软件通过集成第三方密钥管理服务的形式来由第三方提供密钥的生成和管理。

在即时通讯领域，目前主流软件基本都实现了对数据的加密，加密密钥由服务端生成并下发到客户端，加解密动作在客户端完成。一般加密密钥由即时通讯服务器后台管理。也有即时通讯软件通过集成第三方密钥管理服务的形式来由第三方提供密钥的生成和管理。

3.2.2.3. 云安全接入（访问）代理

a) 发展现状

2017 年 360 企业安全集团发布了 CASB 云安全产品——360 云守，除此之外还有杭州臻至 LOCKet、炼石网络 CipherGateway、深信服云盾、深圳云安宝、江苏易安联等

CASB 产品或服务，大部分产品都支持云环境部署，也都采用了加密技术保证数据的安全性，其中多个产品声称支持商用密码算法。

b) 服务框架

1) 360云守

360 云守采用灵活的安全策略，通过认证、标记化和加密方式，确保云端和传输中的数据安全，内置包括 AES 算法、商用密码算法以及特定业务场景的字段加密和标记化算法等在内的数十种特定的安全加密算法，而且通过性能优化措施可以在保证安全的情况下保留原有云应用功能，不影响用户云应用体验。

360 云守提供操作简便的部署，支持正向代理、反向代理 API 部署，可在内部、边界和云端部署。360 云守已经适配国内外的主流云 SaaS 应用，如 Salesforce、GitHub、360 云盘等。

2) 杭州臻至LOCKet

LOCKet 对客户数据进行加密，加密后数据存储于云服务，密钥实行分离保管，保证云服务平台和 LOCKet 都无法查看和使用客户数据，真正做到客户的数据客户做主。

LOCKet 支持 AES-GCM 256 位加密。密钥区块链化，LOCKet 所有的密钥将会部署在全球上万个节点上。

3) 炼石网络CipherGateway

首创基于委托式安全代理模式的 CASB 网关，能够结合业务场景，在云应用部署的关键控制点增加丰富的安全策略，实现云端数据加密、网络流量的业务可见，在满足行业合规的同时保障业务数据安全。

CipherGateway 采用高强度国产商用密码算法、令牌化、格式保留加密等。密钥始终在企业用户侧，并由本地的专业安全芯片保护密钥安全，同时采用业界标准的密钥分散备份方案，确保密钥的安全备份，必要时可由多名密钥管理员恢复密钥。

4) 云安宝

其 CASB 产品在企业数据流向云端之前，对敏感数据实施加密保护，而数据加密的密钥完全由用户掌握，即使云服务商也看不到企业在云端的数据。

支持国产商用密码算法、tokenization、格式保全等加密算法。企业级密钥管理，并可与 KMIP 等无缝集成，密钥由多人分散管理，必要时可由多名密钥管理员恢复密钥。支持以物理旁路、逻辑串联的方式，安装部署在企业内部的任何一个物理服务器或虚拟机上，也可以将加密网关部署到一个公有云平台上。

3.2.2.4. 身份认证服务

a) OAuth

OAuth（Open Authorization Protocol Framework），即开放的资源授权协议框架，由 IETF 发布，目前已发布 OAuth 2.0 协议。OAuth 方便第三方应用安全地资源服务器上的资源，在云服务场景中应用广泛，目前，很多互联网服务公司如 Twitter、Google、Microsoft、新浪、腾讯等都提供了 OAuth 服务。

OAuth 的授权模型如图 3-17 所示：

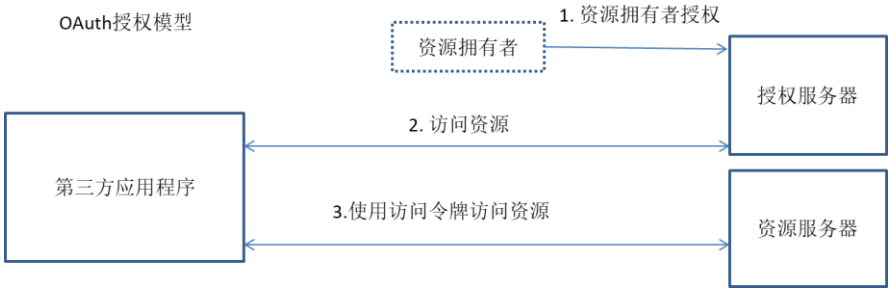

图 3-15 OAuth 授权模型

OAuth 2.0 协议通过引入一个授权层，将第三方应用程序与资源拥有者的角色进行分离，在资源拥有者的授权下，授权实体（即授权服务器）向第三方应用程序发放不同于资源拥有者身份凭据的访问令牌，第三方应用程序使用访问令牌代替资源拥有者口令凭据去访问受保护资源。访问令牌是授权服务器发送给第三方应用程序用于访问受保护资源的凭据，令牌中给出了访问资源的特定范围和访问时长，这个特定的范围和访问时长是由资源拥有者授权同意的，并由资源服务器和授权服务器实施。

OAuth 2.0 应用场景如图 3-18 所示：

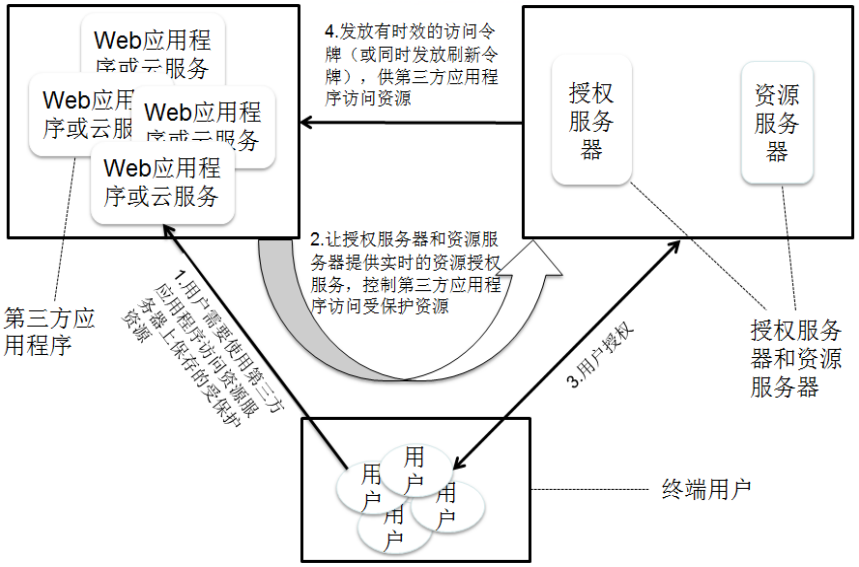

图 3-18 OAuth 应用场景

第三方应用程序是当前互联网上广泛部署的 Web 应用程序、云服务或者其他手机 APP 等应用程序。当用户需要使用第三方应用程序访问资源服务器上的受保护资源时，第三方应用程序将重定向到授权服务器，授权服务器在获取到用户授权后，发放给第三方应用程序有时效性的访问令牌，第三方应用程序使用访问令牌访问受保护资源。

OAuth 2.0 根据第三方应用程序的类型以及不同的使用场景，定义了四种授权许可，第三方应用程序可以使用这四种授权许可向授权服务器换取访问令牌，然后使用访问令牌访问受保护资源。四种授权许可分别是授权码许可、隐式许可、资源拥有者口令凭据许可和第三方应用程序身份凭据许可。

1） 授权码许可

授权码形式的授权许可可用于获取访问令牌和刷新令牌，适合有保密能力型的第三方应用程序。由于该流程是一个基于重定向的流程，所以要求第三方应用程序能够与资源拥有者的用户代理（通常是一个 Web 浏览器）进行交互，并能够接收到来自授权服务器的请求（通过重定向）。授权码许可流程如图 3-19 所示。

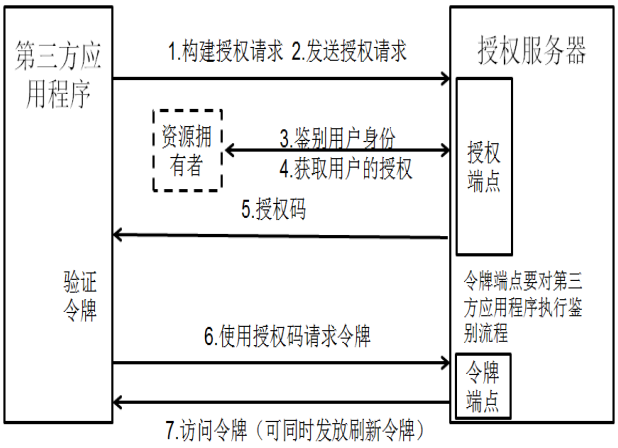

图 3-19 授权码许可流程

2） 隐式许可

隐式许可类型可以用于获取访问令牌，但该类型不支持刷新令牌的发放，适用于操作某一特定重定向 URI 的无保密能力型第三方应用程序。这些第三方应用程序通常是浏览器中脚本语言（如 JavaScript）实现的。隐式许可类型没有包含第三方应用程序的身份鉴别流程，需要依赖于资源拥有者的参与和重定向 URI 的提前注册来验证第三方应用程序。在该流程中，第三方应用程序直接获得访问令牌作为授权请求的结果。被编码到重定向 URI 中的访问令牌可能会暴露给资源拥有者以及在相同设备上驻留的其他程序。

