The Breakdown:

E-signature Vs Digital signature

Overview

An electronic signature is information in electronic form (can be sound, symbol, process, etc.) that is associated or attached to a document. This means that so long as we can demonstrate that the signature is associated with a person and that there was intent to sign, everything is legally binding and accepted (all of this can be seen in Signority's audit trail).

A digital signature is actually a form of electronic signature that uses an encryption algorithm that helps validate who the signer is. It also ensures that the document cannot be tampered with, as the signature becomes invalid if the document is changed after signing. This helps prevent repudiation by the signer, making it almost impossible to deny having signed the signature. Essentially, these issues are some of the biggest challenges to electronic signatures, and digital signatures are able to help overcome these issues.

Electronic Signatures: an overview

You may be wondering how electronic signatures even work in the first place? Before we can get to the difference between digital signatures and electronic signatures, let's discuss what an electronic signature is first.

According to the Canadian Uniform Electronic Commerce Act (UECA), an electronic signature "means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to, or associated with the document." The American equivalent is the Uniform Electronic Transaction Act (UETA) and the Electronic Signature in Global and National Commerce Act (ESIGN). Their definition is "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

At the heart of both definitions is the capture of the intention with which a signature is added. What that implies is that the electronic signature doesn't have to look anything like your handwritten signature when it's applied. It can be a symbol, a typed text, or even an image or sound. So long as the intention is present, then it is legally accepted and binding. In this sense, if the association with a person is demonstrated and the intent to sign is also demonstrated, the signature will meet the signature requirements stated above. This is done through the audit trail and by authenticating and determining who the signers are and what was signed.

Signority's e-signature solution is able to capture all of this data through its detailed audit trail with time stamps, multi-factor authentication methods to validate the signer's identity, and by securely storing the data to prevent tampering.

Digital Signatures: an overview

We've explained what an electronic signature is in the previous section. The digital signature further improves the security and authenticity behind each electronic signature, acting like a digital "fingerprint" for a signer of a specific document.

The biggest challenges with regards to secured signatures have always been:

Is the signer who they say they are?
Is the signature valid and hasn't been forged?
And has the document been tampered with?

In history, to counteract these challenges, the existence of notaries were introduced and played a key role in assuring authenticity and trust of a document.

Similar problems still exist today for the electronic world. However, digital signatures were created to help serve the purposes of notaries in the past. Certification Authorities (CAs), a trusted third party, now serves as the notary in terms of verifying a signer's identity. Rather than being present at the time of signing, like a notary would, a CA acts as a trusted third party organization that ensures the security of the Public Key Infrastructure (PKI) and providing digital certificates for signers, both of which are necessary for a digital signature transaction.

The technology behind secured Digital Signatures

A digital signature is unique to each individual signer. To ensure this, electronic signature solution providers follow a protocol called the PKI. The PKI uses a mathematical algorithm to generate two keys for the signer, a public key and a private key. The two keys together make your digital certificate, which help validate the signer's identity.

When a document is electronically signed and completed, a unique "fingerprint" of a document (called a hash) is generated by using a mathematical algorithm. This hash is, then, encrypted by the signer's private key. The encrypted hash and the document certificate issued by a trusted CA are both attached to the digitally signed document, thereby completing the digital signature transaction.

To validate the signer's identity and verify the signature, the signer's public key is used to decrypt the document hash. During decryption, a new hash is calculated and matched with the original encrypted hash. If the two are the same, the signer is validated, as the two keys must match and create the same hash, as highlighted in the diagram below.

Benefits of Digital Signature

All of this finally brings us to the question, what's the point of all of it and how will it benefit my business? As stated at the beginning, an electronic signature captures the intent and also helps prove who the signer was and what was signed in the first place.

The key benefits of digital signature is that it works with the electronic signature rather than replacing it. When you apply the digital signature to a document, the cryptographic operation helps bind the digital certificate and the data being signed into one unique digital "fingerprint", the uniqueness of the certificate and the data is what makes digital signatures so viable.

As a result, you can be assured of 3 things:

Signer identity is valid – you will know that the signers are who they say they are
Tamper-proofing – you can be ensured that the document hasn't been tampered with, otherwise the signature would be invalidated
Non-repudiation – the signer cannot deny having signed the signature and is possible to prove in court
HSM or Hardware Security Module

For Signority to have digital signatures available for users, it uses a GlobalSign Hardware Security Module (HSM) to help store and manage the digital keys that are used in the digital signing process. It also acts as the key generator for the digital certificate.

Adobe AATL Certificate Policy requires that digital certificates are stored on FIPS-compliant hardware. HSM is FIPS-compliant, which allows Signority to provide digital signatures.

Contact Us:

Toll-free: 1-833-222-1088

hello@signority.com
WWW.SIGNORITY.COM

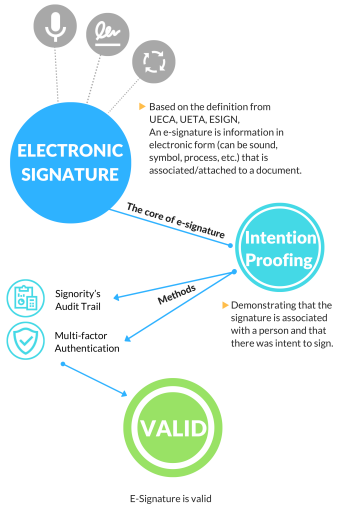
SIGNORITY

A BREAKDOWN:

E - Signture VS Digital Signture

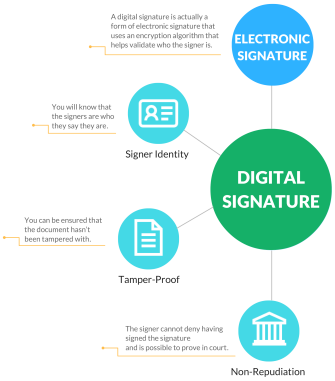
The Process Behind Secured Online Document Signing

01. How E-Signatures work

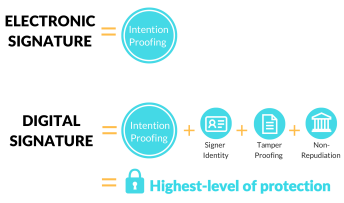


E-Signature is valid

02. How Digital Signatures work



03. Summary



SIGNORITY

www.signority.com