Oregon
BOARD OF EXAMINERS
FOR ENGINEERING &
LAND SURVEYING

670 Hawthorne Ave., Suite 220, Salem OR 97301
Phone: 503-362-2666 Fax: 503-362-5454
Email: osbeels.info@osbeels.oregon.gov

Title: The Difference Between Electronic and Digital Signing
Subtitle – This article was authored by Board members Tim Fassbender, PLS, and Renee Clough, PE, PLS
Text:
Recent concerns and questions raised by the professional community regarding Oregon Administrative Rule (OAR) 820-025-0010, digital seal and signature requirements, have been received by the Oregon State Board of Examiners for Engineering & Land Surveying (OSBEELS) and prompted a discussion about digital signatures and signing final documents. To address these questions and concerns, we have developed this article that will share resources and information to help professional registrants, and the users of their documents, to understand the differences between an electronic signature and a digital signature.

Relevant rules to this topic include:

1) OAR 820-025-0001 – defines digital signature and digital certificate.
2) OAR 820-025-0005(5) – specifies digital signatures as an acceptable alternative to a wet signed signature if specific criteria are met
3) OAR 820-025-0010 – outlines requirements for digital seal and signature for electronic final documents.

A digital signature in compliance with OAR 820-025-0010 utilizes a public-private digital key pair provided through the services of a certificate authority. The private key is known only to the signer and is often in the form of a password. The public key is utilized by the certificate authority to validate the document. To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. In the case of OAR 820-025-0010 this assurance must be provided by using a certificate authority as a trusted third party to associate an identified signer with a specific public key; essentially the certificate acts like a notary. A self-signed certificate is one that is created by the individual signer without the services of a certificate authority; this is not sufficient for purposes of compliance with OAR 820-025-0010.

The term "third party" in all the above cited OAR sections requires specific discussion. Some software will allow the user to make their own digital signature certificate which is often referred to as a self-signed certificate. This is often made in the same software being used to create the particular document but could be made in some other software. The upshot though is that anyone seeking to verify the authenticity of the digital signature will be coming back to signer for that authentication. In the case of a non-self-signed certificate, an entity known as a "Certificate Authority", has made the certificate and verified your identity as part of the process. When the digital signature is applied to the document the local software communicates with that Certificate Authority. Later when someone verifies the signature their local software also communicates with that Certificate Authority. Hence the term "third party", that certificate authority is not you, it is not the person receiving the document - it is a third party. A "third party" Certificate Authority is equivalent to a notary.

The table and discussion below summarize the differences:

Electronic Signatures	Digital Signatures
A Functional term	A legal term
Not technically bound to a specific individual or the result of a validation process	Tied to a specific individual via a PKI-based digital certificate
Created via options such as typed names, scanned images, online tools, or a "click wrap" agreement	Created using a digital algorithm to bind the document using a certificate, resulting in a unique "fingerprint"

Legal, but not easily identifiable to one unique user and can be replicated	Easily identifiable to a unique individual, auditable, and non-replicable
Does not meet OAR 820-025-0010 requirements	Does meet OAR 820-025-0010 requirements

Numerous certificate authorities are available with the ability to interface with a variety of software. Consequently, the process of utilizing a digital signature in compliance with OAR 820-025-0010 is too variable to provide a step-by-step description here.

It should be noted that, with a digital signature, the original is the digitally signed file. Prints of that file, whether to paper or to another digital format (such as pdf), are equivalent to photocopies of a wet signed document. Those prints can be used when a photocopy would be acceptable but not when an original is required. Most software capable of opening a specific file type is also capable of confirming the validity of a digital signature when it necessary to confirm the original has been received. Some software will display this confirmation prominently at the top or side of the screen, others need the user to interact with several layers of menus.

Lastly, it is important to note that OAR 820-025-0005(e) requires a digitally signed document to have the words “digitally signed” in the location where a wet signature would traditionally be placed.

In an effort to continue to address questions from the professional community, as well as provide further direction, the Board will be reconvening the Digital Signatures Task Force. Actions taken by the Task Force may cause information within this article to become outdated. To stay up-to-date on the latest information and resources, we recommend visiting the Board website.

Please refer to the below resources for additional information on the differences between electronic and digital signatures.

- Digital Signature for Engineering Documents – Ranvir Singh, PLS, 2008
- Understanding Digital Signature – Jason Kent, PE, and Ranvir Singh, PLS, 2017