NOTARIUS
Serving professionals

Article 1 of 4

Digital Signatures MADE SIMPLE

A digital signature is a specific form of electronic signature. It is used to confirm authorship and protect the data integrity of electronic documents. When issued and managed by a trusted source such as the governing body of your profession, a digital signature ensures that your documents are protected from tampering.

MODERN TECHNOLOGY IN ANCIENT TIMES

In essence, the digital signature technology is a modern-day descendent of ancient security systems. The following examples are meant to better illustrate how this technology works.

In our first example, a military general issues to each of his commanders a "private and unique key" for which he has in his possession the matching locks. He can then secure secret documents for any or all his commanders with each of their locks knowing that only the designated commander's key can unlock documents destined for him alone. The concept of matching keys and locks is today known as asymmetric key encryption. In other words, what one device locks (i.e. the commander's lock), the other unlocks (i.e. the commander's key).

In a related example, all commanders within that same army can safely communicate with each other by depositing all of their locks in one place that is accessible by them all. However, since all locks look the same, they must each be identified. Therefore, to protect against spies, each lock is engraved by trusted clerical staff with the name of the commander in possession of the matching key. Conversely, a commander may also secure documents for his fellows with his personal lock as a means of proving their origin (author) and protecting their content (integrity). The other commanders can then unlock these documents using the shared public key to which they all have access.

ANCIENT TECHNOLOGY IN MODERN TIMES

In modern-day terms, the same security principle, known as asymmetric key cryptography, is used when you digitally sign your electronic documents. An electronic document is made up of nothing more than binary code (zeros and ones). Digital signature encryption software reads the integrality of this code and generates a unique random mathematical summary of the file called a hash.

The randomness of the hash depends on the encryption level used during the digital signature process. For example, with 1024-bit encryption, countless unique hash possibilities are generated each time a document is digitally signed. Each hash leaves a mark on the document. This mark confirms that you are its author since only you could have generated the hash. It also protects the data integrity of the signed document because a single bit of data change creates a mismatch between the file and the hash, signalling that a change has been made to the document. As a result, you can feel confident that your documents are protected with a digital signature.

Still, the nature of securing documents does imply that you may also allow some select individuals to open them. In the same way that every commander had access to every other commander's lock, so too does every key holder have access to your public signature key, also called a public verification key, that matches your private signature key.

Concerns for data security and integrity are not new concepts. For business use, they are often required for professional or contractual liability reasons. Since business in 2010 is generally conducted electronically, digital signatures are an essential safeguard. Nevertheless, with so many crackers and hackers out there (the equivalent of spies in ancient times), who can you trust to manage your digital signature? In our next article, we will demonstrate how trust is a fundamental component of digital signature management.

For more information, contact us by phone at 1-888-588-0011.
sales@notarius.com