Signature, Validation, Preservation and Custody Service

The new DigitalSign 360° solution to dematerialization

Although continuous (and unstoppable) technology evolution brings everyone convenience, sustainability, ease (among others), it comes at a cost... High complexity of systems and a huge gap in security. A concrete example of this is the electronic signature, where no paper is required, we sign just with an OTP, we sign in bulk... But is that all? Did you know that your signature will probably expire in one or two years?

DigitalSign is working hard on providing a high security and low integration complexity standard, so that the "work-flow" gets complete.

Why should we validate electronic signatures?

Nowadays, it is easy to forge an electronic signature in an almost perfect way. There are several applications in the market that lets you sign electronically, but that signature has no full legal value in Europe (eIDAS Regulation). In this scope, did you know that it is possible to:

- Sign a document, but the signature does not cover the entire document? – leaving a part of a document unsigned takes us to potential unauthorized changes in its content.

- Overlap a signature with an input field, making it vulnerable to hide malicious content/code?

- Sign a document with a certificate that holds your name or your clients name, but the certificate is fake, most likely issued by a non-authorized QTSP

- Even if the signature was made based on a qualified certificate issued by a QTSP, that certificate may be invalid (revoked)?

All of these scenarios have already been reported in the past, and all many may "look green" in the Adobe Acrobat Reader... That's why it is important to rigorously validate a document electronically signed before accept it.

DigitalSign Qualified Validation Service (under eIDAS Regulation) allows you with a single https request, to validate any document against a huge range of attack vectors. We strictly follow every rule imposed by eIDAS, to ensure your document/signature is legitimate and credible. If it is not, you can check, rule by rule, where it fails and why it is not a Valid Qualified European Signature.

Why should we use a Preservation Service?

As mentioned above, a digital signature may be valid for just one more day or by many years. In the world of Digital Signatures, there are standardized 4 main formats:

- B – the signature will be valid only until the signing certificate is valid. If the certificate expire in next month, the signature will expire in next month, and the Document will have a red X stating signature invalid. Usually, when a certificate is issued, it has an expiration date of two or three years.

- T – about validation range, it is identical to format B. It adds a timestamp to the signature, to prove, by an external source, the time of creation of the signature.

- LT – By the time of signing/validation it is added the result of the certificate validation process to the signature, making it valid until the expiration of the timestamp certificate validity. This usually extends the validation time by several years.

- LTA – Finally, this format is identical to LT, but ensures that even after the original timestamp certificate validity, the signature can be re-validated (by adding a new timestamp), to match the validity of the new timestamp certificate. This also can by applied to enhance the cryptographic algorithms used to create the electronic signatures.

DigitalSign preservation service ensures that every document is stored in the LTA format and, additionally, keep track of the documents expiration date to re-validate them, in order to extend the validation time to the infinite. Furthermore, we will generate for you an official report digitally signed by us stating the validation result of your document (a proof of validation).

Again, submitting a document to our preservation service is as easy as making an https request.

