Digital Signatures

What are they, what they aren't and why this matters to us!

Presented to the ANSLS Annual General Meeting, October 2022

By: Jody Isenor, NSLS, P.Eng

In this presentation:

1. Explanation of what digital true digital signatures are
2. Some samples of what are not digital signatures
3. Security and tracking information
4. Why Digital Signatures (or perhaps why not in some cases)
5. Options and Considerations (specifically and broadly)
6. What are other Associations doing?
7. Conclusion
8. Questions (and answers)

Digital Signatures:

A digital signature is a specific type of signature that is backed by a digital certificate, providing proof of your identity.

Digital signatures are recognized as being a more secure type of e-signature because they're cryptographically bound to the signed document and can be verified.

They are like a digital fingerprint, and can be traced and tracked back to the person signing.

Source:
https://www.adobe.com/sign/digital-signatures.html#:~:text=A%20digital%20signature%20is%20a,document%20and%20can%20be%20verified

Not digital Signatures:

1. A .jpg .bmp or other image of your actual signature
2. Any form of a signature that is electronic (i.e. electronic doesn't equal digital)
3. A likeness inserted into a CAD drawing
4. A reproduction of any kind, electronic or otherwise (unless accompanied by a certificate)
5. A photocopy of your signature

Any of the above, unless accompanied by an identity certificate are NOT digital signatures, but are simply electronic signatures

Digital Signature Providers:

There are many providers of true digital signatures, some examples:

1. Adobe
2. Docusign
3. EnTrust
4. Notarius (Engineers NS uses this – optional)
5. Eversign
6. HelloSign
7. Panadoc
8. Signnow
9. Microsoft (software/applications with these abilities)

Security:

Provided mainly by a certificate, which is given based on a verification by the organization or entity you either work for or are associated with.

The certificate validates your signature based on your credentials, which is verified by the application you use (generally via a security code or password)

Upon signing, the document you sign then bears within it (as your signature) the details such as date, time and appends this to the document

After signing, the document generally becomes read only and if edited, the signature properties are then invalidated automatically, making the signature invalid.

An example:

My organization uses EnTrust as the application and credentials are managed by the application and verified by EnTrust and my organization (when it is created).

Here is how I digitally sign a document……..

**Note here that the actual signature shows up as a software specific format, with name, date, and other details.

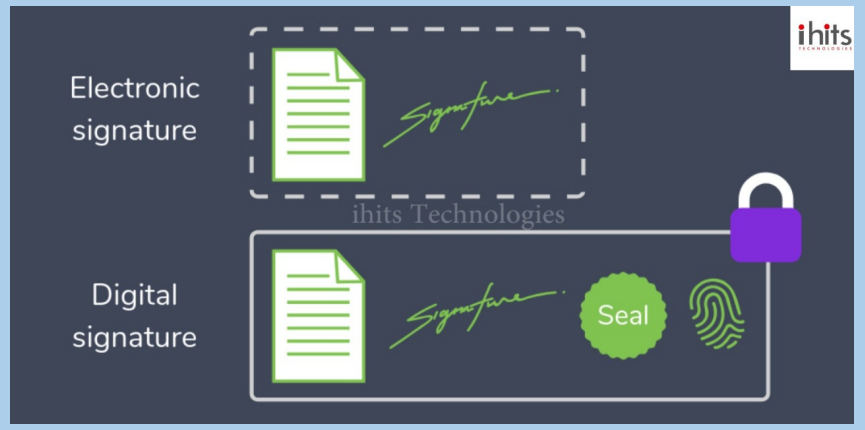
***I could within EnTrust create a digital signature that is an image of my actual signature, and can manage how it appears, but it remains a true digital signature as it is created and verified by the certificate in the background.

Why digital Signatures and Why does this matter?

Can be easier to manage and allow for expedient electronic file storage

Avoid the need to retain paper copies

Safely and securely send electronic plans or data



Electronic document submission – submit an electronic plan or document to a review authority, which may require these in the future

Options and Considerations:

Time – documents can be signed in seconds, without having to print multiple copies and sign each one.

Cost – there is generally a cost to having access to a digital signature application, as well as maintaining certificate verifications (Engineers NS as an example).

Management of certificates – again , time and money involved

Learning curve – need to understand how to use the application and develop a process for signing and retention, i.e. creating a pdf or raster image of a plan, then using the application to insert a true digital signature into that for retention. Generally this is not overly complicated.

What are other Associations Doing?

ACLS - through myCLSS, there is an electronic signature and submission process

NL - nothing as yet, discussion only

NB - on their agenda for discussion this coming February

QC - have been using digital signatures for 15 years; required by cadastral reform; surveyors keep digital files with digital signatures

MB - Council looking into it; not urgent

SK- issues a digital seal but still require a wet signature; up for consideration

NS – being accepted as a part of a PDF (not in best practices nor standards)

BC - have been applying digital signatures in public registries for around 15 years.

AB – manual of standard practice addresses it as a guideline but more on release of digital information; Land Titles allow for digital signatures. Real Property reports still require wet ink but practitioners have been using digital signatures; intend to allow that this year.

Conclusion:

Digital Signatures are here, they are becoming more popular

More and more regulatory authorities (think Service NS etc.) are accepting them and expect more of these authorities to require them!

They are not easily manipulated and add to the security of original documents

Nothing is 100% secure

Passwords and document retention challenges – what happens in the future with digitally signed documents and their validity in various jurisdictions (statute of limitations for liability)

Access to computer or server where original are stored (like your bank card, if someone doesn't have the password, access to files can be difficult or impossible)

May be one way to save you from renting warehouse space to house all of your plans and documents!!

Questions and Discussion