Digital Signing of Test Reports: When is it Required and How to do it Right

The move from paper to digital records has profoundly impacted the world's economies, and the construction testing and inspection space is no different. Along with the benefits of improved efficiencies and reduction in errors across workflows that the digital transformation has brought, it has also come with its own set of challenges. Electronic signatures and seals are just one of the new emerging technologies that can raise questions and doubt over the correct course of action when electronic records must be sealed.

In this article, we will explore the requirements around digital seals as set out by boards of engineers and the best solutions involving technology and process that will meet these requirements. We will answer: what is required from a technical and process standpoint to actually meet the requirements and correctly digitally seal electronic test reports and why?

We also demonstrate how Spectra QEST products can help solve this problem by removing all of the complexity from the process and allowing documents to be sealed at the click of a button. Spectra QEST has partnered with Notarius© (notarius.com) to provide simple and intuitive digital sealing functionality to ensure our customers and their businesses are compliant.

Professional Engineering Seals and Requirements

Professional Engineers are sometimes required to seal construction materials testing reports, or collections of test reports, in their capacity as a Professional Engineer. This requirement is often determined by project specifications or contracts and can vary by region where the work is performed or the type of entity responsible for commissioning. The process of attaching an engineering seal to a document carries with it more weight than a review of the results for correctness and general trends.

According to the **National Society of Professional Engineers**:

The act of signing and sealing engineering documents signifies that (1) the engineering work was prepared by the professional engineer or under the professional engineer's direct control or personal supervision; (2) the signing and sealing professional engineer is of the opinion that the documents contained meet usual and customary engineering standards of practice; and (3) the documents are appropriate for review and approval by the appropriate code enforcement official.

This means the act of digitally placing a Professional Engineer's seal on a document carries more stringent requirements than simply attaching an image of the seal and signature to the document. Boards of Professional Engineers in different states define the requirements for the use of digital seals differently but there tend to be a number of common themes in these requirements. In general, a digital seal needs to be:

- Unique to the individual using it,
- Under the sole control of the individual using it and protected,
- Applied to the document in such a way that subsequent modification of the document invalidates it,
- Verifiable (by a third party).

It should be noted that the requirements of all boards are not created equal, some are less stringent than others and some carry only some of the above requirements while others only imply these requirements (and are open to interpretation).

Meeting the Requirements through Digital Signatures

This section will dive into the details behind how digital signature technology works, how it can help meet the requirements stated above and what prerequisites need to be in place to ensure that the digital signature technology used is actually compliant.

Digital Signature vs. Electronic Signature

Before going too far, it is useful to define the difference between electronic and digital signatures for the purposes of this discussion.

An **electronic signature** is a broad term and is a legal concept distinct from **digital signatures**. An **electronic signature** is a signature created by electronic or optical means and affixed electronically to a document with intent to sign the document. An **electronic signature** can be as simple as a name entered in an electronic document, or an image of a signature attached to a document by a user performing an action while logged into an application. So long as intent to sign the document is present. Electronic signatures can get far more sophisticated in order to provide greater assurance and trust. A **digital signature** is a sophisticated type of **electronic signature** that, when implemented correctly, meets the most stringent boards of engineers criteria for digital seals.

How Digital Signatures Work

A digital signature is a scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient very strong reason to believe that the signed document was created by a known sender, and that it was not altered in transit. How does it work? The short answer is: math, and lots of it.

There are a number of steps to consider in the long answer. We will consider these individually before putting them all together.

Document Hashing

The process begins with a document (or other digital message) that needs to be signed. A hash digest of the document is first calculated using a hash algorithm. Hash algorithms are mathematical functions that have some useful properties, namely:

- Given an input of arbitrary length, they will produce a fixed length output.
- A small change in the input (e.g. one character changed in a document) will cause a large change in the output (a completely different output of the same length).

> The hashing algorithm known as SHA-256, used in digital signing, produces an output that is 256 0s and 1s, regardless of how long the input is. If this article is fed into SHA-256 we get 256 0s and 1s in various positions. If “War and Peace” is fed into it, we also get 256 0s and 1s (though in a quite different order).

For the purposes of this discussion it is helpful to think of the hash digest as a fingerprint of the document.