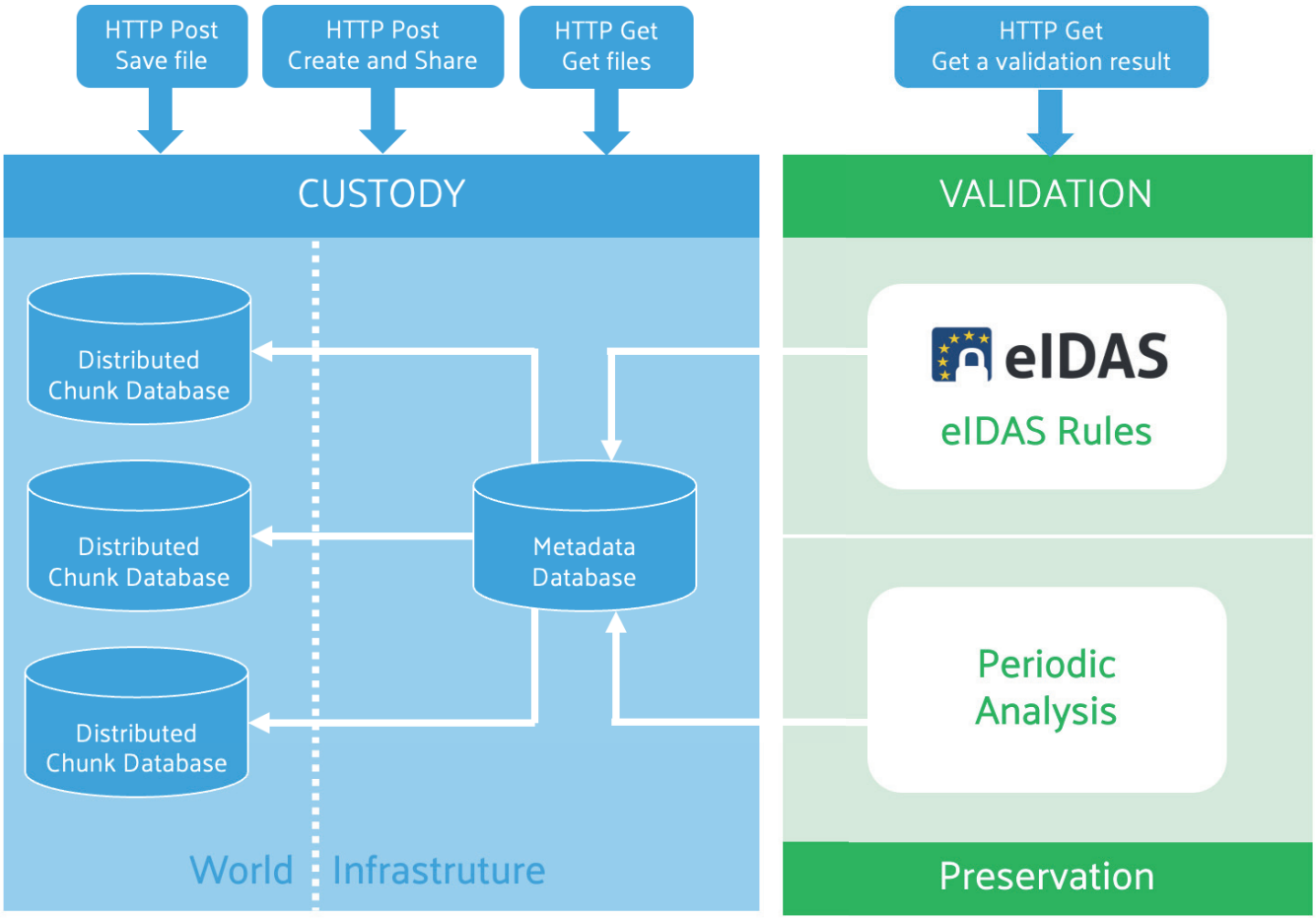
Why do we need a Custody Service?

The importance of our documents is immeasurable, and so it deserves the highest standards in security. For that reason, we built a system where your documents are fractionated in several pieces (chunks), and these chunks are stored in an external distributed database (may be even in your facilities). By splitting the “map” and the “treasures”, we ensure that any attacker cannot retrieve the full document, even if he has access to the databases. For the highest security demands, we can even ensure that the original document is encrypted by you, locally, with a pass-phrase that only you know, and then spited in chunks and spread in the world. We comfortably say this is an impossible to hack solution...

Finally, this service ensures that the documents can be shared securely, or even publicly. And naturally, good capability of search and categorization are major requirements for you to leave the “dossiers” behind and move onto this solution.

How about Integration?

The whole solution (Validation, Preservation and Custody) is deployed in micro-services, ensuring scalability of each service independently. All of them follow strict paradigms of implementation (DDD – Domain Driven Design) and offer an REST API to easy integration. You can even test it in an interactive UI (swagger) before implementing.



Move with DigitalSign on the dematerialization process in a simple and secure way.

We made it simple for you to integrate your actuals solutions with our services with very little code.