ALIBABA CLOUD

阿里云

加密服务
产品简介

文档版本：20200820

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

加密服务CloudHSM（Alibaba Cloud Data Encryption Service）即云密码机，是云上的加密解决方案。加密服务使用经国家密码管理局检测认证的硬件密码机作为服务底层，通过虚拟化技术，帮助您满足数据安全方面的监管合规要求，保护云上业务数据隐私。

借助加密服务，您能够对密钥进行安全可靠的管理，您也能使用多种加密算法来对数据进行可靠的加解密运算。

当您使用加密服务实例时，可以执行各种加密任务：

- 生成、存储、导入、导出、管理加密密钥，包括对称密钥和非对称密钥对。
- 使用对称和非对称算法来加密和解密数据。
- 使用加密哈希函数来计算消息摘要和基于哈希的消息身份验证代码（HMAC）。
- 对数据进行加密签名并验证签名。

如果您已经准备好开始使用加密服务，请参见概述。如果您需要了解有关使用加密服务可以完成的任务的更多信息，请参见应用场景。

2.产品架构

本文档主要介绍了加密服务的产品架构。

- 加密服务实例的租用

  您可以在加密服务资源池中选择一个未被租用的加密服务实例。

- 加密服务实例的映射

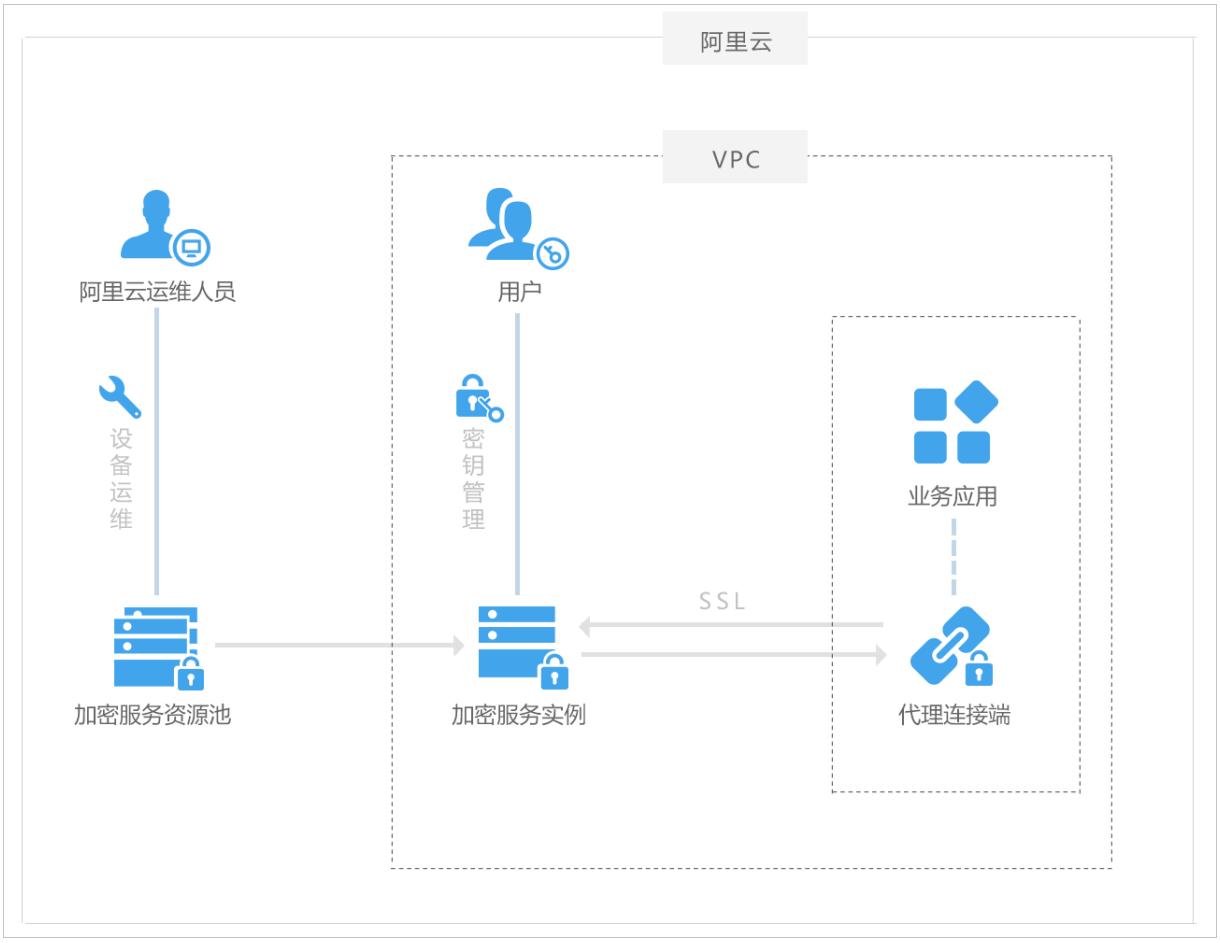
  把加密服务实例映射到您指定的VPC网络中，并给您分配指定的VPC私网IP地址。

