Common Questions About Digital Signatures

notarius

Notarius is a government-grade digital signature service provider with over 20 years of experience serving more than 35 professional associations in a range of industries, including engineering, the legal field, architecture and land surveying. When contemplating a corporate digital transformation, many departments raise questions about legal reliability, compliancy, security, technology and end-user functionalities. This document aims to answer some common questions that may arise when evaluating Notarius' solutions.

LEGAL

Q **Why do professional associations choose to issue digital signatures to their members?**

A Controlling the use of seals and protecting the public is an integral part of an association's responsibilities. In paper form, this is accomplished by placing a seal that embeds the name, member number and designation as a member and is made official by hand-signing and dating the document. But how can associations securely seal official documents in a digital world where a seal can easily be replicated and copied from one document to another? Associations that offer digital signatures choose to control use of seals in a digital world to ensure that only members in good standing can sign official documents. It also allows clients and government agencies to instantly verify that the document has been signed by a professional with the authority to do so.

Q **Can someone continue to use a digital signature after it is revoked?**

A A digital signature belongs to an individual and can only be used by that person. However, in most cases, the signature is issued by the association or an employer and not directly to an individual. Thus, a digital signature can be revoked by the association if a member is not in good standing, or by the employer if the employee has left the company. Once it has been determined that a person no longer has the authority to use their signature, the revocation is instant and the digital signature is no longer operational.

NOTE: The revocation of a signature does not invalidate previously applied signatures (since they were in good standing at the time; it only prevents individuals from signing new documents.

LEGAL (continued)

Q **Why are Notarius digital signatures trusted and recognized by government agencies?**

A Not all digital signatures are issued and controlled in the same manner. Governments tend to limit the number of certificate authorities they will recognize or authorize. Strict guidelines are established and audited to ensure that the approved digital signature certificate authority has the proper technology, security, policy and process in place to guarantee the identity of all digital signatures issued. Notarius was created in the 1990s by Quebec's *Chambre des notaires* (Board of Notaries) to build a government-grade certificate authority recognized by the Government of Quebec's electronic land titles registry. Even today, very few third-party certificate authorities are authorized to issue trusted digital signatures for interaction with government agencies. Notarius is the only third-party certificate authority recognized by multiple provincial governments in Canada.

Q **Are Notarius digital signatures recognized worldwide?**

A Notarius digital signatures are used to sign official documents and meet the standards of many countries. However, each jurisdiction may have specific requirements that must be met in order to be recognized. For example, in France, many agencies will only recognize French certificate authorities. In the United States, requirements for authenticating engineering documents will mostly be limited to a technological baseline, but not specific to a provider or a standard. As such, Notarius digital signatures meet or exceed the minimum requirements for all US states (except Hawaii). It is important to verify local digital signature requirements with recipients prior to submitting signed documents that use Notarius digital signatures.

Of course, other considerations need to be evaluated before making a digital shift. Please feel free to reach out to Notarius for a working session on the subject for further discussion.

SECURITY

Q **How are digital signatures secure? Can they be hacked?**

A Digital signatures are based on cryptography that was originally designed in the 1970s and is still considered the standard to secure different types of data. Digital signatures and their cryptographic derivatives are used in our daily lives to secure websites, communications, documents and financial transactions. If digital signatures were "hacked," the first case of attack would likely be in the financial, military or government sector. An individual's signed PDF document would be the least of a signer's worries.

Q **What are the security protocols in place regarding the Notarius certificate authority?**

A Over the course of the last decade, Notarius has invested heavily in certifications that have set a high standard of security for all Notarius solutions. As such, Notarius is certified ISO 27001 and ISO 9001. Notarius is also on the Adobe Approved Trust List (AATL) and certified eIDAS in Europe. There are only a handful of certificate authorities in the world that can rival Notarius certifications.

Q **What are the contingency plans if a Notarius certificate authority was offline or hacked?**

A The present uptime is 99.99 with full redundancy and multiple data sites. Since the launch of the first Notarius certificate authority in 1998, there have not been any data breaches. Notarius digital signatures are used to secure millions of official documents that must be preserved for decades, in some cases. Security is at the heart of all services at Notarius and Notarius is ISO Certified 27001 for its security protocols.

TECHNOLOGY

Q **Who has access to images of seals and digital signatures?**

A Notarius does not have access to the digital signature, the password used to sign, the image or its usage information (neither the frequency of use nor the content of signed documents). Notarius does not store information related to documents signed and documents are not visible to Notarius in any fashion.

Q **Who has control over the digital signature?**

A Notarius digital signatures could be compared to a digital passport. Digital signatures are issued via a trusted certificate authority such as Notarius. Although Notarius provides the hardware and expertise to generate a digital signature, our partners (i.e. professional associations) or customers (corporate entities or government agencies) have full control over the issuance of these digital identities. Once issued to an individual, the professional has full control over the digital signature and the seal/signature images that may be used to sign a document. Conversely, Notarius can revoke the signature if a subscription is not paid in full and the association/ corporation can revoke the signature if no longer authorized by the issuing body (revocation of professional status or no longer employed).

