Basic Function
Signature preservation

Introduction

This document describes the basic functionality *Signature preservation* 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

This document describes the basic function of *Preserving signatures* in the *TIP-ecosystem*, how existing international/EU standards are applied and what further details and specifications are set within the *TIP-ecosystem*.

Actors in the *TIP-ecosystem* need to store documents that include qualified electronic signatures (and/or qualified electronic seals) and want to retain their legal effect beyond the technical lifespan or beyond ad hoc events impacting the trust chain.

The long term storage of these documents and their signatures/seals themselves is described in the basic function for *Archiving data* and is out of scope for this document. However, relevant dependencies with *Archiving data* are listed in this document.

When storing documents that include qualified electronic signatures/seals it is important to monitor two types of events, planned and unplanned, in order to guarantee and preserve the legal effect of those documents.

- Planned events include the extension of signature beyond the current technical lifespan. This may be a fixed duration, a variable duration such as the lifespan of the associated contract/person or even perpetual storage. Encryption algorithms have an estimated technical lifespan before advances in computer science make them unsafe. At a planned moment in time, before the technical lifespan expires, a workflow invokes the service for *Preserving signatures* to extend the lifespan of the signature/seal.
- Unplanned events: These unplanned events include a breach of trust at the CA of the certificates used in the signature/seal or of a previous preservation. Another type of unplanned event is a notification of an encryption algorithm being re-evaluated as no longer safe or having a reduced lifespan.

For the events described above the basic function *Signature preservation* provides a solution to extend the lifespan of documents including a signature/seal.

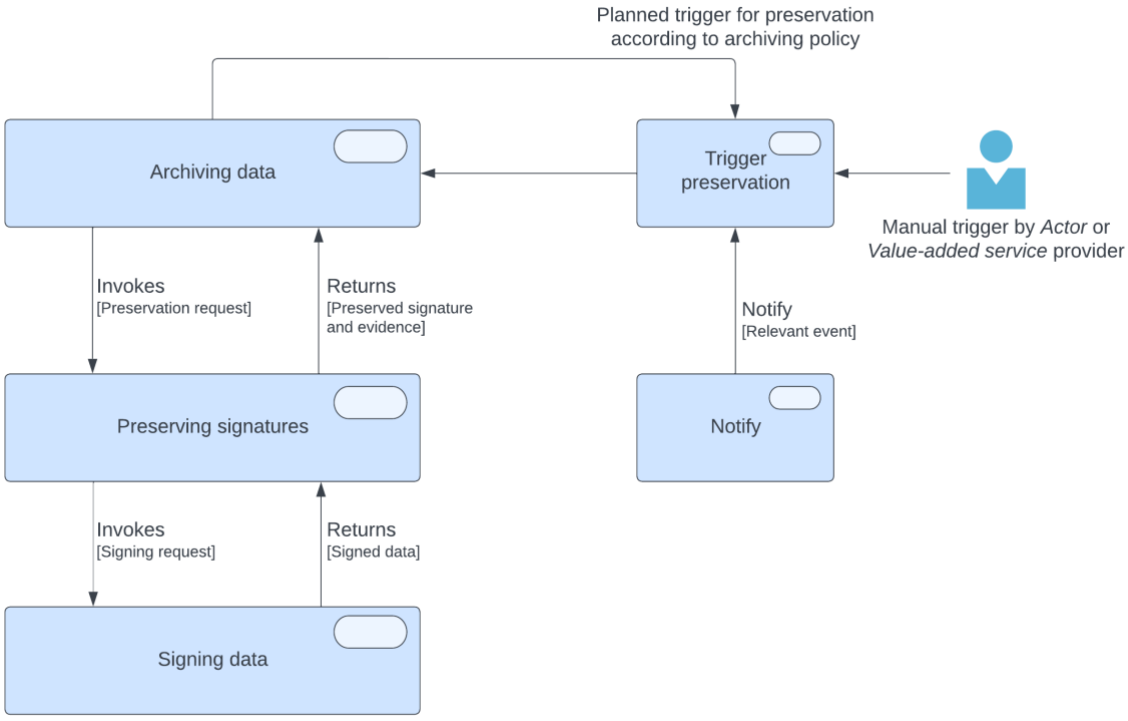
Application

Trusted Information Partners apply *Preserving signatures* to enable *Validating signatures* and *Archiving data* in the long term of various types of information, including:

- Documents, with or without signatures or seals.
- Signatures and seals created using *Signing data*, including data produced during:
    - *Exchanging data*, e.g. evidence produced by the involved *Actor*s or trust service providers;
    - *Attestation of attributes*, e.g. attestations, requests for presentation, or presentations;
    - *Authorizing an actor*, e.g. mandates or other statements about authorisation;

- *Publishing service or chain specifications*, e.g. specification documents.

The basic function *Preserving signatures* ensures future integrity of information. It does so by creating verifiable proof of existence of that information using sufficiently future-proof cryptographic techniques. To enable continued preservation, the basic function also monitors these cryptographic techniques in order to trigger new proof creation in the future. Users of basic function Preserving signatures, such as an implementation of *Archiving data*, are responsible for applying the functionality and monitoring information in such a way that there are no gaps which could compromise the integrity of the information.



