OneSpan
Be bold. Be secure.

SECURITY & TRUST: BEST PRACTICES FOR IMPLEMENTING ELECTRONIC SIGNATURES AND EVALUATING VENDORS

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

Best Practices for Implementing Electronic Signatures and Evaluating Vendors

Security is understandably a top concern with digital transactions, so it is important to make sure your electronic signature provider meets the highest security standards, while ensuring a trusted experience between you, your employees, and customers.

That means more than simply passing a security audit or obtaining a certification. We recommend taking a broader view of e-signature security that also addresses:

- Choosing the appropriate level of authentication
- Protecting e-signatures and documents from tampering
- Making it easy to verify e-signed records
- Ensuring the long term reliability of your e-records, independent of the vendor
- Verifying the vendor has a consistent track record of protecting customer data
- Creating an end-to-end trusted experience through white-labeling and integration with your existing identity and access management (IAM) framework

Taking a multi-pronged approach to electronic signature security will ensure your records can be reliably reproduced as evidence in the event of a dispute.

Taking a multi-pronged approach to electronic signature security will ensure your records can be reliably reproduced as evidence in the event of a dispute. It will also foster customer confidence, protect your organization's reputation, reduce risk of non-compliance fines, limit vendor lock-in, and more.

To help identify the security requirements against which you should evaluate solutions, this white paper answers questions like: How do I know who e-signed a document? How are customers' e-signatures protected? How easy is it to verify whether an e-signed record has been modified? And if using e-signatures in the cloud, how can I be sure my customer data will be protected?

1. Identification, Authentication, and Attribution

E-Signature laws do not say much when it comes to security techniques and technology, but the legal definition of an electronic signature always includes language around signer identity. This means organizations need to take steps to identify and/or authenticate users prior to e-signing, and they need to tie that authentication to the e-signature and e-signed record.

Authenticating users and transactions are top priorities for banks and other organizations conducting business online and via the mobile channel.

Identification

When evaluating how to identify new customers over the web, consider how this is accomplished in other remote channels, such as call centers and by mail. These processes often identify first time applicants using two types of personal information:

- Personally identifiable information
- Non-public personal information

The customer's information is typically verified through a third-party identification service (e.g. Experian, Trans Union, Equifax). Financial service providers, for example, frequently use third-party services, since they are often already accessing credit databases as part of loan applications and other processes. In this case, look for an e-signature solution that integrates with third-party identity verification services.

Authentication

Once a signer's identity is verified, organizations often issue electronic credentials to facilitate future digital transactions. In the case of existing customers, it is highly recommended to leverage credentials you may have already issued (e.g. logins for online banking). Not only are such credentials generally reliable if they have been used over time, it saves the customer the hassle of having to create and remember yet another password.

In addition, organizations in certain geographies or in sectors that deal with high-value, high-risk transactions often use strong, multi-factor authentication services (e.g., OneSpan's Digipass®) at any point during the process. This reinforces trust in the transaction and creates a secure environment so that identities, data and digital lives remain protected. In this case, look for an e-signature solution that can easily integrate with authentication services throughout the e-sign workflow.

While there are many secure and user friendly options for identifying signers online, ultimately the choice of authentication method depends on the risk profile of the process being automated and the underlying digital transaction. The key point here is to authenticate users without diminishing their experience. As such, look for e-signature solutions that offer a wide range of authentication options to better fit your needs and as a result, enable better experiences.

The Distinction Between Digital and Electronic Signatures

The term "e-signature" is often confused with "digital signature". An electronic signature, like its paper equivalent, is a legal concept. Its purpose is to capture a person's intent to be legally bound to an agreement or contract.

A digital signature, on the other hand, is a security technology. Based on public/private key cryptography, digital signatures are used in a variety of security, e-business and e-commerce applications. When used within an electronic signing application, digital signature encryption secures the e-signed data. If an e-signed document is modified or tampered with in any way, digital signature technology will detect it and invalidate the document.

Unlike paper-based contracts and signatures that require careful attention to detail and that rely on the human eye for verification, e-signed contracts based on digital signatures can automatically flag any errors or alterations. Digital signatures, therefore, are the foundation of any reliable electronic signature and a core requirement for a trustworthy solution.

