ALIBABA CLOUD

阿里云

加密服务
产品简介

文档版本：20220627

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是加密服务 05
2.功能特性 06
3.产品优势 09
4.加密服务服务关联角色 10
5.常见术语 12

1.什么是加密服务

加密服务是基于国家密码管理局检测认证的硬件密码机，通过虚拟化技术为您提供的云上密码机服务。通过使用加密服务，您能运用多种加密算法对云上业务数据进行可靠的加解密运算，实现数据保护，同时满足数据安全方面的监管合规要求。

密码机

加密服务支持的密码机类型包括金融数据密码机EVSM（Electronic Virtual Security Module）、通用数据密码机GVSM（General Virtual Security Module）、签名验证服务器SVSM（Sign Virtual Security Module）三种规格。关于每种密码机类型支持的加密算法、接口规范等信息，请参见功能特性。

集群

加密服务提供集群服务，通过将处于同一地域不同可用区、用于相同业务的一组密码机实例关联起来，进行统一管理，为业务应用提供密码计算的高可用性、负载均衡以及横向扩展的能力。一个集群中包括一个主密码机实例与若干个非主密码机实例。集群内一个可用区的密码机实例使用同一子网。您可以通过**同步集群**的操作，将主密码机实例的数据、状态同步到其他非主密码机实例，包括但不限于密钥，应用许可。

安全审计

加密服务支持安全审计服务。通过安全审计服务，您可以将密码机实例的关键运行信息自动保存到对象存储OSS（Object Storage Service）中，并以特定的审计日志格式进行持久化储存，以满足合规和审计需求。审计日志中的信息包括但不限于：注册管理员、添加密钥、导出密钥等操作信息。

> **注意** 目前安全审计服务为Beta版本，仅提供给GVSM和EVSM使用。

应用场景

加密服务适用于以下典型场景：

- 本地机房中的密码机应用迁移到云上服务器

  当您的本地机房密码机应用迁移到云上服务器时，您可以直接使用加密服务替代本地机房密码机，实现数据的加解密、签名验签等功能，保护您的云上数据安全。

- 金融支付相关领域

  例如，在证券、银行支付结算等场景，您可以使用金融数据密码机EVSM实现PIN加密、PIN转加密等来保护金融数据安全；在网联平台支付清算等场景，您可以使用签名验证服务器SVSM实现签名验签、证书解析、证书链验证功能，确保业务的真实性、完整性和不可否认性。

- 为加密应用提供合规的加解密功能

  例如，您可以借助加密服务为阿里云专属KMS实现应用系统敏感数据的加解密，为数据库加密应用实现数据库数据的加解密，为文件加密应用实现文件存储的加解密等。

支持14天免费试用

加密服务支持14天免费试用密码机实例集群。您可以通过申请免费试用，借助密码机实例集群进行开发、测试、概念验证等。试用到期后，阿里云会自动收回所有的试用资源，如果您想继续使用加密服务，请及时付费购买。关于如何申请免费试用实例的更多信息，请参见申请14天免费试用 。

> **注意** 在免费试用期间，您可以在加密服务控制台将试用实例转换为非试用实例，当试用实例变为非试用实例后，实例中的内部数据与集群信息将会保留，您可以继续使用该实例。

相关文档

- 产品优势
- 购买加密服务

2.功能特性

本文介绍EVSM、GVSM、SVSM的功能、接口规范、加密算法和性能参考。

功能特性表

密码机类型	描述
EVSM	• 功能描述 EVSM满足《GMT 0028-2014 密码模块安全技术要求》、《GM/T0045-2016金融数据密码机技术规范》要求，同时支持国密算法的金融业务应用，和其他各类行业IC卡的应用，可用于金融支付领域，确保金融数据安全。EVSM能帮助您实现密码的管理功能，包括PIN加密、PIN转加密、MAC产生和校验、通用数据加解密、签名验证以及密钥管理等。 • 接口规范 ○ 符合的规范：PBOC 2.0、PBOC 3.0、EMV2000、GP、TSM、ESIM和交通一卡通 ○ 支持的指令集：雷卡相关和金融IC卡相关 • 加密算法 ○ 对称加密算法：支持SM1、SM4、DES、3DES、AES（支持128和256位密钥） ○ 非对称加密算法：支持SM2、RSA（密钥长度1024~2048）、ECC（NISTP192/P256、SECP192/256、BRAINPOOLP256、FRP256、X25519） ○ 摘要算法：支持SM3、SHA1、SHA256、SHA384 • 性能参考 ○ 数据通讯协议：TCP/IP ○ 最大并发连接数：256 ○ 测试数据长度32字节，性能如下： ▪ SM1加密运算性能：600次/秒，响应时间：0.006秒 ▪ SM2密钥产生性能：4,000次/秒，响应时间：0.006秒 ▪ SM2签名运算性能：3,000次/秒，响应时间：0.008秒 ▪ SM2验签运算性能：2,000次/秒，响应时间：0.026秒 ▪ RSA2048密钥产生性能：6对/秒，响应时间：8.605秒 ▪ RSA2048公钥运算性能：3,500次/秒，响应时间：0.008秒 ▪ RSA2048私钥运算性能：400次/秒，响应时间：0.018秒 ▪ SM3摘要运算性能：5,000次/秒，响应时间：0.009秒 ▪ SM4加密运算性能：5,000次/秒，响应时间：0.003秒 ▪ AES128运算性能：7,000次/秒，响应时间：0.004秒 ▪ AES256运算性能：6,000次/秒，响应时间：0.004秒

