ITD E-Signature Recommendations

When replacing wet signatures with electronic signatures, the following electronic signature options are available:

- Typing your name into an unlocked document.
- Placing a scanned image of your signature into an unlocked document.
- Attaching a document to an email and stating “I approve,” or “I concur” in the email body.
- Applying a self-signed digital certificate to sign and lock a document from changes to content.
- Applying a trusted digital certificate to sign and lock a document from changes to content.
- Giving the document to a vendor-supplied cloud service to gather signatures from individuals that it authenticates, finally locking the fully-signed document in a trusted digital certificate that locks the document.
- Using the methods required by a business partner or government entity to meet their standards when signing a document they sent to us.
- Signing using custom application software with its own built-in way of signing (like our current leave slip signatures in DOTtime).

Recommendations

We must always defer to established policy or laws that require a particular e-signature choice. For example, see WSDOT’s COVID-19 FAQ for temporary policy updates.

For any of the recommendations below, *please review your individual situation with your AAG.*

1. Use free or low-cost solutions when the signing source is easily verifiable. Ask yourself:
    a. Was the pen signature ever questionable?
    b. Can’t I simply call the signer if I have question about intent?
    c. Low/no-cost solutions include email approvals, typing your name or using your scanned signature image into an unlocked document.
2. Use self-signed digital certificates when you’d prefer the document content to be locked after the first signature and the signing source is easily verifiable. Self-signed digital certificates are free. How-to examples: Adobe Acrobat - Creating Signatures and Adobe Acrobat - Signing Access Approval Form .
3. Use trusted digital certificates when you’d prefer the document content to be locked after the first signature and you’d prefer 3rd party authentication of the signer. Each signer must annually purchase a trusted certificate from a certificate authority. e.g. DigiCert and others.
4. Use WSDOT’s Adobe Sign offering when you’d prefer the document to be locked and you want a 3rd party to authenticate and provide an audit history of who signed, from what device, and when. This solution costs the business area using it on a per signed document basis. Usage examples: Construction Office example introduction to Adobe Sign.

More information about these choices is available in the following table:

E-Signature Usage Scenarios	*Electronic Document Locking*	*Signer Identity Verification*	*Suggested Solution*	*Cost ballpark*
High risk or High value Documents requiring signatures	Required	3rd Party verification	**Cloud service** controlled E-Signature Ceremony (e.g. Adobe Sign, DocuSign, others)	$1-3 per signature package, depending on enterprise overall usage
Documents with average risk (internal or external)	Recommended	Can be determined by common methods.	Digital Certificates applied using **desktop software** like Adobe Acrobat, Bluebeam Revu, and others	Self-signed certs are *free* CA-certs $200-300 per person per year Bluebeam $200-300/person
Low risk Documents where business relationships are strong or we have no concerns of fraud (internal or external)	Optional	Can be determined by common methods.	Scanned image signatures dropped into an unlocked document using any **office productivity software**; typing "I approve and name, date" in lieu of a signature, email approval. Low-tech easy solutions. Usually they rely on email source and timestamp to verify plus phone conversations if there are questions.	No cost
Documents or software sourced from external business partners using their e-signature solution			Accept the **external business partner's solution**, with AAG approval	Likely free – business partner’s paid-for solution
Custom Software Application with form submittal or approval built-in	Data editing controlled by the custom software (CRUD) permissions that control data editing	User is logged in to custom software. Records track activity of users. Signature event could require re-entering their log-in credentials.	**Custom software** written internally or by a vendor	Generally high cost for custom software

Risk is an assessment of **severity** multiplied by **likelihood**.

For e-signatures, severity refers to the negative outcome associated with fraud. Likelihood refers to the chances that fraud could happen for the given document. Has fraud ever happened before with the specific document? Is it more likely to happen if you move to electronic signatures?

The most important question is: did the signer intend to sign? This can often be established by contacting the signer by phone or email and asking them. If email was used to send the signed document, verify the sender email address.

The question of authority to sign cannot be determined from a pen and paper signature, and is not any easier to determine with electronic signatures. (*It is possible to write a custom software application that may provide better assurances of authority to sign. Most of the solutions above do not have this feature*.)

Finally, consider this question when making your decision about e-signature method: *How much harder should it be to sign electronically compared to a wet signature?*

Each of you has different considerations for the specific form being signed. *One size does not fit all.*

For more information, you can review the OCIO's guidance.