THE BUSINESS VALUE OF DOCUMENT SIGNING

Protect Your Identity and Deliver Authenticity in Your Online Documents

Entrust Datacard®

Table of Contents

THE BUSINESS VALUE OF DOCUMENT SIGNING

Protect Your Identity and Deliver Authenticity

Introduction

Document signing certificates enable organizations to digitally sign Adobe, Microsoft Office and other document types, marking them with visual trust indicators that verify the publisher's identity — an indication that the document has not been altered.

With document signing certificates, organizations can authenticate documents, allowing for secure and efficient electronic transmission of official papers, including legal documents, invoices, engineering plans and diagrams, diplomas, and charters while reducing costs associated with printing and maintaining paper files.

This white paper will discuss:

- **The history of document signing**
- **What digital signatures are and how they function**
- **The benefits and objectives of implementing document signing certificates**
- **Real world use cases of document signing certificates**

A Brief History of Document Signing

It would be hard to pinpoint the first ever human document. For millennia, humans have been scrawling notes on walls, stone tablets and parchment, onward through to today where most of us use digital tools to communicate. Along the way, standardized languages and methods for authenticating documents have been developed.

In 1069, Spanish nobleman El Cid made his mark on a military document[1], signing his name so that those who received that document would know it was truly written by him. This is the earliest historical record of a notable person using a handwritten signature to validate a document.

Until very recently, written signatures were the primary means of substantiating documents. In our modern computerized world, signatures have gone digital, with the United Nations officially recognizing digital signatures in 1996. Through the use of digital certificates, people are now able to sign emails, documents and all other kinds of digital media. This not only improves efficiency, it is also the most secure method of authenticating documents in human history.

What is a Digital Signature?

Digital signatures have three main features:

1. Identity assurance
2. Data integrity
3. Non-repudiation

Any recipient of a document signed with a valid digital signature gains trust and confidence that the document is authentic and its contents have not been altered. Digital signatures are legally binding due to this identity assurance and data integrity. The non-repudiation of digital signatures is of enormous benefit to those who wish to use digital signatures in place of traditional, handwritten signatures because it means the authenticity of the signature cannot be denied.

1 http://www.bbc.com/news/magazine-27311868

Document Signing Certificates

Document signing certificates support digital signature for Adobe, Microsoft Office and other documents to secure legally binding documents. Document signing certificates can be created on any desktop to create trusted document verification in real time.

Visual trust indicators show recipients that the sender's identity has been verified by a trusted certification authority (CA) and the document has not been altered during transmission. While paper signatures provide static proof of a document's authenticity, digital document signing certificates provide real-time assurance throughout the document's lifetime, as any changes made after a document is digitally signed are indicated and render the original signature invalid.

Many large governments and organizations depend on digital signatures to sign, protect and transmit official documents. As a result of their dynamic nature, digital document signing certificates have become the standard of digital-signing efficiency, and they have proven to be a reliable tool since their introduction to the world as a feature of the enterprise email software Lotus Notes 1.0 in 1989.

Over the last few decades, technology and software have advanced. In 1990, Microsoft Word became the most widely used word processing software, and Adobe introduced the Portable Document Format (PDF) in 1993. As Word documents and PDFs became more prevalent, the need to sign documents — and not just emails — started to grow.

Adobe Approved Trust List

Aligning the development of digital signature technology with the makers of the software for which they are designed to sign plays a pivotal role in improving the effectiveness of document signing certificates and the overall user experience of digitally signing Adobe PDFs and Microsoft documents. The Adobe Approved Trust List (AATL) is one such program that improves the effectiveness of document signing certificates on Adobe PDFs. CAs are qualified and then added to a Trusted Identity List (TIL) maintained by Adobe. The CA submits an application along with their root certificates to Adobe so that Adobe Acrobat and Reader can check that the signed PDF is secured by a valid certificate that is chained up to the corresponding root certificate on the (TIL). The requirements to become a member of this program are extensive, which promotes the values of digital security, authentication and trust, including generating and storing key pairs in a medium that prevents exportation and duplication, demonstrating the use of strong identification and authorization procedures, and passing a certification authority third-party audit (such as the WebTrust audit for CA) within 18 months of applying to join the program.

