Digital Signature

Supplier handbook - Introduction to Digital Signature

March 2016

2One Global Procurement

enel

Digital signature - overview

- Digital signature is defined as an attestation system for digital document aimed to assure both the “not denial” and the document integrity

- Digital signature posted on a document aims to satisfy the following three requirements:

  › the receiver is able to verify the sender identity (authenticity)

  › the sender can not deny a document signed by him (not denial)

  › the receiver can not modify a document signed by someone else (integrity)

Digital signature - features

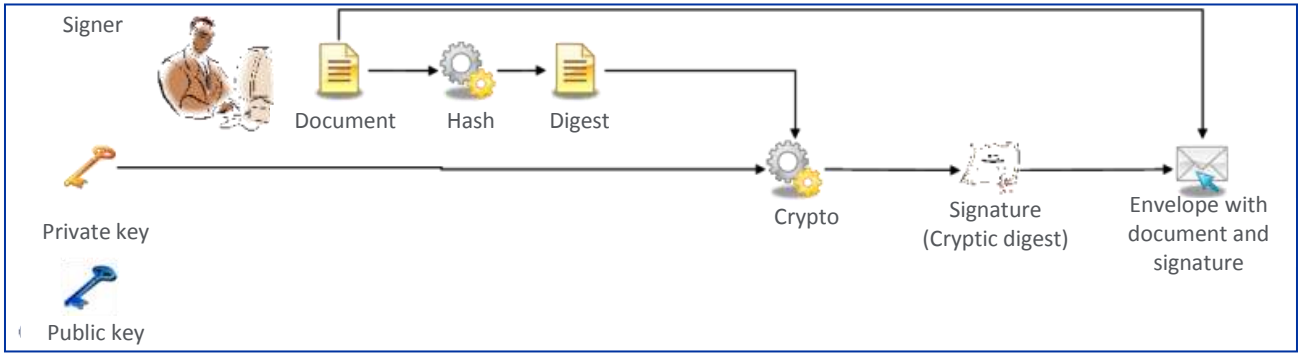
To satisfy the requirements it is necessary that the digital signature tool:

- is based on a cryptic asymmetric keys system
- assures the messages content confidentiality, by preventing whom does not have the “key” (according to cryptic definition) from any interpretation
- provides each user with a pair of certified keys: one private key, not shared with anyone, for decoding the received messages and for signing the sent ones, and a public key available for other users in order to encode the messages sent to him and to decode/verify his signature
- uses keys issued by a certification authority subject to AgID surveillance
- is created through a device with the highest security level (smartcard/USB token)

Digital signature operating flow

Signature process (user A)

In the picture is reported the process followed by user A to sign a document:

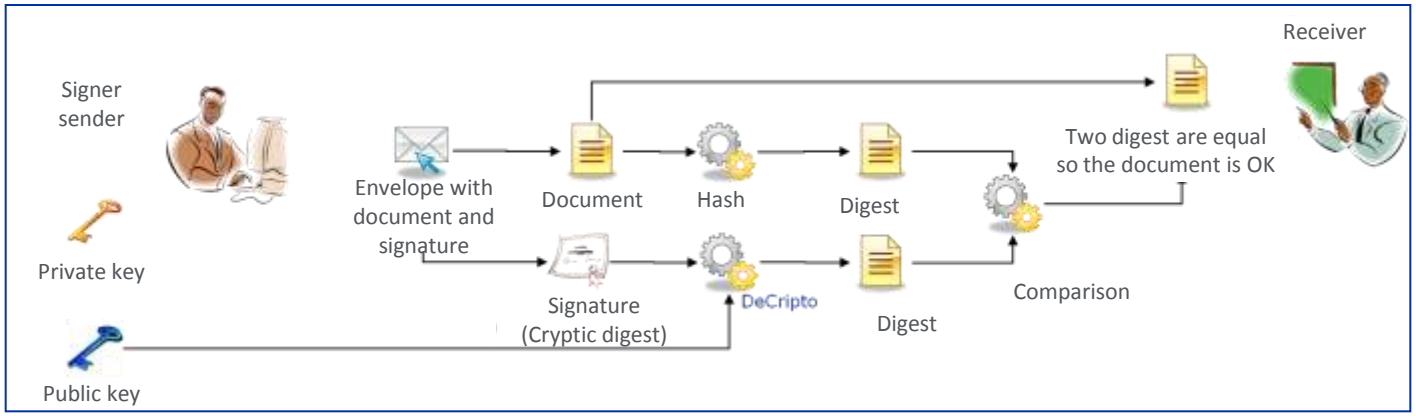


1. The document to be signed is subject to hash algorithm to generate a digest that represents the document univocally
2. The digest is encoded by using the signer private key and then the signature is generated
3. Then document and related signature are inserted in an electronic envelope in order to create the signed document
4. Digital signature is permanently linked to the electronic document in order to add important information used to verify its integrity, authenticity and not denial
5. The user must have a proper kit (smart card, smart card reader and signature software). As an alternative for smart card, the user can use an USB token. Through these tools the user can digitally sign and apply timestamp to any documents

Digital signature operating flow

Verification process (user B)

In the picture is reported the process followed by user B to verify a document:



1. Document and signature is extracted from the envelope
2. The signature is decoded by using the signer public key (user A) and by extracting the original digest
3. The document is subject to hash algorithm to create the current digest to be compared to the original contained in the signature
4. If the two digests are equal the document has not been corrupted and it has been signed by the private key owner who has encoded his signature

Digital signature validity

- The owner certificate has a validity period, but it can be cancelled or suspended before the defined deadline (i.e.: signature device taking away or loss, not correctness of certificate information)
- Certificate cancellation and suspension correspond to the missed signature of the document
- Cancellation is permanently, suspension is a temporary condition of the certificate that can be passed to “cancellation” or “suspension revocation”
- Some criticalities could be related to the use of document digitally signed through certificate subsequently expired, cancelled or suspended
- In this cases the timestamp tool enables the possibility to identify the exact moment in which the document has been signed and to demonstrate that in that moment the certificate was still valid

Digital signature - accepted document formats

Currently Italian law provides for three different document formats to produce file digitally signed:

- **P7M** format -> available since 1999, it is the format that PA must accept
- **PDF** format -> introduced in 2006, it is a standard format that not required any fees to anyone. It has a very wide diffusion and immediate availability (the reader software can be free downloaded from Internet) and it satisfies technical/legal requirements to manage digital signature
- **XML** format -> introduced in 2006 to boost the digital signature diffusion within sectors in which the xml language is typically used for electronic management of documents exchanges (i.e.: banking, public health)

Digital signature - Italian law

- In Italy it is possible to create electronic documents with the same legal validity of paper document with manual signature

- The law framework has been set up since 1977 through the issue of act 59/97 (art. 15) then evolved to receive the European guideline about electronic signature (Guideline 1999/93/CE) that lead to the issue of several amendments to create the current law framework

- On AgID site is available a brief compendium and other information on digital signature

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

- At the following link is available the list of parties authorized to issue digital signature certificates

http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi