digicert®

DIGICERT® DOCUMENT TRUST MANAGER

数字签名、电子印章和时间戳保护您在世界各地的数字文档交易。

让全球业务永不停息

DigiCert® Document Trust Manager 能让组织获得可扩展到各种全球用例的受信任、合规的数字签名、电子印章和时间戳。DigiCert 帮助组织充满信心地遵守美国、欧盟 (EU)、英国 (UK)、瑞士以及世界其他国家 / 地区的行业与地方法规。

遵守世界各地的法律

许多国家的法律要求高保障度数字签名，这些签名由该地区认证的信任服务提供商 (TSP) 颁发的证书所支持。例如，欧盟、英国或瑞士的合格电子签名 (QES) 只能由 DigiCert 等合格信任服务提供商 (QTSP) 颁发。DigiCert 的高保障度数字签名遵循 Adobe Approved Trust List (AATL)、欧盟关于电子交易的电子身份识别和信任服务 (eIDAS) 的法规（第 910/2014 号）、英国 eIDAS 和瑞士 ZertES。

主要优势

- 远程加快文档签名流程 —— 而不影响安全性或合规性
- 可与 Adobe、Ascertia 和 DocuSign 的领先电子签名应用程序配合使用
- 确保电子签名由最高级别的身份保障所支持
- 遵守了解您的客户 (KYC) 或金融与银行业反洗钱 (AML) 等行业法规
- 在美国、欧盟、英国、瑞士和许多其他国家 / 地区获得受信任的电子签名

数字信任优势

随时随地在任何现代移动设备上签名。我们高度灵活的解决方案包括数字身份、证书、技术与自动化选项，以建立强大的数字文档信任。Document Trust Manager 提供：

数字签名

数字签名是一种由数字证书支持的电子签名，使用公钥基础设施 (PKI) 将此数字证书加密绑定到签名字段。数字证书通常被称为数字身份（数字 ID），每个数字证书对个人来说都是唯一的，并在验证个人身份后才能获得。

电子印章

电子印章 (e-seal) 是一种由企业或组织等法律实体使用的数字签名，用于证明文档的来源、真实性和完整性。电子印章可以提供强有力的法律证据，证明文档来源于该实体，并且没有被更改。电子印章通常用于自动化系统，以处理批量发票或工资支票等高通量流程。

时间戳

时间戳是对事件时间和日期的数字签名记录。时间戳提供了附加保障，证明文档、电子签名或电子印章在应用时间戳时是有效的，并且没有被更改。

内置的电子签名信任

并非所有电子签名都生而平等。事实上，有很多不同类型的电子签名 —— 从简单的复选框或平板电脑上的涂鸦图像，到由 DigiCert 等认证机构严格的身份验证所支持的云端的高保障度数字签名。因此，采用将签名人与特定文档明确联系起来的高保障度数字签名有助于保护您的高价值电子交易、跨境电子交易和其他电子交易。

下图显示了不同类型电子签名的各类安全属性、法规遵从性和保障级别：

签名类型	电子签名	数字签名（AATL）	数字签名（受监管 / 合格）
说明	一个宽泛的术语，包括表明接受某一协议或记录的任何电子流程。电子签名最基本的形式可以是在签名行键入姓名或选中复选框。	一种更安全的电子签名，需要使用由信任服务提供商（TSP）颁发的数字 ID，符合 Adobe Approved Trust List（AATL）对身份验证和安全的特定要求。	一种高度安全的电子签名，需要使用由特定地区已认证的 TSP 所颁发的受监管数字 ID，这类 TSP 包括欧盟或瑞士的合格信任服务提供商（QTSP）。
公共信任	无要求	受 Adobe Acrobat 和 Reader 信任	受 Adobe Acrobat 和 Reader 信任 *
数字身份	无需与签字人进行唯一链接	证明签名人的唯一数字身份以加密方式绑定至签名字段（PKI）	证明签名人的唯一数字身份以加密方式绑定至签名字段（PKI）
保障级别（LoA）	**低** 有限或低身份验证	**较高** 需要身份验证	**高** 面对面或等同的严格身份验证
双因素身份验证（2FA）	为文档签名时不需进行	为文档签名时需要进行	为文档签名时需要进行
长期有效期	无要求；可包含在签名工作流程解决方案中	防篡改签章和时间戳应用于已签名的文档	防篡改签章和时间戳应用于已签名的文档
是否等同于手写签名	否	否	符合欧盟、英国和瑞士的特定监管要求 *

主要功能

签名证明
签名人身份、签名时间和与已签名协议加密绑定的文档真实性的有力证据。

可扩展的集成
可与包括 Adobe Acrobat Sign、Ascertia SigningHub 和 DocuSign 在内的领先签名工作流程解决方案配合使用。

远程身份验证
使用现代移动设备和身份证件识别客户、公民和员工。

灵活的部署选项
将 Document Trust Manager 部署为托管、本地或混合式解决方案。

自定义解决方案
创建 Document Trust Manager 的私有实例或使用云签名联盟 (CSC) API 与自定义签名解决方案相集成。

集中控制
使用 DigiCert ONE 平台简化数字 ID 和证书的管理。

受保护的签名密钥
保护在美国、欧盟和瑞士的安全认证环境中托管的经认证的硬件安全模块 (HSM) 和合格签名创建设备 (QSCD) 中用于数字签名的私钥。

保护您的数字文档

随着数字文档迅速取代纸质流程，各组织也在部署受信任的电子印章 (e-sealing) 解决方案，以保护文档的真实性。将电子印章与高保障度数字签名相结合并应用于合同、协议和其他数字文档，有助于为您的组织防范与电子交易相关的潜在网络犯罪或欺诈。

Document Trust Manager 可帮助您确保，通过使用由最高级别的身份保障所支持的电子印章、时间戳和数字签名，您的所有文档都受到保护。

实现数字信任的 DigiCert ONE 平台

DigiCert Document Trust Manager 是 DigiCert ONE 数字信任平台的一部分，该平台将 DigiCert 的数字信任产品统一在现代化的容器化体系结构中，提供高度的可扩展性、部署的灵活性、快速的价值实现和统一的 PKI 管理。

立即开始体验

立即开始体验 DigiCert® Document Trust Manager。请联系您的 DigiCert 客户经理或发送电子邮件至 sales@digicert.com。

DigiCert, Inc. 简介

DigiCert 是全球领先的数字信任提供商，使个人和企业能在进行线上互动时确信其在数字世界的足迹安全无虞。数字信任平台 DigiCert® ONE 为组织提供适用于各类公用与私有信任需求的集中式可见性和控制，以保护网站、企业访问与通信、软件、身份、内容及设备。DigiCert 将其屡获殊荣的软件与其在标准、支持和运营方面的行业领先地位相结合，而且 DigiCert 是全球领先企业的首选数字信任提供商。如需了解更多信息，请访问 digicert.com 或关注 @digicert。