第三方应用程序应能够与资源拥有者的用户代理（通常是一个 Web 浏览器）交互，并能够接收到来自授权服务器的请求（通过重定向）。隐式许可流程如图 3-20 所示。

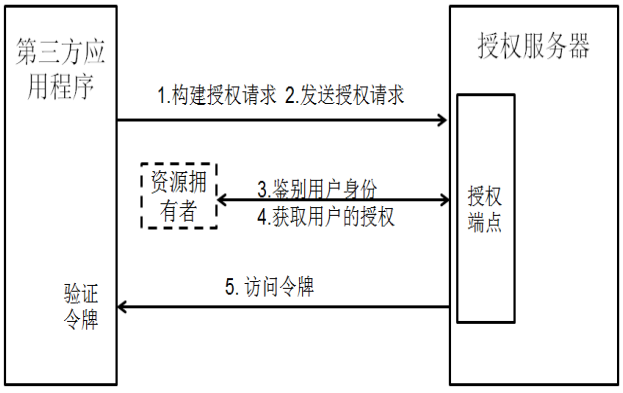

图 3-20 OAuth 隐式许可流程

3） 资源拥有者口令凭据许可

资源拥有者口令凭据许可类型适用于资源拥有者与第三方应用程序之间存在互信的情况，例如，第三方应用程序是操作系统的一部分或者某个特权应用。授权服务器应

当谨慎采用此种类型的授权许可，只有无法采用其他流程时，才允许使用该流程。资源拥有者口令凭据许可流程如图 3-21 所示。

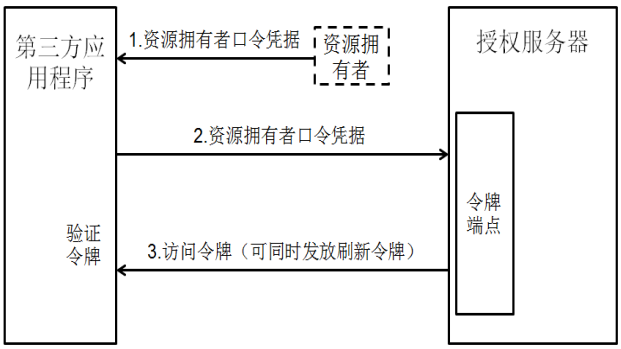

图 3-16 OAuth 资源拥有者口令凭据许可流程

4) 第三方应用程序凭据许可

当授权的范围仅限于第三方应用程序直接控制的资源，或者此前第三方应用程序与授权服务器经过协商同意的其他资源拥有者的资源时，第三方应用程序可以只用自身的第三方应用程序凭据来请求一个访问令牌。第三方应用程序凭据许可流程如图 3-22 所示。

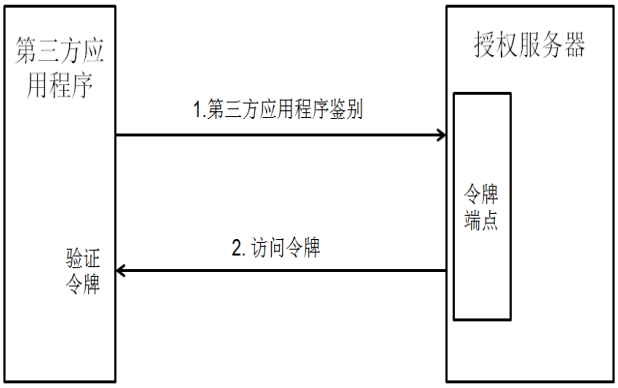

图 3-17 第三方应用程序凭据许可流程

b) FIDO

FIDO（Fast IDentity Online）在线快速身份验证规范主要依赖于安全设备和 Web 浏览器作为客户端来实现 FIDO 客户端的安全环境，允许任何网站和云应用与支持 FIDO 的设备通信，实现便捷、安全的在线用户鉴别。2014 年 12 月，FIDO-UAF-V1.0 和 FIDO-U2F-V1.0 正式发布，2018 年 4 月，W3C 牵头制定的 FIDO 2.0 正式发布，包括 Web 认证（WebAuthn）标准和客户端-身份认证器协议（CTAP）两部分。

FIDO2.0 针对设备、应用的口令安全问题的全面解决方案，同时也解决了所有传统的身份验证问题。FIDO2.0 框架下，用户登录任何网站使用的都是唯一的身份凭证，且不允许离开用户的设备，更不会存储在服务器上，可以很好地抵御网络钓鱼、各种形式的密码窃取和重放攻击；FIDO 加密密钥对于每个网络站点都是唯一的，因此不能用于跨站点跟踪用户。另外，生物特征数据在使用时无需离开用户的设备。

用户可以使用简单的内置方法（例如设备上的指纹读取器或摄像头）或利用易于使用的 FIDO 安全密钥来解锁登录凭据，用户可以选择最适合需求的设备。网站可以通过

简单的 JavaScript API 调用 FIDO 协议进行认证。目前，Google Chrome、Mozilla Firefox 和 Microsoft Edge 在内的主流网络浏览器已经采用了 FIDO 2.0，Android、windows10 和相关的微软技术也内置了支持 FIDO2.0 协议的模块。

FIDO 2.0 的相关规范兼容现有的无密码 FIDO UAF 和 FIDO U2F 用例，并扩展了 FIDO 身份验证的可用性，已经拥有外部兼容 FIDO 的设备的用户可以继续将这些设备与支持 WebAuthn 的 Web 应用程序一起使用，现有的 FIDO UAF 设备仍可以与基于 FIDO UAF 协议的现有服务以及新服务一起使用。

如果说 FIDO UAF 适用典型 B2C（企业-个人）场景，U2F 更适用典型 B2E（企业-雇员）场景的话，那么包含 WebAuthn API 和 CTAP 协议两部分内容的 FIDO2.0 是对多场景的普适支持。

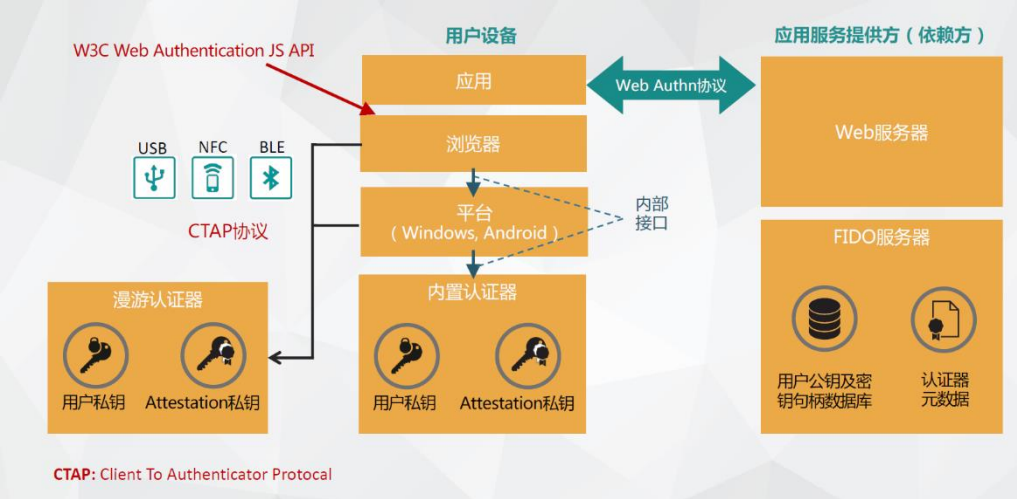

图 3-18 FIDO 2.0 体系架构

FIDO2.0 的最佳适用场景包括：

- ✓ 在设备上通过浏览器使用设备配置的指纹等生物识别能力进行身份认证；
- ✓ 在设备上通过浏览器使用外置Security Key进行身份认证；
- ✓ 在设备上通过另一台设备作为认证器完成身份认证。

c） 基于可信环境的生物特征识别身份鉴别协议

GB/T 36651-2018《基于可信环境的生物特征识别身份鉴别协议框架》定义了基于可信环境的生物特征识别身份鉴别协议，规定可信环境中的生物特征识别密钥管理器应完成的功能以及功能接口参数。

协议框架如图 3-24 所示。

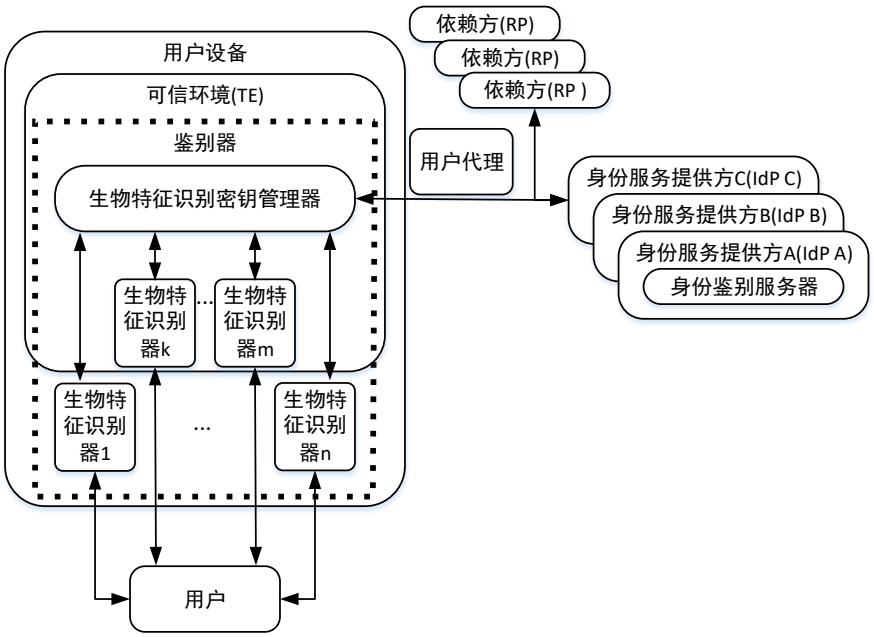

图 3-19 基于可信环境的生物特征识别身份鉴别协议框架

在基于可信环境的生物特征识别身份鉴别协议框架中，用户使用用户设备通过用户代理访问依赖方提供的应用，依赖方使用身份服务提供方（IdP）提供的身份鉴别服务对用户的身份进行鉴别。用户代理可以是安装在用户设备上的浏览器或者其他应用。可信环境部署在用户设备内，用于提供安全可靠的环境，保证用户信息的安全性。图中虚线框内表示鉴别器，包括生物特征识别密钥管理器和生物特征识别器。生物特征识别器将生物特征识别结果返回给生物特征识别密钥管理器。生物特征识别密钥管理器必须部署在可信环境中。生物特征识别器可以部署在可信环境中，也可以在可信环境外部部署。生物特征识别密钥管理器和依赖方可针对生物特征识别器部署的位置采取不同的安全策略。

在用户向身份鉴别服务器进行注册的流程中，用户使用的生物特征识别密钥管理器创建一对新的鉴别公私钥并且将鉴别私钥保存在生物特征识别密钥管理器中，将鉴别公钥注册在身份鉴别服务器中。注册流程见图 3-25。

