accusoft®

E-Signatures vs. Digital Signatures: Which Is Right for Your Business?

Electronic signature adoption has been on the rise among businesses since the Electronic Signatures in Global and National Commerce Act (ESIGN Act) was passed in 2000. With the sudden growth of remote work and emerging pressures to go digital, businesses are struggling to keep pace with the changing global environment. It's imperative that they figure out how to reduce manual, paper-based processes to maintain productivity.

Electronic record keeping enables businesses to complete their first step toward digital transformation. The ability to electronically sign documents anywhere in the world, crossing borders and barriers of distance, allows signers and originators to exchange agreements within minutes. Electronic signatures help businesses decrease their environmental footprint, greatly reduce costs on paper, and shorten document life cycles.

However, there is still a lack of awareness when it comes to the different types of signature technologies available. For example, the terms electronic signature (e-signature) and digital signature are often used interchangeably, but there are critical differences to understand when choosing the right product for your business.

At a high level, **e-signatures** are equivalent to signing documents with a handwritten or "wet signature" and are legally binding under certain conditions. They are ideal when users need to indicate the intent to approve or accept the contents of a document such as a contract, invoice, or lease agreement.

On the other hand, **digital signatures** are a category of electronic signatures that leverage algorithms to generate a unique digital fingerprint. They provide the most secure form of authentication using digital certificates. This extra security ensures signing parties are willfully entering into an agreement, and the agreement cannot be altered after signing.

Continue reading to see the benefits of signature technology and learn innovative ways to streamline daily processes and diminish manual oversight.

E-Signatures

According to the ESIGN act, an electronic signature is defined as “an electronic sound, symbol, or process that is attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”

In simple terms, this could be a graphical stamp of your hand-written signature, recorded verbal confirmation, or even your typed name on the signature line of a document.

Indicating an agreement to a contract, e-signatures are legally recognized and legally binding under the ESIGN Act and counterpart Uniform Electronics Transactions Act (UETA). Three main legal conditions must be met, among other best practices:

1) **Authentication:** Confirms the signer’s identity using various methods such as login, SSN, email address, or IP address.

2) **Intent:** A signer shows clear intent to electronically sign an agreement by typing or drawing their signature into a field.

3) **Retention of Records:** Records must be retained to accurately reflect the agreement by the business, allowing the signer to download a copy of the signed agreement.

Digital Signatures

Digital signatures are a form of an electronic signature, but not all electronic signatures are digital signatures. Digital signatures ensure electronic documents are **authentic** and use **encryption** to verify information has not been altered and is coming from a trusted source.

Complying with strict legal regulations, certificate based digital signatures are the most reliable assurance of a signer's identity. Digital signers are issued a certificate from a certificate authority (CA), and when a user signs a document, they are assigned a public key infrastructure (PKI), binding their identity to the document.

Creating digital signatures is a complex mathematical process only handled by a computer and is more secure than other forms of electronic signatures.

Which Signing Technology Is Right for My Business?

While there are many benefits to electronic signatures, many companies face hesitation to adopt new technologies. Whether the uncertainty stems from the cost, implementation time, onboarding procedures, or adjusting to a learning curve, convincing the stakeholders that these technologies hold value is crucial for success. In order to remain competitive, organizations should identify tedious processes in their workflows and learn how to solve them with technology solutions.

While both electronic and digital signatures are legally binding, most businesses choose the convenience of electronic signatures. However, since e-signatures are not regulated like digital signatures, it is often up to individual businesses to develop and implement their own application and code to conform to the requirements of authentication, intent, and records retention.

While an electronic signature is a graphical image placed on a document, it can't show if someone tampers with the document after signing. Digital signatures ensure non-tampering, verification, and independent adherence to standards.