Attribution

Signature attribution is the process of proving who actually clicked to apply an e-signature. Questions of attribution often come up when looking at processes where staff interacts with customers in a face-to-face environment using the click-to-sign method on a shared device. Consider the use case where a signer is asked to click a button to e-sign on an agent's laptop. The challenge becomes how to prove who was holding the mouse when the e-signature was applied. There are two proven approaches for establishing attribution in these circumstances: affidavits and the use of SMS passcodes sent to personal mobile phones.

Affidavits are the most cost-effective and the easiest way to establish attribution. Just before handing over control of a laptop or tablet to the customer for signing, your employee or representative would be presented with affidavit text affirming they are handing control over to the signer. This transfer of control would be captured as part of the audit trait.

Another option is to use the signer's personal smartphone. Signers can be sent a one-time passcode via SMS text that they would use in order to gain access to the e-sign session.

2. Document and Signature Security

Document and signature security are at the heart of any electronically signed contract or document. As such, there are several points to consider:

- The document and **each** signature must be secured with a digital signature to render the document tamper-proof and ensure that signatures cannot be copied and pasted
- A comprehensive audit trail should include the date and time of **each** signature
- The audit trail must be securely **embedded** in the document and linked to **each** signature
- It must be easy to verify – **independently of the vendor** – that no changes have been made to the signed record
- The document must be **accessible to all parties**

Digital Signature Security - Applied at Each Signature

The document and electronic signatures should be protected using digital signature technology. The digital signature creates a digital fingerprint of the document (called a hash) that can be used at a later point to verify the integrity of the electronic record. If the document is tampered with in the slightest, the electronic signature will be visibly invalidated. This is a unique and significant advantage over the paper world, where it is not always possible to detect whether changes have been made to a document.

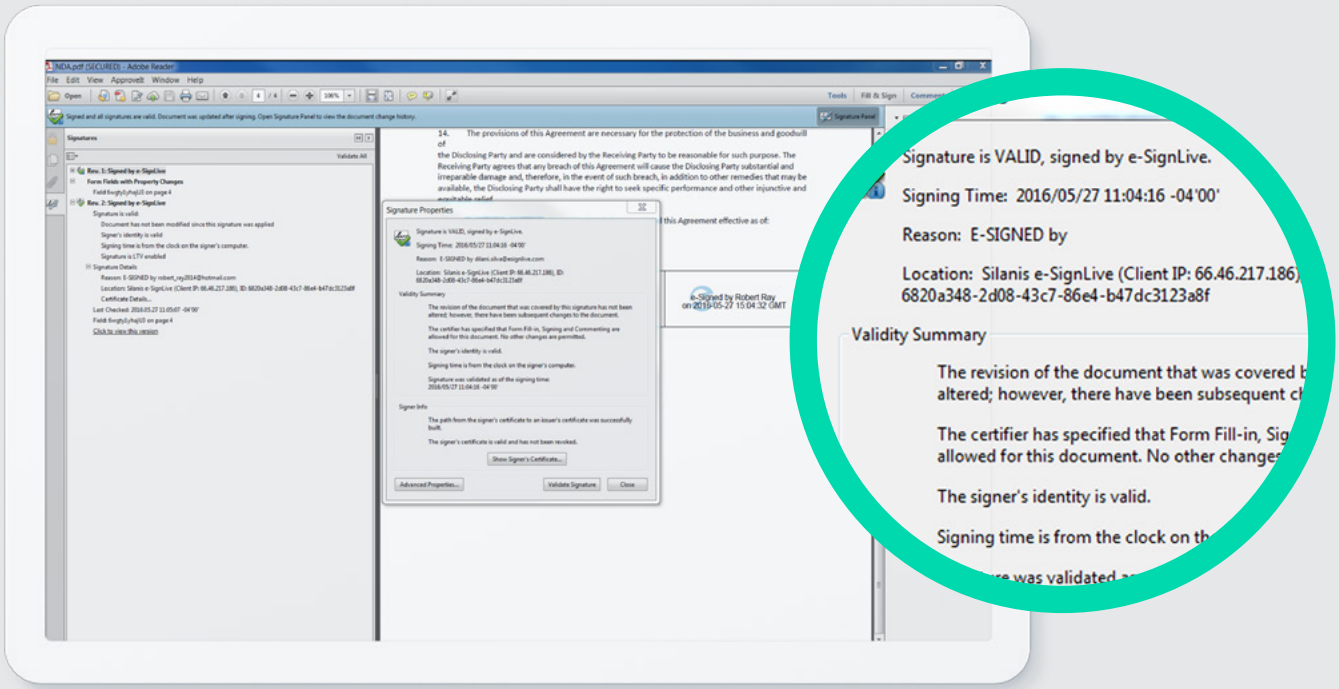
It is worth noting that applying a digital signature as an envelope to a document (once all signatures have been captured) is not a recommended practice. This approach leaves the document and signatures unprotected while the process is being completed and results in the wrong date and time stamp being place on individual signatures. If a signer and a co-signer e-sign a record on two separate days, you want that history reflected in the audit trail. The best practice is to apply digital signature encryption as each e-signature is added to the document. This builds a comprehensive audit trail with the date and time that each signature was applied.

