加密服务

用户指南

用户指南

加密服务使用手册

一、产品使用步骤

1.密钥管理步骤

1.1 笔记本或个人电脑安装加密服务实例配套的管理客户端。

1.2 使用VPN将笔记本或个人电脑拨入您的专有网络（VPC网络）。

1.3 通过管理客户端连接上加密服务实例。

1.4 插入身份卡完成第一次登陆，激活身份卡。

1.5 修改登陆密码。

1.6 开始密钥管理（密钥的创建、导入、备份以及连接授权、访问控制等等）。

1.7 建议您输入密钥以后，及时将密钥备份到您手里的密钥备份卡中。推荐密钥备份卡使用5选3的模式，即同步制作5张密钥备份卡，有其中3张时即可恢复出完整密钥。

1.8 所有的密钥管理都必须依赖身份认证卡（USB key），请务必妥善保管身份卡。如身份认证卡（USB key）丢失，阿里云也无法恢复。

2.安装代理连接端

2.1 代理连接端提供的是通讯链路上SSL加密功能和多个实例之间的负载均衡功能。

2.2 按照代理连接端安装说明，部署代理端。

2.3 通过密钥管理客户端，对代理端进行授权。

2.4 授权通过，加密实例会对代理端下发SSL证书。后续的所有通讯都会进行SSL加密。

2.5 代理端可以配置多个加密服务实例，实现负载均衡功能。

加密服务功能介绍

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

加密服务产品限制

使用限制

1.加密服务实例需要配合阿里云专有网络（VPC网络）一起使用。加密服务实例在购买后，需要在云盾控制台中配置VPC网络、VPC交换机、私有IP地址，才能正常使用。2.私有IP地址末位253-255为网络保留地址，无法进行分配（如强行分配会提示分配失败）。3.加密服务实例出于安全性的考虑，不对公网提供服务，您需要先通过VPN将管理设备拨入到VPC网络中，才能对加密服务实例进行管理。