

8 Trusted Authentication Methods for Digital Signatures

What is Authentication?

Used alone or in combination, authentication methods verify a person's identity to participate in a trusted transaction.

Categories of Authentication



KNOW

Something You Know
e.g. (Password)



HAVE

Something You Have
(e.g. Hardware or software authenticator, Government-issued smart card, Mobile phone)



ARE

Something You Are
(e.g. Biometrics such as fingerprint or facial recognition)



Email Authentication

The signer is sent an email, inviting them to access the digital sign ceremony by clicking a link. Authentication happens with a successful login to the email account



Login Credentials

Before allowing access to the transaction, the sending party's system authenticates the signer. A valid user ID and password are necessary for login



Biometric Comparison

In transactions with unknown signers that carry a high level of risk and value, biometric comparison is frequently employed. Signers can quickly and easily confirm their identity by taking a self-portrait, which will be compared to the photo on their official ID card



Smart Cards and Derived Credentials

When e-signing, authorised personell need to have a smart card or mobile-derived credentials. This type of multi-factor authentication uses the user's PIN along with a smart card or token



Sms Authentication

Utilize a safe, one-time SMS number given to your signer's phone to confirm their identity. To access the documents that need to be signed, the signer must enter the code on the login page



Government Id Verification

Verify distantly unknown people using government-issued identification (such as a driver's license, passport, etc.). Certinal uses digital identity verification to collect, extract, and analyze ID data in order to validate identification documents issued by the government



Digital Certificate

Digital certificates, which are issued by third parties such as Trust Service Providers (TSP) and Certificate Authorities (CA), are used to verify the user's identity while signing documents



Two-factor Authentication

Multi-factor authentication is authentication that creates one-time passcodes (OTP) to be used in conjunction with a PIN or fingerprint as an additional authentication element

Our Featured Customers



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-touse, 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.



9
Offices
Globally



30-50%
increase in
customers'
savings



100%
Compliance with
global and local
eSignatures laws



70+
Countries with
eSignature laws that
Certinal supports



4
Patents



50%
Higher Partner
Commission



100+
Connectors & Open
API 3.0 Standard
Allows Seamless
Integrations



Gartner

Representative
Vendor in **Gartner's**
Market Guide for
Electronic Signatures



Our Trusted Partner

