抗量子签名服务

产品介绍

产品文档

腾讯云

文档目录

产品介绍

产品概述

最近更新时间：2021-11-09 14:18:06

腾讯云抗量子签名服务（Post-Quantum Signature Service，PQSS）是一项能够抵抗量子计算攻击和传统计算攻击的签名服务。相比传统的 RSA/ECC 签名方案，PQSS 使用经过理论论证可以抵抗量子 Shor 算法攻击和传统攻击的签名算法，是一款面向量子时代的安全产品；同时具备更高计算效率和更低资源消耗。PQSS 适合签名需要长期使用，或者对签名效率要求较高的场景。

产品优势

最近更新时间：2021-11-09 14:18:22

长时效性

当前广泛使用的基于大数分解和椭圆曲线的 RSA/ECC 签名算法，可以被量子 Shor 算法破解，在量子计算机出现后不再能安全使用。腾讯云抗量子签名服务使用的是在传统算法领域和量子算法领域都未被破解的算法。
根据专家的预测，最短在未来10年内，量子计算技术将可能产生爆发性增长，量子攻击手段也会随之普及。对于签名需要较长时间使用的场景，如果在量级技术突然爆发时没有合适的防护手段，传统的签名算法将存在较大风险。而使用腾讯云的抗量子签名服务（PQSS），在长远来看会有更高的安全性。

更安全可靠

影响密码算法的安全性另一个重要因素是密钥熵源即密钥生成的随机性。
传统密钥的熵源为软件随机数或经典物理随机数，软件随机源的随机性由算法复杂度及种子的随机性保障，其可预测，可重复，安全性较低；经典物理随机数的随机源建立在难以建模的经典物理过程之上，存在被建模模拟破解的风险。腾讯云的抗量子签名服务（PQSS）使用腾讯云量子密钥管理服务（QMS）来生成密钥，密钥随机源的随机性来源于可理论论证的量子物理过程，其随机比特数等于熵，不可预测，不可重复，因此安全性要好于使用传统随机数生成器的签名算法。

更高效

目前广泛使用的签名算法是基于 RSA/ECC 的非对称算法，运算效率较低。腾讯云的抗量子签名服务（PQSS）使用的是基于哈希运算的签名算法，相比传统的签名算法资源占用更少，计算速度更快。

应用场景

最近更新时间：2021-12-17 10:10:26

长时效性数字签名

抗量子签名服务既能抵抗传统计算攻击，也能抵御未来的量子计算攻击。因此从长远的角度来看，抗量子签名更具有前瞻性，可应用于一些重要且安全时效性要求高的应用场景，例如，各种机构的机要资料中心。

低配置自建 CA 服务器

抗量子密钥服务资源占用少的特性，能够帮助有自建 CA 需求的用户更好的优化资源投入，配置更低的服务器可以承担更多的证书管理工作。因此抗量子密钥服务可应用于低配置自建 CA 服务器。

用户浏览流畅性要求高的网站

抗量子密钥服务资源占用少的特性，如果应用在网站签名上。还能够减少浏览器对证书的验证时间，降低访问延迟，因此非常合应用于要求高流畅性的网站，以满足该网站用户的浏览需求。