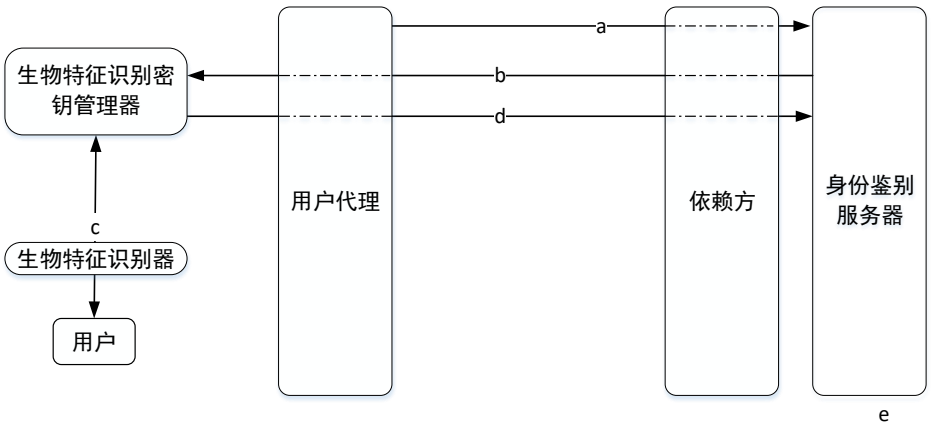

图 3-20 注册流程

1) 用户使用用户设备中的用户代理访问依赖方，当用户需要进行生物特征识别身份鉴别注册时，依赖方将用户定向到身份鉴别服务器（可以使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器，或者使用消息转发方式）。
2) 身份鉴别服务器向用户设备中的生物特征识别密钥管理器发送注册请求消息；用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的注册请求消息时，验证身份鉴别服务器的真实性，验证通过则提示用户选择可用的生物特征识别器，否则拒绝该消息。
3) 用户选择合适的生物特征识别器，使用生物特征识别信息解锁生物特征识别密钥管理器（如果用户之前未将生物特征识别信息登记到该生物特征识别器，则进行登记；如果用户已进行登记，则使用已登记的生物特征识别信息完成解锁过程），完成用户生物特征识别验证。用户生物特征识别验证成功后，生物特征识别密钥管理器创建一对与生物特征识别密钥管理器、身份鉴别服务器相关联的唯一的鉴别公私钥，鉴别私钥保存在本地的生物特征识别密钥管理器，并且不允许从生物特征识别密钥管理器导出。如果生物特征识别密钥管理器没有能力保存鉴别私钥，则该生物特征识别密钥管理器将鉴别私钥进行加密，然后将加密后的鉴别私钥保存在用户设备中，用于加密用户私钥的密钥则保存在生物特征识别密钥管理器中并且不允许从生物特征识别密钥管理器导出。
4) 生物特征识别密钥管理器生成密钥注册数据（密钥注册数据中包含上一步生成的鉴别公钥），然后生成注册响应消息（注册响应消息中包含密钥注册数据，以及使用厂商私钥对密钥注册数据进行签名的签名值），将注册响应消息发送到身份鉴别服务器。
5) 身份鉴别服务器使用厂商公钥验证注册响应消息中的签名，签名正确则提取出鉴别公钥并保存该鉴别公钥(同时应保存该鉴别公钥与用户之间的对应关系)。

在鉴别流程中，用户通过生物特征识别密钥管理器使用鉴别私钥对服务器挑战签名，向身份鉴别服务器证明其拥有该私钥，完成身份鉴别过程。鉴别流程见图 3-26。

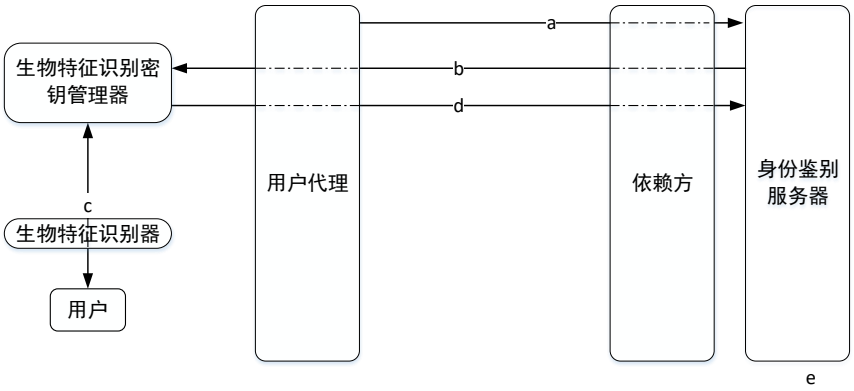

图 3-21 鉴别流程

1) 用户使用用户设备中的用户代理访问依赖方，当用户需要进行生物特征识别身份鉴别时，依赖方将用户定向到身份鉴别服务器（可以使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器，或者使用消息转发方式）。
2) 身份鉴别服务器向用户设备中的生物特征识别密钥管理器发送鉴别请求消息；用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的鉴别请求消息时，

验证身份鉴别服务器的真实性，验证通过则提示用户选择可用的生物特征识别器，否则拒绝该消息。

3）用户选择合适的生物特征识别器，使用生物特征识别信息解锁生物特征识别密钥管理器，生物特征识别密钥管理器选择相应的鉴别私钥对服务器挑战签名。

4）生物特征识别密钥管理器将签名后的挑战发送到身份鉴别服务器。

5）身份鉴别服务器使用相应的鉴别公钥对签名验证成功后，用户鉴别成功。

在注销流程中，身份鉴别服务器删除相应的鉴别公钥，生物特征识别密钥管理器删除相应的鉴别私钥。注销流程见图 3-27。

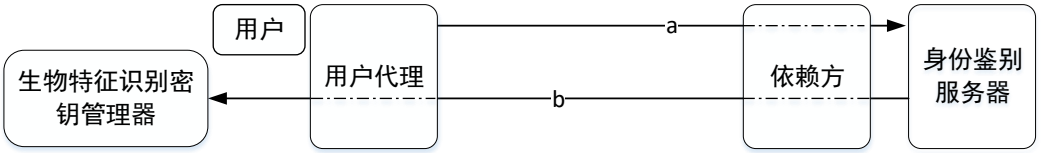

图 3-22 注销流程

1）用户在身份鉴别成功后，发起注销流程，依赖方将用户定向到身份鉴别服务器（可以使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器，或者使用消息转发方式）。

2）身份鉴别服务器删除相应的鉴别公钥，并向生物特征识别密钥管理器发送注销请求消息。用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的鉴别请求消息时，验证身份鉴别服务器的真实性，验证通过则删除相应的鉴别私钥，否则拒绝该消息。

3.2.3.密码应用服务

3.2.3.1. 电子合同服务

a） 发展现状

随着全球信息化进程加快，协议、合同的签署逐渐从线下场景转移到线上场景，代表签署人身份和签署意愿的传统纸质合同也逐步被电子合同取代。自 1996 年联合国推出《电子商务示范法》，并确立电子签名概念及法律效力后，各国际组织、国家及地区纷纷颁布电子签名相关法律。这些立法均确立电子签名概念、法律效力及适用范围，并为电子合同的普及奠定法律基础。

2014 年以来，中国移动互联网进程加快，云计算技术逐步成熟，电子商务的飞速发展也促使我国开始推出更多促进电子合同在各行业落地实践的政策，依托于云计算 SaaS 服务的新兴第三方电子合同平台纷纷涌入市场，基于电子签名技术为互联网金融、O2O 电子商务企业及个人提供在线电子合同缔约、证据托管等服务。2020 年受疫情影响，各行业业务开展更加依托于互联网，因此，各行业密集出台认可电子合同法律效力的政策，助推电子合同行业快速发展。

第三方电子合同平台因其安全性更高、成本更低等明显优势，陆续被多行业的企业用户接受并采纳。传统电子签章厂商也陆续推出自有电子合同产品，但部署模式多以本地化部署为主，以 SaaS 模式为主的第三方电子合同平台主要为“e 签宝”、法大大等新兴企业。近年来，部分企业服务、互联网头部企业也通过推出电子签约或合同管理等相关产品或系统，进入第三方电子合同市场。

b） 服务框架

电子合同服务是指为了满足政府、企业或个人获取和使用电子签名、签署和管理电子合同等需求，为用户提供合同拟定、身份认证、电子签名、电子合同签署验证、合同管理、存证出证、法律服务等相关业务，从而保障用户签署电子合同的合规合法性和安全有效性，提升政府及企业的运营和管理效率，加速数字化办公进程的服务平台。

电子合同相较于纸质合同，签署流程在线化，减少“打印”、“纸质合同邮寄/回寄”等环节，表现为“合同初稿-申请审批-电子签名-交易方签名-合同存储”，促使合同签署周期从原来的一周减少到一天甚至几小时，实现数十倍的缩减。

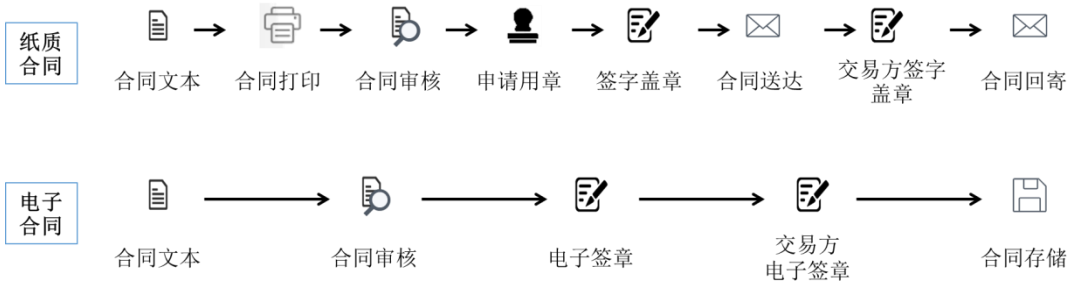

图 3-28 电子合同流程简化示意图

电子合同服务平台主要有本地化部署与基于云的 SaaS 部署模式两种，初步应用阶段，大部分电子合同服务以提供本地化部署模式为主，SaaS 的流程通用化，与具体业务匹配较差，实际利用率比例较低。但随着电子合同的渗透与普及，本地化部署模式低效率、高成本、法律效力易受影响等缺陷凸显，SaaS 部署模式更易满足企业灵活性、及时性、低成本等需求，再加上国家政策的支持，将被更多企业接纳并采购。

区块链、云计算、人工智能等创新技术与电子合同服务平台核心基础技术的结合，为电子合同服务创造出了更多核心技术能力，助力电子合同服务平台提供覆盖合同全生命周期的产品及服务。例如，人工智能技术重点作用于合同管理环节，实现电子合同全生命周期的智能管理；区块链更多应用于合同存证出证环节，保证电子合同的数据存储安全与流转可追溯。

