LAND USE & TRANSPORTATION MEMORANDUM

Engineering, Traffic and Survey

To: Holders of Washington County Road Design and Construction Standards (Road Standards)

From: Stacy Shetler, PE, County Engineer Stacy Shetler Digitally signed by Stacy Shetler Date: 2023.03.22 15:12:18 -07'00'

Date: March 22, 2023

Subject: Engineering Plan Submittal Requirement Updates

Plan submittal requirements in the Road Standards are set forth in Section 210 and Appendix E. To provide efficiency, sustainability, and reduce costs, plans submitted to the County at all stages (plan review, permit issuance, and as-builts) shall be electronic. Applicable electronic plan sheets shall be submitted in PDF file format and shall be stamped and digitally signed by the responsible Engineer of Record. Engineer stamp & signature shall comply with OSBEELS digital signature requirements (for additional guidance, see attached ***Digital Signature Guidelines for Professional Engineers***).

Engineering plan sets that include multiple stamping engineers may encounter issues preserving digital signatures for each engineer. To preserve digital signature integrity, Engineering plans that include digital signatures from multiple engineers may be combined into a single PDF using the Adobe Acrobat Binder/Portfolio tool (or equivalent method approved by the County). This method is used to assemble PDF files while retaining their individual identities, similar to an electronic folder. Individual PDF files can then be extracted by the County to meet OSBEELS digital signature requirements.

EXCEPTIONS

Projects submitted with fewer than eleven (11) plan sheets or originally submitted with "wet signature(s)" are exempt from the above electronic submittal requirements. Projects exempt from the above requirements are still subject to Section 210 and Appendix E of the Road Standards, including submittal of original "wet signed" plans. In addition, applicants must submit a scanned copy of the signed plan set in PDF format with a minimum resolution of 300 dpi (dots per inch).

Please note that projects submitted with a "wet signature" may experience longer processing times due to the physical handling of paper documents. Therefore, it is highly recommended that engineers use digital signatures that meet the OSBEELS requirements. The electronic submittal exemption for number of plan sheets will expire one year from this notice.

Attachments:

Digital Signature Guidelines for Professional Engineers

DIGITAL SIGNATURE GUIDELINES FOR PROFESSIONAL ENGINEERS

PURPOSE

Revised 3/22/2023

In an effort to improve efficiency and stay current on technology, Washington County is requiring digital signatures on most engineering documents. Since digital signature technology is constantly evolving, there is common confusion regarding minimum requirements. This document will assist in ensuring compliance by all partners with the County. Digital signatures provide the following benefits to the County:

- **Reduced Waste.** Using digital signatures reduces the need for paper, allowing projects to be delivered electronically.
- **Increased Efficiency.** Digital signatures streamline the plan development and plan approval process.
- **Reduced Cost.** Reduced costs are the immediate byproduct of reduced waste and increased efficiency. Decreased administrative oversight leads to additional costs savings.
- **Improved Security.** Certification Authorities (CA's) require a strict identity verification process and includes multiple levels of security. A document that is digitally signed and verified by a CA meets rigorous security and legal requirements.

BACKGROUND

When considering whether a digital signature meets OSBEELS requirements, refer to the following:

OSBEELS refers to Oregon Administrative Rule (OAR) 820-025-0010, which states:

(1) A "Digital Seal and Signature" is a signature and electronic authentication process that is attached to an electronic document.

(2) A "Digital Seal and Signature" is not a photocopy, scanned copy, or other facsimile of a signed and sealed hard copy document, nor is it a copy or facsimile of a rubber stamp seal and ink signature, nor is it a copy of a computer-generated image of a seal and ink signature. Seals and signatures in this subsection (2) of the rule are not allowed on final documents.

(3) For electronic final documents, a "Digital Seal and Signature" ("digital signature" is acceptable as an alternative to a stamped or computer-generated image of a seal with handwritten signature in permanent ink, if:

a. The digital signature is unique to the registrant using it;

b. The digital signature is independently verifiable by a Certificate Authority (3rd Party);

c. The digital signature is under the sole control of the registrant using it;

d. The digital signature is linked to the document in such a manner that the digital signature is invalidated if any data in the document is changed;

e. *The electronic file that is the final electronic document contains one digital signature that is permanently linked to it;*
f. *For final electronic files containing a single page, the registrant affixes a computer–generated image of a stamp that bears the phrase "digitally signed" in lieu of and in the location designated for a hand-written signature on that page. The computer-generated image of the stamp must be of a stamp as described in OAR 820-025-0005(1) and (2), including the size prescribed in OAR 820-025-0005 when the page is printed to full size; and,*
g. *For final electronic files containing multiple pages not considered drawings, surveys, or plats, the registrant affixes a computer-generated image of a stamp that bears the phrase "digitally signed" in lieu of and in the location designated for a hand-written signature to the title page, an index page, or a seals page, provided that the stamped page clearly identifies all the other pages comprising the electronic file. The computer-generated image of the stamp must be of a stamp as described in OAR 820-025-0005(1) and (2), including the size prescribed in OAR 820-025-0005 when the page is printed to full size.*

