抗量子签名服务

常见问题

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

常见问题

最近更新时间：2021-11-09 14:19:21

量子计算机对传统加密算法的安全性有什么影响?

基于大数分解和离散对数的 RSA 和 ECC 非对称加密算法、DH 密钥交换方案将不再安全，必须改用其他加密算法；大部分对称加密算法需要加倍密钥长度以保证足够的安全性；大部分摘要算法的安全性不受量子计算机的影响。

什么是抗量子签名服务?

不同于使用 RSA/ECC 算法的传统签名服务，抗量子签名服务使用能抵抗量子攻击的签名算法，在量子计算机出现后仍然可以安全使用。

抗量子签名服务适用于哪些场景?

抗量子签名服务适用于以下场景：

1. 需要长期保存签名的场景，例如，各种机构的机要资料中心。
2. 低配置自建 CA 服务器。
3. 服务量高、或者对性能要求较苛刻的场景，例如，各种拥有海量服务的互联网业务。

如何使用抗量子签名服务?

内测期间，您可以通过腾讯云控制台体验抗量子签名服务。

PQSS 如何计费?

内测期间，PQSS 可免费体验使用。