The goals of preservation can be broken down into three:

- Extending the validity status of digital signatures
- Providing proof of existence of data
- Augmenting externally provided evidence of preservation

Applying *Preserving signatures* is required only for some processes. Where the functionality is not required, application should be decided on a case-by-case basis. Reasons for not applying the functionality include the purpose of the information (e.g. it could be a contract with only very short-term effect), cost (e.g. the risk of signature compromise might be negligible), and privacy (e.g. users may choose to keep some documents out of scope).

In the *TIP ecosystem*, *Preserving signatures* is scoped and related to other basic functions. This does not exclude the possibility that Trusted Information Partners also apply the services for other purposes or with wider scope, but TIP policies and agreements will only apply to the defined scope. The scoping is as follows:

Basic function	Manages lifecycle	Persists data	Receives	Returns	Depends on
Archiving data	Data lifecycle: how long should it be conserved, how quickly should be obtainable	Documents, signatures, seals, validation information, event logs	Trigger preservation from Acting space	Preservation status to Acting space	Preserving signatures
Preserving signatures	Cryptography lifecycle	Preservation policies, event logs	Preservation Request from Archiving data	Preserved signature & Evidence to Archiving data	Signing data, Validating signatures
Signing data	Clock cycle	Certificate revocation status, signature creation data, event logs	Signing Request from Preserving signatures	Signed data to Preserving signatures	None

Note that this means that within the *TIP-ecosystem*, an implementation of *Preserving signatures* does not archive data itself, but is used by the basic function *Archiving data.*

Implementation of *Preservation signatures* within the *TIP-ecosystem* can be done via one of several implementation options. These options may constitute a growth path, choosing an option in the short term to be replaced by a more mature integrated option in the future.

Implementation option	Trust service provider
1	Each *Actor* creates their own policies and practices, potentially contracting a *Value added provider* for Signature preservation.
2	Each *Actor* creates their own policies and practices, utilizing a *Value-added provider* for qualified Signature preservation.

3	The *Actor*'s acting space integrates with a *Value-added provider* for Signature preservation[1] using standardized policies and practices.

For implementation option 2 and 3, the implementation must be a service, which interacts with consumers over two protocols:

- Preservation protocol: *Actors* and/or *Value added service* providers for Archiving data present preservation objects (including original data and evidence) and the *Value added service* provider for Signature preservation returns evidence that one or more of the preservation goals were met.
- Notification protocol: *Actors* and/or *Value added service* providers for Archiving data subscribe to updates produced by a *Value added service* provider about security risks related to earlier preserved material (i.e. phasing out cryptographic techniques), and use these as triggers to request new evidence over the preservation protocol for any relevant affected data.

Preservation evidence includes:

- Digital signatures (from *Signing data*)
- Time-stamps (from *Signing data*)
- Evidence records
- Validation data (e.g. CRLs, OCSP responses) (from *Signing data*)
- Validation reports (from *Validating signatures*)

Agreements

- In TIP one generic overarching preservation policy will be used for preserving signatures
- Preservations of signatures must always be qualified within TIP

Preservation policies include the following aspects to be further detailed at local level:

- Legal aspects including liability
- Policy and security requirements
- Minimum service levels, and possibly other procedural agreements
- Technical interface requirements

[1] cf. eIDAS (nieuwe nummerverwijzing van de nieuwe wet hier invoegen)

Standards

- Adopt TS 119 511 and TS 119 512

Best practices

The provider for the Basic function for *Archiving data* must be fully aware that their service is in the lead of the data lifecycle and must invoke the *Preserving signatures* service based on planned and unplanned events.

It is very important to note that workflows for *Preserving signatures* are in place when *Archiving data*, even when the initial goal is not to store documents with signatures/seals beyond their expected technical lifespan. An example would be a 2 year storage objective using algorithms with over 15 years of lifespan. In case of unplanned events *Preserving signatures* is to be invoked to ensure the guaranteed 2 year storage objective.

- Daily CRL check for CA-certificates used in signatures/seals (Certificate: is the certificate with which the preservation object has been signed still valid (not expired or revoked))
- Daily notification service check (as provided by *Value added service* provider for *Preserving signatures*, regarding encryption algorithms and other security issues)

Supplier(s)

The basic function Preserving signatures in TIP shall be in accordance with eIDAS deemed as a Qualified Trust Service. The *Value-added service* provider must be, as stipulated in eIDAS, by a 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 function Preserving signatures does not require central management from TIP. The functionality is accessed on the basis of bilateral agreements between *Value-added service* providers (i.e. QTSPs) and *Actors*.

In case a default generic preservation policy is to be provided for the TIP ecosystem this will require creation, maintenance, approval and publication by the TIP governance.

For a domain specific preservation policy, the governance in that domain is responsible for the creation, maintenance, approval and publication.

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 meet the requirements set forth in the eIDAS Regulation. The Rijksinspectie Digitale infrastructuur4 (RDI) is the Dutch supervisory body.

Costs

Value-added service providers for the basic function Preserving signatures will seek to monetize their services, either by subscription, pay-per-use, or other payment scheme. Any payment scheme can be used as long as there is transparency on costs and service levels before an *Actor* consumes the services.

Optionally the governance structure in a domain may choose to implement a financing agreement that covers the use of the basic function for Preserving signatures for the *Actors* in that domain, or if this basic function is invoked according to the *Chain specification(s)* in that domain.