Digital Signing of Test Reports: Choosing A Certificate Authority

The reliability and trustworthiness of digitally signed documents is heavily reliant on the choice of a good Certificate Authority (CA), as discussed in the article **Digital Signing of Test Reports: When is it Required and How to do it Right?**.

Certificate issuance, endorsement and life-cycle management is one of, if not the, most important parts of the digital signing puzzle to get correct. A lot of trust needs to be placed in the certificate authority responsible for issuing the certificate that is used in the signing process. It is crucial, therefore, to be aware of who the certificate authority is when utilizing digital signing and be confident that the responsibilities of a certificate authority are central and core to the business of the organization fulfilling this role.

This article explores some of the considerations that should be taken into account when selecting a Certificate Authority for digital signing certificates and how Spectra QEST's partner in the digital signing feature set, Notarius© (notarius.com), measures up.

Digital Signatures and Certificate Authorities

A digital signature is an electronic signature that is fully or partially reinforced through cryptography. Given the present state of information technology, it is the best signature method to ensure the integrity and origin of an electronic document. However, the process is sufficiently complex and made up of enough separate parts that mistakes and bad processes can severely diminish the value of digital signing. One of the key requirements of a trustworthy digital signing process is the choice of CA to issue the certificates that are used to sign documents.

Certificate Authority Considerations

The CA issues a digital certificate that allows a person to digitally sign a document based on a Public Key Infrastructure (PKI).

The basic premise is that the CA is vouching for a strong link between an individual's identity, his or her private key and information certified in the public certificate (including their public key). The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The purpose of a CA is to manage the signer's enrollment and certificate life cycle, which includes generation and issuance, distribution, renewal and rekey and revocation of certificates. The Certification Authority maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

Identity Verification and Management

In order to guarantee strict compliance with the requirements for digital seals as set out by various boards of engineers, the certificates used to digitally seal and sign documents as a Professional Engineer should be issued to the individual rather than an organization or department.

When issuing certificates to an individual, the CA must have a high level of confidence that the certificate is being issued to the correct individual under the correct name.

Notarius performs face-to-face identity verification, requiring proof of identification with a government-issued photo ID to initiate the issuance of digital certificates. Notarius only accepts identities recognized by a federal, provincial or territorial government.

Notarius certifies the professional status or employer of the signatory for each signature. When it certifies the professional status, Notarius is the only North American company that establishes partnerships with a growing number of professional bodies and associations so that they validate professional status and revoke it at will, all in accordance with their mission to protect the public (for a professional association).

Authentication

Once the identity of a new customer has been validated, the CA must ensure that the customer has secure, reliable and exclusive authentication in order to obtain his/her digital certificate every time a document is digitally signed. Does the CA apply robust methods in order to achieve these objectives?

Notarius has strict rules securing the issuance of the digital certificate to its rightful owner. Once in possession of the certificate, the signatory must use two-factor authentication to sign documents.

Chain of Trust

Does the CA maintain a secure and reliable chain of trust with publicly documented evidence of who can authorize which key event in the life cycle of a digital certificate (excluding signatures), such as its issuance, activation, revocation and renewal? Such a chain of trust is required in order to react promptly in the event of a security breach. Does the CA apply a robust method in order to achieve this objective?

Notarius maintains a detailed audit trail that accurately and irrefutably documents who allows or initiates each key event in the life of a digital certificate (excluding signatures by the user).

IT and Human Processes

The PKI is based on the management of IT processes and human processes. In the first case, have these processes been designed to maximize security and not simply to reduce costs?

The parts of the PKI that depend on human processes must be designed with due care in order to reduce the risks of fraud and errors. Did the CA do this in a way that is reliable and certified?

Notarius was founded and built on the primary concern for the robustness and security of its IT and human processes. Notarius is therefore regularly checked and certified ISO 27001 and 9001. Notarius was the first CA in North America to be certified ISO 27001 in 2007.

Continuous Optimization

IT relating to digital signatures and the environment in which digital signatures are used are constantly evolving. Does the CA adapt itself and optimize its PKI on a regular basis?

Notarius is continually improving their product offering, and are currently working to provide cloud-based Adobe Approved (AATL) certificates for signing actions that take place entirely in the cloud.

Third-Party Certifications

There are a number of certifications that exist in order to ensure that a CA meets the above requirements to ensure a trustworthy signing process.

Notarius operates its own trusted certificate authority, which is certified ISO 27001, ETSI 319-411, and approved by Adobe (AATL) & Microsoft (Microsoft Trusted Root Certificate Program).

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.