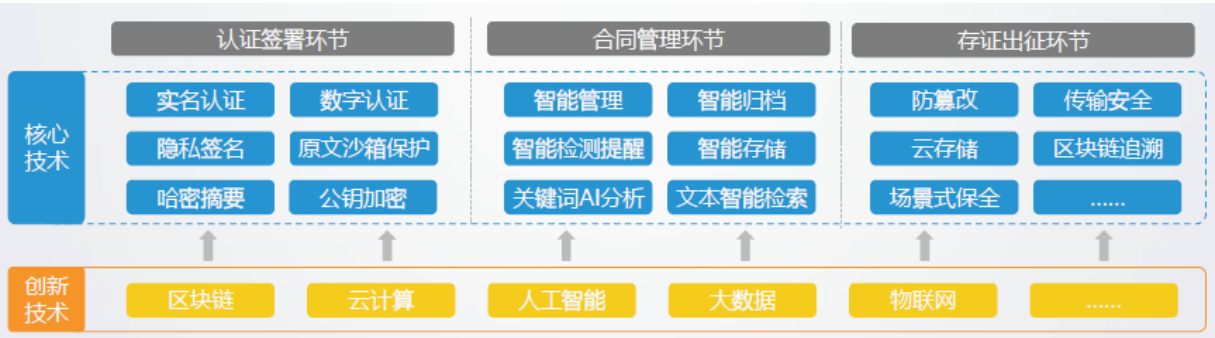

图 3-29 第三方电子合同服务平台技术服务框架

（引自：亿欧智库《 2020年全球第三方电子合同平台发展报告》）

长远来看，创新技术与第三方电子合同平台核心技术的结合，将帮助电子合同服务平台构建闭环服务，并提升电子合同安全性，保障法律效力。

4. 密码功能服务的框架与模式

4.1. 技术框架

密码功能服务基于多种网络基础设施、密码基础设施、计算基础设施等提供的资源，通过虚拟化、密码算法、密码协议、密码技术等技术，实现可向外提供的密码运算功能和密码管理能力，并提供与服务能力相匹配的运营管理、安全审计和运维支撑。用户侧通过其应用程序或业务系统，使用服务提供的密码功能完成其所需的业务操作。密码功能服务可能会依赖于第三方提供的审计、测评评估、密码基础技术、密码产品等，其技术框架可归纳为图 4-1：

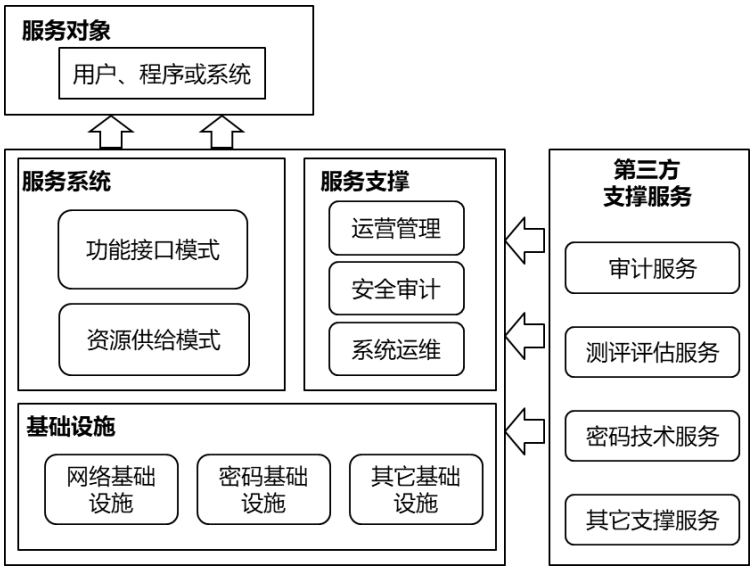

图 4-1 密码功能服务技术框架

（1） 基础设施

密码功能服务的建设和运行依赖于一系列硬件、软件、网络等通用基础设施，可能还包括云计算基础设施、安全防护基础设施，甚至密码机、PKI 公钥基础设施等密码基础设施，这些基础设施为服务提供了所需的基础运行环境和所需的安全防护能力、基础的密码计算能力。

（2） 服务系统

服务系统与用户的应用程序或业务系统直接对接，通过编程 API 接口、通信协议或密码应用程序等接收其服务请求，并根据其请求内容按照服务系统设定的处理策略，调用系统内特定的某项或一组密码功能，完成密码运算，并向用户的应用程序或业务系统反馈处理结果。

服务系统提供的密码运算服务可根据服务提供模式的不同，可以通过资源方式或功能接口方式呈现。

（3） 服务支撑

为了保证服务的有效运行和安全运行，密码功能服务一般需提供与服务水平和服务能力相适应的对服务系统的运营管理、安全审计、运维支撑等各种支撑服务，还可能包括用户自服务系统，为用户提供自主管理和配置能力。

（4） 第三方支撑服务

密码功能服务可引入第三方的安全审计服务、检测服务等作为服务支撑，也可以采用第三方的技术、密码产品、服务等作为自身服务活动的支撑。例如，电子签名、电子合同服务可通过合法的电子认证机构（CA）为用户以及业务相关方颁发数字证书、提供各种证书服务。

4.2.服务模式

根据用户的密码应用需求，典型的密码功能服务的服务模式可以分为通过资源方式或功能接口方式呈现，如图 4-2 所示。这两种服务模式可以构成从底层到上层的层级关系，低层可为上层提供支撑，并且每一类也可直接为用户提供服务，选择哪类的服务取决于其信息系统的部署环境和边界。

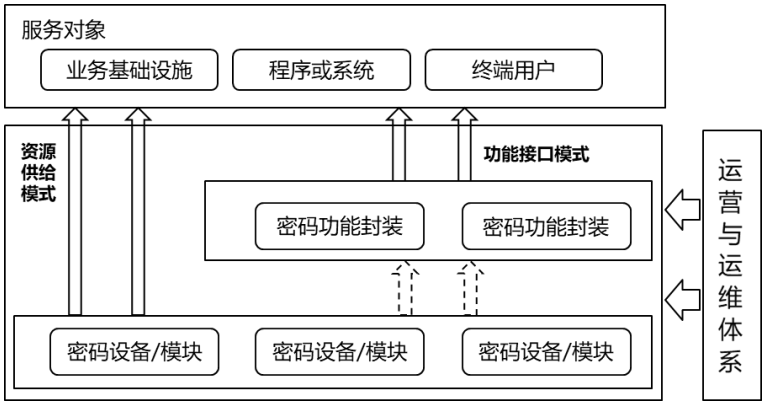

图 4-2 典型的服务模式示意图

4.2.1.资源供给模式

以资源供给模式呈现的密码功能服务，基于服务方式提供虚拟密码机等密码基础资源，主要满足用户在建设密码支撑系统或密码应用系统时，通过购买服务而无需购买物理设备来获得密码基础资源，也无需配备机房资源和运维资源。

以资源供给模式呈现的密码功能服务，可通过虚拟化方式为部署在同一个物理环境中的多个业务系统提供服务，这种情况下，一般不支持跨地域提供服务。典型的场景是云计算服务商建设平台化密码系统，租户在其提供云主机和虚拟网络上部署业务系统时，可同时租用其虚拟密码资源。

4.2.2.功能接口模式

以功能接口模式呈现的密码功能服务，将密码功能按照不同场景的需求以在线网络报文服务、SDK 的方式提供给用户或者用户的业务系统，如签名验签、时间戳等。密码功能服务主要满足用户在建设密码应用系统时，通过在各个需使用密码的环节调用相应服务来完成特定的安全功能的需求，用户无需关心密码功能如何实现，仅需直接调用服务或通过策略配置获得一组符合业务策略的密码功能服务。

以资源供给模式呈现的密码功能服务，通常以交互报文协议、应用开发接口等方式，为各种业务系统提供服务，能够支持跨地域、跨物理环境的各种业务。典型的场景是业务系统可以通过集成电子签名服务的应用开发接口，借助电子签名服务，实现所需的电子签名。

4.3.运营模式

由于本文件所针对的密码功能服务的范围是 “以第三方运营服务的方式提供密码功能”，因而，服务提供方与相关方之间通常会涉及承诺与认证问题。

在提供服务之前，服务提供方应保证其服务通过了国家法规所规定的认证。认证活动通常会对服务分级、分类，对其服务能力、服务水平、服务质量进行检测与评估。若通过某个类别和级别的认证，服务应仅向其许可的类别和级别业务或用户提供服务。

在提供服务时，需要服务提供方向相关方声明其服务水平、服务能力以及服务安全性,作为对使用方的承诺,服务方应保证能够按照承诺履行其责任。对于密码功能服务，又需要重点说明对密钥的安全管理、密码功能的正确性以及服务过程的可追溯方面的承诺。服务方应承诺保证用户的密钥仅可由其掌握、使用或授权使用，保证密码功能是其发起和授权进行的，保证可根据用户操作的完整过程确认服务的安全可信。

5. 密码服务相关标准化情况

5.1.国际密码服务相关标准化情况

国外的密码服务发展比较先进的区域主要是美国和欧盟国家，NIST、ETSI、ISO、IETF、WebTrust 等标准组织或行业典型联盟组织发布了一系列密码服务相关的标准要求。

5.1.1.欧盟

欧盟早期在密码服务方面的发展主要是围绕电子签名服务， 1999 年颁布了《电子签名统一法律框架指令》（Directive 1999/93/EC），并于 2014 年颁布了欧盟“新电子签名与信任服务法规”（regulation (EU) No 910/2014）（俗称 eIDAS）是 1999 年 Directive 1999/93/EC 的替代，从政策层面、基础设施层面、适用层面等方面规范了电子身份的认证路径、电子签名效力、保护拥有者隐私权益。欧洲标准化委员会（CEN，Comité Européen de Normalisation）和欧洲电信标准协会（ETSI，European Telecommunications Standards Institute）制定和发布了包括电子签名生成与验证标准、签名生成相关设备标准、密码算法套件标准、签名相关服务标准、信任应用服务供应商标准、信任服务状态列表供应商标准等方面的电子签名标准要求，构建了完整的电子签名标准体系。

电子签名服务之外，ETSI 还发布了关于量子密码加密、量子密钥分发、隐私保护、电子证据保全以及移动互联网、物联网、云服务的密码应用要求等方面的一系列服务标准。此外，德国也针对加密服务供应商提出了通用保护标准要求。

