Understanding E-Signatures: A Beginner’s Guide

Content Summary
1. Overview
2. Technology / Terminology
3. Compliance & Legality
4. Security
5. User Adoption
6. The E-Signing Process
7. Solution Options
8. Conclusion

Electronic signatures have seen significant adoption in the past decade within insurance, lending, government and other industries. Replacing manual, paper-based processing with automated, electronic signing processes has enabled organizations large and small to significantly reduce the cycle times, errors and costs associated with getting customers, partners, supplier and employees to review and sign documents needed to close new business, authorize decisions, and move operations forward.

Indeed, the impact electronic signatures have on an organization’s ability to deliver superior customer service, increase operational efficiency and improve bottom line results has often far exceeded initial expectations.

This beginner’s guide introduces business and IT executives to the key concepts and considerations for moving to paperless, signing processes, including:

1. Technology / Terminology: How solutions have evolved over the years to handle greater levels of complexity and automation, and what technologies they use at their foundation.

2. Compliance & Legality: How electronic signatures can help organizations to strengthen their legal and compliance position by capturing more comprehensive evidence than is possible with pen and paper.

3. Security: The three levels of security that need to be addressed in order to effectively mitigate risk: 1) user security, 2) document security, and 3) process security.

4. User Adoption: How to make the e-signing process easier than pen and paper, including the three requirements for ensuring that users adopt a solution.

5. E-Signing Process: What options are available for designing an electronic signing process that supports a variety of business requirements and environments.

6. Solution Options: A review of the three key solution options: 1) on-premises solution, 2) dedicated cloud service (SaaS), and 3) shared cloud service (multi-tenant SaaS).
1. Technology / Terminology

The core technologies used to develop electronic signature solutions have evolved tremendously over the years. The solution you choose will depend on the complexity of your business processes and transactions, and what level of automation you are seeking. Below are the key technologies and terms that you should be familiar with.

**Digital Signature**

The term digital signature refers to the encryption / decryption technology used as the foundation for a variety of security, e-business and e-commerce products. Based on public/private key cryptography, digital signatures are used in secure messaging, public key infrastructure (PKI), virtual private networks (VPN), secure socket layers, and electronic signatures.

Contrary to what the name might suggest, a digital signature alone is not a type of electronic signature. Rather, digital signature encryption can and should be used by electronic signature applications to secure the data and verify the authenticity of a signed record. Further, a digital signature alone does not capture a person’s intent to sign a document and be legally bound to an agreement or contract.

**Electronic Signature**

An electronic signature, like its paper equivalent, is a legal concept. The U.S. Electronic Signatures in Global and National Commerce Act (E-SIGN) defines an electronic signature as “an electronic sound, symbol, or process attached to, or associated with, a contract or other record and adopted by a person with the intent to sign a record.” Based on this definition, an electronic signature can be broken down into the following components: 1) a method of signing, 2) data authentication; 3) user authentication; and 4) capture of intent.

While many electronic signature solutions on the market may meet the baseline requirements outlined by the E-SIGN Act, organizations looking to minimize the risk of unenforceable records should aim to set the bar higher.

**Electronic Signature Process Management**

E-Signature process management builds on top of digital signatures and electronic signatures to execute transactions from start to finish, while automating the enforcement of business rules. The solution uses digital signature technology to secure and authenticate users, data and the signing process itself, while ensuring that all internal business controls, legal requirements and compliance requirements are met as documents are presented to people for review, acceptance and signing.

This is especially important in self-serve, web environments where there isn’t anyone to guide customers through a signing process, as well as for more complex transactions where documents and legal disclosures must be presented to people in the right order, and where signing processes and documents may differ between geographic locations. Further, an electronic signature process management solution typically integrates with an organization’s front and back-end systems to pull the correct documents and pre-approved data, and then return all documents once they are correctly completed so that downstream processes can be automatically triggered.

**E-SIGN Act**

The Electronic Signatures in Global and National Commerce Act (E-SIGN) is a U.S. Federal law that was passed in 2000 that enabled the use of electronic records and signatures for commercial transactions. The act essentially enables organizations to adopt a uniform e-signature process across all 50 states with the assurance that records cannot be refused by a court of law solely on the basis that they were signed electronically.

