



**A must-read primer to get
started with e-Signatures**



Trust, security, and compliance take center stage as organizations adopt digital signature solutions to adapt to the new normal.

Based on a technology standard called Public Key Infrastructure (PKI), electronic signatures are rapidly replacing handwritten signatures worldwide due to the heightened level of identity security and assurance. Moreover, digital signatures are a good fit for everyday use cases, including executing sales and vendor contracts, onboarding new hires, filling registration forms, and issuing employee certificates. They eliminate unnecessary paperwork, boost organizational productivity, and promote digitalization. By automating the signature workflow, companies experience significant improvements in speed of business, cost-effectiveness, and traceability. And they reduce their carbon footprint by removing paper-based processes.

Further, the COVID-19 pandemic has highlighted the need for digitalizing the process of sending documents and receiving signatures. Electronic signatures are transforming how businesses engage customers, business partners, and vendors in today's socially distant world.



What is available today?

e-Signatures are legally binding and use certificates and cryptographic keys to help users sign documents online quickly and conveniently. There are three types of electronic signatures:

- **Standard electronic signature** is simply a signature in electronic format, which doesn't necessarily require identity verification or signatory authentication. Such digital signatures are widely used for low liability risk documents across a variety of use cases.
- **Advanced electronic signature (AES)** requires identity verification, including multi-factor authentication, to protect documents with higher liability risk, with each signature linked to a specific signer. In the event of a dispute, the burden to prove the validity of the signature is on the signer.
- **Qualified electronic signature (QES)** comes with an added layer of security and requires a trust certificate issued by a third-party trust provider. The signer must verify their identity face-to-face in a live environment – in person or via audio/video conferencing. According to European Union's eIDAS regulation, QES is considered equivalent to a handwritten signature. It is used to safeguard documents with the highest level of liability risk.



How do e-signatures help enterprises?

Speed: Digital signatures are faster to execute than wet signatures, which require documents to be physically mailed to the signer.

- **Professionalism:** e-Signatures are an excellent way to position yourself as a professional entity capable of delivering exceptional value to partners and customers.
- **Added information:** With e-signatures, signers can include contact information, build trust in their business email, and create awareness about their brand.
- **Manageability:** Digital files are easy to share and store, and digitally signed contracts are simpler to amend during future negotiations.
- **Security:** More secure than wet signatures, e-signatures are based on public and private keys, preventing forgery or malicious use.
- **Cost:** Digital signatures significantly reduce the cost of printing and mailing paper-based documents.



e-Signatures in action

Digital signatures can help your organization enhance efficiency, identity security, and user experience across business functions, especially in highly regulated, largely paper-based industry verticals like BFSI and insurance.

Here is a table that lists popular use cases across industries and critical business functions:

Industry	Sample Use Cases
BFSI	Digitalize your agreements and contracts to minimize fraud; Capture detailed audit trail; Ensure seamless authentication for superior customer experience
Insurance	Deliver omnichannel experience with end-to-end transactions completed online; Get documents signed in the presence of witnesses; Streamline authentication methods
Government	Automate contract management; Enable highly compliant, cloud-based, and mobile-supported digital signatures
Staffing & Recruiting	Enhance the experience for your candidates by streamlining your onboarding processes
Technology	Accelerate the buying process with automated customer-facing workflows
Healthcare	Assure parties that the document is authentic and has not been modified



Business Function	Sample Use Cases
Finance	Automate signatures for invoicing, purchase orders, and audit sign-offs
Facilities	Ensure successful execution of agreements and manual activities such as sign-ins at the front desk
Human Resources	Automate management of employee-related documents and forms
Marketing	Streamline signing of documents like creative signoffs, SOWs, freelancer agreements, agency contracts
Legal	Manage and execute lengthy legal agreements with precision and ease
Customer/Technical Support	Electronically send documents, get signatures, and improve the customer experience



How secure are e-signatures?

By boosting the transparency of online transactions, e-signatures help build trust among enterprises and their customers, vendors, and partners. Not only are they alternatives to wet signatures, but they also provide a mechanism to prove that a document was not altered since it was last signed. e-Signatures leverage the following techniques and tools to ensure signatures are legitimate and tamper-proof:

- **Hash function:** Using a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other types of data, a fixed-length string of numbers and letters or 'hash' is created. That acts as a one-way function.
- **Public key cryptography:** This method uses a key pair system – a public key to encrypt the data and a private key to decrypt it.
- **Public Key Infrastructure (PKI):** Encompasses standards, policies, people, and systems to enable the distribution of public keys and validate signers' identities using digital certificates.
- **Digital certificate:** These are issued to a signer by a certificate authority (CA) after their identity is validated. They contain the signer's public key and are digitally signed by a CA.



Are e-signatures recognized globally?

