Technical Information about 'Safe Stamper File'

Digital File Certification

February 2025

1.- How it works

Users must access the service from Safe Stamper's official website. From there, they enter the "Files" service and upload the file they wish to certify.

The file is uploaded to Safe Stamper's servers, which act as witnesses to the existence of the file at that exact date and time.

The duration of the process to submit and certify the file will depend on its size. Once completed, the user can download a PDF certificate that includes the digital hashes to identify the file. The certificate includes a URL that allows other people to verify it, as long as the user has not chosen to restrict access with a password.

Additionally, there is now the possibility of not uploading the file at all. Instead, the hashing process can be done locally on the user's computer, ensuring confidentiality in the case of sensitive files. This way, only the cryptographic hash is sent to Safe Stamper's servers for certification, without exposing the content of the file.

2.- Certification Document Technology

The PDF certificate includes four cryptographic hashes or algorithms: MD5, SHA1, SHA256, and SHA512. Once obtained, they appear in the PDF along with the date the file was submitted, the file name, and its size. The document is digitally signed and timestamped.

These hashes are calculated based on the file submitted by the user. They allow, if necessary, to demonstrate with certainty which file was certified, as only that specific file will be able to generate the exact same hashes.

The certificate constitutes reasonable and valid evidence to prove the existence of the file at the specified date, thanks to the recognized electronic signature of the organization behind Safe Stamper: Safe Creative SL.

Therefore, both video and certificate combined constitute a rigorous and valid technical evidence, sufficient to confirm the information it contains.