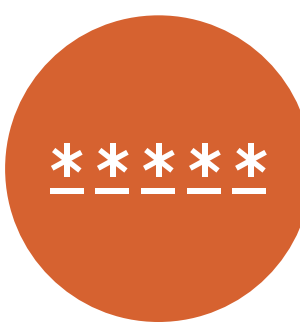# 10 Trusted Authentication Methods
For E-Signature Transactions

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

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.

SMS AUTHENTICATION
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.

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

GOVERNMENT ID VERIFICATION
Verify unknown individuals remotely using government-issued IDs (e.g., driver's license, passport, etc.). OneSpan Sign leverages digital identity verification to capture, extract, and analyze ID data in order to authenticate government-issued identity documents.

BIOMETRIC COMPARISON
Biometric comparison is 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 their government-issued ID document to verify their identity in seconds.

KNOWLEDGE-BASED AUTHENTICATION (KBA)
When the e-sign service is integrated with 3rd party ID verification services like Equifax, the signer is presented with knowledge questions in real time.

SMART CARDS AND DERIVED CREDENTIALS
Federal employees and contractors require a smart card or mobile derived credentials when e-signing. This is a form of multi-factor authentication: the smart card or mobile device combined with the user's PIN.

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.

DIGIPASS
Digipass® is a multi-factor authentication solution that generates one-time passcodes (OTP) for use with another authentication method, such as a PIN or fingerprint.

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
(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 a fingerprint or facial recognition)

Examples of E-Signature Authentication

Channel	Transaction	Sample Authentication Method
ONLINE	MORTGAGE APPLICATION	Banking portal login credentials or valid email address + SMS OTP
ONLINE	INTERNAL EMPLOYEE REVIEW	SSO or email authentication
ONLINE	VENDOR CONTRACT	Username & password + Vendor ID #
MOBILE	BANK ACCOUNT OPENING	ID Verification with biometric comparison and government ID verification 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