- 加密服务实例管理

  您可以通过VPN或专线接入VPC，使用USB Key对加密服务实例进行初始化并管理密钥。

- 加解密调用

  您的业务应用通过代理连接端调用加密服务实例。代理连接端提供SSL加密通讯和负载均衡功能。



3.功能特性

加密机根据功能特性不同，分为金融数据密码机EVSM、通用数据密码机GVSM。本文档介绍了金融数据密码机EVSM和通用服务器密码机GVSM的功能特性。

金融数据密码机EVSM的功能特性

江南天安金融数据VSM（EVSM）是以现代密码技术为核心的主机安全模块，具有自主密钥管理机制，能将密码运算过程封装在内部完成，为业务系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加密、签名的产生和验证等，保证业务数据产生、传输、接收、处理整个过程的安全性、有效性、完整性、不可抵赖性。

金融数据密码机EVSM满足《GM/T0045金融数据密码机技术规范》要求，可用于金融支付领域，确保金融数据安全，并符合金融磁条卡、IC卡业务特点的，主要实现PIN加密、PIN转加密、MAC产生和校验、数据加解密、签名验证以及密钥管理等密码管理功能的云加密实例。

支持的加密算法：

算法类型	说明
对称密码算法	支持SM1、SM4、DES、3DES、AES（支持128、256位密钥）
非对称密码算法	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

支持的基础服务功能：

- 支持雷卡相关指令集
- 支持金融IC卡相关指令集
- 支持国密算法的金融业务应用
- 支持PBOC 2.0和3.0规范
- 支持EMV规范的应用
- 支持GP规范、TSM规范、ESIM规范的应用
- 支持交通一卡通规范的应用
- 支持其它各类行业IC卡的应用
- 支持通用数据加解密、签名验签、摘要计算、密钥管理等服务功能

性能参数：

- 数据通讯协议：TCP/IP
- 最大并发连接数：64
- SM1加密运算性能：600次/秒
- SM2密钥产生性能：4000次/秒
- SM2签名运算性能：3000次/秒
- SM2验签运算性能：2000次/秒
- RSA2048密钥产生性能：10对/秒
- RSA2048公钥运算性能：3500次/秒

- RSA2048私钥运算性能：400次/秒
- SM3摘要运算性能：5000次/秒
- SM4加密运算性能：5000次/秒
- AES128运算性能：7000次/秒
- AES256运算性能：6000次/秒

通用服务器密码机GVSM的功能特性

通用数据密码机GVSM是运行于SJJ1528云服务器密码机内的类同服务器密码机系列产品的VSM（虚拟密码模块）。具有自主密钥管理机制，将密码运算过程封装在内部完成，为业务系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加密、签名的产生和验证等，保证业务数据产生、传输、接收、处理整个过程的安全性、有效性、完整性、不可抵赖性。

通用服务器密码机GVSM满足《GM/T0030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，能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的云加密实例。

支持的加密算法：

算法类型	说明
对称密码算法	支持SM1、SM4、DES、3DES、AES（支持128、256位密钥）
非对称密码算法	支持SM2、RSA（密钥长度1024~4096）、ECC（NISTP256、BRAINPOOLP256、FRP256）
摘要算法	支持SM3、SHA1、SHA256、SHA384

支持的基础服务功能：

- 支持国密GMT-0018-密码设备应用接口规范
- 支持PKCS#11接口规范
- 支持SUNJCE接口规范
- 支持国密算法的PKI业务应用

性能参数：

- 数据通讯协议：TCP/IP
- 最大并发连接数：64
- SM1加密运算性能：600次/秒
- SM2密钥产生性能：4000次/秒
- SM2签名运算性能：3000次/秒
- SM2验签运算性能：2000次/秒
- RSA2048密钥产生性能：10对/秒
- RSA2048公钥运算性能：3500次/秒
- RSA2048私钥运算性能：400次/秒
- SM3摘要运算性能：5000次/秒
- SM4加密运算性能：5000次/秒
- AES128运算性能：7000次/秒
- AES256运算性能：6000次/秒

4.产品优势

加密服务产品包含以下优势。

安全的密钥存储

使用硬件密码机保护客户密钥，且密码机符合国家密码管理局（GM/T 0029-2014）和中国人民银行（PBOC1.0/2.0/3.0）等多项要求。

安全的密钥管理

设备管理和密钥管理权限分离。阿里云只能管理密码机硬件设备，主要包括监控设备可用性指标、开通和停止服务等。密钥完全由您管理，阿里云没有任何方法可以获取您的密钥。密钥管理体系通过国家密码管理局的安全检测和认证。