Physical Token Component

Public key pairs are generated on hardware security modules (HSMs) that store the private key. HSMs are highly secure so that the private key cannot be exported or used by another party to make a signature. Some CAs provide Crypto-as-a-Service by offering hosted HSMs, or an HSM can be purchased and managed on-premises. Certificate signing keys can also be stored on a USB token, which are often used for low volume use cases. The minimum requirement for storing signing certificate keys has been established at FIPS (Federal Information Processing Standard) 140-2 Level 2, which requires that the hardware have features such as tamper-evident coatings or seals (that would need to be broken to access the plaintext cryptographic keys) and security parameters inside the module.

Document Signing Certificate Types

Document signing certificates can support a variety of digital signing scenarios, including signatures for individuals, groups or organizations. Additionally, document signing certificates can also support manual or automated signing, making them both a flexible and efficient digital signing option.

Benefits and Objectives of Document Signing Certificates

Data Integrity

Think of digital signing like putting a stamp or seal on a traditional document. Centuries ago, you could tell if a message had been tampered with if a seal was no longer intact. The invention of digital signing and hashing offers a similar, but much improved way to ensure that a document has not been altered. The signatory, in both cases, is the person putting their final stamp of approval on the document.

THE BUSINESS VALUE OF DOCUMENT SIGNING

But how does this process work?

The publisher cryptographically hashes the document into a fixed length number (i.e., 160-bits, 256-bits, etc.). The length is fixed for efficiency so that the hash for books such as "Jack & Jill" and "War and Peace" will be the same length. The hash is encrypted using the private key. The document, encrypted hash and certificate string are provided to readers. The readers decrypt the hash with the public key, which is in the document signing certificate(s). The reader also hashes the document. The reader then compares the two hashes. If they match, the publisher has signed the document and the reader verifies that the document content has not changed.

Trusted Identity

Most publicly trusted digital certificates, including document signing certificates, require third-party identity verification, which is usually carried out by a CA.

In order for the document signing certificate to establish trust, the CA generates a root certificate, which software developers embed into their applications. The root certificate acts as the link in the chain of trust between the CA and the software developer's software.

In the case of document signing, a signature may contain an identity — the organization name, department, and an email address of the individual or group that will be signing the documents. When signed, the identity will be displayed on the document to let the recipient know who signed it and when it was signed.

The software displaying the signature acts as the third-party verification and is embedded within the certificate root chain. The signature display provides assurance to the end user that they can trust in the information they are reading in the document, that the information comes from the expected source and, combined with the data integrity aspect, the information contained in the document is what was written by the signatory.

Any organization can set up their own public key infrastructure to issue digital certificates for signing. However, privately issued certificates will not be trusted by other public devices. This means that you need to use a third-party CA if you want to get automatically, publicly trusted digital signatures.

Non-Repudiation

The digital signature in document signing certificates must be undeniably authentic in order to be legally binding. Such a state of signing authenticity is known as non-repudiation meaning the legitimacy of the digital signature cannot be repudiated or refused.

Thus, if someone signs a document using a digital signature, we need to be able to show that only that person could have had control over that signature at the time. With digital signatures, the most important way to prove non-repudiation is to ensure that only the signing party has control over the private key that is used to establish the identity.

Document signing certificate private keys are stored and generated on FIPS 140-2 Level 2 tokens. These hardware devices protect the private key. Once a private key has been generated on the device, it cannot be removed. The devices are protected with pins and possibly even more complex authentication requirements to make sure that if the hardware is stolen or compromised, only the person who knows the authentication code can access the private key. All of this security is in place to ensure non-repudiation and to help make these signatures legally binding.

Lifetime Authentication

CAs are able to equip their document signing technology with the ability to maintain the validity of digitally signed documents for the document's life time. Any changes made to the document will render the digital signature invalid, signaling that the document has been changed and making any agreements and digital signatures in the previous document also invalid on the newly changed document.

Revocation

Digital certificates can be revoked if the user thinks their identity or the certificate's private key has been compromised. Revocation will invalidate the signature from any future use. Software that supports digital signatures will perform a revocation check when the document is opened. The signature will contain a link where the software can go and perform the check. If the revocation service returns a response that the certificate and signature have been revoked after the signature was applied to the document, the signature will appear as invalid with a number of visual indicators in the document.