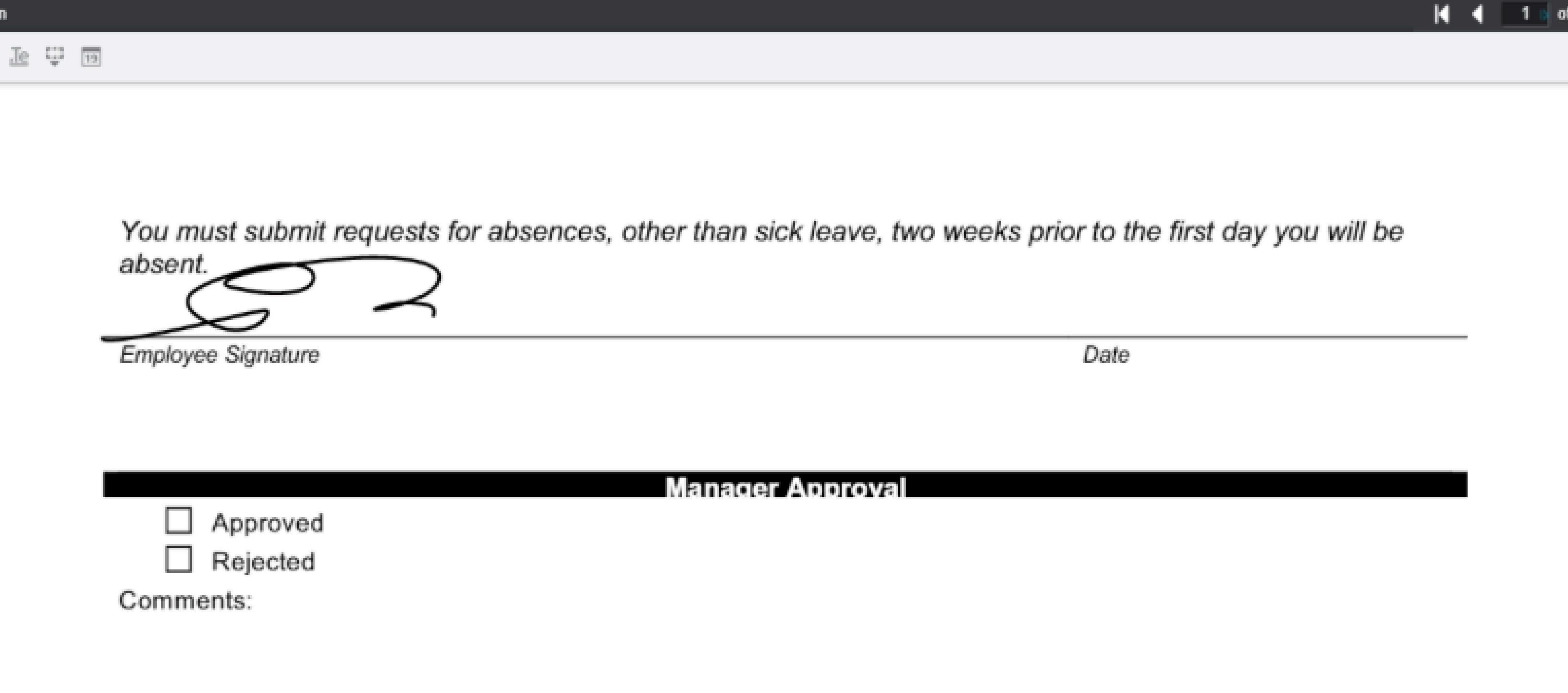
Identifying business drivers and security requirements help determine the appropriate electronic signature technology. Below are questions to evaluate when reviewing the three scenarios described in the following section.

- What is the level of sensitivity, assurance, and required proof of signer authenticity for documents to be signed?

- What processes and workflows does the organization need to design when deploying electronic signatures in their current technology?

- Will there be a need to route documents for additional role signatures and approval signatures?

- Does your organization follow any specific industry standards or compliance providing stakeholders a digital version of documents with certifying signature?



You must submit requests for absences, other than sick leave, two weeks prior to the first day you will be absent.

Employee Signature *Date*

Manager Approval

□ Approved

□ Rejected

Comments:

Scenario 1: Stamp Signature and Authentication

Stamping electronic signatures is the most common method used in low-risk workflows where issuing digital certificates to signers is not needed. Company standards should follow best practices for protection from repudiation.