表 5-1 欧盟 ETSI 电子签名服务相关标准

序号	类别	主要标准及内容
1	签名产生与验证标准类	EN 319 122 CAdES 加密信息语法格式签名 EN 319 132 XML 格式签名 EN 319 142 PDF 格式签名等多种格式数字签名
2	签名生成及相关设备类	EN 419.212 电子身份标识、鉴别与信任服务安全模块接口

		CEN/TS 419.221 信任服务提供商密码模块保护概要 TS 119432 远程电子签名生成协议 EN 419.211 签名生成设备保护概要 EN 419.241 服务端签名的信任服务系统 EN 419.251 身份鉴别设备的安全要求等
3	密码算法集标准类	TS 119 312 密码算法套件
4	支持签名及相关服务的信任服务提供商标准类	EN 319 412 证书概要 EN 319 411 证书服务商安全要求 EN 319 421 时间戳服务商安全要求 支持 AdES 的服务商签名产生协议 支持 AdES 的服务商验签协议
5	信任应用服务提供商标准类	SR 019 510 长期数据保存服务 EN 319 401 信任服务提供商通用政策要求 EN 319 522 电子挂号递送服务、电子挂号邮件服务 EN 319 403-1 信任服务提供商符合性评估
6	信任服务状态列表提供商标准类	TS 119 612 信任服务列表提供商安全性要求、信任列表、测试规范等

表 5-2 欧盟 ETSI 其它密码服务相关标准

序号	类别	主要标准及内容
1	量子密码加密	TR 103619 量子安全的迁移策略和建议 TR 103618 基于量子安全的分层身份加密
2	量子密钥分发	TS 103744 量子安全混合密钥交换 TR 103570 量子安全密钥交换 GS QKD 008 量子密钥交换模块安全规范
3	隐私保护	TS 103 485 隐私保护机制和验证
4	电子证据保全	TS 103 643 司法领域电子证据保全技术要求
5	物联网/车联网	TS 103645 消费者物联网的网络安全：基本要求 TR 103644 智能电表的安全性设计方案 TS 102941 智能交通系统中的安全、信任和隐私管理
6	云服务	TR 103304 移动端和云服务中的个人身份信息保护

5.1.2.美国

美国在密码服务标准制定方面进展相对缓慢，NIST 先后发布了电子签名标准、PKI 基础设施标准、加密密钥管理、安全网络交易 TLS 服务器证书管理、联邦政府应用加密标准导则等方面的标准规范。

表 5-3 美国 NIST 密码服务相关标准

序号	类别	主要标准及内容
1	密钥管理	NIST SP - 800-57 密钥管理建议，主要针对加密密钥管理
2	PKI 基础设施标准	NIST SP -800-32 公钥技术及联邦 PKI 基础架构
3	身份认证	NIST SP-800-73-2 个人身份验证接口规范 NIST SP-800-78 个人身份验证密码算法和密钥管理要求

4	电子邮件	NIST SP - 800-177 可信电子邮件

5.1.3.国际标准化组织

ISO 是标准化领域中的一个国际性非政府组织，负责大部分社会领域的标准化工作。ISO 在密码服务方面的标准化工作主要集中在基于椭圆曲线密钥交换协商协议的数字签名服务加密套件、基于椭圆曲线的密钥交换安全服务加密套件、NFC 密钥管理、量子密钥交换等方面。

IETF 是国际互联网工程任务组，是一个由为互联网技术工程及发展做出贡献的专家自发参与和管理的国际民间机构，主要负责互联网相关技术规范的研发和制定。IETF 的密码服务标准主要规范集中在网络通信中的身份认证，如 OAuth 授权管理、网络身份验证中的消息加密语法、密钥协商和交换、电子邮件身份验证、web 消息加密等，典型的如 RFC 6749 OAuth 2.0 授权框架、RFC 7521 OAuth 2.0 客户端身份验证和授权授予的断言框架等。

WebTrust 是由全球两大著名注册会计师协会 AICPA（美国注册会计师协会）和 CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。WebTrust 认证是电子认证服务行业中唯一的国际性认证标准，针对 CA 机构的电子认证服务提出了一组相关认证标准《WebTrust-认证机构的原则和标准》，对电子认证服务的安全策略、业务披露、服务标准、环境控制等明确审计要求，面向的服务范围包括 SSL/TLS 基线、代码签名、扩展验证签名等。

5.2.我国密码服务相关标准化情况

5.2.1.国家标准

在国内，密码服务尚未形成界限明晰的产业形态，因此也尚无直接针对密码服务的标准制定或发布。但是，与国际标准状态类似，围绕电子认证服务、电子签名服务、云计算服务的安全要求、大数据服务安全要求、密钥管理要求等形成了一系列标准。

5.2.1.1. 云服务相关标准

密码服务的组织架构和服务方式与云服务有很高的相似度，且基于云提供密码服务是当前密码服务的主要形式之一，因此，云计算服务安全相关标准对密码服务的标准化尤其有较高的借鉴意义。

云计算服务安全相关国家标准主要如下：

表 5-4 密码服务相关国家标准

序号	标准名称	主要内容
1	GB/T 31167-2014《信息安全技术 云计算服务安全指南》，修订版处于征求意见阶段	标准描述了云计算服务可能面临的主要安全风险，提出了政府部门采用云计算服务的安全管理基本要求，及云计算服务的生命周期各阶段的安全管理和技术要求。
2	GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》，修订版处于征求意见阶	标准描述了以社会化方式为特定客户提供云计算服务时，云服务商应具备的信息安全技术能力。适用于对政府部门

	段	使用的云计算服务进行安全管理，也可供重点行业和其他企事业单位使用云计算服务时参考，还适用于指导云服务商建设安全的云计算平台和提供安全的云计算服务。
3	GB/T 35279-2017 《信息安全技术 云计算安全参考架构》	标准规定了云计算服务的安全参考架构，分角色描述了应采取的安全措施、安全功能组件以及承担的安全职责。
4	GB/T 34942-2017《信息安全技术 云计算服务安全能力评估方法》	标准依据 GB/T 31168-2014 描述了规定了开展云计算服务安全能力评估的原则、实施过程以及针对各项具体安全要求进行评估的方法，适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估，或者云服务提供商开展自评估，也适用于对政府部门使用的云计算服务进行安全管理，也可供重点行业和其它企事业单位使用云计算服务时参考。
5	GB/T 36325-2018《信息技术 云计算 云服务级别协议基本要求》	标准给出了云服务级别协议的构成要素，明确了云服务级别协议的管理要求，并提供了云服务级别协议中的常用指标。
6	GB/T 36326-2018《信息技术 云计算 云服务运营通用要求》	标准给出了云服务总体描述，规定了云服务提供者在人员、流程、技术及资源方面应具备的条件和能力。

GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》定义了云服务涉及主体及安全责任边界，描述了以社会化方式为特定客户提供云计算服务时，云服务商应具备的信息安全技术能力，与 GB/T 31167-2014《信息安全技术 云计算服务安全指南》构成了云计算服务安全管理的基础标准。《安全能力要求》和《安全指南》两个配套标准在 2019 年开始重新修订，目前处于征求意见稿阶段，以下分析结合了征求意见稿的修订内容。

《安全能力要求》分为一般要求和增强要求，根据云计算平台上的信息敏感度和业务重要性的不同，云服务商应具备的安全能力也各不相同。根据云服务商在保证云计算环境中客户信息和业务的安全时应具备的基本能力，针对云服务商更进一步细化提出 11 个方面的安全能力要求，即：系统开发与供应链安全、系统与通信保护、访问控制、数据保护、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员，物理与环境保护。《安全能力要求》认为云计算环境安全性由云服务商和客户双方共同保障，根据云计算服务的不同服务模式下云服务商和客户对计算资源的控制范围，确定了各自的安全责任边界，如下图。

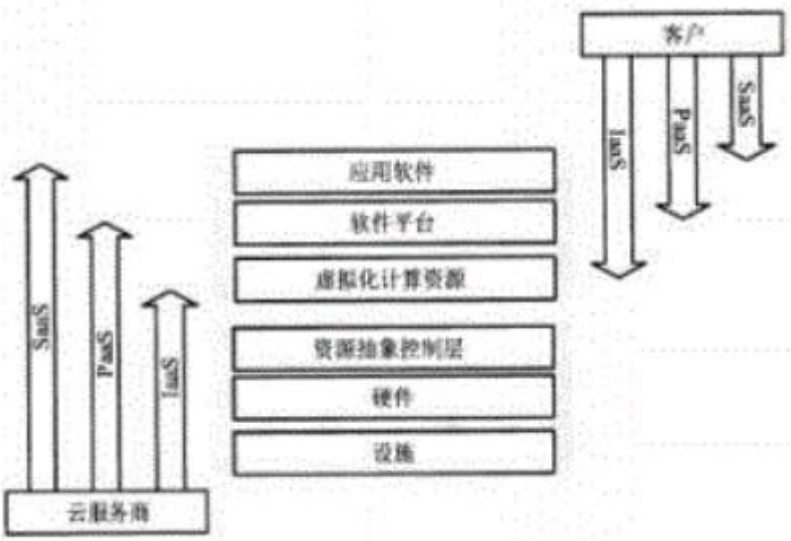

图 5-1 GB/T 31168-2014 标准定义的服务模式与控制范围的关系

GB/T 35279-2017 《信息安全技术 云计算安全参考架构》从云计算的业务执行流程出发，将云计算的相干方定义为 5 类角色：云服务商、云服务客户、云审计者、云代理者和云基础网络运营者，并明确了各类角色在云服务中所承担的责任。该标准基于云计算的特性、IaaS/PaaS/SaaS 的 3 层服务模式及 5 类角色分层次构建了云计算安全参考架构，如图 5-2 所示，各角色应分别负责各自范围内的安全能力建设。