Hash Encryption

The calculated hash digest is then passed through yet another mathematical algorithm, this time a **signing** algorithm. Signing algorithms are based on another set of mathematical functions with a number of interesting properties. These functions, known as asymmetric key functions, have the following useful properties:

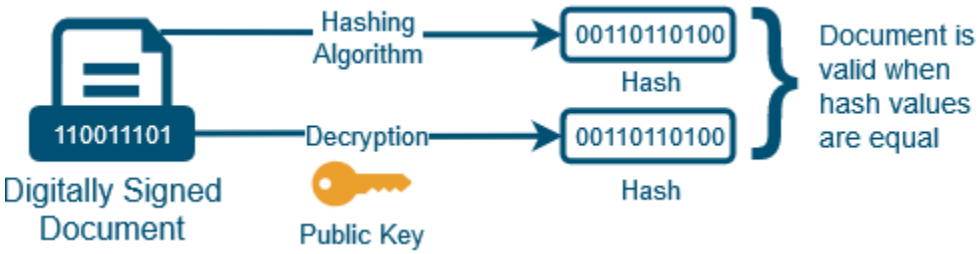
- They have two numbers that “solve” the function, these numbers are called the **keys** of the function,
- Given an input of plaintext (like our document or our document’s hash digest) and one of the two keys, the output of the function is apparent gibberish (i.e. it becomes encrypted),
- Given an input of the encrypted text and the **other** key, the output of the function is the original plaintext (for example, our document hash digest),
- Given the function, one of the keys, the plaintext **and** encrypted version of that text, figuring out the other key is very hard to the point where it’s not possible in a feasible timeframe even with the most powerful computers. This provides a high level of security if we can keep one of the keys secret.

Public key cryptography relies on these properties of asymmetric key functions by recognizing that if one key is kept very secret and only ever known by one person (i.e. the sender in our case) then the second key can be made public to allow secure communication. Data encrypted with the private key of the sender (that only they know) can be decrypted by their public key (that everyone knows). Put another way: if some encrypted data is able to be decrypted by an individual’s public key, and we have confidence that their private key is very secret, then there is a good level of confidence that the data:

- Was not tampered with in transit, and
- Comes from who we think it comes from (i.e. the owner of the private key).

The hash digest, then, is encrypted with the sender’s private key and this encrypted data is attached to the document prior to transmission.

Verifying a Signed Document



The document is transmitted and, upon receiving the document and the encrypted hash attached to it on the other end, the recipient does two things:

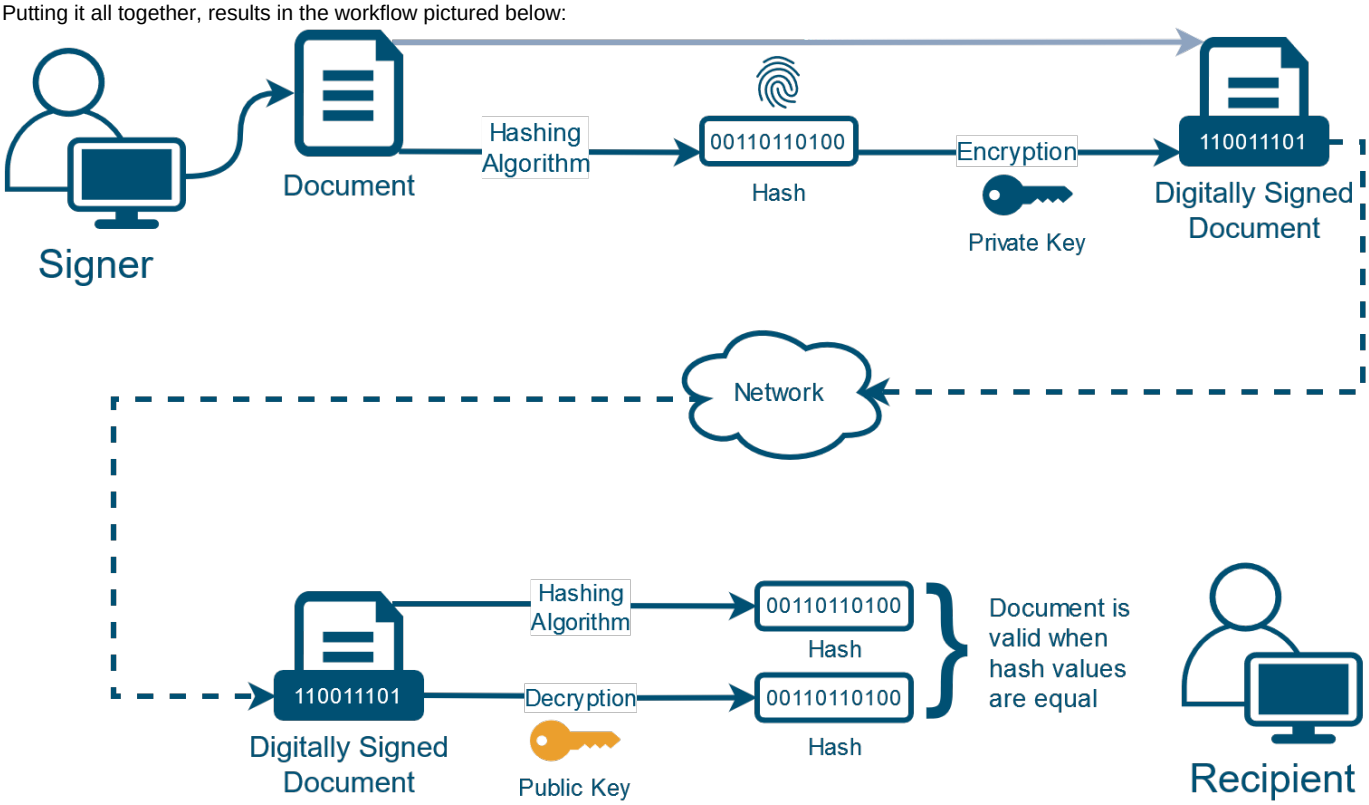
1. Calculates a hash digest (i.e. fingerprint) of the received document using the same hash algorithm as the sender did
2. Decrypts the encrypted hash digest attached to the document by the sender using the sender's public key

