Archiving data

Introduction

This document describes the basic function *Archiving data* 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 mail to info@trustedinformationpartners.nl .

The functionality is described in below in the following categories.

Description

eArchiving, or electronic archiving, refers to the systematic process of storing and managing digital records for long-term preservation and retrieval. This modern approach replaces traditional paper archiving, allowing organizations to efficiently manage their documentation in a digital format.

eArchiving is much more than a backup or converting everything to PDF/A.

eArchiving provides preservation making sure that digital documents and data remain intact and retrievable over time. (a document is not the same as a file: it is a combination of metadata, context, signatures etc.)

eArchiving also provides means to proof integrity and validity. Important aspects are preventing bitrot, providing proof of existence by using hashing, (qualified) timestamps and proof of validity since signature validation can expire.

Benefits for eArchiving?

For	Reasons
Business	• Critical records • Data loss prevention • Contracts • Statistical purposes
Legal compliance	• Retention periods • Limitation of liability • GDPR
Public administrations	• Openness of government • Archive law • Cultural-historical value
Private person	• Equal information position • Self-reliance

Electronic archiving under eIDAS 2.0 versus eArchiving

In eIDAS2 "electronic archiving means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period."[1]

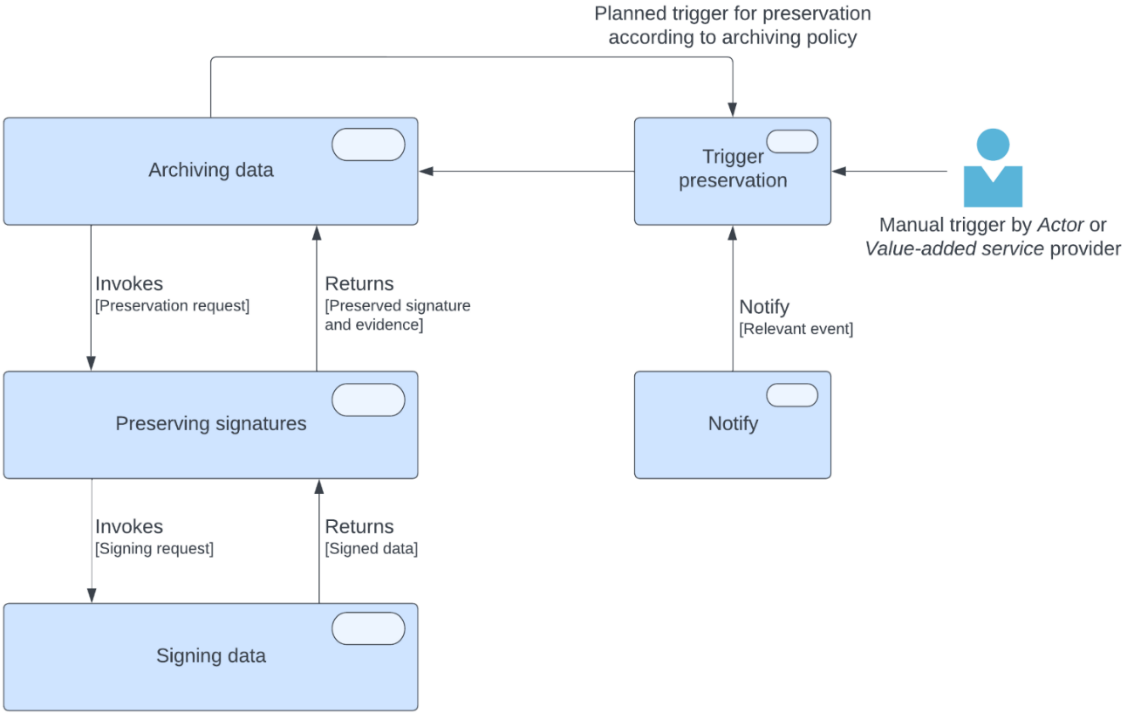
[1] https://ec.europa.eu/newsroom/repository/document/2024-22/eIDAS_Trust_Electronic_Archiving_Services_supported_by_the_eArchiving_Initiative_to4u8jdCPacvkjEhLY4ncfFRA_105792.pdf)

“they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.”

In eIDAS 1.0 there was no trust service for electronic archiving. There already was for several years a separate initiative called eArchiving (also spelled E-ARK) which is intended for a much wider scope of digital archiving for many functions in the digital society.

Electronic archiving as meant under eIDAS 2.0 has very similar objectives, but is not identical, to the eArchiving initiative.

The figure below gives an overview of how different TIP basic functions interact with each other. As shown, archiving data is not only used for archiving electronic documents but also for signature preservation. The basic function *Archiving data* serves as the orchestrator for invoking the basic function *Preservation of signatures*, which is a passive service invoked by others.


Planned trigger for preservation according to archiving policy
Archiving data
Trigger preservation
Manual trigger by Actor or Value-added service provider
Invokes [Preservation request]
Returns [Preserved signature and evidence]
Notify [Relevant event]
Preserving signatures
Notify
Invokes [Signing request]
Returns [Signed data]
Signing data

Application / Applicability

Key objectives of TIP basic function *Archiving data*

In the TIP ecosystem, the basic function *Archiving data* has the following key functions:

1. Secure storage and preservation of electronic data and electronic documents belonging to (or under stewardship of) the Actor.
2. Secure storage and preservation of electronic data and electronic documents from third parties received by the Actor.
3. Secure storage and preservation of relevant audit trails from all acts performed by that Actor in their acting space. (N.B. the audit trails themselves can be considered electronic data and electronic documents as well)

What data is to be archived?

