# 加密服务

## 产品简介

# 产品简介

加密服务(Alibaba Cloud Data Encryption Service)是云上的加密解决方案。服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的监管合规要求，保护云上业务数据的隐私性要求。借助加密服务，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

## 功能描述

### 数据加密

数据是企业的核心资产，每个企业都有自己的核心敏感数据。包括企业自身的敏感数据，如合同、交易、流水等，企业用户的敏感数据，如身份证、银行卡等。这些数据都需要加密服务来保护不会被他人获取。

### 加密算法支持

全面支持国产算法以及部分国际通用密码算法，满足用户各种加密算法需求。

对称密码算法：支持SM1、SM4、DES、3DES、AES

非对称密码算法：支持SM2、RSA（1024-2048）

摘要算法：支持SM3、SHA1、SHA256、SHA384

### 金融行业支持

符合中国人民银行标准和规范的金融行业定制加密需求，全面支持金融支付领域的加解密需求

PIN码的产生/加密/转加密/验证等

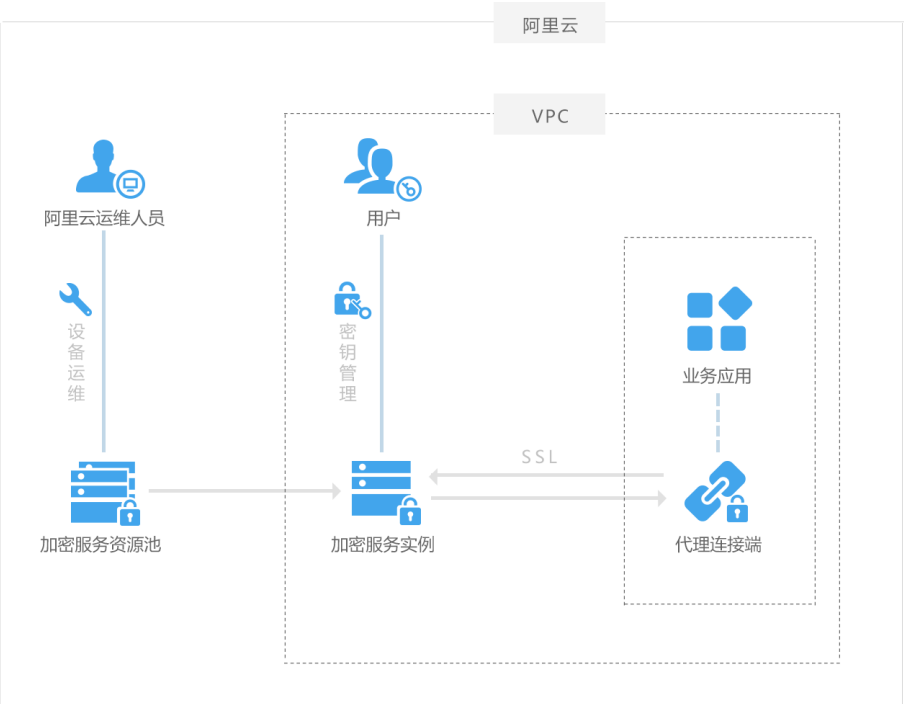
ARQC的生成/验证、脚本加密、脚本MAC等

MAC1计算及验证、MAC2计算及验证、TAC验证等

外部认证、更新密钥、内部认证等

敏感数据加密、转加密、报文MAC计算及验证等

CVV/CVN产生及校验、PVV/PVN的产生及校验




## 1.加密服务实例的租用

在加密服务资源池中选择一个未被租用的加密服务实例分配给客户。

## 2.加密服务实例的映射

把加密服务实例映射到客户指定的VPC网络中，并分配客户指定的VPC私网IP地址。

## 3.加密服务实例管理

客户通过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。

## 4.加解密调用

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。

## 加密服务支持的加密算法

| 加密算法分类 | 加密算法 |
| --- | --- |
| 对称密码算法 | 支持SM1、SM4、DES、3DES、AES |
| 非对称密码算法 | 支持SM2、RSA(1024-2048) |
| 摘要算法 | 支持SM3、SHA1、SHA256、SHA384 |

# 加密服务产品优势

## 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、停止服务等。密钥完全由客户管理，阿里云没有任何方法可以获取客户密钥。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客户的 VPC 专有网络中，通过客户指定的私网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，让客户安全地生成、存储和管理用于数据加密的加密密钥，在不牺牲应用程序性能的情况下符合严格的密钥管理要求。

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

金融业务系统的加密服务使用场景主要包括银行卡号，身份证，PIN码等敏感信息的存储。

政务系统的加密服务使用场景主要包括涉密业务的敏感信息存储。

企业财务系统的加密服务使用场景主要包括合同，财务等敏感信息存储。

# 加密服务发展历史

## 产品公测

2015年12月22日，加密服务开始公测。

# 产品商业化

2016年3月16日，加密服务开始正式商业化。

# 加密服务名词解释

## 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。