

8 Things to Look for in a Digital Signature Vendor

- Authentication and Identification** Users must prove they are who they say they are by validating or accessing some type of shared information.
- Audit Trail** A feature that tracks the actions of signers and documents in each transaction to provide evidence of the entire transaction taking place.
- Notice and Consent** ESIGN and other laws require that users know they are engaging in an electronic signature process and must be able to opt out.
- Signature and Intent** The user must take actions to electronically sign documents to clearly indicate the intention to sign.
- Association** The signature must be linked to the data or records being signed to prove the connection between them.
- Integrity** A user's signature must be tied to the version of the document they are looking at during signing. Documents must remain the same after they sign, and the document should alert the reader if anything has changed.
- Verification Independence** You should choose a vendor that does not require an online link back to the vendor to validate signatures.
- Long-term Standing** Signatures should be based on standards to be considered valid not just today but decades down the road.

Want to learn more about what makes a digital signature legal?
Click here to download our **free** white paper.