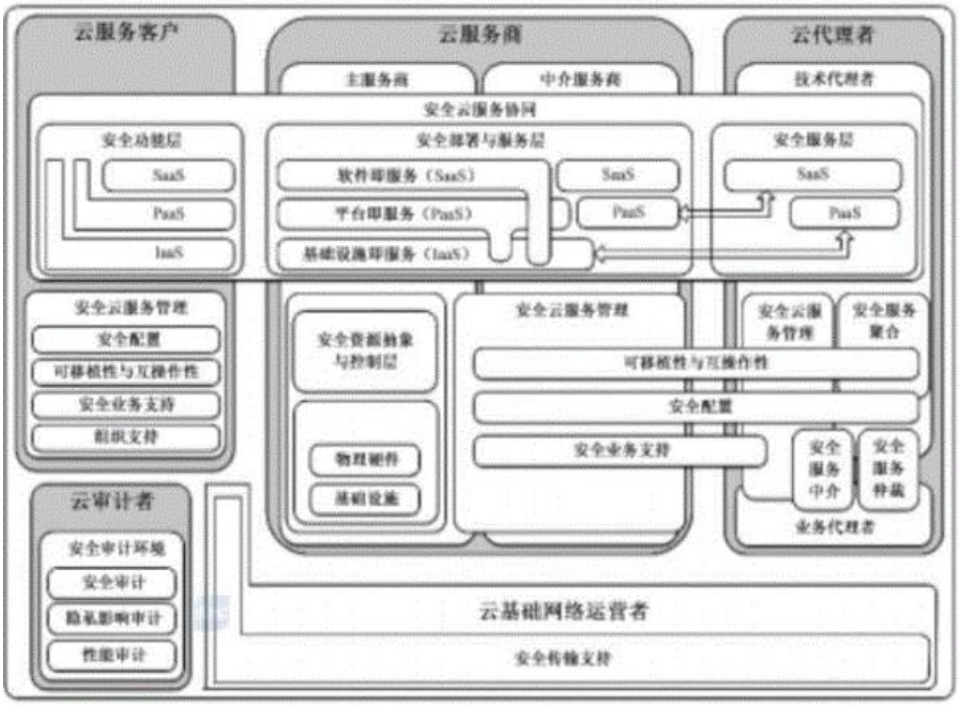

图 5-2 GB/T 35279-2017 云计算安全参考架构

GB/T 34942-2017《信息安全技术 云计算服务安全能力评估方法》与《安全能力要求》配套，规定了开展云计算服务安全能力评估的原则、评估内容、实施过程、评估证

据定义及保存，并对应 10 类的安全能力要求分别给出了相应的评估方法，如图 5-3 所示。

图 5-3 GB/T 34942-2017 云计算服务安全能力评估实施过程

GB/T 36326-2018《信息技术 云计算 云服务运营通用要求》面向 IaaS/PaaS/SaaS 不同的云服务类别，结合云服务的外部特征，抽取出共性的云服务运营要素，给出具体的运营要求，规定了云服务提供者在人员、流程、技术及资源方面应具备的条件和能力。人员要素包括人员管理、岗位结构以及人员技能；流程要素分为运营管理层和运维操作

层两个层面；技术要素包括资源池化技术、计量技术、监控技术、调度技术和多租户技术等；资源要素分为基础设施资源和支撑环境；安全要素包括安全保障技术和安全管理。

5.2.1.2. 密码服务技术相关标准

1）公钥基础设施

基于 PKI 的身份鉴别是密码服务的重要分类，目前我国还没有针对云计算环境下的基于 PKI 身份鉴别的标准，但是，我国在公钥基础设施相关标准方面发展完善，紧跟国际标准发展方向。例如，PKI 系统类的标准 GB/T 19771-2005《信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范》、GB/T 21053-2007《信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求》、GB/T 25055-2010《信息安全技术 公钥基础设施安全支撑平台技术框架》等均以国标的形式发布，电子签名方面的标准如 GB/T 15851-1995《信息技术 安全技术 带消息恢复的数字签名方案》、GB/T 17902.2-2005《信息技术 安全技术 带附录的数字签名 第 2 部分:基于身份的机制》等也已指导相关电子签名系统或应用的实施多年。

2）鉴别与授权

在鉴别与授权方面，全国信息安全标准化技术委员会已开展了相关工作，发布并实施了 GB/T 28455-2012《信息安全技术 引入可信第三方的实体鉴别及接入架构规范》、GB/T 39205-2020 《信息安全技术 轻量级鉴别与访问控制机制》、GB/T 38542-2020《信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架》、GB/T 36651-2018《信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架》、GB/T 36633-2018《信息安全技术 网络用户身份鉴别技术指南》等一系列标准，通过对国内外数字身份鉴别和授权管理技术进行研究总结，为数字身份服务建立规范。此外，还形成了 GB/T 29242-2012《信息安全技术 鉴别与授权 安全断言标记语言》和 GB/T 30280-2013 《信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言》等支撑性标准。

3）身份管理

相较于国际标准组织在身份管理方面的发展情况，我国在该方面发展相对缓慢，目前发布实施了 GB/T 31504-2015《信息安全技术 鉴别与授权 数字身份信息服务框架规范》、GB/T 32419.6-2017《信息技术 SOA 技术实现规范 第 6 部分：身份管理服务》等标准规范，针对公民身份数字化形成了系列标准规范，如 GB/T 36632-2018 《信息安全技术 公民网络电子身份标识格式规范》、GB/T 36629《信息安全技术 公民网络电子身份标识安全技术要求》等。

5.2.2.密码行业标准

近年来，在密码行业标准中，密码标准化委员会也在积极开展密码服务相关课题的研究和标准的研制，包括证书认证系统、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标准研究与制定，但还未形成体系化的密码服务标准体系。

5.2.2.1. 云密码服务相关标准

密码行业围绕基于云服务的各类密码技术、密码功能提供开展了一系列的标准制定和标准研究，目前多数仍处于研制过程中，仅有《基于云计算的电子签名服务密码标准

体系研究》、《加密通信服务体系技术要求研究》、《基于互联网的存储加密服务标准体系研究》等标准研究已经完成。

表 5-5 密码行业云密码服务相关的标准

序号	标准名称	主要内容
1	基于云的电子签名服务技术要求	标准描述了基于云的电子签名服务的密码技术需求，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	基于云的电子签名服务实施指南	标准明确了应用数字证书的场景下，基于云计算的电子签名服务的密码安全需求，提出了基于云计算的电子签名服务系统实施指南。适用于指导基于云计算的电子签名服务系统的建设和相关产品开发、检测和管理。
3	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。
4	基于互联网的存储加密服务标准体系研究	研究基于互联网的存储加密服务的现状、技术应用，并对安全需求进行分析和归类，提出了加密存储服务标准体系框架。
5	加密通信服务体系技术要求研究	研究了主流的统一通信服务的典型系统和主要协议，并分析基于互联网和云计算的托管型统一通信即服务（UCaaS）的密码应用需求，提出加密通信服务的密码应用总体框架，并从总体、基础、应用、检测和管理五个方面提炼出加密通信服务的密码应用标准体系。
6	云（服务器）密码机技术规范	标准研究在云计算环境下，密码机实现密码设备虚拟化、多租户密码资源安全隔离、密码计算资源池化、密码服务远程调用安全保护等关键特性的安全技术要求、管理和检测要求、相关协议和接口等。
7	云服务器密码机管理接口规范	标准规范了云计算管理平台与云服务器密码机的通讯接口，指导云服务器密码机产品研发，促进云服务器密码机推广，引导云加密市场健康发展。
8	云密码资源池技术要求研究	对云密码资源池管理中涉及到的安全问题进行研究，从流程、体系等角度提出密码资源池安全管理方案建议。
9	云证书认证系统密码及其相关安全技术规范	研究如何利用云计算技术优势，将云的高效、高可靠、弹性扩展等特点在证书认证系统中应用，以满足海量证书认证的高性能和扩展性需求。针对新的需求，研究解决这些安全问题的新技术。针对云 CA 的设计、建设、运行管理提出新的安全要求。
10	电子合同服务平台密码应用技术研究	研究电子合同服务技术框架，从电子合同的生命周期管理、信息结构、业务流程、系统功能等层面分析信息安全需求和挑战，从密钥管理、身份鉴别、数据传输、数据存储和取证溯源等角度研究密码技术在电子合同各个业务环节和活动中的应用功能，并提出密码技术应用和安全管理要求，为构建安全可靠的电子合同服务平台提供指引。

5.2.2.2. 身份鉴别服务相关标准

我国对国际上云计算中身份鉴别方面的主要技术和协议（如 OpenID、OAuth、FIDO）进行了采标，并根据我国实际情况进行了补充完善，形成和实施了《开放的身份鉴别框架》、《开放的第三方资源授权协议框架》，正在制定《在线快捷身份认证密码应用技术规范》。此外，还组织研究了《云计算身份鉴别服务密码标准体系》。

1）GM/T 0069-2019《开放的身份标识鉴别框架》

标准规定了建立在《开放的第三方资源授权协议框架》之上的终端用户身份鉴别协议框架，定义了框架参与实体的要求、鉴别协议流程以及关于终端用户信息的声明等。适用于终端用户访问网络应用时的身份鉴别需求，尤其适用于用户访问多种不同安全域的应用场景中，用户身份鉴别的开放、测试、评估和采购。

2）GM/T 0068-2019《开放的第三方资源授权协议框架》

标准规定了第三方资源授权协议的流程、不同类型的授权许可、协议各端点的功能要求以及系统实体之间传递消息的格式和参数要求等。适用于在互联网跨安全域应用场景中，身份鉴别与授权服务的开发、测试、评估和采购。

3）《在线快捷身份鉴别密码技术应用规范》

该标准规定了在线快捷身份鉴别协议，包括通用在线快捷身份鉴别协议和双因素在线快捷身份鉴别协议等。适用于在线快捷身份鉴别协议的开发、测试和评估。

4）GM/Y5002-2018《云计算身份鉴别服务密码标准体系》

该标准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，以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。

6. 密码功能服务安全要求和评估标准建议

6.1. 密码功能服务存在的风险

由于本文所讨论的密码功能服务通常由第三方独立建设和运营，因此，存在一系列风险，主要包括：

1）服务相关责任无法界定的风险

在密码功能服务活动中，服务提供方需要提供服务水平协议来声明关于服务的承诺，包括服务水平、服务质量、服务连续性、服务安全性等等，也可称为“服务策略”。 如果服务策略不能清晰表达关于服务能力的约定，会给应用方带来风险和隐患，甚至在出现各种问题时无法妥善界定各方责任。这就需要制订关于服务策略的框架标准，给出服务策略的基本框架。

2）服务提供方能力能否匹配承诺的风险

在明确服务策略之后，服务方需要说明其能够通过各种技术和管理手段，能够保证按照约定提供服务，也可以称为“服务业务规则声明”。如果服务技术能力不足，无法按照服务策略的约定提供服务，同样给应用方带来风险和隐患。这就需要制订服务业务规则声明标准，给出服务业务规则声明框架。

