TIP Trusted Information Partners

Basic function *Validating Signatures*

Introduction

This document describes the basic functionality Validating Signatures the *TIP-ecosystem;* validating a qualified signature, seal or timestamp.

Words printed in italic refer to definitions described in the document basic functions and definitions for the *TIP-ecosystem*.

Note: This document is published for consultation purposes and can be updated to a 1.0 version after implementation by TIP Partners. Comments on this document are appreciated via a message on our LinkedIn account.

The functionality is described in below in the following categories.

Description

The basic function *validating signatures* allows you to get assurance about the validity of an electronic signature, seal or timestamp.

In this context, validate means to confirm legal validity. Note that this term can be confused with checking or verifying a digital signature but they have different meanings.

Article 32 eIDAS lists the requirements for validating an electronic signature. These are:

- the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
- the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- the signature validation data corresponds to the data provided to the relying party;
- the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- the electronic signature was created by a qualified electronic signature creation device;
- the integrity of the signed data has not been compromised;
- the requirements provided for in Article 26 were met at the time of signing.

The basic function validate sign must therefore be able to check the above requirements and give an opinion/judgement on them. Important here is that the requirements are interpreted in the same way by all parties involved and that the same standards are used. The parties involved need an agreement of which signature policy is used.

ETSI has published a standard on how to verify a signature and it is described in ETSI TS 119 102-1 V1.2.1 (2018-08).

Should a service provider demonstrate that it performs validation signing in accordance with the requirements, the way is open to have this validation service qualified as described in Article 33 eIDAS.

Application

The practical application of the basic function validating signatures is basically a need of the receiving party of the signed statement. The receiving party wants to know if the signature is legally valid. This provides assurance that in the event of a dispute you can prove to a judge that the signature met the requirements mentioned in art 32 eIDAS.

From the perspective of the recipient of a signed document, the validation function is outlined below[1]:

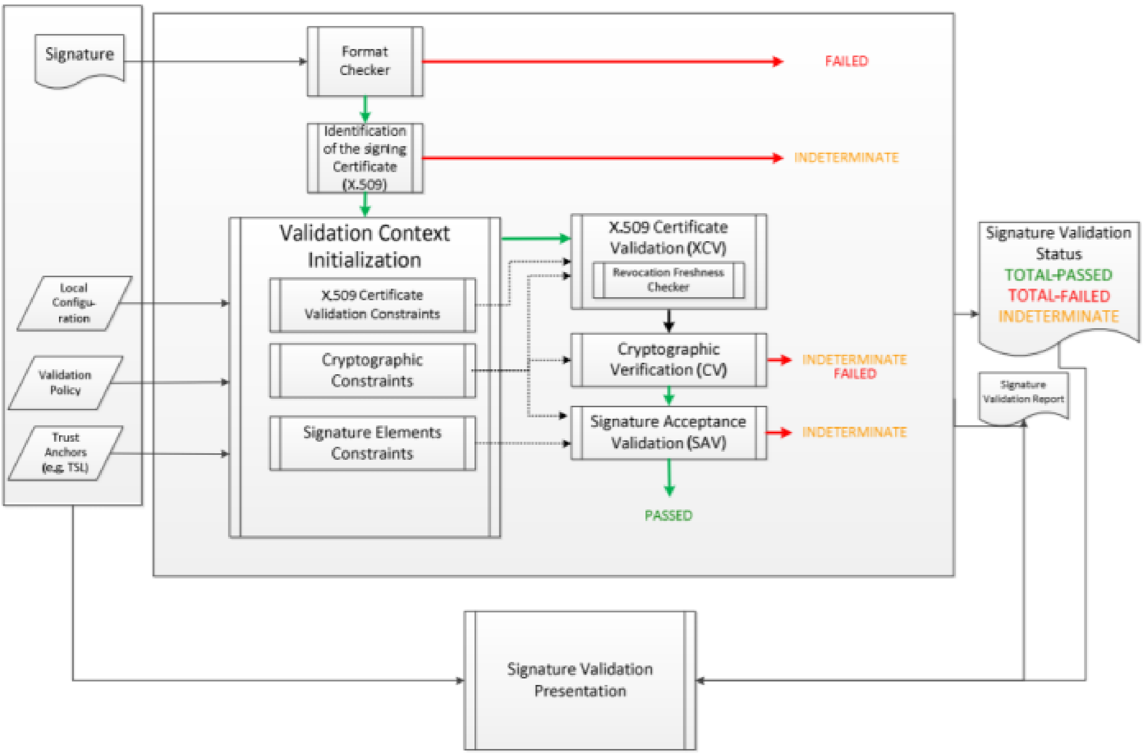
Signature
Format Checker
FAILED
Identification of the signing Certificate (X.509)
INDETERMINATE
Validation Context Initialization
X.509 Certificate Validation Constraints
Cryptographic Constraints
Signature Elements Constraints
X.509 Certificate Validation (XCV)
Revocation Freshness Checker
Cryptographic Verification (CV)
INDETERMINATE
FAILED
Signature Acceptance Validation (SAV)
INDETERMINATE
PASSED
Local Configu-ration
Validation Policy
Trust Anchors (e.g. TSL)
Signature Validation Status
TOTAL-PASSED
TOTAL-FAILED
INDETERMINATE
Signature Validation Report
Signature Validation Presentation

Ilustración 1 Basic Signature Validation ETSI TS 119 172-1

Validation in practice

Currently, there are already APIs and software available that perform certain validity checks. Acrobat reader has a a verification function integrated. The European commission[2] and Evotrust offers also a service. If the TIP ecosystem want to develop and standardise signing policies a specific validation service has to be developed.

