腾讯云 CA

产品简介

腾讯云

文档目录

产品简介

产品概述

最近更新时间：2023-11-15 15:22:22

腾讯云 CA 是什么?

腾讯云 CA 符合《中华人民共和国电子签名法》和《电子认证服务管理办法》等相关法律法规要求，具备工信部相应牌照。

腾讯云 CA 具备多种相关资质，支持多种国产加密算法，其数字证书安全认证体系设计和建设符合各项安全协议与标准，可为用户提供数字证书申请、审核、制作、颁发、存档、查询、废止等全过程服务及以数字证书为基础的多场景安全应用解决方案，确保网上传递信息的机密性、完整性、真实性与不可抵赖性。

目前，腾讯云 CA 可为千行百业用户提供个人长效证书、企业证书、事件证书、时间戳服务等全类型数字证书产品，此外可支持私有化部署、电子签章系统及其他基于 CA 的丰富拓展应用，满足不同用户个性化需求。

主要功能

最近更新时间：2024-03-20 10:31:41

数字证书服务

提供个人证书、企业证书、事件证书、文档签名证书、代码签名证书等用户数字证书的全生命周期管理，包括证书签发、证书补办、证书更新等。

RA 服务

负责用户信息录入和证书业务管理。

签名验签服务

基于数字证书、数字签名等技术，为用户提供数字身份认证、数字签名验证、数据加密等服务，有效解决电子文件签名可靠性、真实性、不可否认性等痛点及难点。

时间戳服务

基于国家标准时间源及 PKI 技术，为用户提供精准、可靠、安全的时间数据，支持行为留痕过程中的不可抵赖性，解决以时间可信为基础的法律定责等问题。

相关概念

PKI/CA 基本概念	解释
公钥基础设施 PKI（Public Key Infrastructure）	是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。PKI 的核心组成部分 CA（Certification Authority），即认证中心，它是数字证书的签发机构。数字证书，有时被称为数字身份证，是一个符合一定格式的电子文件，用来识别电子证书持有者的真实身份。
数字证书（Certificate）	数字证书也称电子证书（以下简称证书），是一种由特定机构（CA）数字签名的、包含公开密钥以及公开密钥拥有者信息的电子文档。如同现实生活中公安机关颁发的居民身份证一样，数字证书是网络环境中的一种身份证，用于证明某一实体（例如人、服务器等）的身份。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。
CA 中心（Certificate Authority）	CA 是采用公开密钥基础技术，专门提供网络身份认证服务，负责签发和管理数字证书，且具有权威性和公正性的第三方信任机构。CA 即 Certificate Authority，是 PKI 体系的核心组成部分，业界通称为认证中心。
RA	RA 即 Registration Authority，是 PKI 体系中的注册审批系统，是 CA 的组成部分

(Registration Authority)证书审核注册中心	和向用户的延伸。LRA 即本地 RA，是面向最终用户的申请审核机构，与 RA 共同完成为用户办理证书申请、身份审核、证书下载、密钥更新、证书吊销以及密钥恢复等业务，RA 并不签发证书。
公钥和私钥	根据非对称密码学的原理，每个数字证书持有人都持有一对密钥，即公钥（Public Key）和私钥（Private Key），公钥与私钥作数据的互为加解密使用。公钥通常以数字证书的形式公开发布。私钥由证书持有者在本地生成，只能由证书持有者秘密掌握，证书持有者应当妥善保管并注意保密，不能在网上传输。
证书吊销列表(Certificate Revocation List，CRL)	是一种包含吊销的证书列表的签名数据结构。CRL 是证书吊销状态的公布形式，CRL 就像信用卡的黑名单，它通知其他证书用户某些电子证书不再有效。
唯一甄别名(Distinguished Name, DN)	在数字证书的主体名称域中，用来唯一标识证书用户的名称，体现用户的唯一性。例如可以用户名、证书类型、RA 名称、CA 名称以及国家名称等的一定规则的组合作为 DN 来标识一位证书用户。
明文	需要被隐蔽的消息。
密文	明文经变换形成的隐蔽形式。
密钥	加密和解密过程所需要的秘密参数。
机密性	数字签名可以加密要签名消息的杂凑值，保证了签名消息的机密性。
完整性	数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者用发送者的公钥解密被加密的摘要信息，然后用 HASH 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。
不可抵赖性	数字签名可以鉴别身份，不可能冒充伪造，那么，只要保好签名的报文，就好似保存好了手工签署的合同文本，也就是保留了证据，签名者就无法抵赖。在数字签名体制中，要求接收者返回一个自己的签名表示收到的报文，给对方或者第三方或者引入第三方机制。如此操作，双方均不可抵赖。
对称密码算法	典型的国际对称密码算法包括：DES/3DES、AES、RC4。 国密对称算法：SM1、SM4。
非对称密码算法	由于在加密和解密过程中，所使用的密钥是不同的，从这个意义上讲，密钥的使用是非对称的，因此被称为非对称密码算法，典型的非对称算法包括：RSA、DSA、ECC、SM2
哈希算法	哈希算法（Hash Algorithms）也称为散列算法、杂凑算法或数字指纹，是可以将任意长度的消息压缩为一个固定长度的消息的算法。 常用的哈希算法包括 MD 系列算法和 SHA 系列算法，其中 MD 系列算法有 MD2、MD4、MD5、RIPEMD 算法等，SHA 系列算法有 SHA0、SHA1、SHA256、

