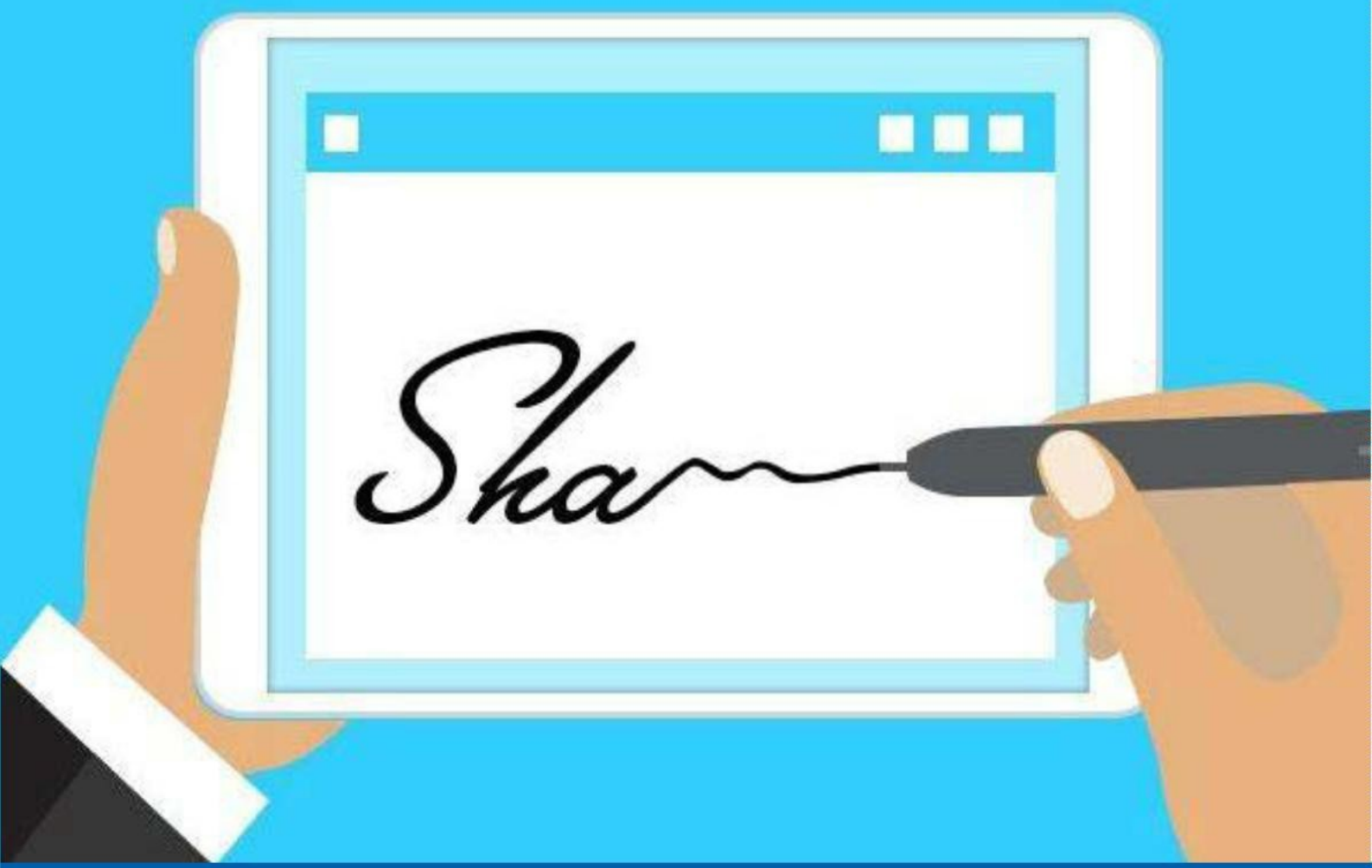
简化数字签名

在当今的数字时代，大多数企业都支持无纸化。
无论是转换实验室文件，工程图，合同，还是贷款申请 - 一般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。