The validator in the TIP ecosystem must check the signature on validity of: identity, authority, used signature policies and the chain specifications.

Signature policies

Signatures, seals and timestamps can be used for a variety of purposes.

- Signatures allow natural persons, officers of legal entities and holders of trust roles to make a declaration of their position with respect to the contents of the signed data.

[1] QValidation-Service-Policy-v.2.7.pdf (anf.es)

[2] https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation)

- Seals are created in the name of an actor and serve to create assurance about the origin and integrity of data.
- Time stamps are used to guarantee the existence of information at a certain time in the past. They can be used independently or in conjunction with signatures and seals.

Signatures, seals and timestamps can be applied in combination with signature policies. A signature policy gives meaning to a signature and ensures its acceptance by defining rules that describe the technical and procedural requirements for creating, augmenting and validating electronic signatures. See Table 1 for a summary of the assurances that can be created through the application of signatures, seals, timestamps and signature policies. Creating assurance around the signing authority of the signer is beyond the scope of the basic Signing function.

Table 1: application of signatures, seals, time stamps and signature policies

	Integrity	Origin**	Act of will	Time	Context
Signature	X	X	X	(X)*	
Seal	X	X		(X)*	
Timestamp	X			X	
Signature policy					X

*If combined with time stamp(s)

**Origin of natural persons and or entities

Agreements

Agreements are the concrete elaboration of basic principles into directly applicable "rules" that apply to all actors acting within the TIP ecosystem. Agreements provide direction on how information chains should be accessed through the TIP ecosystem and how basic functions and value-added services can be developed.

For the basic function *Signing*, TIP aligns with the European eIDAS Regulation (EU No. 910/2014) and its associated infrastructure and standards. In line with the basic principle Highest Reliability Level, the level Qualified is used within the TIP ecosystem. This means that, as part of the basic Signing function, the eIDAS trust services described in Table 2 are applied.

Standards

Standards describe at the operational level how agreements can be implemented. Where possible, TIP aligns with existing best practice standards.

Table 2 links the various forms of signing to the agreements and standards that apply to them. ETSI has published a technical guideline (ETSI TR 119 100) that provides direction on the use of the underlying technical standards (e.g. CAdES, PAdES and XAdES).

Table 2: agreements and standards for signing

Application	Agreement	Standard
Signature	Meets the requirements for qualified electronic signatures / seals / timestamps as defined in eIDAS (EU Regulation No. 910/2014)	qualified electronic signature (*eIDAS, art 3, sub 12*)
Seal		qualified electronic seal (*eIDAS, art 3, sub 27*)
Timestamp		qualified electronic timestamp (*eIDAS, art 3, sub 34*)

Best practices

In addition to following the standards described above, it is recommended to follow the best practices listed below. However, this is not a requirement.

- Signatures, seals and timestamps are implemented based on the guidelines described in ETSI TR 119 100.
- Signatures, seals and timestamps are provided with a signature policy in accordance with ETSI TS 119 172.
- For the signing of PDF documents, the PAdES standard (ETSI EN 319 142) is used.
- For the signing of XML files, the XAdES standard (ETSI EN 319 132) shall be used.
- For signing data other than XML and PDF, the CAdES standard (ETSI EN 319 122) is used.
- To maximize reuse of data the baseline profiles for PAdES, XAdES and CAdES are applied where possible; B-B, B-T, B-LT, B-LTA.

Supplier(s)

As stipulated in eIDAS, Qualified Trust Services are provided by Qualified Trust Service Providers (i.e. Qualified Trust Service Providers - QTSPs). See the EU Trusted List Browser for an overview of QTSPs.

Administrator(s)

The basic functionality *Signing data* does not require central management from TIP. The functionality is accessed on the basis of bilateral agreements between suppliers (i.e. QTSPs) and actors.

If a policy about validating a signature is needed / created then management should also be performed on it. This policy would then apply to the TIP ecosystem. And that policy should then also be managed.

Supervisory Assessment Body

As stipulated in eIDAS Article 17, each EU member state is responsible for appointing a supervisory body to ensure that qualified trust service providers meet the requirements set forth in the eIDAS Regulation. The Rijksinspectie Digitale infrastructuur RDI (new name Agentschap Telecom) is the Dutch supervisory body.

Around validation, the RDI will possibly play a role in obtaining the qualification. It is not clear here whether adherence to the TIP established validation policy is also in scope or whether this is a responsibility of the system itself.

Costs

Prices for the use of the basic Signing functionality come about on the basis of bilateral agreements between suppliers and actors using this functionality.

A customer can choose to use a (qualified) verification service. This service provider can then charge for performing this operation. In that case, a qualified verification service should also become a recognized role in the TIP ecosystem.