ELECTRONIC SIGNATURE VERSUS DIGITAL SIGNATURE

The term *electronic signature* is defined as any signature stored in an electronic format and covers a wide range of types. Scanned signatures, computer generated signatures (i.e. writing with a pen on a tablet), self-created signatures, and *digital signatures* are all examples of an *electronic signature*. Since most forms of *electronic signatures* lack any form of identity validation, they can not be audited for legal purposes.

Digital signatures, per OSBEELS requirements, adds a layer of security to *electronic signatures* by utilizing a *Personal Key Infrastructure* (PKI) into the signing process as a way to identify both the party requesting a signature and the party providing one. A personal PKI is issued to an individual by a *certificate authority* who verifies their identity.

As an example, Bob receives a private signing key from certificate authority ABC, Inc. When Bob goes to sign a drawing, he utilizes this private signing key to digitally sign the drawing. Behind the scenes, a public key is embedded into the drawing and is transmitted to any recipient who opens the drawing. When someone opens the drawing, the public key is checked against the certificate of company ABC, Inc. to ensure the individual identified has been verified. This process has three layers of security: the individual private key, the transmitted public key, and the certificate of company ABC, Inc.

Digital signatures have the following benefits:

- Digital signing requires the use of a digital certificate that utilizes a signing algorithm. This creates a unique electronic fingerprint that can be validated in the document.
- The digital certificate that is used for digital signing is issued to only one individual, for whom his/her identity has been verified by an independent company. This provides a credential that is like a driver's license or passport in terms of security.
- When a document is digitally signed, it will include multiple auditable attributes including name of signer, date and time stamp, unique digital fingerprint, and details of the certificate.
- When using tools such as Adobe, the signature is validated every time the document is accessed.
- From a legal perspective, based on policies that govern digital signing, the signature is recognized as belonging to the individual to whom the certificate is associated.

WHAT IS A CERTIFICATE AUTHORITY (3RD PARTY)?

OSBEELS requires that *"the digital signature is independently verifiable by a Certificate Authority (3rd Party)."* This terminology is directly defined in the digital signature security industry. A Certificate Authority (CA) is an organization that attests to the binding between an identity and cryptographic key pair. In general terms, a CA verifies the identity of an organization and/or individual and issues a private key that matches the identity. The verification of identity by a CA usually involves a very rigorous process, requiring verification of employment records, federal employee ID number, social security number, driver's license, etc. Since a self-signed certificate does not include this rigorous verification process, it does not meet the requirements of OSBEELS.

There are two separate types of private keys issued by a CA, an organizational private key and an individual private key. For an organizational private key, the CA verifies the identity of both the organization and the individual applying for the key. This type of key is used when an individual's affiliation to an organization is required for legal documents. An individual private key only verifies the identity of an individual and does not include any affiliation to an organization. Since OSBEELS only requires a digital signature to confirm the identity of the signing engineer, an individual private key is sufficient.

HOW TO CHECK IF A DIGITAL SIGNATURE IS COMPLIANT

As a signing engineer, the easiest way to know if you are using a 3rd party Certificate Authority is if you must contact an outside agency to issue a digital signature key file. Many software products market the ability to "digitally sign" documents, but oftentimes this only means that they support 3rd party certificates. You will still need to contact a Certificate Authority to receive a private key. Similarly, most PDF products allow you to self-create a certificate by typing in your name and create a secure password. This is known as a self-signed certificate and does not meet OSBEELS requirements.

Once a document has been digitally signed, it can be easily validated to determine if the signature was created by a Certificate Authority or if it was self-signed. Per OSBEELS requirements, Washington County will only accept Engineer of Record digital signatures that were issued by a Certificate Authority. Washington County will not accept self-signed certificates.

Opening a document with digital signatures will often automatically bring up the signatures pane. Otherwise, you can also right-click the digital signature and select "Signature Properties." At this point, you can click "Show Signature Certificate" to bring up a detailed window. In this pane, you can click through multiple tabs to check on the details and trust. A signature that was signed with a Certificate Authority will have a 3rd party listed in the "Issued by:" field. A self-signed certificate will have the same name as the signer in the "Issued by:" field. See following page for examples of both types of certificates.