If the two hash digests match, we know we have the original document, and we very are confident it was sent by the owner of the private key.

> Why bother calculating a hash digest and signing that rather than digitally signing the entire document? The signing functions are limited to encrypting a message the same size as the keys so we have to provide it only a shortened version of our message.
>
> The original message could be broken down into chunks of the right size and each piece could be encrypted but this would result in an encrypted file that is two or three times larger than the original. Calculating and encrypting the hashes is far more efficient.

The Whole Digital Signing Process

Putting it all together, results in the workflow pictured below:



There are quite a few steps above, some of them sufficiently complex to allow errors and mistakes to creep in. It is important that each part of the signing process is completed to industry best practices in order to provide the necessary level of confidence in the resultant documents. We go on to review a couple of areas where things can go awry.

Keys, Certificates and the Certificate Authority

The keys for signing and verifying signed data are stored in computer files called **certificates**. In the context of signing documents, the signer will have a certificate file that contains their public and private key. When signing a document, the software performing the action will use the signer's private key from their certificate. It will also attach a certificate to the document that contains only the signer's public key. When a recipient opens the document in software able to verify digital signatures, the software will use the public key from the attached certificate to verify the document in the manner shown above. Many commercial software applications can sign and verify documents and data in this manner, including many popular PDF viewers like Adobe Acrobat or the simple verification solution from Notarius, VerifiO.

The theory behind digital signing is heavily reliant on the correct treatment and use of the public and private keys (and therefore, the certificate) of the signer. ***Certificate issuance, endorsement and life-cycle management is one of, if not the most, important parts of the puzzle to get correct.***

Important considerations with regard to handling of the public and private keys (certificates) include:

- The private key must be kept well protected, and remain a secret known only to the signer, and
- The public key must be communicated to everyone that receives signed document, and
- The public key communicated with the signed document actually belongs to the individual that it claims to.

How does one ensure the secrecy of the certificate of their private key? To ensure secrecy, the file should never be transmitted over the public internet, and it should never come into the hands of anyone except the signer. These are not trivial problems to overcome when dealing with digital files.

The distribution of the public key is taken care of when the signing software automatically attaches it to the PDF documents that are sent, but there must be a way to trust or verify that the public key used to sign a document actually belongs to the correct individual. It is possible to create your own certificate, on your own PC with any name and claim to be whomever you like; they are just files after all.

This is where certificate signing comes in. It is possible to make use of digital signing again, but in a slightly different way, to create a **chain of trust** in the form of chains of certificates where a trusted entity can use **their** private key to sign the certificate of an individual. This action will endorse the fact that the certificate belongs to the person it says it belongs to. If one can trust the entity vouching for the individual certificate, there is a chain of trust to the certificate's ownership.

An entity that issue certificates and vouches for the identity of the owners of those certificates is called a Certificate Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. If we trust the CA that issued a certificate to the signer to do a good job of verifying that signer's identity, then we implicitly trust the public key does actually belong to the individual (as they are mathematically bound together). If we further trust that the certificate has been handled securely and that the private key within it has remained secret throughout its lifecycle, something that CAs and their processes help to ensure, we trust that only that individual can use the certificate and we can therefore trust in the signing process.

It is important to emphasize that a lot of trust must be placed in the certificate authority responsible for issuing the certificate that is used in the signing process.

