DGTAX FOCUS

QUALIFIED ELECTRONIC SIGNATURE

Qualified electronic signature (FEQ) - or digital signature - is the result of an IT process, based on data encryption, which allows an electronic signature to be inseparably associated with an IT document, i.e. a set of bits representing facts, acts or data with legal significance.

Any natural person who applies for a digital signature can obtain one.

THE LEGAL FRAMEWORK OF REFERENCE

The national legislation of reference on digital signatures is the Digital Administration Code (CAD), Legislative Decree No 82 of 7 March 2005.

The specific subject of signatures is driven by European Regulation 910/2014 (also known as eIDAS), which has been fully operational since 1 July 2016.

WHAT IS A DIGITAL SIGNATURE

A digital signature is a type of (electronic) signature based on a cryptographic key mechanism that allows the subscriber to affix a unique distinctive mark to a digital document.

Article 24, Legislative Decree 82/2005 outlines the features of the digital signature.

> "1. A digital signature must refer uniquely to a single subject and to the document or set of documents to which it is affixed or associated.
>
> 2. The affixing of digital signatures supplements and replaces the affixing of seals, punches, stamps, marks and brands of any kind for any purpose provided for by the legislation in force.
>
> 3. A qualified certificate that, at the time of signing, has not expired or been revoked or suspended must be used to generate the digital signature.
>
> 4. In accordance with the technical rules referred to in Article 71, the validity of the qualified certificate must be ascertained, as well as the identification elements of the digital signature holder and the certifier and any limits on its use. The guidelines shall also define the mode, including temporal features, for affixing the signature.
>
> 4-bis. The affixing to an electronic document of a digital signature or another type of qualified electronic signature based on a revoked, expired or suspended electronic certificate shall be equivalent to a non-signature, unless the suspension status has been cancelled. Revocation or suspension, however motivated, shall take effect from the moment of publication, unless the revoker, or the person requesting the suspension, proves that it was already known to all the parties concerned.
>
> 4-ter. The provisions of this Article shall also apply if the electronic signature is based on a qualified certificate issued by a certifier established in a State outside the European Union when one of the following conditions is met
>
> > (a) the certifier meets the requirements described in the eIDAS Regulation and is qualified in a Member State;
> >
> > (b) the qualified certificate is granted by a certifier established in the European Union that meets the requirements described in that Regulation;
> >
> > (c) the qualified certificate, or the certifier, is recognised under a bilateral or multilateral agreement between the European Union and third countries or international organisations."

It is therefore a type of electronic signature that - by complying with special technical requirements - guarantees authenticity, integrity, reliability and legal validity of documents, granting the same legal value as a handwritten signature.

FEATURES OF DIGITALLY SIGNED DOCUMENTS

Digital signatures enable legal value to digitally signed documents, by means of an IT process that gives three fundamental qualities an e-signed document:

- Authenticity (the signatory assumes responsibility for the content of the document);
- Integrity (the document is unchangeable after the effectiveness of the signature);
- Non-repudiation (the document cannot be disowned by the signatory).

Therefore, once signed a computer document can be used for legal purposes and opposed to third parties.

HOW THE DIGITAL SIGNATURE WORKS

Each subscriber is assigned a pair of "keys" (two sets of binary numbers of 2048 bits) by the certifying body (the "Agenzia per l'Italia Digitale"):

- A "public" key, so called because it is known to all interested parties (which identifies in certain the holder of the signature certificate) and
- a "private" key, which functions under the exclusive control of the holder, and encrypts the electronic document to be signed.

The private key is installed on a device (a microchip) that is assigned to the subscriber, and can only be used together with a secret code (the personal identification number, i.e. PIN).

DIGITAL SIGNING OF A COMPUTER DOCUMENT

To sign a computer document, the holder uses software that works in three stages.

1. It calculates the footprint (unique and unchangeable) of the computer document by means of the so-called "hash" function;
2. Sends the footprint of the document to the secure environment where the private key (signature device) is kept and where the signature is generated; this, to be activated, must be validated using the holder's PIN. Once the key has been activated, the signature device encrypts the footprint of the document in such a way as to bind the signature to both the signatory and the signed text;
3. Applies the digital signature to the document.

The result of the operation is the digitally signed document.

Each provider follows its own procedure and provides specific software to perfect the signing process; to affix one's signature, therefore, one must use the specific software of the provider from which the digital signature was obtained.

VERIFICATION OF THE DIGITAL SIGNATURE OF A COMPUTER DOCUMENT

To verify the validity of the signature, the recipient uses specific software that

1. Extracts the public key from the holder's certificate
2. Decrypts the file with document and signature
3. Using the hash function, recalculates the footprint
4. Verifies that the footprint transmitted by the sender and the one recalculated by the recipient are identical.

If the result is positive, the signature is valid.

The signature validity verification operation can be performed with any software product (not specific to the partner that generated the digital signature).

HOW TO OBTAIN A DIGITAL SIGNATURE

A natural person can obtain a digital signature by contacting an authorised provider.

Digital signatures can nowadays be alternatively

A. contained on physical devices (hardware) delivered to the holder, e.g:

- a smart card;
- a USB stick, or

B. managed with "remote" solutions (service); in this case the user does not receive a physical object, but thanks to the use of cloud solutions accesses their digital signature remotely, through the use of physical devices (e.g. smartphones) that provide "one-time-passwords" (OTP).

The authorised providers in Italy are, at the time of writing, 18; the list can be found at

https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/IT

To obtain a digital signature, therefore, it is necessary to

- Find an authorised provider;
- Purchase the digital signature device/service,
- Finalise recognition of one's identity (in person, at home or via the web), by presenting a valid proof of identification;
- Activate the purchased kit, using the different procedures that vary for each provider.

Once activated, a digital signature is affixed using the specific provider's software (typically, a document to be signed is selected and the specific procedure is carried out).

FUTURE APPLICATIONS AND USES

Digital signatures have become mandatory in many administrative and business processes.

Electronic invoices, electronic court proceedings, financial statements and the submission of specific administrative deeds to the public administration are signed digitally.

In the future, it may be so that digital signatures completely replace traditional ones.

FOR MORE INFORMATION CONTACT

tax@dgtax.it - www.dgtax.it - +39 02 433 551

2022 – DGTAX – ALL RIGHTS RESERVED