云加密机

产品简介

腾讯云

文档目录

产品简介
- 产品概述
- 产品功能
- 产品优势
- 应用场景

产品简介
产品概述

最近更新时间：2022-07-06 17:23:55

云加密机（Cloud Hardware Security Module，CloudHSM）是基于国密局认证的物理加密机，利用虚拟化技术，提供弹性、高可用、高性能的数据加密和密钥管理等云上数据安全服务，满足金融，互联网等行业加密需求，保障用户的业务数据隐私安全。

数据安全

服务底层使用硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的合规要求，保护云上业务数据的隐私。

弹性扩展

采用云服务密码机的虚拟化技术，可根据用户业务需要，弹性的增加和缩减后端的虚拟实例，从容应对业务高峰压力，节约资源和成本。

接口兼容

采用硬件芯片实现各类密码算法，提供与实体密码设备相同的功能与接口，可兼容传统应用并方便其向云端迁移。

方便云上使用

便于和您腾讯公有云上的业务和产品结合，在同一个 VPC 网络下，实现高效的数据加密和密钥管理。

产品功能

最近更新时间：2022-07-06 17:23:59

金融数据密码机 EVSM

金融数据密码机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，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。

加密算法

- **对称算法**：SM1/SM4/DES/3DES/AES128/AES256
- **非对称算法**：SM2、RSA(1024-2048)、ECC(NIST P192/P256、SECP192/256、BRAINPOOLP256、FRP256、X25519)
- **摘要算法**：SM3、SHA1/SHA256/SHA384

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 PBOC2.0/3.0 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

- 数据通讯协议：TCP/IP
- 最大并发连接：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

通用服务器密码机提供通用的密码服务接口，能独立或并行的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。

加密算法

- **对称算法**：SM1/SM4/DES/3DES/AES128/AES256
- **非对称算法**：SM2、RSA(1024-4096)、ECC(NIST P256、BRAINPOOLP256、FRP256)
- **摘要算法**：SM3、SHA1/SHA256/SHA384

基础服务功能

- 支持国密 GM/T 0018 密码设备应用接口规范。
- 支持 PKCS#11 接口规范。
- 支持 SUN JCE 接口规范。
- 支持国密算法的 PKI 业务应用。
- 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

- 数据通讯协议：TCP/IP
- 最大并发连接：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

签名验证服务器 SVSM

签名验证服务器提供基于 PKI 体系和数字证书的数字签名、验证签名等运算功能，可以保护关键业务信息的真实性、完整性和不可否认性。

加密算法

- **对称算法**：SM1/SM4/DES/3DES/AES128/AES256
- **非对称算法**：SM2、RSA(1024-4096)、ECC
- **摘要算法**：SM3、SHA1/SHA256/SHA384

基础服务功能

- 支持 PKCS#1 签名验证。
- 支持 PKCS#7 签名验证。
- 支持 PKCS#7 数字信封。
- 支持 xml、二维码、条码、电子签章、时间戳等签名验签功能。
- 自持基本对称加解密和摘要运算功能。
- 支持证书解析、证书链验证等功能。
- 支持人民银行二代支付类相关业务接口。
- 支持网联平台支付清算相关业务接口。
- 支持银联无卡支付业务相关接口。
- 支持海关跨境电商相关业务接口。

性能

- 数据通讯协议：HTTP
- SM2 Attach 签名运算性能：2100次/秒
- SM2 Attach 验签运算性能：1100次/秒
- SM2 Dettach 签名运算性能：2200次/秒
- SM2 Dettach 验签运算性能：1200次/秒
- SM2 Raw 签名运算性能：2300次/秒
- SM2 Raw 验签运算性能：1300次/秒
- RSA2048 Attach 签名运算性能：350次/秒
- RSA2048 Attach 验签运算性能：1500次/秒
- RSA2048 Dettach 签名运算性能：330次/秒
- RSA2048Dettach 验签运算性能：1800次/秒
- RSA2048 Raw 签名运算性能：400次/秒
- RSA2048 Raw 验签运算性能：2300次/秒

托管物理密码机 GHSM

通用服务器密码机 CryptoEngine：提供高适配性的密码服务接口，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加密实例。

加密算法

- **对称算法：**SM4/DES/3DES/AES128/AES192/AES256
- **非对称算法：**SM2、RSA(1024-4096)、ECC(P/K/B 233-571曲线、BrainpoolP系列曲线、Curve25519、Curve448)
- **摘要算法：**SM3、SHA1、SHA224/SHA256/SHA384/SHA512、SHA3-224/SHA3-256/SHA3-384/SHA3-512

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 SUN JCE 接口规范。
- 支持国密算法的PKI业务应用。

性能

- 数据通讯协议：TCP/IP
- 最大并发连接：2048
- 测试128连接并发性能如下：
- SM2密钥产生性能：144000次/秒
- SM2签名运算（32字节）性能：11700次/秒
- SM2验签运算（32字节）性能：23400次/秒
- RSA2048密钥产生性能：48对/秒
- RSA2048公钥运算性能：72000次/秒
- RSA2048私钥运算性能：4000次/秒
- SM3摘要运算（4096字节）性能：22400次/秒
- SM4加密运算（16字节）性能：350000次/秒
- AES128运算（16字节）性能：350000次/秒
- AES256运算（16字节）性能：350000次/秒