	SHA3算法等。 国密的哈希算法只有SM3一种。

工作原理

最近更新时间：2023-11-15 15:22:22

基于数字证书的身份认证

数字证书是强身份认证机制，私钥具有唯一性，只有私钥的主人才能够用私钥做签名操作，从证书中提取的公钥去验证证书私钥生成的签名，如果签名验证通过，则可保证证书的持有者的身份真实性。
基于数字证书的身份认证一般用于关键业务系统的登录，使用数字证书作为身份认证的手段，证书用户登录。

基于数字签名的抗抵赖

使用自己私钥进行非对称加密，被称为数字签名，使用对方公钥进行非对称解密，被称为签名验证。由于证书的私钥仅持有者才拥有私钥，因此使用私钥实现的数字签名可以被用来证明操作的不可否认性。

基于加解密的保密性

在使用数字证书进行加解密的应用场景中，通常一端使用公钥进行加密，另外一端使用私钥进行解密。

基于电子签名的电子签章

电子签章是电子签名一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。
数字证书在电子签章的应用场景中，电子印章替代传统的实物盖章，使用线上化手段生成的 PDF 电子合同、电子协议及电子单据可以结合数字签名技术加盖电子印章，签章后的电子 PDF 文件与纸质实物盖章或手写签名具有同等的法律效力。

非对称加解密

- 每个通信实体都拥有一对密钥。
- 这对密钥同时产生，具有互补的关系。
- 密钥用途不同，一个是公钥，用于非对称加密和安全密钥协商，另一个是私钥，用于身份验证和数字签名确认。

产品优势

最近更新时间：2023-11-15 15:22:22

竞争优势

保障财付通亿万交易量安全

- 支持微信支付过亿数字证书需求量级。
- 高可用、高安全、高稳定 。

认证、存证一站式方案

集成慧眼+区块链服务，从身份认证到发放证书再到出证报告，一站式能力提供。

持有工信部和国密牌照，支持国密算法，具备信创资质

支持国密 SM2 、SM3 算法，满足国密改造，商用密码评审信创要求。

丰富扩展能力，灵活部署方案

私有化证书/签章系统，签署文件不出本地，保证数据存储安全。

核心方案与价值

私有化签章系统

提供印章管理、合同发起及签署可视化页面，发放签署证书的能力。

安全身份认证系统

支持“用户名+密码”认证、软证书认证、USB 智能卡认证等多种认证方式，集中系统级别的授权管理。

商密安全性评估

从软硬件层面评判现有系统的商用密码合规风险，并给出系统改造升级方案。

移动支付安保方案

联合财付通打造移动支付管理控件，提供支付终端、用户身份、交易数据及交易内容等安全保障功能。

OA 安全解决方案

支持 PC 端及移动双终端，以 PKI/CA 技术解决 OA 使用中的盗用账号、越权访问、数据篡改等信息安全问题。

应用场景

最近更新时间：2023-11-15 15:22:22

教育

- 个人证书标识学生身份，K12阶段学籍信息不丢档。
- 加密系统对系统内的数据进行加密传输，对使用人进行身份标识。
- 出具可靠验签报告，解决行为纠纷。

医疗

- 医生开处方、病人签署医疗告知书、药剂师给药、护士术后护理、远程会诊等随时随地用可信身份安全接入，确保诊疗全流程安全合规。
- 为医疗电子文书各方电子签名增加法律效力，避免后续纠纷。
- 至信链存证，医疗数据加密保全。

政务

腾讯云 CA 为政务系统实现互认互信、数据安全互通、身份统一认证夯实安全能力基础，同时依托腾讯完善的产品体系，推动政务资源整合，促进政府各部门高效协同办公，为广大人民群众和企业提供更多便捷、安全、合规的信息化政务服务。

传媒

- 提供真实数字身份和可信时间戳能力，将媒体内容与人、事件、行为有效关联。
- 全程记录媒体从业人员行为、保障媒体信息发布真实性，打造基于可信身份和行为负责的健康网络文化空间。

金融

通过可信的数字身份和可靠的电子存证规避用户身份识别风险、保障交易过程中电子文件完整、真实、不可抵赖，降低运营成本的同时提升用户体验，维护各方合法权益。

工业

工业4.0时代，腾讯云 CA 助力企业实现设备、人员、产品、物料、监控等生产各环节统一安全接入。打破信息孤岛，促进生产智能管理、上下游供应链高效协同，为客户带来切实业务价值。