Wet signature vs. Electronic Signature vs. Digital Signature

July 22, 2020 by Riaan de Villiers

This articles explores the differences between paper based, electronic and digital signatures.

A comparison of wet signatures to electronic and digital signatures

What is a wet signature? In 1677 England passed the law "Statute of Frauds" that specified certain contacts must be in writing and signed. The new law became the driving force that would see the signing of documents become an everyday occurrence.

A signature on paper, or wet signature, is any mark that a person places on a paper document to signify that they agree to the stipulations specified in the document. Furthermore, the signature serves to identify the signer since each person's signature is unique to them.

While wet signatures can be trusted, they do present some problems. Signatures can be forged, paper-based processes are slow and they can be costly in terms of time and money.

To overcome the inherent weaknesses of signing on paper, electronic and digital signatures have become more and more popular.

What is an electronic signature?

Any mark that is made on an electronic document with the intention to serve as a signature is seen as an electronic signature and in South Africa is considered to be legal for signing most documents.

However, electronic signatures are low trust signatures since an electronic signature does not contain any evidence to tie the identity of the signer to the document and there is no proof that the document did no change after signing.

In order to protect against these weaknesses, digital signatures were introduced.

Digital signatures

High trust digital signatures leverage public key cryptography to protect documents. In order to digitally sign a document a user is first issued a digital certificate that ties their real-life identity to a digital identity. At the time of signing the user's digital certificate is embedded into the document to serve as non-refutable evidence of the signer's identity. Multi-factor authentication such as passwords and one-time PINS can help make verifying the signer's identity even stronger. Strong encryption techniques protect the documents against tampering and free applications such as Adobe Reader can automatically verify that a document has not changed after signing.

To further increase security, the document can be timestamped to serve as forensic proof of the time of signing. In a court, the party looking to rely on the digital signature will have the necessary evidence to proof the identity of the signer and that the document has not changed after signing.

Advanced Electronic signatures

Advanced Electronic signatures, in South Africa, are a subset of digital signatures where the signing certificate is issued by a vendor that has been accredited by the South African Accreditation Authority.

These signatures are deemed by law to be particularly reliable and carries *prima facie* validity, in other words, if a dispute arise it is up to the person that disputes the signature to proof that the signature is not valid.

Advanced Electronic signatures carries the highest trust and can move the burden of proof away from the defendant on to the plaintiff.

LAWtrust offers a variety of electronic and digital signing solutions, including Advanced Electronic Signatures to suit the requirements of any organization.

To find out more about electronic and digital signing, please do not hesitate to contact LAWtrust.