Individual and Organizational Certificates

There is an interesting consideration on how certificate authorities issue certificates: they're not just for individuals. Many organizations obtain certificates to certify the identity of the organization or a department within the organization. Using these organizational-level certificates, documents can be signed on behalf of an organization. This is a very common approach employed by cloud-based signing solutions. The certificate used will often belong to the organization providing the cloud-signing service. The signing action will, therefore, provide confidence that the document was signed using that service and has not been tampered with. Whether there is confidence in the individual's identity that completed the signing action will depend on how much confidence there is around:

The identity verification carried out by the organization

- Can you sign up with a name other than your own?
- What assurance is there that users are in the real world who they say they are on the service?

Authentication processes when logging in and performing the signing actions

- How much protection is there from non-legitimate users hijacking credentials of legitimate users?

In the strictest reading of the requirements set out by boards of engineers utilizing an organizational or departmental level certificate for signing documents rather than one tied to an individual does not meet the requirement of the signature being solely under the signer's control.

Trust

Ultimately, digital signing is about providing confidence in the integrity of a document and the identity of the individual signing the document so that trust between the two parties exchanging documents and the way the document is transported is not needed. Along the way, however, there are plenty of areas where trust *is* necessary. Namely, to have confidence in a signed document, one must have confidence in the following steps:

The signing algorithms in the toolset performing the signing action

- Has it been developed and maintained utilizing the latest industry best practices?
- Is Long Term Validation part of the process?
- Has the process been vetted and verified by independent third parties?

The certificate being used for the signing process

- Is the certificate tied to an individual rather than an organization or department?
- Has the individual's identity been verified to an appropriate degree prior to the certificate being issued?
- Has it been issued and vouched for by a reputable and appropriately certified certificate authority?
- Has it been treated correctly throughout its life, keeping the private key secret? That is, has the signer had sole control over the private key throughout its lifecycle?

If the above prerequisites are met then digital signing fulfills the requirements for digitally sealing electronic documents from a control and process perspective.

Seal Appearance Management

Boards of engineers also define requirements for the appearance of engineering seals. From the actual design of the seal to how big it must be on a printed document as well as what extra information is required alongside the seal image in the signature.

When it comes to a visual representation, digital signatures can have images embedded along with accompanying text that contains extra details around the signing event, such as the name of the signer. Most commercial products capable of digitally signing documents will require a signature field to be defined and use half of the space for the image and the remaining half of the space in the field will be filled with the extra text. This can make placing a 2” diameter stamp on a Letter sized report a challenge. The defined signature field must be 4” long by 2” high and this rectangle, which takes up 8.5% of a Letter sized page, will ideally not overlap any other elements on the report so that the explanatory text and seal are both legible. Locating this much free space on a test report can be troublesome where a lot of data must be presented.

File Management

Once an appropriate digital signing process is in place, with well managed certificates, there is the secondary issue of workflow and management of the digitally signed files to worry about. Signing PDF files on a desktop and utilizing a folder to store files results in multiple copies of documents floating around that can quickly get confusing. There is the original unsigned version, the signed version and any subsequent revisions. With thousands of reports in play for any one project manager this can quickly get overwhelming.

Digital Sealing on Construction Hive

Construction Hive allows you to take all of the above considerations into account and meet the requirements for digital engineering seals in a correct and efficient manner. Spectra QEST have partnered with Notarius, an organization that has provided digital signing certificate services for over 25 years in North America. Notarius are a certificate authority that is ISO 9001:2015 and ISO 27001:2013 certified as well as being certified by Adobe and Microsoft and appearing on their Trust Lists. Spectra QEST have leveraged Notarius' technology to bring robust, well trusted and certified digital sealing functionality to Construction Hive.

The process is built into the existing QEST Platform workflow, which already removes shuffling of files, and comes pre-loaded with presets for each US state for seal sizing. The end user simply needs to press a button to digitally seal a report that has been distributed via Construction Hive. Alternatively, documents can be sealed in bulk from the search results page, similarly with a single button press.

The sealed documents will meet or exceed all technical and visual requirements as set out by the various boards of engineers.

About Spectra QEST

Spectra QEST is a software development and services company specializing in solutions for the construction materials engineering, testing, inspection and production industries. Founded in January 1984, Spectra QEST offers the most comprehensive construction materials quality platform on the market today. With offices located in Adelaide, South Australia, and Sacramento, California, it services customers in North America, Europe, Australasia and the Middle East. These customers include leading international construction companies, construction materials and geotechnical engineering companies, construction materials manufacturers, and government bodies.

Availability and Purchase

Please contact Spectra QEST to take advantage of the efficiency gains of the streamlined and automated digital sealing process for Professional Engineers in Construction Hive.
