IDnomic

Digital signatures: A security imperative for today's open and fast-paced world

Internet connectivity makes today's world more open than ever before. Organizations and individuals alike are exposed to new online threats every day. At the same time, we all want to go faster. We want to finalize a contract within minutes or buy something almost instantaneously – and all digitally, and without that traditional face-to-face contact.

Digitization not only holds the key to speeding up processes but also to increase security in today's increasingly open world. But how do we digitize the part of process that traditionally sees us put pen to paper – the signature?

In this expert advice, I present digital signatures, demonstrate how they improve the user experience while enhancing security, then finally share my top tips on how best to implement a digital signature solution.
Let me start by talking through the different types of digital signature.

Not all digital signatures are the same

There are, in fact, three levels of digital signature:

- The **basic signature** encrypts a document's fingerprint using an asymmetric cryptography algorithm. It mainly ensures a document hasn't been modified during transmission (integrity).
- The **advanced electronic signature** (ADES) adds some additional information to strictly identify who signed a document and in what context it has been done: when, what for, with what trust anchor.... The ADES signature aims to consider a signature as a secure transaction that can be verifiable for a long time after its creation.
- The **qualified electronic signature** is an ADES signature done with a more secure identity within a more secure cryptographic environment. It uses a qualified electronic certificate and the signature is done using a qualified signature creation device, which could be an evaluated smartcard or a hardware security module (HSM). Both are crypto processing devices that calculate the cryptography for the signature.

Tapping into knowledge and experience

Implementing a digital signature, while greatly beneficial, can be quite complex. After all, you need to manage processes, identity lifecycles and integration into an application. You also need to understand legal implications.

The technical standards that define how to create and use digital identities and signatures must be perfectly understood. Adhering to those standards is crucial to guarantee another actor can verify the identity and signature. You also need knowledge about cryptography and specific devices, such as Hardware Security Modules (HSM) and their 'key ceremony'.

Look at the state-of-the-art security suites, which can deliver the necessary components including not only the digital signatures but also the PKI and the timestamp servers. A complete suite will also integrate the HSM you need to protect your keys and/or could be based on an Appliance integrating both HSM and Trust application functions. But take care to adopt a solution that has been evaluated and certified by trusted third parties, such as the French National Information Systems Security Agency (ANSSI).

Engaging an experienced partner with the necessary technical and business knowledge is crucial for success.

Making digital signatures a success

If you are currently exploring how digital signatures can help you make your processes faster and more secure, I have a few tips for you:

1. Start by identifying your specific security needs. In many cases, an advanced electronic signature is sufficient, especially when combined with a mutual agreement to legalize its use. The qualified signature, which is for applications that need very strict signatures such as legal work, is more complicated to obtain because it requires external audit works.

2. Be mindful of user acceptance because the digital signature introduces new ways of working. Communicate the changes with your users and also consider their ways of working. In the hospital example, doctors will not want to authenticate each time they create a prescription.
The application must consider this.

3. You need to take care of the legal environment. Some domains have their own specific rules – the tax and the health domains, for instance. In Europe, you must also comply with the eIDAS regulation. eIDAS specifies what a good electronic identity and an identity provider look like, how best to deliver good identities and how they work with the digital signature. It also regularizes the centralized digital signature server.

4. A good electronic identity is a pre-requisite for a good digital signature. You can buy an electronic identity (an electronic X.509 certificate) from a public certification authority. In some cases, be aware that you don't need to implement a PKI into your own Information System.

5. Start with one application that you can capitalize on, particularly when using a digital signature server. The digital signature server centralizes the electronic identity, delivering it to any type of application on any type of device via a cloud-based signature service. It's easier to deploy compared to the smartcard alternative and now fully authorized by the eIDAS regulation.

Tapping into knowledge and experience

Implementing a digital signature, while greatly beneficial, can be quite complex. After all, you need to manage processes, identity lifecycles and integration into an application. You also need to understand legal implications.

The technical standards that define how to create and use digital identities and signatures must be perfectly understood. Adhering to those standards is crucial to guarantee another actor can verify the identity and signature. You also need knowledge about cryptography and specific devices, such as Hardware Security Modules (HSM) and their 'key ceremony'.

Look at the state-of-the-art security suites, which can deliver the necessary components including not only the digital signatures but also the PKI and the timestamp servers. A complete suite will also integrate the HSM you need to protect your keys and/or could be based on an Appliance integrating both HSM and Trust application functions. But take care to adopt a solution that has been evaluated and certified by trusted third parties, such as the French National Information Systems Security Agency (ANSSI).

Engaging an experienced partner with the necessary technical and business knowledge is crucial for success.

Pierre-Jean Aubourg
Director of Professional Services of Atos IoT Security department

After five years at SYSECA – the IT services subsidiary of the Thomson group (now Thales) – Pierre-Jean Aubourg joined Bull Engineering as head of electronic messaging projects. He contributed to its very first security projects in 2001, and later became Director of the Payments Systems and PKI division in Bull's security Business Unit. Now acting as Director of Professional Services of the Atos IoT Security Department. In this role, he is responsible for integration services for the product line including MetaPKI and MetaSign. Pierre-Jean Aubourg has a higher degree (DESS) in electronics and industrial computing, and is a graduate of the French Ecole des Techniques du Génie Logiciel.

For more information: atos.net/digital-identities

CT_J2710_200924_MT_FS_SECURITY