Note, that depending on the software (Adobe, Bluebeam, etc) and type of certificate used by the signer, different messages may appear in the signature certificate pane:

- **Invalid Policy.** This usually refers to utilizing a private key that is not on Adobe's Trusted List. Since the Trusted List isn't exhaustive, this error message doesn't signify that the digital signature is invalid.
- **Certificate Isn't Trusted.** This message usually means that the Certificate Authority's root certificate does not exist on the machine. Depending on the product used, sometimes the root certificate must be manually downloaded to gain trust. Otherwise

an individual may override the trust settings. Trust is not required to meet OSBEELS requirements.

- **Certificate Has Expired/Been Revoked.** This error message is rare, since most products won't allow using a digital certificate if it has been expired or revoked. This error message must be resolved by downloading a new private key or download a new root certificate.

APPROVED CERTIFICATE AUTHORITIES (3RD PARTY)

OSBEELS does not provide a list of Certificate Authorities that meet minimum identity verification requirements. However, there are a few lists that engineers may utilize. Note that both lists are not exhaustive and may include Certificate Authorities that do not meet OSBEELS requirements. The signing engineer must conduct due diligence to ensure minimum requirements are met. In most situations Washington County will not check the Certificate Authority utilized. In rare cases, the County may check the Certificate Authority against both lists below:

- **Adobe Approved Trust List (AATL).** This is a vetted program by Adobe for Certificate Authorities that meet the credential assurance requirements set forth by the AATL. To see the list, visit https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html
- **Oregon DOT Authorized Certificate Authority Vendors.** This is the list provided by Oregon Department of Transportation for digital delivery of project documents. To see the list, visit https://www.oregon.gov/odot/ETA/Documents_ETA/Digital-Cert-Auth-Vendors.pdf

WASHINGTON COUNTY QA/QC COMPLIANCE CHECKLIST

All plans submitted to Washington County that include digital signatures will be reviewed for compliance using the following criteria:

1. Are the words "Digitally Signed" used in lieu of a handwritten signature on the engineer's seal?
   - If **NO**, engineer seal and signature is ***not*** compliant with OSBEELS requirements.
2. Does the certificate viewer include the statement "This is a self-signed certificate"?
   - If **YES**, engineer seal and signature is ***not*** compliant with OSBEELS requirements.
3. Does the certificate viewer list the engineer's name in ***both*** the "Issued By:" field and the certificate name directly above?
   - If **YES**, engineer seal and signature is ***not*** compliant with OSBEELS requirements.

ADDITIONAL RESOURCES

- OSBEELS: Seals and Signatures requirements.
  - https://www.oregon.gov/osbeels/maintaining/pages/seals-and-signatures.aspx
- OSBEELS: The Difference Between Electronic and Digital Signing.
  - https://www.oregon.gov/osbeels/Documents/Resources%20for/TheDifferenceBetweenElectronicAndDigitalSignatures.pdf
- OSBEELS: Digital Signature Examples
  - https://www.oregon.gov/osbeels/Documents/Form/DigitalSigExamples-2021.pdf
- Oregon DOT: Digital Signatures for Engineering Documents, Ron Singh 2008.
  - https://www.oregon.gov/osbeels/Documents/Resources%20for/2008_OSBEELS_DigitalSignaturesForEngineeringDocuments.pdf
- Oregon DOT: Authorized Certificate Authority Vendors.
  - https://www.oregon.gov/odot/ETA/Documents_ETA/Digital-Cert-Auth-Vendors.pdf

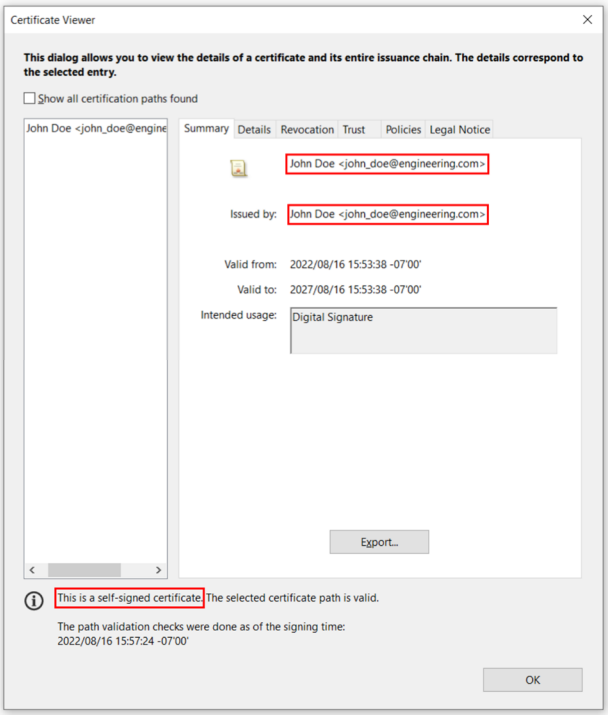
DIGITAL SIGNATURE EXAMPLES

Example 1 (non-compliant)

