Basic function
Signing data

Introduction

This document elaborates on the basic function *Signing data*. Implementing this function is the focus of one of the first implementation phases of the *TIP-ecosystem*.

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

Signing data is an important basic function in the *TIP-ecosystem* as it provides trust to transactions and specific kinds of communication. It ensures that *Actors* can prove the origin, receipt, delivery, integrity, sender, approval and creation of electronic documents.

The basic function *Signing data* makes use of the Public Key Infrastructure[1]. The basis for *Signing data* has become widely accepted with the introduction of the eIDAS regulation (910/2014) and will become generally available by the launch of European Digital Identity Wallets[2]. In the *TIP-ecosystem*, it is the way to authenticate data (e.g. confirming authorisation or consent).

To provide a sufficient level of trust in the *TIP-ecosystem*, Electronically signing digital contracts and electronically sealing the contents of digital documents, messages and adding time stamps is carried out with qualified certificates.

The basic functions *Exchanging data* and *Preserving signatures* make use of *Signing data.* The basic function *Signing data* is useless without the basic function *Validating signatures.*

Applicable elements

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.

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 conjunction 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

	Certainty about				
	Integrity	*Origin*	*Expression of will*	*Time*	*Contents*
Signature	*X*	*X*	*X*	*(X)**	
Seal	*X*	*X*		*(X)**	
Timestamp	*X*			*X*	
Signature policy					*X*

*If combined with time stamp(s)

Below is a non-exhaustive overview of applicable elements for *Signing data.*

- Signing of human-readable documents or data for different purposes.

ETSI TS 119 172 -1 - V1.1.1 supplies 6 standard commitment types as a starting point:

- Proof of Origin
- Proof of Receipt

- Proof of Delivery
- Proof of Sender
- Proof of Approval
- Proof of Creation
- Note: new commitment types can be created, within signature policies as long as these are centrally defined, maintained and publicly available.

- The standard use of Signature policies is advised above commitment types. A signature policy goes beyond the ETSI commitment type and supplies an extensive definition on actors, actions, rules, obligations and rights that are applicable when adding a signature or seal.

Agreements

For the basic function *Signing data*, the *TIP-ecosystem* 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 function *Signing data*, the eIDAS trust services described in Table 2 are applied.

Table 2: agreements and standards for signing

Application	Appointment	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*)
Time stamp		qualified electronic timestamp (*eIDAS, art 3, sub 34*)

- The ETSI guideline of What You See Is What You Sign (wysiwys) is applicable for all human initiated signatures.
- In order to optimise the processing step of qualified human signed data or documents, without compromising the integrity of the data itself, we follow the standard of combining human readable and machine-readable data in one dataset.
- Non-repudiation is enforced by the certificate used.
- Signatures can be created/generated by natural persons.
- Seals can be created/generated by Actors being both humans on behalf of a legal entity and machines.
- Validation of signatures or seals within the *TIP-ecosystem* should be possible in at least two ways:
    - Human interaction, by using an app or website
    - Machine 2 machine, by exposing endpoints to actors which can be used in the ecosystem
    - Note: an extensive description is given in the basis function *Validating signatures*
- Stored, signed or sealed data should -in certain cases- be re-signed or re-sealed on a specific interval to ensure the validity and integrity over time of the data and cryptographic strength of the signature or seal itself. This is described extensively in the basic function *Preserving signatures*.

Standards

The next table contains an overview of applicable standards for the basic function *Signing data*.

Topic	Standard
ETSI standards	ETSI TS 119 192 V1.2.1 (2023-02) ETSI TS 119 172-1 V1.1.1 (2015-07) ETSI TS 119 172-2 V1.1.1 (2019-12) ETSI TS 119 172-3 V1.1.1 (2019-12) ETSI TS 119 172-4 V1.1.1 (2021-05)

Best practices

In addition to following the standards described above, it is recommended to follow the best practices listed below.

- 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) is used.
- For the signing of JSON files, the JAdES standard (ETSI TS 119 182-1 V1.1.1 (2021-03)) is used.
- For signing data other than XML, JSON and PDF, the CAdES standard (ETSI EN 319 122) is used.
- To maximize reuse of data the baseline profiles for PAdES, XAdES, JAdES 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 (QTSPs). See the EU Trusted List Browser for an overview of QTSPs.

Administrator(s)

The basic function *Signing Data* does not require central management from TIP. The functionality is provided by *Acting spaces* and *Value-added service* providers (e.g. wallets and cloud signing services).

Regulator(s)

As stipulated in eIDAS Article 17, each EU Member State is responsible for appointing a supervisory body to ensure that qualified Trust Service Providers (TSP) meet the requirements set out in the eIDAS Regulation. Authority Telecom (AT) is the Dutch supervisory body as far as QTSPs are concerned.

Costs

If *Signing data* is not carried out (for free) from European Digital Identity Wallets, prices for the use of the basic function *Signing data* are established on the basis of bilateral agreements between *Value-added service* providers and *Actors* who use this functionality via *Acting spaces*. Payment is made through the basic function *Making payments*.