10 Authentication methods for secure eSignature transactions

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

2 Login credentials
The signer is authenticated by the sending party's system prior to accessing the transaction. Login requires a valid user ID and password.

3 SMS OTP
Verify your signer's identity via a secure one-time SMS code sent to their phone. The signer enters the code into the login page to access the documents that require signature.

4 Secret challenge question
The signer must successfully answer challenge questions. These are referred to as "shared secrets" because the question and the answer sets are pre-selected ahead of time.

5 Digital verification
Verify unknown individuals remotely using government-issued IDs (e.g, driver's license, passport, etc.). OneSpan Sign leverages digital identity verification to extract and analyze ID data in order to confirm the signer's identity.

6 Biometric comparison
Typically used for high risk, high value transactions with unknown signers. Signers can take a selfie and it will be compared against the photo on the government-issued ID document to verify their identity in seconds. Passive and active liveness detection help confirm that the person is real.

7 Knowledge-based authentication
OneSpan Sign is integrated with a 3rd party service like Lexis Nexis to present the signer with challenge questions in real time, based on data in consumer databases.

8 Smart cards and derived credentials
Federal workers use smart cards or mobile credentials that contain an embedded digital certificate. To access it, users authenticate via a PIN and sometimes biometrics.

9 Digital certificates
Issued by 3rd parties like Trust Service Providers (TSP) and Certificate Authorities (CA), digital certificates are used at the time of signing to validate the user's identity.

10 Passkeys
FIDO-based passkeys provide strong multi-factor, phishing-resistant authentication using mobile device-based biometrics. Passkeys work exceptionally well for frequent signers.

Definition of 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

HAVE
Something you have

ARE
Something you are

Examples of eSignature authentication

Channel → Transaction → Sample authentication method

Channel	Transaction	Sample authentication method
Online	Mortgage application	Banking portal login credentials or valid email address + SMS OTP or passkeys
Online	Internal employee review	SSO
Online	Vendor contract	SMS OTP or passkey

Channel	Transaction	Sample authentication method
Mobile	Bank account opening	ID verification with biometric comparison or KBA (new customer)
Mobile	Government employee procedure (vacation request)	SSO (federal employees also use a smart card or derived credential)
Call center	Insurance claim	Valid email address or customer portal login credentials

Whether you are configuring an automated eSignature workflow via API or manually sending a one-off request for signature, adding authentication is a simple yet powerful step to secure your digital agreements, data, and reputation.