章节 1: “ 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 。这很有道理。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。一般术语是“内容冲击”——意思是信息量迅速超过了市场的消费能力。更进一步说，许多预测表明，数字内容的增长速度实际上是每两年翻一番。

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。

警告：内容超载！

章节 2: 概念

数字签名背后的理论是可以理解的，即使很多人不能背诵一个正式的定义。这些电子签名有效地加密了具有难以复制、重复或妥协的独特数字代码的文件。

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。
但是采用数字签名的道路并不总是那么容易。毕竟，有一系列可用的解决方案——在市场上制造混乱。

章节 3: 深入研究数字签名

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是至关重要的：电子和数字签名。注意，这两者是不一样的。

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。不可否认性不是问题，因为签名者不能根据用户的私钥否认签名。数字签名是专门为确保文档完整性而设计的——这就是为什么来自文档的唯一代码如此重要的原因。

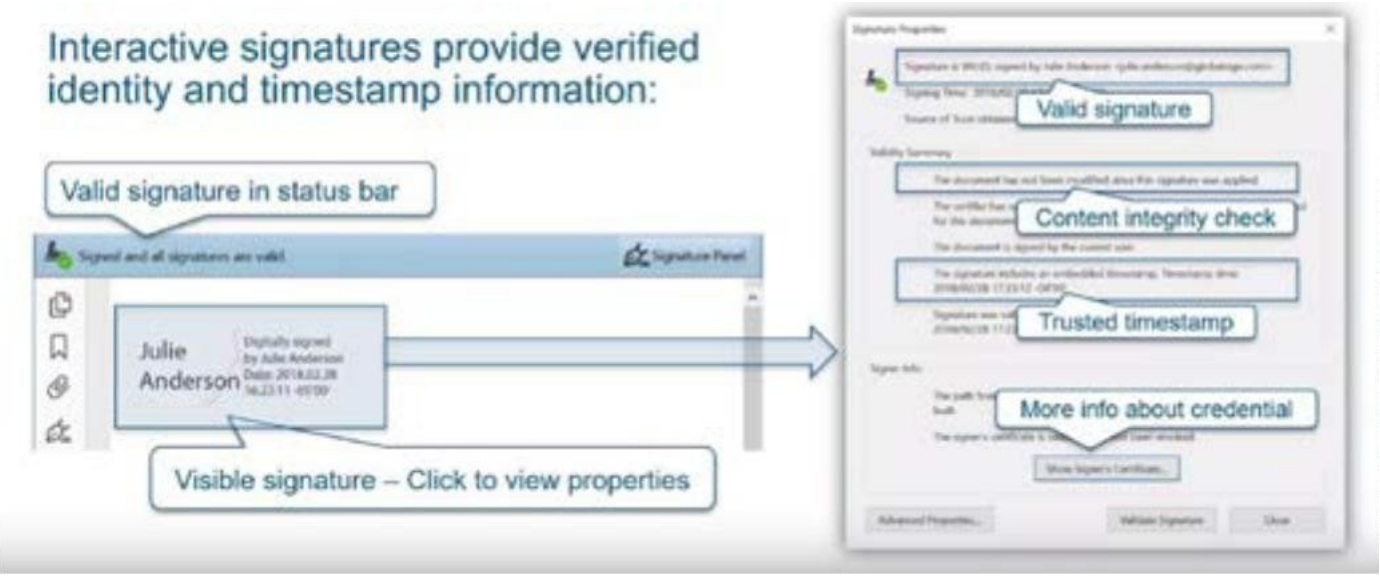
数字签名的另一个关键因素是它能够证明签名后内容没有被更改。强的解决方案总是包含时间戳——确保签名在特定的日期 / 时间应用。更进一步，现在出现了新的规定，指定可接受的签名的“类型”。事实上，欧洲的 eIDAS(电子识别、认证和信任服务) 已经更新，并正在建立国际标准和必要的基准。

数字签名满足许多电子签名规则的要求：

1. 对于签名者来说是独一无二的
2. 能够辨认签名者的 → 第三方验证身份
3. 由签字人独占 → 私钥保护
4. 与数据相关联，这样任何变化都可以被检测到 → 加密散列检查
5. 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总是由两个主要的文档根存储库支持——称为“ Adobe 授权信任列表” (AATL) 和“ Microsoft 根信任列表”。对于签署人来说，为了获得公众的信任， CA 的根总是包含在这些程序中。



