OneSpan Sign

eSignature Security Checklist

Signer Identity Verification

The first time you interact with someone online, it's important to verify their identity to be sure they are who they say they are. When evaluating eSignature solutions with integrated ID verification, ask if the solution supports:

Digital ID verification using document verification (with optional facial comparison).	Document verification is the process of scanning a government-issued ID document to determine if it is legitimate, and comparing the photo on the ID against a selfie provided by the applicant.
Liveness detection.	Liveness detection (i.e., when the person blinks or smiles to prove they are present) helps ensure they are not using a photo to impersonate anyone.

Cloud And Data Security

When evaluating solutions, verify if the eSignature vendor:

Publishes security practices, certifications, and the results of security audits.	Due diligence around security practices and infrastructure could expose past privacy breaches, incidents of data loss/leakage, or other risks such as insufficient cloud security expertise.
Has a consistent track record of keeping customer data secure.	Verify that the eSignature platform uses strong data encryption in transit and at rest, and stores data within an encrypted database volume to ensure an encrypted channel for all communications.
Provides a SOC2, FedRAMP-compliant, and ISO certified eSignature solution.	Leading cloud infrastructure service providers are designed and managed according to security best practices and comply with a variety of regulatory, industry, and IT standards for security and data protection.
Has global data centers to satisfy in-country data residency requirements.	Always-on disaster recovery sites in different geographic regions allow for rapid recovery, should a disaster affect primary facilities.

Signer Authentication

When you require a signature from an existing customer, their credentials need to be verified before accessing the signing ceremony. Ask if the eSignature solution supports:

Ability to leverage existing credentials (SSO).	This gives an organization the ability to use existing credentials (e.g., a passkey) to login to the signing ceremony.
Remote user authentication through email.	Ask the signer for their email address and email them a link to the signing ceremony. The link takes them to a secure site where they will sign. This helps authenticate the signer because they accessed the link through their email account. We recommend pairing this with a second authentication method, such as SMS one-time passcode.
Remote user authentication through knowledge-based authentication (KBA).	OneSpan Sign can connect to LexisNexis, a third-party credit bureau, to obtain a multiple-choice questionnaire that is generated in real time and presented to the signer.
Q&A authentication.	Secret challenge questions are agreed upon beforehand over the phone, and are used by the signer on the login page. The signer must answer the questions before gaining access to the documents.
Smart cards.	Government organizations need the ability to eSign using digital certificates stored on PIV and CAC smart cards.
Support for digital certificates.	Some of the highest assurance signing processes require that the signer use a digital certificate issued by an independent certificate authority (CA).
Ability to adapt the authentication method.	No two signing processes are exactly alike. You should be able to adapt your authentication to the risk profile of your organization and to each process.
Ability to configure different authentication methods within the same transaction.	If needed, add extra security for each signer. For example, internal signers can sign only with email authentication, while external signers use SMS-OTP or ID verification.

Document And Signature Security

An eSignature solution should secure the final eSigned document so you have integrity and reliability for the long term. When evaluating solutions, determine whether:

The document and each signature are secured with a digital signature.	This safeguards the integrity of the signed document so it is tamper-sealed, enforceable, and compliant. Look for a solution that immediately tamper-seals the document as soon as the first person is done signing.

Audit Trail Security

Evaluate whether the eSignature solution allows for the following:

Is the audit trail securely embedded in the document?	All electronic signatures, time stamping, signer identity, and location should be embedded directly within the document for each signer. That provides the "who, when, where" directly in the document without having to refer to a separate document.
Does it include the date and time of each signature?	If a signer and a co-signer eSign a record on two separate days, that history must be reflected in the audit trail. To enable this, make sure a digital signature is applied as each eSignature is added to the document.
Is it linked to each signature?	This provides versioning, which allows you to see the signing history and view the document exactly as an earlier signer did.
Do you have a single record that covers all events, including ID verification?	The audit trail should be comprehensive, yet simple to access and read, in order to stay compliant.
Can you verify documents and signatures offline?	Allowing the signed document to be validated independently of the eSignature software provides vendor independence.

White Labeling

The ability to fully white-label the eSign process puts the spotlight on your brand. This increases customer completion rates and reduces the risk of phishing scams. When evaluating solutions, ask if it:

Allows you to fully remove the vendor's brand from the UI.	Customers expect to see your brand throughout the process, not the eSignature vendor's. This helps create a trusted experience.
Can integrate with your own email servers.	Integrating with your email servers ensures the eSign emails are sent from your domain (e.g., @yourcompany.com). Using your brand's domain is a key defense against phishing and impersonation attacks.
Allows you to customize...	• The content and appearance of email notifications • The colors, logo, headers, navigation bars, and footers • Dialog boxes and error messages

About OneSpan

OneSpan provides security, identity, electronic signature, and digital workflow solutions that protect and facilitate digital transactions and agreements. The Company delivers products and services that automate and secure customer-facing and revenue-generating business processes for use cases ranging from simple transactions to workflows that are complex or require higher levels of security. Trusted by global blue-chip enterprises, including more than 60% of the world's 100 largest banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at
OneSpan.com

Contact us at
OneSpan.com/contact-us