密码机类型	描述
GVSM	• 功能描述 GVSM满足《GMT 0028-2014 密码模块安全技术要求》、《GM/T 0030-2014 服务器密码机技术规范》要求，提供国际通用的密码服务接口，支持国密算法的PKI（Public Key Infrastructure）业务应用。GVSM能帮助您独立或并行为多个应用实体提供密码服务和密钥管理服务。 • 接口规范 ◦ 国密GMT0018-2012密码设备应用接口规范 ◦ PKCS#11接口规范 ◦ SunJCE接口规范 • 加密算法 ◦ ◦ 非对称加密算法：支持SM2、RSA（密钥长度1024~4096）、ECC(NIST P256、BRAINPOOLP256、FRP256) ◦ • 性能参考 ◦ 数据通讯协议：TCP/IP ◦ 最大并发连接：64 ◦ 测试数据长度32字节，性能如下： ▪ SM1加密运算性能：600次/秒，响应时间：0.006秒 ▪ SM2密钥产生性能：4,000次/秒，响应时间：0.006秒 ▪ SM2签名运算性能：3,000次/秒，响应时间：0.008秒 ▪ SM2验签运算性能：2,000次/秒，响应时间：0.026秒 ▪ RSA2048密钥产生性能：6对/秒，响应时间：8.605秒 ▪ RSA2048公钥运算性能：3,500次/秒，响应时间：0.008秒 ▪ RSA2048私钥运算性能：400次/秒，响应时间：0.018秒 ▪ SM3摘要运算性能：5000次/秒，响应时间：0.009秒 ▪ SM4加密运算性能：5000次/秒，响应时间：0.003秒 ▪ AES128运算性能：7000次/秒，响应时间：0.004秒 ▪ AES256运算性能：6000次/秒，响应时间：0.004秒

密码机类型	描述
SVSM	• 功能描述 SVSM满足《GMT 0028-2014 密码模块安全技术要求》、《GM/T 0029-2014签名验签服务器技术规范》要求，提供基于PKI体系和数字证书运算功能，包括XML、二维码、条码、电子签章、时间戳等签名验签功能和证书解析、证书链验证功能。 您可以在以下场景中使用SVSM，保证业务信息的真实性、完整性和不可否认性。 ◦ 人民银行二代支付 ◦ 网联平台支付清算 ◦ 银联无卡支付业务 ◦ 海关跨境电商 • 接口规范 ◦ 支持PKCS#1签名验证 ◦ 支持PKCS#7签名验证 ◦ 支持PKCS#7数字信封 • 加密算法 ◦ ◦ 非对称加密算法：支持SM2、RSA（密钥长度1024~4096）、ECC ◦ • 性能参考 ◦ 数据通讯协议：TCP/IP、HTTP、HTTPS ◦ 最大并发连接：1,000 ◦ 测试数据长度256字节，性能如下： ▪ SM2 PKCS#7 Attached带原文的签名运算性能：2,100次/秒，响应时间：0.009秒 ▪ SM2 PKCS#7 Attached带原文的验签运算性能：1,100次/秒，响应时间：0.018秒 ▪ SM2 PKCS#7 Detached不带原文的签名运算性能：2,200次/秒，响应时间：0.009秒 ▪ SM2 PKCS#7 Detached不带原文的验签运算性能：1,200次/秒，响应时间：0.025秒 ▪ SM2 PKCS#1 Raw裸签名运算性能：2,300次/秒，响应时间：0.006秒 ▪ SM2 PKCS#1 Raw裸验签运算性能：1,300次/秒，响应时间：0.018秒 ▪ RSA2048 PKCS#7 Attached带原文的签名运算性能：350次/秒，响应时间：0.78秒 ▪ RSA2048 PKCS#7 Attached带原文的验签运算性能：1,500次/秒，响应时间：0.025秒 ▪ RSA2048 PKCS#7 Detached不带原文的签名运算性能：330次/秒，响应时间：0.018秒 ▪ RSA2048 PKCS#7 Detached不带原文的验签运算性能：1,800次/秒，响应时间：0.025秒 ▪ RSA2048 PKCS#1 Raw裸签名运算性能：400次/秒，响应时间：0.075秒 ▪ RSA2048 PKCS#1 Raw裸验签运算性能：2,300次/秒，响应时间：0.011秒