Timestamping

When a digital signature is applied to a document, a digital timestamp may follow. The timestamp will show the exact time and date that the document was signed. Timestamping is critical when it comes to supporting signature revocation and making sure that signatures are valid well after the certificate has expired.

When revoking a signature, the user is likely saying that they do not want their signature to be used in the future to sign any documents. If their previously signed documents have been timestamped, those signatures will remain valid. Digital certificates have validity periods and do expire. Timestamping ensures that signatures remain valid even after the certificate itself has expired, allowing for long term digital signatures to be used on documents.

Capitalize Digital Signature Laws

Business in the digital age moves very quickly. Laws surrounding the validity of digital signatures have been enacted to recognize their place as a credible technology that improves business efficiency. The United Nations signed the UNCITRAL Model Law on Electronic Commerce in 1996, which led several nations to develop their own digital signature laws such as the U.S. Federal ESIGN Act, GLBA, HIPAA, PCI DSS and the US-EU Safe Harbor Framework.

Real World Use Cases

Banks

One of the largest financial institutions in Canada uses document signing certificates to create an efficient and secure process to allow their customers to easily apply for new financial services.

The financial institution offers new financial services in bulk to their customers. After the customer fills out a form to apply for the financial service and digitally signs it, the financial institution emails back a completed copy that has been digitally signed by their approval team. The digital signature process allows the financial institution to provide a higher level of security and save money by reducing the amount of paper and mailing traditionally required for financial service application. Additional security is provided in this case because the document cannot be modified after it has been signed.

Supports Green Office Initiatives

Document signing certificates are paperless, which reduces the cost and environmental impact of doing business with print and paper. Additionally, document signing certificates are a great solution for paperless backup and archiving of digital documents.

Efficiency

In many cases, organizations that are not using digital signatures or a digital document workflow have to spend a great deal of time each day signing documents and delivering them electronically. A good example might be an internal employee who needs to apply for a corporate credit card. The employee would receive the form to apply by email, print off the form, sign it with a physical signature, scan the document and email it back to their finance department for processing. With a digital document workflow that supports digital signing, this whole process could be completed without having to print or scan any documents. In industries where signing occurs frequently, such as health care, real estate and finance, this can help save countless hours per year.

Universities

Some universities leverage document signing certificates as a way to digitally sign student transcripts. Getting a transcript can be a painful, slow and expensive process. Typically, students must either physically go into the registrar's office or request a transcript online. The registrar must then print the transcript, stamp it with a special seal to prove authenticity and deliver the document back to the student. There is also usually a cost associated with requesting a transcript. Using a digital signature allows pioneering universities to return the transcript as a digitally signed PDF document. The student can get their transcript in seconds, at a much lower cost, and the university can also reduce their own cost and manual work while providing a more secure version of the transcript.

Government Entities

Many federal, state and local government entities have mandated that engineering and architectural documents be digitally signed.

THE BUSINESS VALUE OF DOCUMENT SIGNING

Five Key Takeaways

1. Digital signatures provide data integrity and identity assurance in a way that is much more secure than traditional handwritten signatures and include visual indicators of trust as shown below:

This document has been certified by a valid trusted signature using the Adobe trust process and cannot be repudiated by the author. Certified documents may allow users to complete forms or also sign documents.

This document has been signed by a valid trusted signature using the Adobe trust process and cannot be repudiated by the author.

This document was signed using an untrusted certificate and cannot be verified.

This document has been altered or tampered with since signing.

2. Document signing certificates offer a means to digitally sign Microsoft, Adobe and other types of documents to enable users to efficiently authenticate documents. Document signing certificates eliminate the need to print, sign, scan and email documents that need to be signed.

3. Document signing certificates are secure and reliable in that they are timestamped and non-reputable. There are laws all over the world that allow digital signatures to be legally binding.

4. Any document signed with a document signing certificate that is tampered with is no longer valid. Visual notification will be provided to the end user that something has changed in the document since the author signed it.

5. Document signing certificates grant an added layer of mobility for those who use them, allowing large institutions to engage in business agreements with their customers, employees and/or members in a fast, secure and efficient manner.

About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences—whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

Entrust Datacard®

Corporate Headquarters

U.S. Toll-Free Phone: 888-690-2424
International Phone: +1-952-933-1223

info@entrustdatacard.com
entrustdatacard.com