Because the act is technology-neutral and doesn’t favor any one type of solution over another, the onus is on the organization to determine how it plans to meet the E-SIGN Act’s requirements for capturing signing intent and authenticating data and signers.
2. Legality

Since the passing of the E-Sign Act, the question most organizations now have is not whether electronic signatures are legal, but rather, how reliable are they in helping organizations to defend their position should a legal dispute arise. The key to ensuring an enforceable e-signed record and staying out of court in the first place, is to capture and reproduce as much electronic evidence as possible.

As most organizations have experienced, the majority of legal disputes do not challenge whether a person has signed the document in question, or whether the signature in the document belongs to the person. Rather, the most common contract disputes concern the terms and conditions, or how well the person understood the agreement. “That’s not what I signed”, “I didn’t see the information / document”, and “I didn’t understand the information” are common arguments used.

This is underscored by recent judgments suggesting that it is not simply enough to have secure electronic records and signatures. In a landmark ruling on the admissibility of electronically stored information (ESI), US Magistrate Judge Paul W. Grimm discussed examples of the essential elements of an effective e-contracting process, notably “creating and securely archiving and retrieving an audit trail of the entire ESI management process, from the steps to verify the identity of the persons signing the record all the way through to sealing electronically the document and then securely archiving and retrieving the e-contract.”

Moreover, Judge Grimm noted, “These same steps enhance the overall persuasiveness of the hard copy of the e-contract as well.” - Excerpted from Lord, Bissell and Brook LLP, “From E-Discovery to E-Admissibility” “Lorraine v. Markel” and What May Follow,” June 2007.

Creating persuasive electronic evidence, as described above, can be accomplished by recording and reproducing the exact process used to build the person’s understanding of what they were agreeing to and signing. This includes the exact appearance and order of all of the web screens, documents and legal disclosure that were presented to people; how long they spent on each page; and all actions that they took during the review and signing process, such as clicking on buttons to accept, sign, initial and confirm.

Indeed, the more evidence an organization captures about what process was used, the more persuasive the evidence becomes and greater the chance that the signed document will be enforced in a court of law.
Security is always top of mind when organizations consider moving their signing processes online. Proper security fosters confidence amongst signers and ensures adoption, as well as ensures records can be reliably reproduced. To mitigate e-signing risks, security must be applied at three levels: 1) at the user level, 2) at the document level, and 3) at the process level.

**User Authentication**

Security at the user level helps attribute the signature to a specific person. During an electronic signing process, the identity of the person is verified or “authenticated” prior to signing documents, and then stored as part of their electronic signature.

Two popular methods for authenticating users include personal information verification (PIV) and credentials. PIV involves asking people to supply unique information about themselves, such as their address and telephone number, social insurance number, passport number, a line item in a revenue report, etc. While some transactions require that the information be then verified against the organization’s internal database or a 3rd party database, it is not required.

Once a person’s identity has been verified online, electronic credentials are often issued for subsequent transactions. Credentials include something the person knows (i.e. user ID / password), something the person has (i.e. digital certificate, smart cord, password token), or something that the person is (i.e. fingerprint).

When correctly executed, security at the user level deters people from claiming “It wasn’t me who signed” or “That’s not my signature”.

**Document Authentication**

Document security prevents the contents of a document from being modified and signatures from being copied into another document without visible detection. Digital signature security applied to a document at the time of signing is verified each time the document is opened. If a change is detected, the electronic signatures contained within the document will be visibly invalidated.

A signature audit trail should also be embedded within the document to enable additional security and signing information to be verified. This can include user authentication information, the method used to capture people’s signing intent (i.e. click-to-sign, signing on a pad, etc.), date and time stamping information, and the digital certificate that was used to secure the document.

The electronic signatures should also be permanently bound to documents and travel with them at all times to enable the documents to be securely emailed, stored and viewed from any location.

**Process Authentication**

The goal of process authentication is to prove what took place during the signing process, as described in the “legality” section of this article. This is accomplished by recording all the web pages, documents, legal disclosures and actions taken by users, and linking it to final e-signed documents in a manner that enables the process to be accurately reproduced from start to finish.

Electronic signature process management solutions capture evidence of the entire signing process, and create a cryptographic link between the process and the resulting electronic records. The electronic evidence enables organizations to demonstrate that the documents were presented in a consistent and compliant manner, regardless of the end-user’s system capabilities.

Reproducing all aspects of the transaction is especially important in web-based transactions because websites do not typically maintain complete logs of everything that took place during a transaction.