Detailed Audit Trail Embedded in the Document

All electronic signatures, time stamping, and audit trails should be embedded directly within the document rather than stored separately in the cloud or "logically" associated in a vault or proprietary database. In addition to being more secure and easier to manage, there are two very pragmatic reasons for this.

First, document authenticity can be verified independently of the e-signature software, meaning you do not need to worry if a verification link back to a server will be valid years from now or if it will give you a “page not found” error message. Whether or not you maintain an account on the e-signature service, or whether your vendor is even still in business, your documents are not affected since you, your customers, and other stakeholders do not have to go online to check the document.

Verifying Document and Signature Integrity within OneSpan Sign



Second, you do not have to store the e-signed record in the e-signature service. The record can securely travel through any email, storage, or archiving system without being compromised or requiring additional programming. This gives you the flexibility to manage your e-signed records in a manner that meets your long-term records retention policies. In other words, the e-signed document can be indexed, stored and retrieved easily in the system of record of your choice, and you can leverage your investments in those systems.

A Simple Way to Verify Document Integrity

Look for intuitive, one-click signature and document verification. If the verification process is too cumbersome, users may wrongly assume that the document and signatures are valid, without proper verification.

When verifying a document that has been e-signed with OneSpan Sign's software, users click on the signature block. This opens the audit trail and automatically verifies both signer authentication and document validity (as shown on page 5).

A one-click process such as this simplifies the user experience, leading to greater confidence in the e-signature process and the reassurance that any errors or fraudulent actions will be detected. Plus, there is no need to train business users or customers how to verify a document.

> Avoid e-signature solutions that require you to access a server to verify the signatures or document. Not only is this inconvenient for users, it introduces major problems if you terminate your subscription or if the vendor goes out of business."

3. Cloud Security

Today's e-signature solutions are available both on-premises and in the cloud. While an on-premises deployment offers maximum control, a growing number of organizations of all types and sizes are opting for the cloud for a variety of reasons, such as speed-to-market and cost savings.

For e-signature transactions involving sensitive customer data, using a cloud service raises additional security and data privacy considerations beyond the ones we have mentioned already. We strongly recommend researching the company that hosts your e-sign service to understand their security practices, certifications, track record, and the frequency of their security audits. Due diligence around their security practices and infrastructure could expose past privacy breaches, incidents of data loss/leakage, or other risks such as insufficient cloud security expertise. Other elements to evaluate include:

- The security of human processes and administrative access to systems
- The security and physical environmental controls
- The security of the networking infrastructure, operating systems and services

Furthermore, verify that the e-signature platform utilizes strong data encryption in transit and at rest, and stores data within an encrypted database volume to ensure an encrypted channel for all communications.

At OneSpan, we partner with leading cloud infrastructure service providers such as Amazon Web Services, IBM SoftLayer, and Microsoft Azure. These providers are designed and managed according to security best practices and comply with a variety of regulatory, industry, and IT standards for security and data protection, including: ISO 27001, SOC 1/2/3, HIPAA, FIPS 140-2, FISMA, and much more.