3.产品优势

本文介绍加密服务的五大优势，包括满足监管合规要求、丰富的行业标准接口和加密算法、弹性扩展、高可用性和安全的云上加密。

满足监管合规要求

加密服务支持的密码机已通过国家密码管理局的检测认证，并且符合密码行业的技术规范，包括《GMT 0028-2014 密码模块安全技术要求》、《GM/T 0045-2016金融数据密码机技术规范》、《GM/T 0030-2014 服务器密码机技术规范》、《GM/T 0029-2014签名验签服务器技术规范》。

丰富的行业标准接口和加密算法

加密服务支持丰富的行业标准接口和加密算法。例如EVSM在支持原有金融业务安全需求的基础上，扩展了SM1、SM2、SM3、SM4国产密码算法在金融领域中的应用支持，并且符合PBOC2.0、PBOC3.0、GP等应用规范，以及建设部、交通等行业规范。

关于加密服务支持的接口规范和加密算法的更多信息，请参见 功能特性。

弹性扩展

在使用加密服务时，您可以根据实际情况，灵活地调整部署购买的密码机的数量，通过负载均衡来满足不同的加解密运算要求。

集群高可用性

加密服务支持集群管理的功能。您可以将购买的多个密码机添加到一个集群中，快速增加密码机的高可用性，降低业务中断及核心数据丢失风险。

便捷的云上使用

借助加密服务，您可以将购买的密码机部署在您指定的VPC专有网络中，通过指定的私网IP地址进行安全管理和调用，便捷地与云服务器上的业务配合使用。

4.加密服务服务关联角色

本文介绍加密服务服务关联角色AliyunServiceRoleForHSMLogDelivery的应用场景、权限以及如何删除该角色。

AliyunServiceRoleForHSMLogDelivery应用场景

加密服务提供的安全审计服务需要获取对象存储OSS（Object Storage Service）云服务的资源的访问权限，故加密服务设置了服务关联角色AliyunServiceRoleForHSMLogDelivery。关于服务关联角色的更多信息，请参见服务关联角色。

AliyunServiceRoleForHSMLogDelivery权限说明

AliyunServiceRoleForHSMLogDelivery的权限包括：获取OSS Bucket列表及指定路径的读写权限。

关于AliyunServiceRoleForHSMLogDeliver的权限的详细信息，请参考如下内容：

```
{
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "logdelivery.hsm.aliyuncs.com"
        }
      }
    },
    {
      "Action": [
        "oss:GetObject",
        "oss:PutObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "acs:oss:*:*:*/aliyun-hsm-audit-log",
        "acs:oss:*:*:*/aliyun-hsm-audit-log/*"
      ]
    },
    {
      "Action": [
        "oss:ListBuckets"
      ],
      "Effect": "Allow",
      "Resource": [
        "acs:oss:*:*:*"
      ]
    }
```

删除服务关联角色

如果您不再使用加密服务中的安全审计服务，您可以删除AliyunServiceRoleForHSMLogDelivery。在删除该角色前，需要先确保当前阿里云账号下没有正在使用的密码机实例，并关闭该账号下的安全审计服务，然后在RAM控制台删除该服务关联角色。如果当前阿里云账号的密码机实例已投入使用，则您不能删除AliyunServiceRoleForHSMLogDelivery。

关于关闭安全审计服务的具体操作，请参见 关闭安全审计服务 。关于删除服务关联角色的具体操作，请参见 删除服务关联角色。

5.常见术语

本文介绍加密服务相关的术语。

密码机实例

密码机实例是密码机的硬件加密模块虚拟化形成的资源。密码机实例与硬件加密模块具有同样的合规性，可以实现加密服务的所有功能，具备对数据的加解密运算能力。

身份认证卡

身份认证卡（又称USB Key）是加密服务的唯一身份识别信息，可以配合密码机的客户端管理工具管理密钥。