



# 简化数字签名

无缝有效的文档处理现在是大多数企业的关键需求。

# 目录

- 3 介绍
- 4 走向数字化
- 5 概念
- 6 深入了解数字签名
- 8 市场挑战
- 9 展望未来





# 介绍

无论是转换实验室文件、工程图、合同还是贷款申请——普遍的共识是纸张是麻烦的，难以管理和昂贵的。这就是为什么准确地数字化内容如此重要。

在全球范围内，我们的数字足迹很大——而且只会越来越大。为了简化电子转换，无缝和有效的文件处理现在是大多数企业的关键要求。数字签名是关键。

# “走向数字化”

分析人士估计，在本世纪末之前，现存的数据将超过40万亿GB。电子文档是业务的需求——驱动更动态、协作和无缝的工作流程。它们不仅节省了时间和金钱，还让组织比以往任何时候都更快、更聪明地工作。

但每天产生的内容量可能会让人不知所措。在“内容冲击时代”，信息量迅速超过了市场的消费能力。许多预测表明，数字内容的增长速度每两年翻一番。

这不仅给数据消费者带来了问题，也给那些试图快速轻松地处理文档的企业带来了问题——无论是合同、贷款申请还是工程计划。这个问题的核心是数字签名。



在这十年结束之前，  
将存在40万亿GB的  
数据



数字内容的增长率每  
两年翻一番



这个问题的核心是  
数字签名



# 概念

数字签名背后的概念是，它们使用难以复制、重复或妥协的独特数字代码有效地加密文档。

强数字签名确保消息内容在传输过程中不会被更改。这一过程确保了几乎任何形式的在线内容——从电子邮件到在线订单。该过程涉及一个复杂的数学过程，整合通过字符序列表示的唯一数值。



只有计算机才有资格生成这种类型的组合。但是采用数字签名并不总是那么容易。毕竟，有一系列可用的解决方案——在市场上制造混乱。



# 深入了解数字签名

在采用一种解决方案而不是另一种解决方案之前，解决一个常见的混淆领域至关重要：  
电子签名和数字签名的区别。

## 数字签名不同于电子签名，它具有以下核心优势

### 01

文件是真实的，  
来自经过验证  
的来源

### 02

由可信组织  
验证的签名者身份  
(证书)

### 03

签名支持  
不可否认  
性

### 04

在文件内  
容上创建防篡  
改密封

### 05

嵌入式可信  
时间戳支持  
不可抵赖性和  
审计日志

数字签名是一种以密码技术为基础的电子签名。这些产品证实了文件的真实性和来源的可靠性——因为它是经过第三方验证的。用户可以与签名进行交互，并查看发件人的身份。数字签名是专门为确保文档完整性而设计的，并使用签名者的私钥进行签名——这就是为什么从文档中派生出的唯一代码如此重要。

数字签名的另一个关键元素是它能够证明签名后内容没有被更改。强的解决方案总是包含时间戳——确保签名在特定的日期和时间应用。已实施规定指定可接受的签名“类型”，并定期更新必要的基准和国际标准，如欧洲的eIDAS（电子识别、认证和信任服务）。

## 数字签名满足许多电子签名规则的要求：

- ✔ 对于签名者来说是独一无二的 → 第三方验证身份
- ✔ 能够辨认签名者的
- ✔ 由签字人独占 → 私钥
- ✔ 与数据相关联，这样任何变化都可以被检测到 → 密码哈希校验
- ✔ 时间戳 → 包含可信时间戳

在数字签名解决方案中，另一个关键领域是“私钥”。每个数字签名都使用每个用户唯一的“私钥”——这意味着签名由签名者唯一拥有。


最后，所有可信的数字签名都要有多个文档根证书库中的一个作为支持，比如“Adobe认可的信任列表”（AATL）和“Microsoft根证书列表”。对于签署人来说，为了获得公众信任，证书颁发机构的根证书总是包含在这些程序中。

## 交互式签名提供 经过验证的身份和时间戳信息



Digitally  
signed by  
Marketing  
Date:  
2023.10.18  
11:16:15  
+01'00'

### × Signatures

- ✓  Rev. 1: Signed by Marketing <marketing@globalsign.com>
  - Signature is valid:
  - Source of Trust obtained from Adobe Approved Trust List (AATL).
  - Document has not been modified since this signature was applied
  - Signer's identity is valid
  - The signature includes an embedded timestamp.
  - Signature is LTV enabled
- > Signature Details
  - Last Checked: 2023.10.18 11:19:59 +01'00'
  - Field: Signature2 on page 1
  - [Click to view this version](#)



