ds | verify

by digitalsign

User's Manual

Content

Over the past few years, we have been witnessing an increasingly fast technological transformation, influencing the various sectors of society, namely, the way we operate our business relationships, where paper and handwritten signatures took a central role in the formalization of legal transactions. Nowadays, as a result of this technological evolution, it is already possible to conclude legal transactions in a faster, more agile and sustainable manner, thanks to the increasingly evident adoption of the dematerialization of physical processes, replacing paper and handwritten signatures by electronic documents and electronic signatures.

However, this transformation has brought with it new challenges, as well as new requirements for digital processes, so that we can ensure not only the evolution of procedural logistics, but also greater legal certainty for all parties involved in the use of these new tools.

Given this new reality, the European Parliament felt the urgency to respond to the clear need to standardize European e-commerce, namely by publishing Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014. This Regulation established the undeniability of legal effects, as well as their admissibility as evidence, upon the conclusion of a contract in electronic format with the affixation of electronic signatures to it. In addition, the same Regulation states that a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member States.

In this context, the qualified electronic signature differs from other electronic signatures, as it is positioned as the one it has a higher level of technological security and consequently legal certainty.

Furthermore, the qualified electronic signature is the only one that has a legal effect equivalent to a handwritten signature, creating, when properly affixed to an electronic document, a presumption of authenticity, integrity and non-repudiation, and thus providing full proof of the provisions contained therein.

Considering all this, it is essential to have tools capable of demonstrate whether a given qualified electronic signature is valid or not. Due to the technology involved in creating and affixing qualified electronic signatures, the way we can verify whether a qualified electronic signature is, in fact, valid, differs from the way we can verify whether a handwritten signature is valid. We already emphasize that, unlike handwritten signatures, the validation of qualified electronic signatures is immediate, secure, simple and effective, as we will demonstrate throughout this document.

In the presence of this need, DigitalSign, as a Qualified Trust Service Provider, created **DS Verify - a qualified service for the validation of qualified electronic signatures or qualified electronic seals.** In accordance with the provisions set out in Article 32 of Regulation No. 910/2014. 910/2014, all users are allowed to validate the authenticity and integrity of qualified electronic signatures or qualified electronic seals, ensuring full dematerialization of processes, with all the legal security required for this purpose.

How is a qualified electronic signature or qualified electronic seal validated

In order to validate a qualified electronic signature, the qualified validation service must follow the requirements established in article 32 of Regulation no. 910/2014, namely: i) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of the eIDAS Regulation; ii) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; iii) the signature validation data corresponds to the data provided to the relying party; iv) the unique set of data representing the signatory in the certificate is correctly provided to the relying party; v) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; vi) the electronic signature was created by a qualified electronic signature creation device; vii) the integrity of the signed data has not been compromised; viii) the requirements provided for in Article 26 were met at the time of signing.

Therefore, after DS Verify has checked all these requirements, **it will provide you with the correct result of the validation process and allow you to detect any security issues or confirm that the qualified signature or qualified electronic seal is indeed valid.**
After the user places the electronic documents he wants to validate in Verify , it will automatically show one of three possible results :

TOTAL-PASSED: When cryptographic checks of the signature (including checks of hashes of individual data objects that have been indirectly signed) are successful, as well as all checks prescribed by the signature validation policy have passed. That is, **the qualified electronic signature or qualified electronic seal is valid.**

TOTAL-FAILED: Cryptographic checks of the signature failed (including checks of hashes of individual data objects that were indirectly signed), or the signature certificate is proven to be invalid at the time of signature creation, or because the signature is not in compliance with one of the core standards, as the cryptographic verification building block is unable to process it. That is, **the qualified electronic signature or qualified electronic seal is invalid.**

INDETERMINATED: the results of the checks carried out do not allow checking whether the signature is valid or invalid. However, **if this is the result, then it means that this is not a valid qualified certificate.**

In addition to these results, which are immediately available on the user's platform, it is also possible to view the results in greater detail, since DS Verify provides two reports on the validation process of the qualified signatures or seals:

Summary Report: this report allows the user to access information about the validation process of a specific qualified certificate in a simplified way. It presents not only the type of signature used, but also the number of signatures present in the electronic document, as well as timestamps, containing the hash of the document, date and time at which the signature was added to a certain electronic document. In addition, it has all the details of the qualified certificate used, namely, the name of the signer, the certificate format, the identification number, among others.

Detailed Report: this report allows the user to check all the details of the validation process in a detailed way, namely at the technical level. This report contains all the elements mentioned in the summary report, additionally allowing the user to deepen the technical reasons that led to a non-valid result, namely through the sub-indications linked to the main indication (TOTAL-FAILED or INDERTEMINATED). For more information about the sub-indications, please see (link).

What is the Validation Policy

In addition to these results, which are immediately available on the user's platform, it is also possible to view the results in more detail, since DS Verify provides two reports on the validation process of the qualified signatures or seals:

Any qualified validation service must provide its services using a validation policy. This policy defines the set of validation constraints to be used to validate the qualified electronic signatures or qualified electronic seals submitted and processed by DS Verify.

Thus, the Verify validation policy validates qualified electronic signatures and indicates whether they are Advanced Electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC), or a Qualified Electronic Signature (QES). All certificates and their related chains supporting the signatures are validated according to the Trusted Lists of the EU Member States (this includes the signer's certificate and the certificates used to validate the certificate validity status services - CRLs, OCSPs, and timestamps).

That said, all electronic devices submitted in Verify will be processed and validated according to the validation policy 1.3.6.1.4.1.25596.5.1.1.*

* Validation Policy: Validates electronic signatures and indicates whether they are Advanced Electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified Electronic Signature (QES). All certificates and their related chains supporting the signatures are validated according to the Trust Lists of the EU Member States (this includes the signer's certificate and the certificates used to validate the certificate validity status services - CRLs, OCSPs, and timestamps).

4

Processing of Personal Data

The files submitted in this validator will only be analyzed for the purpose of validating the existing electronic signatures, in accordance with the policy 1.3.6.1.4.1.25596.5.1.1. We also inform you that the submitted documents are deleted immediately after the conclusion of this process, and there is no further processing of any information regarding the content of the submitted files, namely personal data.

DS Verify also does not use any kind of cookies.

How to use Verify

Click on the camera above and watch the DS Verify usage vídeo.

digitalsign

Largo Padre Bernardino Ribeiro
Fernandes 26, 4835-489 Guimarães

✉ geral@digitalsign.pt

☎ +351 253 560 650

🌐 www.digitalsign.pt