Various regulations enacted by governments worldwide and more than enough legal precedent imply electronic signatures are valid, legally binding, and widely used in most countries. The Uniform Electronic Transactions Act (EUTA) and Electronic Signatures in Global and National Commerce Act (ESIGN) in the U.S. and the Electronic Identification and Trust Services Regulation (eIDAS) in the European Union are popular regulations that outline critical requirements for electronic signatures to be recognized as valid.

However, that brings up the question: how does one ensure the electronic signature solution they are looking to adopt is globally compliant? For example, according to EUTA, documents such as property transfers, court documents, creation and execution of wills, uniform commercial code, adoption, divorce, and other aspects of family law, are illegal to sign electronically. A future-ready electronic signature solution must be equipped to navigate those region-specific legal nuances and deliver a watertight signing workflow.



The way forward

This guide highlights the many benefits of deploying an agile, next-generation electronic signature solution. But what makes such a solution a good fit for your organization? Here is a checklist of features you must consider when you're ready to adopt an e-signature solution:

- It should be certified to meet stringent regulatory and security requirements and be globally compliant.
- It should have intuitive features, drag-and-drop functionality, and a user-friendly interface.
- It should produce comprehensive audit reports for non-repudiation.
- It should enable bulk signing and approval with bulk consent.
- It should provide Witness eSigning capabilities via audio/video conference.
- It should easily integrate with contract lifecycle management, CRM, and other enterprise systems.
- It should offer multiple authentication methods, including email link click authentication, phone OTP, signing password, and account-based authentication.



Certinal – The solution to the question of to sign or esign

Certinal eSign is a digital signature solution integrated with Zycus contract management services to provide the efficacy needed in keeping with the mission to go paperless.

Using Zycus Certinal, contracts can be created and shared securely for approvals, thus eliminating cumbersome paper-based workflows. Certinal eSign uses Artificial Intelligence (AI) to speed-up document reviews and implement safeguards for greater accuracy. Certinal also highlights important facets such as expiry dates in contracts in real-time. With each signer's digital imprint tracked and not just for cosmetic purposes, the digital footprint of the signature logged at every point of its usage provides a complete audit trail.

When the workforce is distributed, regulations dictate fewer human touchpoints, and the market demands everything to be done faster; Certinal bridges the gap in documentation signature, validation, and compliance.

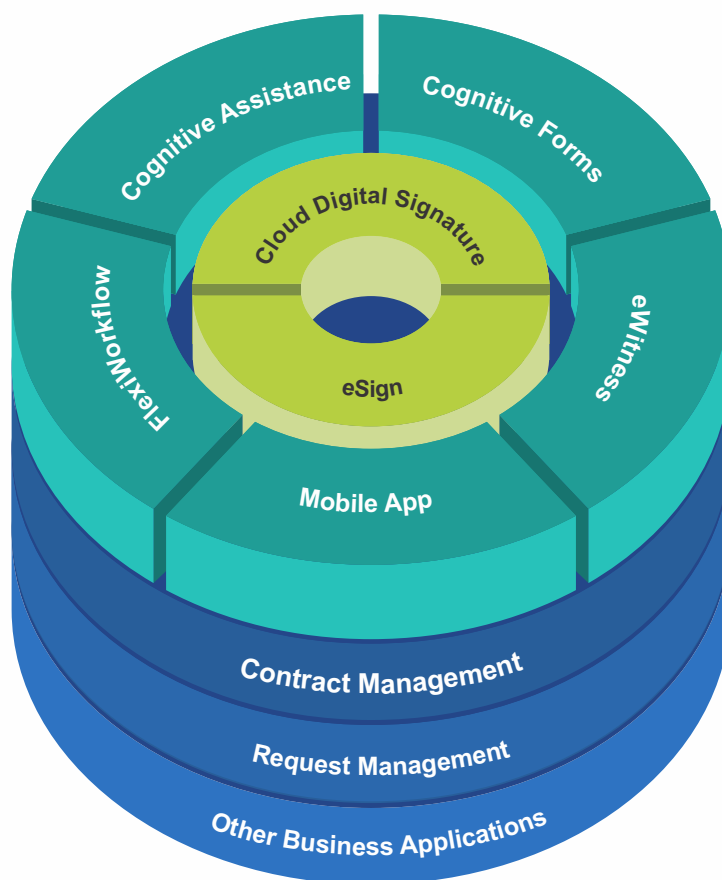
Certinal eSign does that and more.

Schedule a demo today to experience our trusted, secure, and globally compliant e-signature solution.



Why trust Certinal?

Certinal is a wholly owned subsidiary of Zycus, the pioneer in Cognitive Procurement. A familiar name and market leader with years of experience in managing critical contracts & agreements, Zycus boasts of over Fortune 1000 enterprise clients and deployments of procurement and sourcing suite of products. Digital Signing has always been a focus area for Zycus. Thus Certinal was born with the stated goal of offering a best-in-class Digital Transaction Management solution that will be easy-to-use, 100% secure to deploy, and legally compliant around the world. We stand committed to providing a one-stop solution to large enterprise customers, compliant with various security standards and conforming to different regional regulations.



Email- switchto@certinal.com