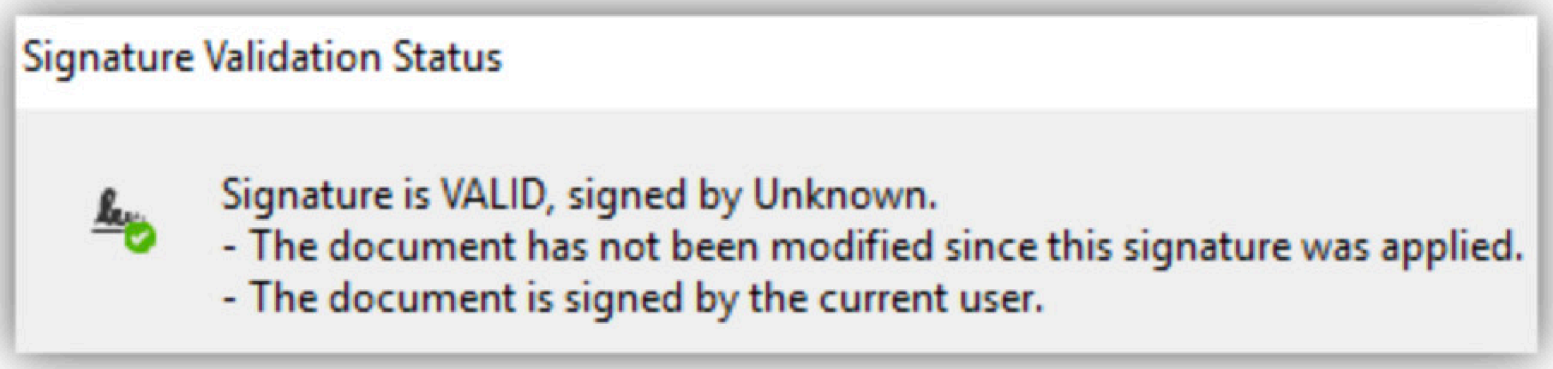
A typical use case could be an absence request form from HR where the employee signature capture is embedded in a web application. Here, the server simply applies a stamp acknowledging that the user has signed the document, before moving it through a workflow.

Another use case could be the deployment of a new hire orientation process. Consider Mary from Company XYZ needs Bob to sign an offer letter:

-Mary uploads the offer letter to an online document viewer such as PrizmDoc Viewer.
-After receiving credentials or other single factor authorization, Bob **authenticates** his identity by logging into the company's password protected portal to view and sign the document.
-Bob agrees with the offer, **intends** to be bound to the agreement, and uses PrizmDoc Viewer's eSignature feature to electronically sign the document.
-Once the document is finalized, Bob downloads a copy and maintains a record for himself.
-Mary **retains a record** of the electronically signed document, including any fillable form data via the web form API, in the company's document management system, integrated with PrizmDoc Viewer.

Advantages: These signature solutions are easy to deploy and cost less than digital signatures since no significant client PKI software is required. Authentication can be through the application or alternative authentication mechanisms.

Disadvantages: These solutions may be less secure because they lack tamper-evidence mechanisms.



Signature Validation Status

Signature is VALID, signed by Unknown.
- The document has not been modified since this signature was applied.
- The document is signed by the current user.

Scenario 2: Approval Signature(s) and Digital Certificate Verification

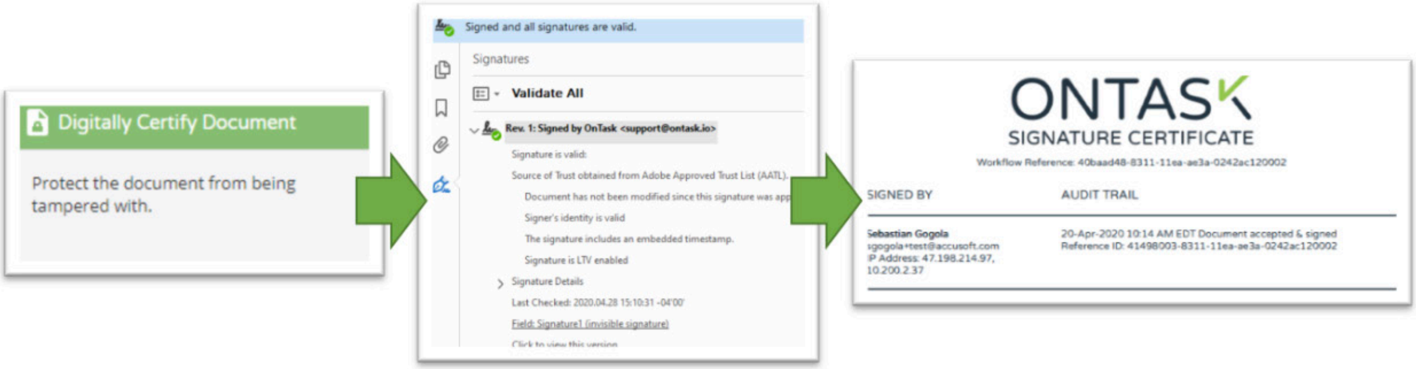
In our second scenario, building off the first, Mary has received Bob's offer letter and needs to gather final approval from other parties, such as the hiring manager. Mary can apply multiple approval signatures to the PDF, giving her the ability to detect and prevent unauthorized changes to a document as well as confirm the identities of the signers (digital ID issuers).

Using ImageGear, administrators can embed digital signatures into their applications to compare document contents from the time of signing to validation, throwing an error if there is a mismatch between the decrypted hashes.