产品优势

最近更新时间：2022-07-06 17:24:07

云加密机拥有以下产品优势：

- **高安全性加密算法**
- 对称加密算法：SM1、SM4、DES、AES。
- 非对称加密算法：SM2、RSA（1024-2048）ECC 等算法。
- 摘要算法：SM3、MD5、SHA1、SHA256、SHA384 等算法。
- **权责分离**
  云加密机提供权责分离的管理体系和严格的身份认证方法，保障权限安全可控；您可完全把控密钥管理的权限和应用访问的权限，除被授权人或者授权应用外，其它人或者其它应用都无法使用密钥和数据。
- **弹性扩展**
  采用云服务密码机的虚拟化技术，可根据您的业务需要弹性增加和缩减后端的虚拟实例，从容应对业务高峰压力，节约资源和成本。
- **便捷管理**
  提供与实体密码设备相同的功能与接口，可完全兼容传统应用并方便其向云端迁移。数据加密实例与VPC策略绑定，可以方便和您腾讯云上的业务结合，实现可靠、高效的数据加密和密钥管理服务。

应用场景

最近更新时间：2022-07-06 17:24:10

云加密机可应用于以下场景：

敏感数据加密

- **面临挑战**
  - 黑客攻破网络，拖库导致数据泄露风险。
  - 用户非法访问，篡改数据、泄露数据风险。
- **解决方案**
  - 数据在数据库存储是通过 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 生成和管理的方式，保证了加密密钥的安全性。
- **客户价值**
  降低明文数据被泄露和篡改的风险，提升了系统的健壮性和客户价值。
- **应用领域**
  可应用于电商、门户、Web 站点等需要对数据加密保护的系统应用。

金融支付加密

- **面临挑战**
  - 支付业务需要硬件密码设备保证系统安全性。
  - 支付业务需要确保支付数据在传输、存储过程中完整性、保密性，支付身份认证和支付过程的不可否认性等。
- **解决方案**
  - 通过 VSM 生成和管理支付终端、支付渠道的主密钥和工作密钥。
  - 通过 VSM 提供完整周期的 PIN 加密传输和验证，传输报文的完整验证。
  - 通过 VSM 提供支付介质或者用户身份的认证。
- **客户价值**
  符合业务需求，保障业务的安全性。
- **应用领域**
  可应用于 POS 收单、互联网支付、预付费卡支付等各类第三方支付应用中。

基于加密服务实现 SSL 卸载

- **面临挑战**
  - Web 应用服务器的证书和私钥缺乏保护，面临安全风险。

- 安全要求高，需要支持 SSL 卸载能力。

- **解决方案**
  - 通过 VSM 生成和管理服务器的私钥和证书。
  - 通过 VSM 提供 SSL 卸载的能力。
- **客户价值**
  保障服务器私钥和证书的安全性。
- **应用领域**
  - 云上的等保三级系统、需要做密码测评的所有系统。
  - 适合于银行、保险、企业等多领域。

企业信息系统加密

- **面临挑战**
  - 企业各类信息系统存有大量企业资产、财务报表、人员信息等敏感数据，存在泄漏风险。
  - 企业各类信息系统存有大量用户信息，需要认证企业用户身份和权限。
- **解决方案**
  - 通过 VSM 生成和管理各类型企业信息系统所需的对称和非对称密钥管理。
  - 通过 VSM 提供用户身份认证服务。
  - 通过 VSM 提供敏感数据加密服务。
- **客户价值**
  保障企业资产安全性，避免非法用户授权的访问。
- **应用领域**
  可应用于大型企业和事业单位。

电子票据

- **面临挑战**
  - 电子票据类应用的用户身份真实性需要安全手段保证。
  - 票据数据的生产，传输，存储过程中的完整性和安全性需要安全手段进行保证。
- **解决方案**
  - 通过 VSM 生成和管理各类型的对称密钥和非对称密钥。
  - 通过 VSM 提供对称和非对称密钥的数据加密、解密、转加密等服务。
  - 通过 VSM 提供证书签发、数据签名、数据验签、身份认证等服务。
- **客户价值**
  有力的保障了电子化安全性，促进电子化业务发展。
- **应用领域**
  - 可用于电子病例、电子发票、电子合同、电子保单等各类应用。

- 可用于银行、保险、政务、企业等多种领域。

构建密钥管理体系

- 密码机采用多级密钥管理体系，逐层保护。
- 支持密钥生命周期的安全管理，构建安全的密钥管理体系。
- 密钥生命周期包括如下几点：
  - **密钥产生：** 密码机支持产生高质量的随机密钥。
  - **密钥存储：**密码机支持安全存储对称密钥、RSA 密钥和 SM2 密钥，任何时候密钥不以明文形式出现在密码机外。
  - **密钥的安全使用：**密钥由其属性决定使用的许可范围和算法。
  - **密钥备份恢复：**密码机支持内部密钥的安全备份和恢复，可用于实现互备或负载的多台设备间的密钥同步。