

# 抗量子签名服务

## 常见问题

## 产品文档



腾讯云

## 【 版权声明 】

©2013–2022 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 【 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。