Signers can apply approval signatures and verify digital certificates, provided the certificates used to sign the PDF are trusted. Developers can leverage a signature handler to specify the algorithm used to encode the signature, which is stored directly into the file to obtain the signed PDF document.

Advantages: These signatures expedite business approval procedures by capturing electronic approvals and embedding them within the actual PDF, proving that signer(s) have approved the content of a document.

Disadvantages: The contents of the document are locked once there is an approval signature, so no stamp signatures or annotations would be allowed post-signature.



Digitally Certify Document

Protect the document from being tampered with.

Signed and all signatures are valid.

Rev. 1: Signed by OnTask <support@ontask.io>

Signature is valid:

Source of Trust obtained from Adobe Approved Trust List (AATL).

Document has not been modified since this signature was app

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Signature Details

Last Checked: 2020.04.28 15:10:31 -04'00'

Field: Signature1 (invisible signature)

Click to view this version

ONTASK

SIGNATURE CERTIFICATE

Workflow Reference: 40baad48-8311-11ea-ae3a-0242ac120002

SIGNED BY	AUDIT TRAIL
Sebastian Gogola sgogola+test@accusoft.com IP Address: 47.198.214.97, 10.200.2.37	20-Apr-2020 10:14 AM EDT Document accepted & signed Reference ID: 41498003-8311-11ea-ae3a-0242ac120002

Scenario 3: Workflow Routing and Multi-Person Approval Processes

In our third scenario, consider forms that are sent to multiple participants for approval or authorization of payments. For example, procurement procedures where stakeholders in different routing stages must provide separate approvals.

Using our workflow management tool, OnTask, parties are able to certify the form before approval, assuring recipients the form is authentic and was sent from the issuing organization. It also assures the issuing organization that they are receiving the same form that was originally sent.

This type of software allows the signer to use PKI-based credentials to digitally sign an electronic document. The validity of the certificate can be checked any time a user opens the document in a PDF reader and views the signature information.

Advantages: The level of assurance is stronger than electronic signatures using only a password, and document integrity is maintained via standards-based digital signatures.

Disadvantages: Implementing internal client-based PKI can be costly and complex if not using managed services to help reduce administration and deployment burdens.

Conclusion

Manually signing documents is cumbersome and can result in a lengthy process or a record going unsigned. Even handwritten signatures risk being challenged to verify documents have not been tampered with. Businesses around the world can overcome these challenges by implementing electronic or digital signatures.

The advantages of using these types of signing technologies are:

- **Authentication**: A specific user is the bound owner of a signature and does not need a notary public or trusted authority.
- **Integrity**: Documents received by the signer are ensured to be the same document sent by the originator.
- **Efficiency**: Agreements can be signed within seconds from anywhere in the world using an internet connection.

For low-risk workflows where issuing digital certificates to signers is not needed, integrating PrizmDoc Viewer with your document management system (DMS) or other content management solution will provide users with the ability to sign and date documents or forms without leaving the application.

Conclusion

To evaluate Accusoft's HTML5 viewer and web APIs for document manipulation and modification in your own environment, download a trial now. We offer ready-to-run Docker Images as well as Windows and Linux installers.

For specific industries such as government, healthcare, or finance that must adhere to stricter authentication and security policies for their documents, ImageGear is a great choice. It allows developers to incorporate approval signatures into digital signature workflows in existing applications, as well as validate certificates for tamper protection. To try ImageGear for .NET, click here.

If organizations want the same level of security as ImageGear without the development time and effort, then our SaaS solution, OnTask, may be a better fit. On top of ensuring secure, trackable transactions with digital signatures, this workflow management solution can help automate entire document lifecycles. Start a free 14-day trial of OnTask today.

About the Author

Sebastian Gogola

Sales Engineer

Sebastian joined Accusoft in 2019 and works as a sales engineer supporting the company portfolio. He is a native of the greater Boston area and earned his degree in Network Administration after moving to Florida. Sebastian focuses on technical pre sales, serving all aspects of sales activities and sales channel development. Having worked in previous engineering and technical business development roles, he enjoys working with RESTful APIs and learning full stack development. In his free time he enjoys working on his personal blog, practicing piano, golfing, kayaking or running.

About Accusoft

Accusoft is a software development company specializing in content processing, conversion, and automation solutions. From out-of-the-box and configurable applications to APIs built for developers, we help organizations solve their most complex content workflow challenges. Our patented solutions enable users to gain insight from content in any format, on any device with greater efficiency, flexibility, and security.