We also apply numerous other security measures at the application layer to ensure the OneSpan Sign platform is secure and customer data is protected. As the first and only cloud e-signature solution provider to complete a Service Organization Control (SOC) 2 Type 2 attestation, OneSpan Sign maintains the strictest of controls.

OneSpan Sign was also the first e-signature solution to be hosted on a FedRAMP compliant cloud, a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

OneSpan Sign's carrier grade availability is ensured through the use of multiple availability zones and geographic regions, and by 24/7 monitoring (see the OneSpan Sign Trust Center at https://trust.esignlive.com/). An always-on disaster recovery site in a different geographic region allows for rapid recovery, should a disaster affect our primary facilities.

4. Data Residency

As organizations support borderless digital business scenarios and move customer-facing transactions to the cloud, there is a growing need to ensure that data is protected and complies with local data privacy laws. Forrester Research Inc. reported that, "Data residency will become a stronger requirement. E-signature falls under the scope of EU data privacy rules. S&R [security and risk] pros must consider data residency requirements when assessing storage options from e-signature providers, especially if they opt for storage in the cloud."[1]

This is particularly true in regulated and compliance-driven industries that often need granular transparency into and control over where transactional data resides – right down to the city, data center, and even the serial number of the server.

OneSpan offers both public and private instances of OneSpan Sign in the US, Canada, the United Kingdom, Germany, and Australia. By leveraging the global data center networks of

our technology partners, we can also spin up new instances of OneSpan Sign in other regions of the world. This not only helps fulfill in-country data residency requirements, but also enables organizations to quickly scale and expand their operations globally.

5. End-to-end Trust

Customer experience is at the heart of digital transformation. As organizations leverage third-party solutions to support their digital transformation projects, their reputation often hinges on actions that are typically beyond their control. So what can a company do to protect its brand and reputation when working with third-party solution providers?

Our advice is to white-label the entire e-sign experience so that your brand, and only your brand, appears across the transaction (not the vendor's brand). This creates a trusted experience between you and your customer, protects your brand, protects your customers, and helps to achieve the highest completion rates possible. Look for the vendor's ability to:

- Integrate with your email servers to allow emails to be sent from your domain (e.g., @yourbank.com) instead of the vendor's
- Customize the colors, logo, and the visibility of elements such as header, navigation bar, footer, etc.
- Customize the content and look-and-feel of email notifications
- Customize dialog boxes and error messages

White Labeling as a Defense against Phishing

Phishing is one of the most common and successful social engineering schemes. Phishing tricks people into clicking malicious links in emails or SMS messages, for example, to download malware or provide confidential data to criminals. The rise of web-service impersonation attacks, a type of phishing attack using a recognized brand, involves fake websites and emails that prompt people to give up their credentials to criminals. With the stolen credentials, attackers can login and impersonate the victim to steal funds – a problem compounded by the fact that people tend to re-use the same credentials across web services, potentially giving criminals access to multiple accounts.

It is increasingly common for hackers to pose as third-party vendors in phishing emails to end-users. According to TechRepublic, web service vendors such as Microsoft, PayPal, and DocuSign are among the top 10 brands most targeted by criminals in phishing schemes.[2] Because these are widely recognized brands, such phishing attempts yield high click rates.

While multi-factor authentication is the best defense against hackers trying to gain unauthorized access to your end-users' accounts, fully white labeling your e-signature workflow can help minimize the risks from phishing and impersonation attacks. If you are using an e-signature solution where the vendor's logo and brand are a prominent part of the e-signature experience, your end-user will logically create an association between your company and the e-signature vendor. If the vendor experiences a security or data breach, it can affect your organization by association. Furthermore, a vendor-branded experience puts your signers at risk. When a customer of yours is the recipient of a phishing scam, its main goal is to exploit their identity and personal information. If successful, it will impact their trust in your business and can cause them to rethink their relationship with you.

While white labeling cannot prevent phishing attacks, it makes the task more difficult for attackers and in doing so, reduces the incidence. As a digital security company that has prevented billions of dollars in potential fraud, we recommend white labeling every aspect of the e-signature experience.