Checklist Item 1. **NO** ✗

Checklist Item 2. **YES** ✗

Checklist Item 3. **YES** ✗

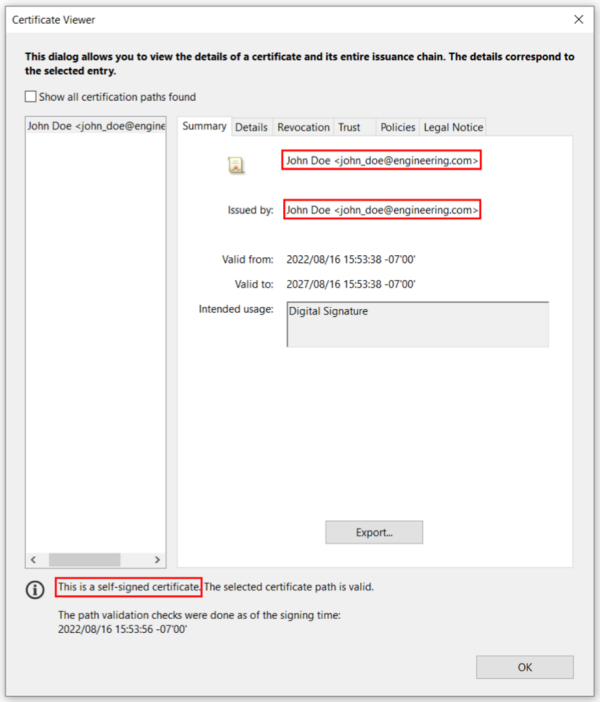


Example 2 (non-compliant)

Checklist Item 1. **YES** ✓

Checklist Item 2. **YES** ✗

Checklist Item 3. **YES** ✗

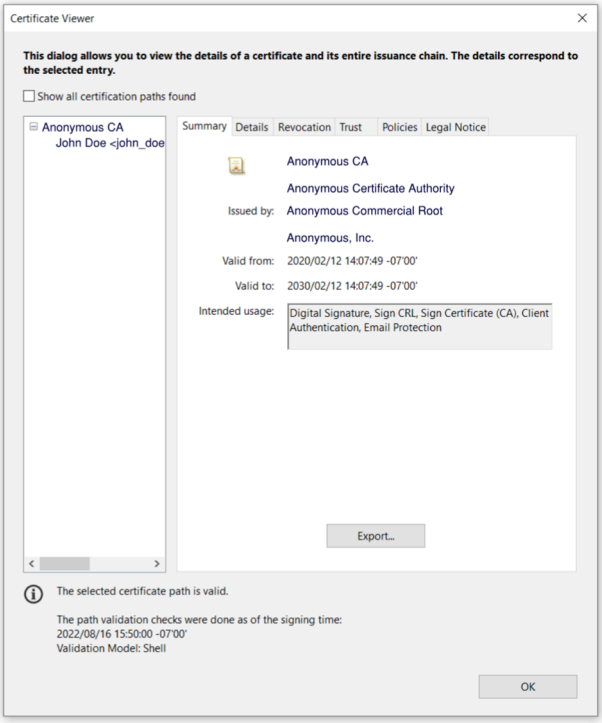


Example 3 (compliant)

Checklist Item 1. **YES**

Checklist Item 2. **NO**

Checklist Item 3. **NO**



GLOSSARY OF TERMS

Authenticate	To verify the identify of an individual/company/entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a document and/or the originator of a document.
CA Certificate	The CA certificate is the certificate containing the public key that corresponds to the CA private signing key used by a CA to create or manage certificates.
CA Private Signing Key	The CA private signing key is the private key that corresponds to the CA's public key listed in the CA certificate and used to sign documents.
Certificate	A digital representation of information that (a) identifies the certificate authority issuing it, (b) names or identifies its subscriber, (c) contains the subscriber's public key, (d) identifies its operational period, and (e) is digitally signed by the certificate authority issuing it.
Certificate Authority	A certificate authority is an organization that attests to the binding between an identity and cryptographic key pair. This is accomplished once the identity has been rigorously verified.
Digital Signature	A digital signature is the result of securing a document through use of cryptography. To digitally sign a document is the act of applying a digital signature. A recipient of a document with a digital signature can accurately determine if the signature private key matches the accompanying public key and whether the document has been altered since the digital signature was applied.
Encryption	The process of transforming data into an unintelligible form, in such a way that the original data can only be recovered using a decryption process.
Key Pair	Two related keys having the properties that one key can be used to encrypt a message that can only be decrypted using the other key.
Private Key	The key of a signature key pair used to create a digital signature, belonging to the signer of a document.
Public Key	The key of a signature key pair that is embedded into a signed document that is used to validate a digital signature.
Root Certificate	A root certificate, also known as a trust anchor, is the encompassing trust certificate for all public/private keys generated from a particular CA.