When correctly executed, security at the process level deters people from claiming “I wasn’t presented with that information” or “I didn’t understand what I was signing”.

Once a person’s identity has been verified online, electronic credentials are often issued for subsequent transactions. Credentials include something the person knows (i.e. user ID / password), something the person has (i.e. digital certificate, smart cord, password token), or something that the person is (i.e. fingerprint).

When correctly executed, security at the user level deters people from claiming “It wasn’t me who signed” or “That’s not my signature”.

Document security prevents the contents of a document from being modified and signatures from being copied into another document without visible detection. Digital signature security applied to a document at the time of signing is verified each time the document is opened. If a change is detected, the electronic signatures contained within the document will be visibly invalidated.

A signature audit trail should also be embedded within the document to enable additional security and signing information to be verified. This can include user authentication information, the method used to capture people’s signing intent (i.e. click-to-sign, signing on a pad, etc.), date and time stamping information, and the digital certificate that was used to secure the document.

The electronic signatures should also be permanently bound to documents and travel with them at all times to enable the documents to be securely emailed, stored and viewed from any location.
4. User Adoption

If the e-signing process is perceived as being more difficult to use than pen and paper, people will revert back to the old way of signing documents.

While security is critical for mitigating legal and compliance risks, organizations must also carefully balance security with usability so as to not jeopardize adoption. If the e-signing process is perceived as being more difficult to use than pen and paper, people will revert back to the old way of signing documents. Usability is just as critical for ensuring adoption amongst customers, partners and suppliers, as it is for internal stakeholders. Solutions that promote high user adoption typically have the following characteristics:

**Zero-Download**

Users are provided with the ability to instantly e-sign documents over the web without having to download or install any special plug-ins or additional software, as this has been known to increase drop-off rates. This can be accomplished by enabling users to sign by clicking on a button on-screen using their mouse. A zero-download solution is also recommended for field force and point-of-sale / service processes so that software and hardware do not need to be distributed on the company representative’s or agent’s computer systems.

**Guided and Automated Process**

Users are guided through the signing process and workflow is automated in order to save time, and prevent errors and data omissions. Typically, documents are presented to users sequentially in the correct order and visual cues prompt users to sign and initial in all of the right places. Users are prevented from signing in the wrong places and submitting documents if they forgot to sign in all designated areas or failed to enter any required information related to the application or contract agreement. Further, as users sign, additional signing information is automatically added along with their signatures, such as their name, title, company and date.

**Branded Process**

The user interface of the e-signing process can be customized to match the company’s website in order to reinforce their brand and to inspire confidence in the process. This is especially important in self-serve web environments where there may not be a company representative available to provide immediate support and reassurance.
5. The E-Signing Process

One of the most common questions organizations have about electronic signatures is “what does it look like, and how does it work?”. The answer depends entirely on the organization’s process. An enterprise, e-signature solution should provide flexible options for creating an e-signing process, and enable organizations to choose the best methods based on their unique process requirements for each sales or service channel in order to ensure an optimal user experience.

The diagram above illustrates a number of options for building end-user e-signing processes.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Access</th>
<th>Authentication</th>
<th>Consents</th>
<th>Presentation</th>
<th>Affirmation</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Email</td>
<td>J. Smith</td>
<td>Username / Password</td>
<td>Screen-based Review</td>
<td>Signature Pad</td>
<td>Secure Download</td>
</tr>
<tr>
<td>Web</td>
<td>Email</td>
<td>J. Smith</td>
<td>Password</td>
<td>Screen-based Review</td>
<td>Click-to-Sign</td>
<td>Paper Copies</td>
</tr>
<tr>
<td>Branch</td>
<td>Email</td>
<td>J. Smith</td>
<td>I Agree</td>
<td>Screen-based Review</td>
<td>Paper-based Review</td>
<td>Paper-based Review</td>
</tr>
<tr>
<td>Call Center</td>
<td>Email</td>
<td>J. Smith</td>
<td>Challenge / Response SMS Validation</td>
<td>Paper-based Review</td>
<td>Paper-based Review</td>
<td>Paper-based Review</td>
</tr>
</tbody>
</table>

**Channel:** The person fills out an application form on the organization’s website, visits a retail branch, contacts an agent / representative or the call center.

**Access:** The person is provided with a link to the e-signing process from within the application process itself, or an email containing the link is sent to the person inviting him / her to the e-signing session.