Additional Considerations for Security & Risk Professionals

According to Forrester Research Inc., security and risk (S&R) professionals have been increasingly responsible for the success of their organization's identity and access management (IAM) initiatives.[3] Too often however, S&R pros fail to recognize that e-signature technology is more than just a signature and miss opportunities to influence how e-signatures are integrated within their organization's existing IAM framework. It is therefore the responsibility of S&R pros to contribute to designing an optimal end-to-end digital experience.

Forcing customers to authenticate themselves repeatedly and unnecessarily during the digital transaction impacts the quality of their experience. S&R professionals play a critical role in ensuring that e-signatures integrate seamlessly with existing IAM capabilities and avoid creating a clumsy experience for customers.

Many financial services companies and insurers, for example, already rely on third-party authentication services since they are often accessing credit databases as part of their everyday account opening and new application processes. Look for solutions that can integrate with these types of third-party services – at any point in the transaction – to create the most optimal customer experience.

Conclusion

Digital experience is a top priority as it affects employee and customer experiences – and organizations want both.

Enabling trusted experiences requires security. With electronic signatures it is important to take a broad view of security, from signer authentication to vendor independence.

It is also important to remember the need to balance security concerns with the usability of the solution. A good way to avoid over-engineering your security requirements is to recognize that your business processes (whether on paper or electronic) already have many security safeguards in place.

Trust and security are at the heart of digital transformation. At OneSpan, we have more than 20 years of experience delivering e-signatures and authentication solutions to ensure a secure experience across all digital and mobile channels. We can guide you in successfully digitizing your business processes, while providing your customers with a trusted and secure experience – no matter your use case, channel, or geography.

[1] Forrester Research, November 12, 2015, S&R Pros Must Play An Outsized Role In Selecting And Implementing E-Signature

[2] TechRepublic https://tek.io/33T04aW

[3] Paraphrased from concepts discussed in August 2015 Report, Forrester's Risk-Driven Identity And Access Management Process Framework

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
OneSpan.com/sign

Security for E-Signatures and E-Transactions: Best Practices Checklist

USER IDENTITY, AUTHENTICATION, AND ATTRIBUTION	
✔	Flexible user identification methods: • Remote user identification through third-party databases (i.e., dynamic knowledge-based authentication) • Remote user identification through personal information verification (PIV)
✔	Ability to upload images as part of the e-sign transaction (e.g. photo of a driver's license)
✔	Flexible user authentication methods: • Remote user authentication through user ID and password • Email address verification through e-sign session invitation • Remote user authentication through static knowledge-based authentication (i.e., secret challenge questions) • Ability to customize the challenge questions • Ability to leverage existing credentials • Ability to fully white-label the e-sign process to reinforce an end-to-end trusted experience
✔	Ability to configure different authentication methods within the same transaction
✔	Flexibility to adapt the authentication method to: • The risk profile of your organization • EACH process being automated
✔	Flexible options for in-person signature attribution: • Hand-off affidavits • SMS password (PIN) sent to a personal mobile device
✔	• Integration with strong, multi-factor authentication solutions (i.e., OneSpan's Digipass)
✔	Ability to sign using client-side certificates ("qualified certificates" under eIDAS) associated to an individual person
DOCUMENT AND SIGNATURE SECURITY	
✔	Audit trail information must be securely embedded in the document
✔	The document and EACH signature must be secured with a digital signature
✔	A comprehensive audit trail should include the date and time of EACH signature
✔	The audit trail must be securely embedded in the document and linked to each signature
✔	One-click signature and document verification (e.g., ability to verify documents and signatures offline, without going to a website)
✔	Ability to download a verifiable copy of the signed record with the audit trail
CLOUD AND DATA SECURITY	
✔	Flexibility in deployment methods to align with your IT and data security policies: • On-premises deployment • Public and private cloud deployment, hosted on world-class cloud infrastructure platforms such as Amazon, IBM and Microsoft
✔	SOC 2 and FedRAMP compliant e-signature solution
✔	Publishes security practices, certifications and the results of security audits
✔	Has a consistent track record of keeping customer data secure
✔	Global data centers to satisfy in-country data residency requirement