章节 4: 市场的挑战

虽然一些数字签名解决方案解决了一些问题，但并不是所有的解决方案都完全符合强制性的合规性和合法性要求。这很重要，因为确保数字签名合法是首要任务。

除了法律之外，另一个障碍是技术部署。换句话说，100% 确定解决方案完全与每个业务、技术基础设施或正式流程兼容。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 USB 令牌或硬件安全模型 (HSM)。这意味着在硬件维护和令牌管理方面的大量投资。

- 混淆哪些类型的签名是可用的和可接受的
- 硬件投资和维护
- 集成到现有工作流中的定制开发工作
- 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。

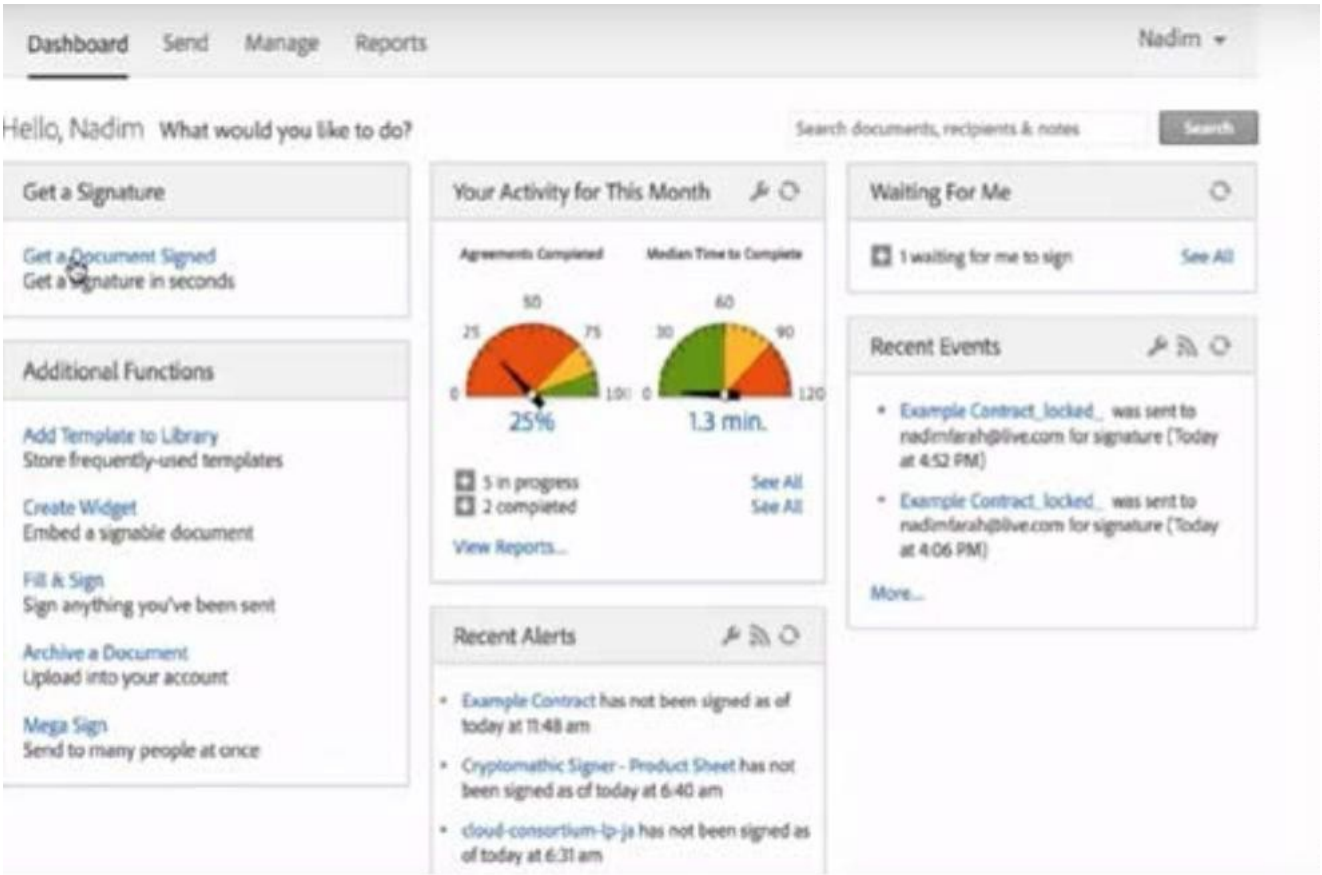
事实上，并不是所有的数字签名都是一样的。要列入这一类别，该过程应该包含广泛的签名行为和安全级别——从检查框或输入首字母到使用基于加密的数字签名。选择几乎是无穷无尽的。那么，你如何知道哪种数字签名方案适合你呢？