3）服务提供方安全技术实施的风险

由于本文件主要针对的密码功能服务本质上是一种技术服务，借助网络提供密码功能，保障和提升系统安全性，因此，要考虑其建设、实施和运行过程中的各个环节中的安全风险。因此，有必要提出密码功能服务的各项安全要求和指南类标准，包括基础设施安全、服务系统安全、业务接入安全以及外部技术支撑安全。

4）安全保障能力的风险

密码功能服务需要强有力的运行保障措施才能保证平稳运行、按照约定提供服务。因此，要考虑服务提供方的安全保障能力，需要针对密码功能服务的安全保障风险，制订各类安全保障标准，包括运维保障、安全管理、安全审计以及其它各种安全保障。

5）服务过程违规操作的风险

由于密码功能提供者和使用者分离，服务提供者在提供服务时的合规性至关重要。存在服务提供方的内部人员违规操作的风险。需要考虑服务提供者的操作人员是否会在用户和服务的过程中，不按照流程操作，导致出现安全问题。

例如，操作人员在用户注册服务时有可能会对部分用户不严格执行核验导致某些用户身份真实性存在问题，给服务提供者带来损失；系统管理人员有可能会对部分用户地密码资源正确设定访问控制，导致本该仅由用户控制地密码资源被无关实体使用。

密钥安全使用是密码功能服务的关键安全要求。当密钥存储在服务提供者的密码设备中，在服务提供者的网络和设备中完成密码功能，或进行密钥的管理操作时，需要考虑服务方的管理人员、操作人员或运维人员是否能够接触到用户密钥，是否能够在用户不知情的情况下使用这些密钥达到自己的目的；服务提供方是否采取了充分的技术和非技术手段，防止这种情况的发生。

因此，有必要在密码功能服务的相关技术要求类标准、运维保障类、安全管理类、安全审计类标准中，加入防范违规操作、证明操作合规性的要求。

此外，为了保障上述的各种技术措施、管理措施能够落实到位，还需要借助外部评估认证手段，检查服务建设和运行过程是否合格、正确、有效，因此需要制订各种密码功能服务评估标准，指导针对密码功能服务的评估认证活动。

6.2. 密码标准体系框架

为了积极促进密码行业的升级转型，促进商用密码在各个业务领域的广泛应用，规避密码功能服务面临的各类风险，应按照《密码法》，对密码功能服务进行认证，这就需要对密码功能服务制定一系列标准规范，作为开展测评认证的基础。

建议的标准体系如图 6-1 所示：

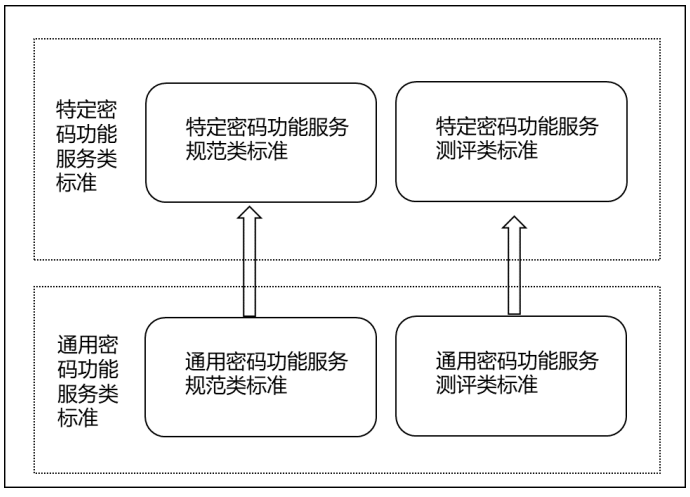

图 6-1 标准体系框架

在图 6-1 中，密码功能服务相关标准体系主要包括：通用类密码功能服务标准和特定类型的密码功能服务标准。

通用类标准包括规范类和测评类，面向一般性的密码功能服务，提出密码功能服务共性的安全技术要求和安全保障要求等规范，为各类密码功能服务提供总体架构层面的参考以及检测评估依据。

对于特定类型的密码功能服务，如果该类型密码功能服务安全要求及检测评估要求能够被通用类标准完全涵盖，可在通用类的基础上，根据不同类型密码功能服务的特殊性，针对性地定义其规范类要求和测评类标准。

密码功能服务标准体系是现有密码标准体系的一部分。密码功能服务是密码的一种特定的应用模式，是现有标准体系应用类和测评类的场景放大，因此可融入现有标准体系。因此，上述的“规范类标准”属于现有密码标准体系中“应用类”标准，而“检测评估要求”则属于密码测评类标准。提供密码功能服务过程中所需的密码基础类标准、基础设施类标准、产品类标准均与现有的标准体系框架一致。至于各种接口类标准，包括服务对外接口、服务内部各种密码系统、产品、模块等接口、协议，可采用现有的接口标准，例如 GM/T0018、GM/T0020 等，对其中特殊的接口，可在现有接口类标准的基础上进行修订补充。

6.3. 通用规范类标准

通用规范类标准针对各类密码功能服务共性的安全需求，提出适用于通用密码功能服务的安全规范。应参考密码产品的安全要求，并结合服务类标准的要求提出，明确密码功能服务安全能力表述方式，提出安全要求。

密码功能服务可根据服务特性和所面向业务领域的不同进行分类，及本章所述“特定类型的密码功能服务”，例如电子签名服务、密钥管理服务等；原则上密码功能服务安全能力可分为一级、二级、三级、四级，与网络安全等级保护、密码应用安全评估中的等级相对应，在密码功能服务标准体系中，建议针对具体类型的服务进行分级，通用密码功能服务类的标准中不描述分级。

通用要求类标准又包括密码功能服务参与方及安全职责划分、实施声明的策略框架和业务规则声明框架，以及通用的安全技术要求和安全保障要求。

6.3.1. 通用密码功能服务策略框架

服务应向相关方声明其服务策略，包括服务的适用场景、各参与方的职责、责任。服务策略框架主要用于约束和指导密码功能服务提供者针对具体服务制定服务策略。

通常情况下，服务参与方应包括务客户、服务提供方、技术提供方、服务依赖方，各参与方之间的关系见图 6-2。

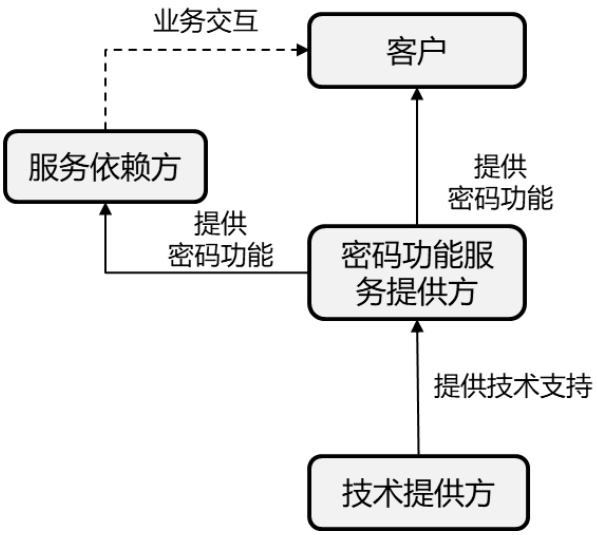

图 6-2 各参与方关系图

密码功能服务的客户通常在自身的业务过程中，委托服务提供者为其完成一个、一组或多个、多组密码功能。客户则负责密码应用安全、密码功能集成安全。

密码功能服务提供方，根据用户和业务的需要，通过技术和非技术手段，提供所需的密码能力。服务提供方负责建设密码基础设施安全和服务系统安全、服务过程安全、数据安全等，以及相应的运营、运维、管理安全，提供相应安全保障。

密码技术提供方，根据密码功能服务提供方的需求，为其提供符合法律法规以及技术标准的硬件、软件、网络设施或系统，相关的各类技术支撑，以及密码设备、密码模块、密码产品以及密码系统、密码技术，以支撑服务的正常运行。密码技术提供方负责所提供技术、硬件/软件产品、设施、设备、模块及系统的安全。

密码功能服务依赖方，依赖于用户通过服务所提供的密码功能或功能运行结果，驱动其业务过程的继续运转。密码功能服务依赖方负责与所依赖服务集成的安全。

6.3.2.通用密码业务规则声明框架

密码功能服务应支持向相关方提高其业务规则声明，说明其采用了适用、安全的技术、管理等措施，满足其服务策略中的各项声明，具备承担策略声明中描述的各项责任。业务规则声明包含服务提供方提供一般网络服务或云服务过程中的物理设施建设情况、网络部署规划、服务设计、运行维护、审计管理等等方面，同时应声明身份鉴别、密钥管理等重要内容。

6.3.3.通用密码功能服务安全技术要求

可通过《通用密码功能服务技术要求》标准提供，对各类具体服务提出要求，也可在此通用安全要求的基础上制定具体的要求。

密码功能服务可以抽象为如图 6-3 所示框架模型，利用各种基础设施以及第三方的各种支撑服务，向外提供各种密码能力、密码管理能力，并提供与服务相匹配的运营管理、安全审计和运维支撑。用户侧借助相应的各种应用程序或业务系统，使用密码功能服务提供的功能完成其业务操作。

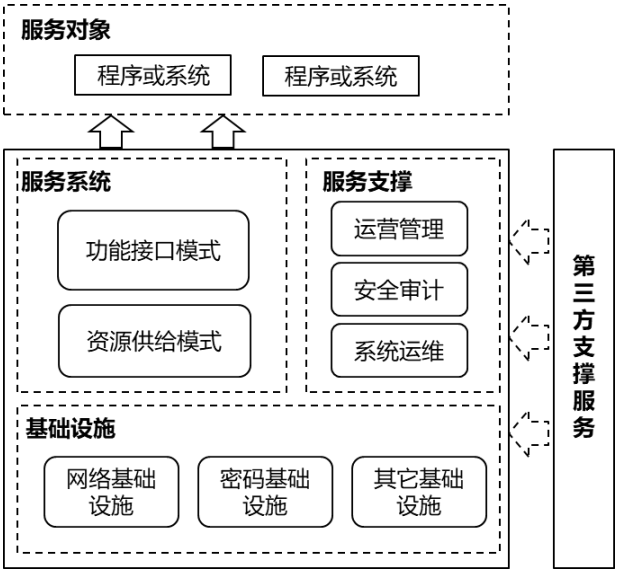

图 6-3 密码功能服务框架模型图

密码功能服务的安全技术方面可分为基础设施安全、服务系统安全、业务接入安全、外部技术支撑安全等。

6.3.3.1. 基础设施安全

基础设施安全应包括物理安全防护能力、网络安全防护能力、计算安全防护能力，也包括利用各类密码模块、密码产品和密码系统为基础设施提供的密码安全能力。

基础设施安全要求应符合 GB/T 39786 所要求的相应信息系统密码应用安全等级的需求，同时，应逐级提出为基础设施提供密码安全能力的密码模块、密码产品和密码系统的安全能力要求。