Q **What is a certificate authority?**

A A certificate authority is a trusted third party that issues digital signature certificates to confirm a signer's identity. The certificate authority also offers ways to verify whether a certificate is still valid, expired or revoked.

Q **What is transmitted to a Notarius certificate authority (server) when digitally signing a document with an internet connection?**

A When a document is digitally signed (when connected to the internet), a signature request will be sent to the Notarius certificate authority to verify if the digital signature is valid. Once the request is received, the certificate authority will respond (positive or negative) and send the result back to the PDF. In the case of a negative response (expired or revoked), it will clearly indicate to the PDF reader that the certificate is not valid. If the response is positive, it will embed the proof that the digital signature was valid when the document was signed. This proof (OCSP response or CRL) is integrated into the PDF and, since it is digitally signed, cannot be removed or altered without compromising the integrity of the signed document.

Q **Can someone sign offline?**

A Users do not need to be online to apply a digital signature. However, if a digital signature is executed when connected to the internet, a proof of validity (OCSP response or CRL) will be embedded into the PDF. If the signer is offline, they will still be able to sign the document, but without the addition of the proof that the digital signature was valid when the document was signed. However, even if proof is not embedded, a recipient can manually verify the status of valid digital signature. Notarius recommends that signers be connected to the internet when digitally signing documents that will need to be kept for a prolonged period, but it is still common and functional to sign offline. A common use case for signing offline is when a signer is in a remote location with limited internet access.

Q **What is OCSP and an OCSP response?**

A An online certificate status protocol (OCSP) is a common protocol used to obtain the revocation status of a digital signature. Not all certificate authorities have setup an OCSP for validation by an outside source. Most reputable third-party providers will use an OCSP or CRLs to allow recipients to validate digital signatures. If a vendor does not offer this capability, it should be a source of concern since it means that the recipient will not be able to verify the status of the digital signature. For example, self-issued digital signatures in Adobe Reader do not provide an OCSP, making them impossible to verify securely.

Q **What is a CRL?**

A A certificate revocation list (CRL) is a list of all revoked digital signatures associated with a certificate authority. It is one method used to validate the status and authorisation to use a digital signature.

Q **What is PDF/A-3?**

A First and foremost, a PDF is an open standard that allows users to produce electronic documents that are very similar to paper. Being an ISO-standardized format, many governments have adopted the PDF standard as a common standard for producing and archiving electronic files. PDFs can be produced in various ways to meet certain technical requirements. For example, PDF/X is common format for professional printers. PDF/A, including PDF/A-3, are ISO standard-based formats specifically designed for long-term archiving. The key benefit of PDF/A-3 is that it allows a signer to attach any file format (DWG, BIM, JPEG, etc.) in a PDF and secure the integrity of the content with a digital signature.

APPLICATION

Q **Can multiple people sign the same PDF document?**

A PDF files can have multiple digital signatures applied on the same document. For example, a document could have a digital signature applied by a signer, a reviewer and an approver.

Q **Can we sign DWG, BIM or other data files?**

A A digital signature is based on a standard protocol that is designed to work in a variety of technological environments. Digital signatures will work with Outlook, Word and PDF formats. It is also possible to sign BIM or DWG files but, for these types of formats, signing them using PDF/A-3 is recommended.

Q **Can someone mark up a signed PDF document?**

A In the same way that a paper document can be marked up, a digitally signed PDF can be marked up with comments, red-lining and other forms of information layered on top of the signed PDF document. However, since a digital signature acts as a wrapper on the original content, the source information (text or images) cannot be readily altered. For example, an engineering drawing can be signed and a reviewer can redline the document but cannot change the content of the drawing. Furthermore, if any mark-ups are placed on the document, the PDF will clearly identify that the document has been altered since the digital signature was applied.

Q **Can someone modify or alter a signed PDF document?**

A As discussed in the previous answer, a signed document can be marked up but cannot be easily altered. If a digitally signed document were to be altered, the digital signature would be removed from the file, thus rendering the document a copy of the original. For example, in paper form, a wet signature original can be photocopied, thus creating a copy of the original and this copy can be easily modified and altered. The same is true for an original electronic PDF with a digital signature. It can be "reprinted" as a PDF and the new document then becomes a copy of the original. This copy can be altered but, for the recipient, it is a copy since the digital signature is no longer part of the PDF.

Q **Can anyone verify the validity of a digital signature?**

A When a digital signature is applied on a PDF, it is possible to verify the details of the digital signature in the most common PDF readers, such as Adobe. The recipient can also choose to trust the signer and, if the same digital signature is used, automatically trust the digital signature for future document validations. Combined with the OCSP response and CRL provided when signing online, a recipient can trust the identity of the signer and protect themselves from potential identity impersonation.

For More Information

notarius.com | 1-888-588-0011 | info@notarius.com

notarius

Digital transformation.
Legally reliable documents.