章节 5: 前进的方向

尽管市场混乱，但肯定有更好的办法。答案可以在云的力量中找到。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。

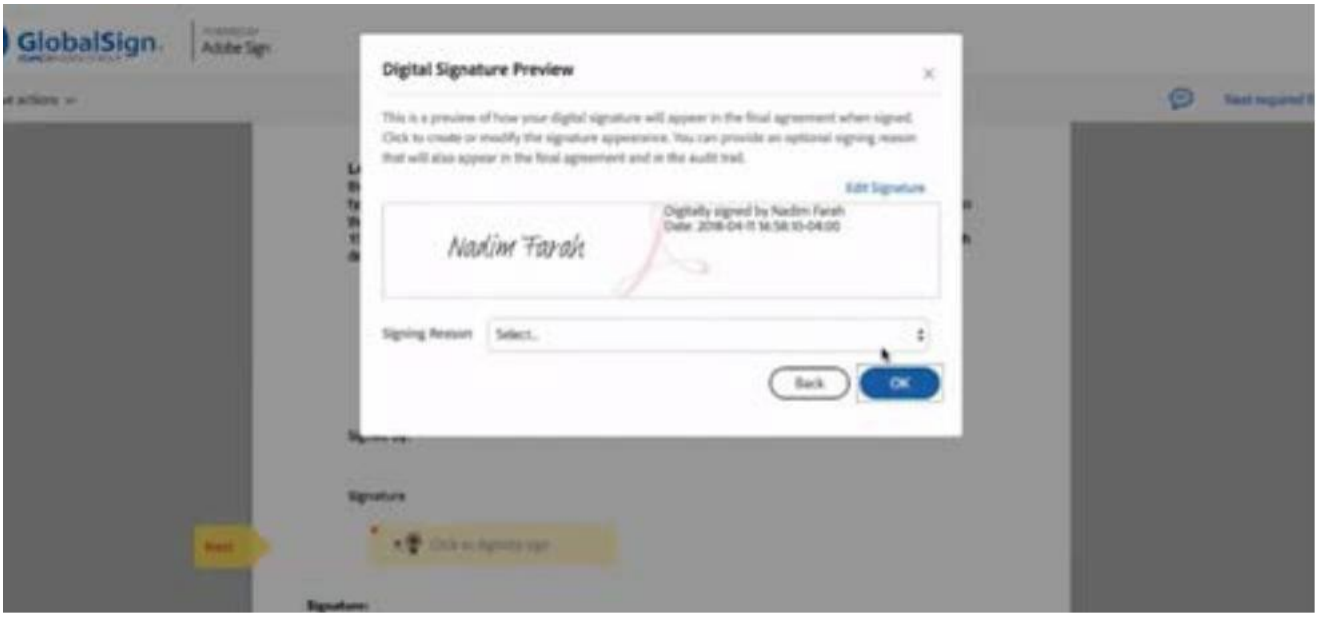
这种高度可扩展的云服务是 api 驱动的数字签名服务，消除了实现障碍并降低了总成本。与传统的需要令牌或硬件安全模块 (HSMs) 的文档签名产品不同， GlobalSign 的数字签名服务具有高度可扩展性和 API 驱动，可以轻松地与商业和自定义文档工作流解决方案集成。这消除了对安全硬件的新需求。