**Authentication:** The person enters his / her personal information or credentials, and is brought into the e-signing session. For in-branch signing, the person presents his / her credentials in paper format.

**Consent:** The person is presented with the E-SIGN Consent form, as required by U.S. law. If he / she does not consent to the use of electronic signatures, the person is provided with the ability to sign the documents using pen and paper.

**Presentation:** The person is presented with all required documents and legal disclosures on-screen. The documents can also be printed and presented in paper format for in-person signing sessions.

**Affirmation:** The person indicates his / her acceptance of legal disclosures and signs and initials documents by clicking on a button on-screen, or by hand-scripting his / her signature on a signature capture pad, iPad or other mobile device.

**Delivery:** The person is provided a secure, tamper-proof copy of the e-signed documents in electronic format, or in paper format.
6. Solution Options

The right solution will depend on the complexity of the business process that requires automating; the level of integration with an organization’s front and back-end systems; available IT and budgetary resources; and time-to-market requirements.

There are three broad categories of electronic signature solutions available on the market today: 1) a dedicated, on-premises solution, 2) a dedicated cloud service, and 3) a shared cloud service. The right solution will depend on the complexity of the business process that requires automating; the level of integration with an organization’s front and back-end systems; available IT and budgetary resources; and time-to-market requirements.

Dedicated On-Premises E-Signature Solution

Deployed behind an organization’s firewall, a dedicated on-premises solution requires an up-front investment and dedicated IT resources. This, however, is offset by the flexibility and control provided by the system. Because it is a dedicated instance of the solution, it is fully configurable and customizable to the organization’s unique brand, business process, compliance and IT requirements. It also gives organizations in highly regulated industries with stringent compliance and privacy requirements complete control over where the servers are located and data is stored.

A dedicated on-premises solution is typically available as an enterprise license. The licensing model makes it possible to anticipate precise costs over time and may provide a lower total cost of ownership, especially at higher volumes.

Dedicated Cloud Service

Electronic signature solutions are also available as a dedicated cloud service. This type of e-signature solution enables organizations to configure the service to their requirements, and seamlessly integrate e-signatures into their processes and systems. However, the cost and provisioning of the servers, hardware and software falls to the service or solution provider, thereby producing up-front time and cost-savings for the organization.

Cloud-based e-signature solutions can be licensed on a transactional basis. The elasticity of this pricing model may offer cost-savings, especially for organizations whose peak volumes occur during specific weeks or months of the year.

Shared Cloud Service

An electronic signature service can also be delivered as a shared service over the cloud. This option provides the fastest time-to-market at the lowest barrier to entry because the signing processes come ready to go, right out of the ‘virtual’ box.

This option is often referred to as ‘multi-tenant’, meaning that every organization that signs up for the service shares the same server, user interface, signing process, and storage device. Because shared cloud services are pre-configured, organizations have less flexibility to customize the signing process. They also do not have the ability to integrate the service with internal systems in order to achieve straight-through processing. Documents must be manually uploaded, prepared for e-signing and filled in by the person originating the signing process.

Applications that are well-suited for a shared cloud service include: Insurance policy delivery; real-estate documents, e-contracting, NDAs, sales agreements, SOWs, expense reports, and purchase orders.

A shared cloud service can be offered as a subscription or transactional basis.

Choosing the Right Solution For Your Needs

Each electronic signature solution has its strengths and limitations. The right solution depends on your process and compliance requirements, your time-to-market needs, and your budget and personnel resources. The first thing you must determine is the level of customization that your organization requires.
Conclusion

The evolution of electronic signatures over the past decade has made it easier and more affordable for organizations of all sizes to move to secure and reliable e-signing processes with the assurance that customers will embrace the technology and that e-signed records can provide even stronger legal evidence than its pen and paper counterpart.

To read more about the various subjects presented in this beginner’s guide, click on the links below:

- FAQs: Your Most Pressing Questions Answered
- How to Build Your Business Case and Calculate ROI
- Taking E-Signatures to Court
- How Much Security Is Enough
- How to Choose Between an On-Premises and SaaS Solution

About Silanis

Silanis’ solutions have processed hundreds of millions of e-signatures since the company was founded in 1992 (50 million in 2010 alone), making them the most widely used e-signature solutions. The world’s largest insurance and financial services companies, government agencies, and service providers depend on Silanis to accelerate business transactions and reduce costs while improving compliance with legal and regulatory requirements.