SECURITY & TRUST:

BEST PRACTICES FOR IMPLEMENTING ELECTRONIC SIGNATURES AND EVALUATING VENDORS

Digital transformation is changing the way we live and work. Across all industries and at all levels of government, organizations are providing services through digital and mobile channels. To create end-to-end digital experiences for their employees and customers, they are turning to third-party technologies like e-signatures. But how do these solutions protect company and customer data? How is data encrypted between the user, device and e-sign service? And how are users authenticated before being given access to the transaction?

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. It will also foster customer confidence and 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 & 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.

USER AUTHENTICATION GLOSSARY

- User identification: The process of verifying someone's identity, e.g., through government-issued photo ID or personal information.
- User authentication: The process of verifying user credentials.
- Personally identifiable information (PII): Information used to trace an individual's identity, such as name, SSN, date/place of birth, mother's maiden name, email address, etc.
- Non-public personal information (NPI): Personally identifiable information that is not publicly available, such as an account number or information in a credit report.
- Knowledge-based authentication (KBA): A means of authenticating someone by asking secret questions.
- User attribution: The ability to prove who actually clicked to apply an e-signature. This is a concern in face-to-face transactions when using click-to-sign on a shared device.

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., VASCO'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.

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.

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.

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.

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.

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:

❶ 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.

❷ 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.

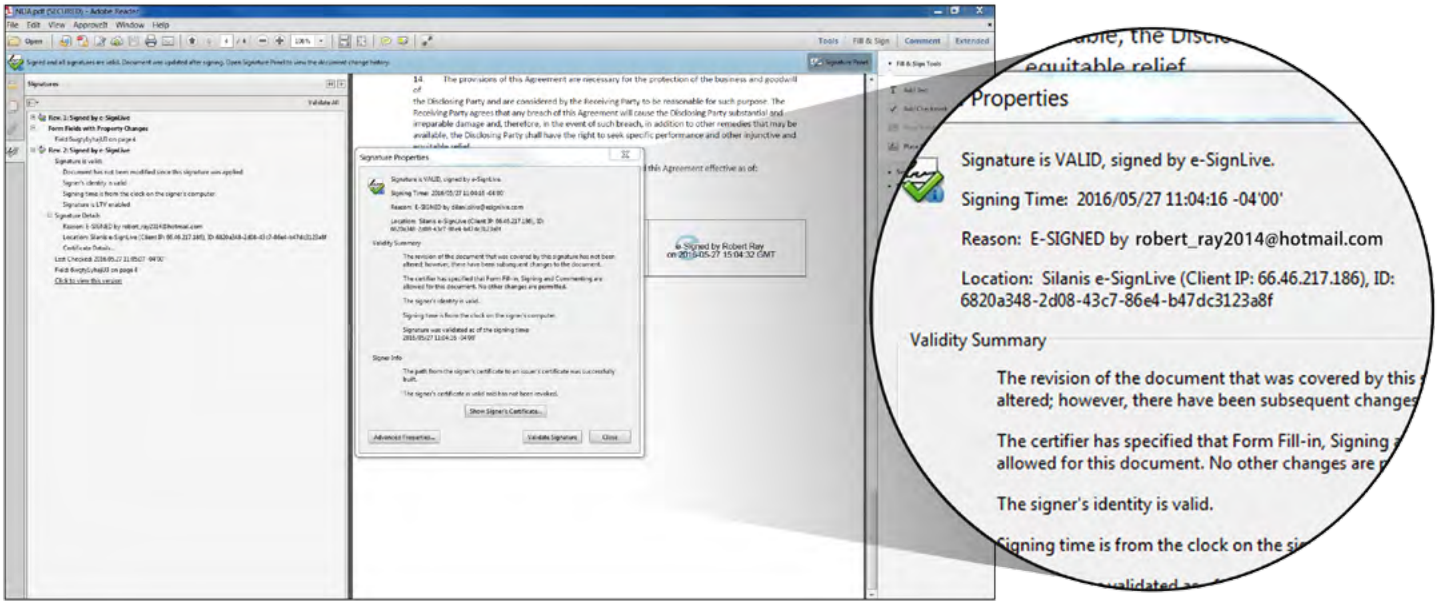
A simple way to verify document integrity

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 eSignLive's software, users click on the signature block. This opens the audit trail and automatically verifies both signer authentication and document validity.

A one-click process such as this simplifies the user

Verifying document and signature integrity within eSignLive



Properties

Signature is VALID, signed by e-SignLive.

Signing Time: 2016/05/27 11:04:16 -04'00'

Reason: E-SIGNED by robert_ray2014@hotmail.com

Location: Silanis e-SignLive (Client IP: 66.46.217.186), ID: 6820a348-2d08-43c7-86e4-b47dc3123a8f

Validity Summary

The revision of the document that was covered by this s altered; however, there have been subsequent changes

The certifier has specified that Form Fill-in, Signing a allowed for this document. No other changes are p

The signer's identity is valid.

Signing time is from the clock on the si

validated as of

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.

3- CLOUD SECURITY

Today's e-signature solutions are available both on-premises and on 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 eSignLive, 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 eSignLive 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, eSignLive maintains the strictest of controls.

eSignLive is also the only 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.

> 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.

eSignLive's carrier grade availability is ensured through the use of multiple availability zones and geographic regions, and by 24/7 monitoring (see the eSignLive 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. recently 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.

eSignLive offers both public and private instances of eSignLive 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 eSignLive 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 company's 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?

The advice we give our customers is to white-label the entire e-sign experience so that their brand, and only their brand, appears across the transaction (not the vendor's brand). This not only creates a trusted experience between you and your customer, it protects your brand 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.

Furthermore, according to Forrester Research Inc.[2], security and risk (S&R) professionals have been increasingly responsible for the success of their organization's identity and access management (IAM) initiatives. 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. Together with our parent company VASCO, 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.

Last updated: August 2016

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

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

For more information, contact a representative at

1-888-745-2647

or visit the eSignLive website today.

FREE TRIAL

About eSignLive™ by VASCO

eSignLive™ is the electronic signature solution behind some of the world’s most trusted brands. Regulated industries and top analyst firms recognize **eSignLive** products and services for their ability to balance the highest levels of security and compliance with ease-of-use while automating any process – from the simplest, internal signing workflow to the most complex, customer-facing transactions. Available in the cloud and on-premises, the **eSignLive** solution offers a scalable platform to support an organization’s digital transformation strategy across the enterprise – today and tomorrow.

eSignLive is the trade name of Silanis Technology Inc., a VASCO group company. VASCO Data Security International Inc., a global leader in authentication, electronic signatures, and identity management, enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions and protect assets across financial, enterprise, e-commerce, government and healthcare markets.
Learn more at **www.esignlive.com**

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., VASCO'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 & 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 requirements