方便的云上使用

加密服务实例部署在您的VPC专有网络中，通过您指定的私网IP地址进行管理和调用，很方便地与云服务器实例上的业务配合使用。

弹性扩展

您可以根据实际情况，灵活地调整租用的加密服务实例数量，通过负载均衡来满足不同的加解密运算要求。

满足监管合规要求

加密服务使用通过国家密码管理局检测认证的密码机，让您安全地生成、存储和管理用于数据加密的加密密钥，在不影响应用程序性能的情况下符合严格的密钥管理要求。

5.应用场景

加密服务适用于阿里云上所有用户，主要使用场景包括支持SSL加密流量安全卸载、保护证书颁发机构 (CA) 的私有密钥、敏感数据保护、Oracle数据库加密。

对SSL加密流量进行安全卸载

应用领域：HTTPS网站、CDN产品等。

面临的挑战：

- SSL卸载会消耗大量的Web服务器资源，降低Web服务器的可用性，影响Web服务器的使用效率。
- Web服务部署在云服务器上，SSL证书的私钥文件存储在虚拟硬盘上，存在泄漏私钥文件的风险。
- Web应用传输高价值的敏感数据时，需要严格控制和保护SSL证书的私钥，保护加密数据的安全和隐私。
- 需要支持国密算法，或者需要对SSL证书的私钥文件进行完全的控制。

解决方案：

- 通过加密服务生成安全存储私钥。
- 为网关或Web服务器提供支持国密和国际卸载的密码套件TaSSL。

为您带来的价值：

- 降低Web服务器的性能压力，提高客户端的访问速度。
- 您可以完全控制SSL证书私钥文件的使用，加强了私钥文件的保护，提升了Web服务的安全性。
- 支持国密算法SSL流量卸载，满足国密应用要求。具体请参见基于加密服务的SSL安全卸载。

PKI和CA应用

应用领域：PKI和CA领域、金融和政务等领域。

面临的挑战：PKI和CA系统需要满足安全合规要求，采用合规的密码模块。

解决方案：

- 通过VSM提供密钥生成和管理功能。
- 通过VSM为CA、RA、KMC等模块提供各种密码运算服务。
- PKI和CA签发数字证书，应用到各种身份认证、抗抵赖、数字签名等场景。
- VSM支持标准的SDF、PKCS11、JCE接口。

为您带来的价值： 保证了您的私有密钥符合监管合规要求，从而保障了业务的安全性。

为Oracle数据库启用透明数据加密 (TDE)

应用领域：Oracle数据库加密。

面临的挑战：Oracle数据库支持透明数据加密（TDE）、列加密和表空间加密，加密密钥的产生和存储的安全性需要受到保护。

解决方案：

- 通过VSM产生数据加密密钥并进行密钥分发，并进行主密钥生命周期的管理。
- 数据加解密在本地完成（软算法或者对接VSM）。

为您带来的价值：

- 启用透明数据加密 (TDE)可以解决与安全相关的法规遵从性问题。

- 数据库用户和应用程序透明地解密表中的数据。
- 数据透明地解密为数据库用户和应用程序。
- 数据库用户或应用程序不需要管理加密密钥。
- 作为安全管理员，确保敏感数据是安全的，以防存储介质或数据文件被盗。

敏感数据加密

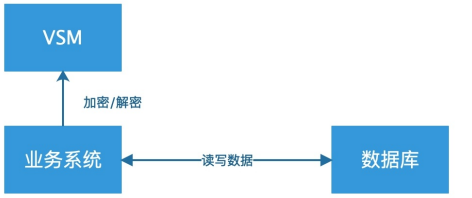
应用领域：政务、电商、门户、WEB站点等各类包含大量个人敏感信息的系统应用中。

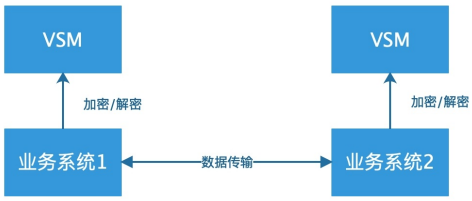
面临的挑战：

- 黑客攻破网络，拖库导致数据泄露风险。
- 内部非授权用户非法访问，篡改数据、泄露数据风险。

解决方案：

- 数据在数据库存储时通过VSM加密后存储，保证数据的机密性。
- 数据在数据库存储时通过VSM进行完整性校验，保证数据的完整性。
- 加密密钥采用VSM生成和管理，保证了加密密钥的安全性。具体请参见敏感信息加密。





为您带来的价值：

- 杜绝了明文数据泄露、被篡改的风险。
- 提升了系统的健壮性。

6.常见术语

本文档介绍加密服务相关的术语解释。

加密服务实例

硬件密码机虚拟化形成的资源实例，实现硬件密码机的所有功能，具备一定量的加解密运算能力。

身份卡

USB Key，加密服务实例的唯一身份识别，配合加密服务实例的管理客户端软件对加密服务实例中的密钥进行管理。

代理连接端

配合加密服务实例使用的业务代理软件，对通讯内容提供SSL加密，同时也能在多个加密服务实例之间实现负载均衡功能。

TaSSL

TaSSL是由江南天安公司推出的天安版国密OpenSSL，它是一套开放源代码的安全套接字层密码学基础库，包括主要的密码算法、常用的密钥、证书的封装管理以及SSL/TLS协议，并提供丰富的API接口。

7.联系我们

如果在使用加密服务的过程中，有任何疑问，请您通过客服联系阿里云。您也可以加入钉钉用户群（钉钉群号：31926331）与阿里云加密服务安全专家进行沟通。

请您使用钉钉扫描下方的二维码加入钉钉用户群。