如果服务在云服务商提供的基础设施上提供，该云服务所提供的基础设施应获得“可信云服务”认证通过，其认证级别与密码功能服务级别相匹配；如果服务在自建的云架构基础设施上提供，则应进行与“可信云服务”认证级别等同的评估。

6.3.3.2. 服务系统安全

服务系统安全指密码功能服务框架模型中服务系统所应具备的安全能力，应包括密钥安全保护能力、密钥安全使用能力、密码安全计算能力、数据安全保护能力等，同时应具备服务的安全隔离能力，确保每个用户的服务以及相关数据互不影响。

服务系统安全要求应符合 GB/T 39786 所要求的应用与数据安全、密钥管理方面相应等级的要求，以保证客户信息系统密码应用的合规性。由于密码是保证信息系统安全的重要支撑，密码功能服务又通常涉及为多个信息系统提供支撑，因而，服务系统安全性要求类标准应当是标准体系的重点，对很多具体密码功能服务而言，很可能划分成多个单独的标准而出现，其中应包括密钥安全管理、密码计算安全等内容。

密钥安全管理部分应明确提出服务提供方在密钥完整生命周期内应采取何种措施保证密钥安全，要求应涵盖密钥产生、分发、存储、使用、更新、归档、撤销、备份和销毁等环节中密钥机密性、完整性和可用性几个方面。应明确托管在服务端的密钥相关的拥有者身份鉴别机制要求、访问控制以及存储使用中的隔离要求，明确密钥不能被除拥有者和授权使用者外的其他方获取和使用的要求。

密码计算安全部分应明确提出为用户提供服务以及相关过程中密码算法选用的相关要求，对选定的算法，应明确算法过程要求、算法参数选择要求，算法过程与密钥相关的要求等等。尤其标准应强调算法过程对密钥的使用，应明确提出对托管在服务端的密钥，使用时由密钥拥有者或授权使用者同意或授权，标准应明确关于密钥使用的“同意”和“授权”可以划分为哪些安全级别，这些级别分别应达到哪些安全性要求。

数据安全部分应明确提出为用户提供服务以及相关过程中数据安全的相关要求，明确在服务过程中用户数据的安全防护要求，包括数据的分级分类，数据的传输、存储、运算等环节的要求。应在标准中明确服务交互过程中，各种数据传递过程中完整性保护的要求、防篡改的要求。

安全隔离能力要求应明确提出服务的过程中，多个租户之间的隔离要求，包括密钥隔离、数据隔离等，应明确为每个租户形成隔离的密码运算空间，其隔离方式可包括密钥隔离、进程隔离、网络隔离、物理隔离等。

6.3.3.3. 业务接入安全

业务接入安全指用户应用程序或业务系统通过服务提供的编程 API 接口、通信协议或密码应用程序，连接到服务完成密码功能程。应明确提出对服务侧身份鉴别以及身份管理的要求，对于重要业务。明确要求服务侧支持基于密码的强身份认证或基于双因素的身份认证。

同时，由于密码功能服务通常会为用户侧提供安全接入能力。应对其提供的接入侧支撑能力提出明确要求，应包括接口安全、通信安全等，并明确提出安全接入或集成的相关要求。如果服务侧要求接入者使用密码技术进行接入认证，应明确对所提供接入支撑的密码合规性要求。

最后，还应明确提出对业务过程合规性要求以及第三方审计的要求，服务应能够向用户、审计系统或第三方审计机构证明在服务过程中自始至终是安全合规的。

6.3.3.4. 外部技术支撑安全

外部技术支撑安全指提供服务过程中，所采用第三方的各种服务作为技术支撑时，必须保证外部支撑技术、产品和服务本身的安全。例如，基于云的电子签名、电子合同服务可通过合法的电子认证机构（CA）为用户以及业务相关方颁发数字证书、提供各种证书服务。应明确要求服务提供方具备对第三方技术技术、产品和服务的安全性、合规性进行检测的能力。

6.3.4.服务安全保障要求

密码功能服务需通过一系列的技术手段和管理手段保障服务的持久可用和服务对象的应用安全，具体地包括服务运维保障、安全管理、安全审计以及其它的安全能力。可通过《通用密码功能服务安全保障要求》标准提供，对各类具体服务，可以此标准中的要求为准，也可在此通用安全要求的基础上制定具体的要求。

6.3.4.1. 运维保障

运维保障指对用以提供服务的软件、硬件、网络、设备等进行运行维护，以及应急保障。

根据不同等级应用系统对服务系统持久性、应急恢复的容忍度，应逐级提出应具备的保障措施和达到的保障水平。

6.3.4.2. 安全管理

安全管理指对提供服务的系统中人员、资源、过程、技术进行的运营管理，以及具备完善的安全计划、服务业务提供策略及服务水平协议或服务承诺等。针对用户自主参与度较高的服务，如用户需基于所提供服务根据自身业务需求进行进一步开发的密码功能服务，服务提供方还应提供完整的服务指导性文档，包括用户使用指南、集成开发指南等。

根据不同等级应用系统对密码功能服务安全管理的需求，应逐级提出各级服务应具备的以上要素的水平、完整度或必需具备的措施、制度、方案等，以及相应管理措施对用户的透明度。

6.3.4.3. 安全审计

安全审计指对提供密码功能服务的系统中各项活动进行全链条追踪和追溯。

密码功能服务应保证其向外提供服务过程及自身配置管理过程的全流程可追溯，相关记录保存时间和支持的追溯粒度可根据不同等级定义要求。

6.3.4.4. 其他安全保障

其它安全保障主要指所引入第三方支撑服务的安全保障要求，可以通过定义服务提供方所需提供的资质证明文件、测评报告等方式提出要求。如，对于引入第三方密码技术提供方的情况下，提供方的服务系统或产品及相关安全管理、安全保障措施应通过网络安全等级保护相应等级的测评，或通过国家密码管理局的安全性审查，符合相关的国家/行业标准要求。

6.4. 通用评估类标准

通用评估类标准是为了配合密码功能服务的各种安全要求，给出评估要求。可通过《通用密码功能服务评估要求》标准提供，各类具体服务可遵循此标准，也可在此通用参考架构的基础上制定具体某一类型服务的评估标准，作为密码评估的准则与框架，密码功能服务评估应包括定义评估原则、评估内容、评估证据和评估实施过程。

6.4.1. 评估原则

第三方评估机构在对密码功能服务进行评估时应遵循客观公正、可重用、可重复和可再现、灵活、最小影响及保密的原则。

6.4.2. 评估内容

评估内容是密码功能服务安全评估准则的核心内容。密码功能服务的安全评估包括以下内容：

针对服务对外提供的服务策略进行评估，重点是评估服务策略是否符合《通用密码功能服务策略框架》的要求，是否符合国家相关法律法规的要求，是否就用户关心的关键问题进行了承诺和告知，承诺和告知的描述是否规范化。

针对密码功能服务的《业务规则声明》进行评估，评估服务提供者为实现其服务策略中的承诺，是否采取了适当的技术手段和管理手段，论证所采用技术手段和管理手段的有效性。尤其是作为第三方服务运行时，需要评估通过网络进行交互的输入和输出数据是否满足承诺的机密性，仅对合适的实体保持可见。

针对密码功能服务的建设、运行、维护和应用的实际情况进行评估，评估其服务相关的基础设施、网络、服务系统、保障系统以及相关的管理体系是否按照《业务规则声明》来建设和运行，从而确定其承诺和指标的真实性。

针对密码功能服务在一段时间内的运行记录进行评估，评估其服务各种措施在实际运行中是有效的。

6.4.3.评估证据

所有评估活动产生的结果都应有相应的证据支持，证据应得到妥善保管，以防止篡改、泄密、损坏、丢失等有损证据的行为。评估证据包括但不限于各种文档、图片、录音、录像、实物等。

6.4.4.评估实施过程

密码功能服务安全评估的整个过程应包括评估准备、评估方案编制、现场实施、分析评估。

评估准备阶段包括接受并审核被评估方提交的密码功能服务安全计划，以及拟评估对象范围、拟提供的安全能力证据、评估进度安排等，组建相应的评估实施团队。

评估方案编制阶段包括确定评估对象、评估内容和评估方法，并准备测试用例。

现场实施包括根据评估方法审核被评估方提供的安全能力证据的有效性、真实性和完整性，评估安全控制措施的实际实施情况，形成实施结果描述。

分析评估包括分析安全能力证据，评估是否与对应安全等级要求能力匹配，是否与服务业务提供策略及服务水平协议或服务承诺服务水平协议等一致，是否存在安全风险，形成评估报告。

6.5.特定类型密码功能服务标准

特定密码功能服务在建设、设计、实施、服务、运营运维中，可遵循通用类的密码标准，也可在通用类密码功能服务标准的基础上，制定适合特定类型服务的标准。通常可包括特定类型服务的《技术要求》、《实施指南》、《测评标准》。例如，基于云的电子签名服务，目前正在制定的标准有《基于云计算的电子签名服务技术要求》、《基于云计算的电子签名服务技术实施指南》，将来还可以考虑配套编制《基于云计算的电子签名服务技术测试和评估标准》。

每一类具体的服务可依据具体服务内容，可基于通用密码功能服务的《技术要求》、《实施指南》、《测评标准》制定该类密码功能服务的《技术要求》、《实施指南》、《测评标准》，对该类服务内容进行进一步标准化，对通用要求没有涵盖到的内容，提出明确要求，同时，可针对每一类特定的密码功能服务，可根据其所面对的业务场景和安全要求、服务质量要求，考虑进行服务分级。

参考文献

[1]《中华人民共和国电子签名法》
[2]《中华人民共和国密码法》
[3]《中华人民共和国网络安全法》
[4] GB/T 31167-2014《信息安全技术　云计算服务安全指南》
[5] GB/T 31168-2014《信息安全技术　云计算服务安全能力要求》
[6] GB/T 34942-2017《信息安全技术　云计算服务安全能力评估方法》
[7] GB/T 37932-2019《信息安全技术　数据交易服务安全要求》
[8] GB/T 39786-2021《信息安全技术　信息系统密码应用基本要求》