为任何文档和工作流解决方案添加公开可信的数字签名， GlobalSign 易于使用，使其简单且具有成本效益，同时仍能跟上不断增加的监管要求，在电子商务的世界中有效地执行。

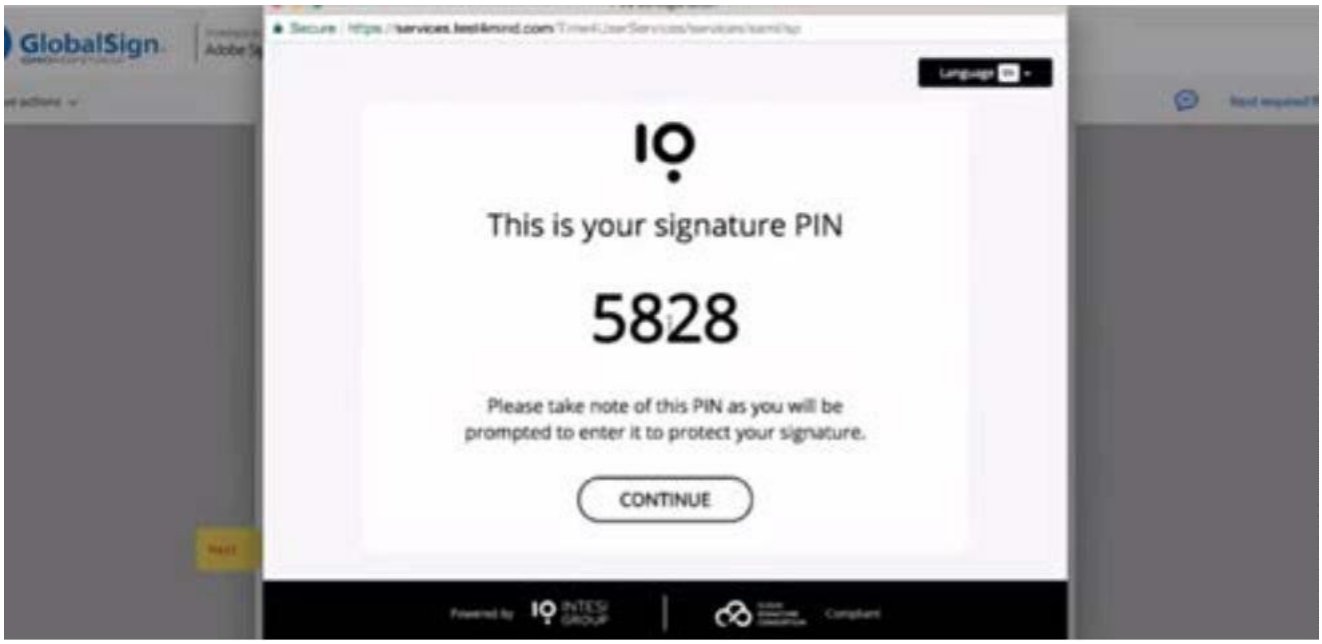


GlobalSign 基于云的解决方案由易于使用
和直观的仪表板驱动，以管理整个数字签名生命周期。

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。下图是



数字签名可以在几分钟内很容易地预览和导入



GlobalSign 解决方案的每一层都包含了安全和加密。

这也是最安全的，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工作流解决方案集成。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 还与奥赛 (Odyssey) 、 Ascertia 和 Pitney Bowes 等一系列文档工作流提供商合作，使实现变得更加轻松。

GlobalSign 提供了广泛的技术选择，从桌面到云和整个企业。消除了有效数字签名的一些最大障碍，这些解决方案最终使任何规模的企业都可以优化文档工作流，满足合规标准并拥抱数字时代。

看看 GlobalSign 今天如何帮助你。今天观看我们关于数字签名的新网络研讨会，然后联系我们获取更多信息 ....

想了解更多有关数字签名的信息？

访问我们的 DSS 产品页面

GlobalSign 办公地址
上海市普陀区陕西北路 1438 号财富时代大厦 706 室

电话：021-60952260