# 市场挑战

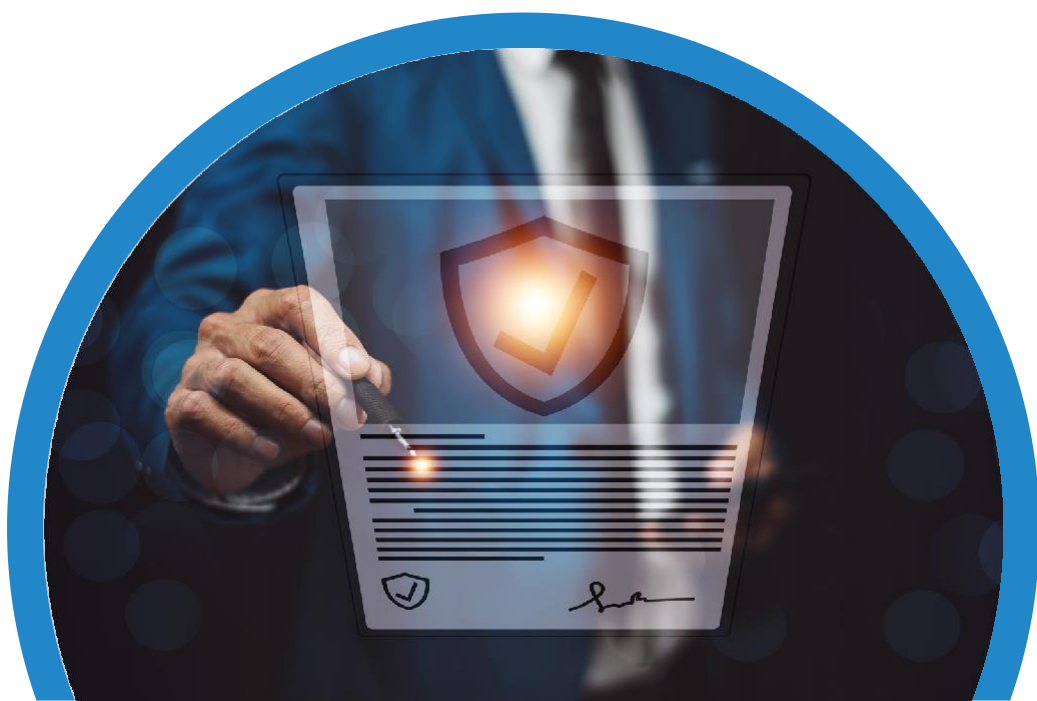
虽然一些数字签名解决方案解决了一些问题，但并非所有解决方案都完全符合合规性和合法性要求。这一点很重要，因为许多组织要求在法律合同中使用数字签名。

除了法律之外，另一个障碍是技术部署。解决方案必须与每个业务、技术基础设施或正式流程完全兼容。另一个障碍是成本。有效的数字签名由兼容的加密硬件提供支持——通常是硬件安全模型（HSM）或USB令牌。这意味着在硬件维护和令牌管理方面的投资。

- **对于可用和可接受的签名类型的混淆**
- **硬件投资和维护**
- **使用REST API集成到现有的工作流中**
- **内部密码专业知识**

真正的数字签名也会受到文档工作流或管理系统的阻碍。这些基础设施对于定制和自动化流程是必不可少的。

事实上，并不是所有的数字签名都是一样的。要列入这一类别，该过程应该包含广泛的签名行为和安全级别——从检查框或输入首字母到使用基于加密的数字签名。选择几乎是无穷无尽的。那么，你如何知道哪种数字签名方案适合你呢？





# 展望未来

答案可以在云中找到。将数字签名过程移动到云端是在一个平台中构建合法且符合要求的签名所需要的全部。GlobalSign的数字签名服务（DSS）就是这样一种基于云计算的解决方案——整合了从签名到确认的所有内容，而无需离开客户的环境。

## GlobalSign的数字签名服务提供所有您需要在—一个基于云的服务中申请合法许可和合规的数字签名



对任何文档的哈希值进行数字签名



签名证书  
保险



私钥存储在GlobalSign  
基于云的HSM上



可信时间戳服  
务



响应中包含吊销检查  
(需要长期验证)

这种高度可扩展的云服务是API驱动的数字签名服务，消除了实现障碍并降低了总成本。与传统的需要令牌或硬件安全模块（HSMs）的文档签名产品不同，GlobalSign的数字签名服务具有高度可扩展性和API驱动，可以轻松地与商业和自定义文档 workflow 解决方案集成。这消除了对安全硬件的新需求。

GlobalSign使在任何文档和 workflow 解决方案中添加公开可信的数字签名变得简单且具有成本效益，易于使用，同时仍能跟上在电子商务世界中有效执行的监管要求所驱动的数字签名需求的增长步伐。

# GlobalSign基于云的签名解决方案有助于管理整个数字签名生命周期

GlobalSign建立在高度可扩展的、基于云的PKI平台上，支持公共可信的数字签名，同时降低成本、维护和内部专业知识等障碍。GlobalSign处理可信签名所需的所有加密组件——例如签名、证书签发、密钥管理、时间戳以及与外部验证服务的集成。该产品也是最安全的，没有数据库的私钥可以泄露，也没有文档存储——即使是以散列形式。

作为一个基于云的API驱动的解决方案，GlobalSign可以轻松地与任何电子文档 workflow 解决方案集成。拥有现有产品（定制或商业）的公司可以快速实现该服务。此外，GlobalSign还与 Adobe Acrobat Reader、DocuSign和iLovePDF等一系列文档 workflow 提供商合作，使实现更加无缝。

GlobalSign提供了广泛的技术选择，从桌面到云和整个企业。这些解决方案消除了有效数字签名的一些最大障碍，使任何规模的企业都可以优化文档 workflow，满足合规标准，并更好地拥抱高效、可持续的签名实践。



[观看webinar](#)



[联系我们团队](#)



## 关于GMO GlobalSign

作为全球最具影响力的认证机构之一，GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的组织、大型企业、云服务提供商和物联网创新者能够进行安全的在线通信，管理数百万已验证数字身份以及自动化认证和加密。其大规模的PKI和身份解决方案支持构成物联网的数十亿项服务、设备、人和物。GMO GlobalSign是日本GMO云KK和GMO互联网集团的子公司，在美洲、欧洲和亚洲设有办事处。欲了解更多信息，请访问<https://www.globalsign.cn>。

### GlobalSign

CN



上海市普陀区陕西北路1438号财富时代大厦706室



+86 021 60952260



[www.globalsign.cn](http://www.globalsign.cn)