The TIP basic function *Archiving data* does not prescribe what data must be archived. This is determined by the business process and/or whatever data the Actor wants to archive for whatever reason. Domain governance can help to set a standard on what data is to be archived for specific use cases, and what the respective retention duration is.

Archiving profiles are used to set the data formats of the archived data and which conversions can be done on the data.

Two key patterns: who contracts the eArchive?

Research in this topic has shown two schools of thought regarding eArchiving. Actors acts as a Subscriber: the Actor (citizens and entrepreneurs) contract an eArchiving solution of their choice, or an Actor solely acts as a Relying party: the Actor has access to their data scattered across multiple eArchiving solutions contracted by others (such as employers). Both patterns seem to be discussed between the European Commission and the eArchiving service providers.

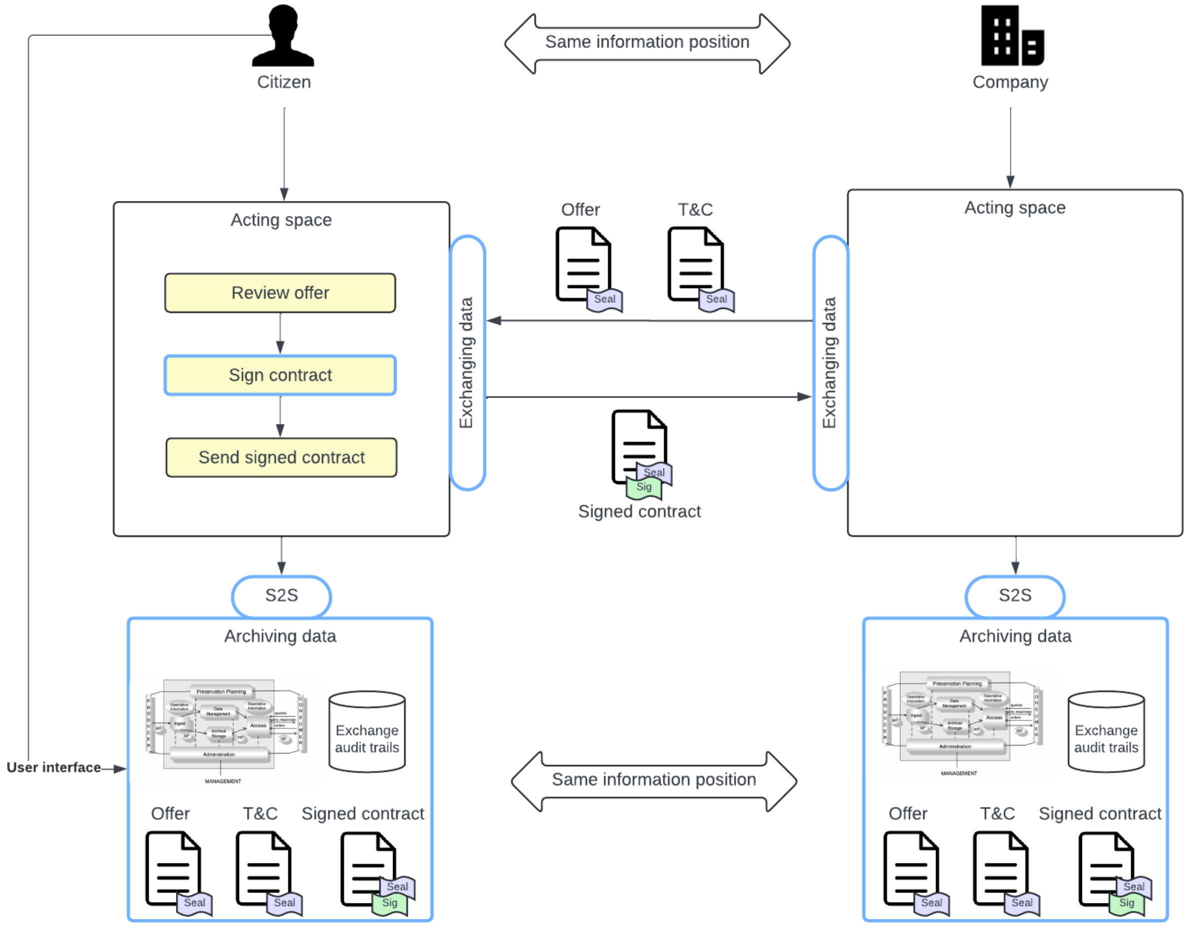
A. ***The Actor contracts the eArchive service provider of their choosing.***
   All Actors should be able to have access to their own eArchiving solution and therefore determine themselves what data to archive and their retention duration. For instance as integrated functionality in the Acting Space (e.g. Wallet) under sole control of the Actor. This pattern is simpler as it does not require a governance framework. This pattern is described in this document.
   Benefit of this pattern is that it requires no additional governance. There is no dependency on others than Actor and their eArchiving QTSP. Drawback is that this model can lead to more duplication of data.
B. ***The Actor has access to their data stored in the eArchive(s) contracted by others.***
   In this pattern Actors have access to documents relevant to them that are stored in an eArchive of another Actor; the Actors are Relying Parties. Example: access to your contract in the eArchive contracted by the energy provider. In this model the Acting Space (e.g. Wallet) provides access to your data stored over multiple eArchiving solutions. This pattern requires a method for knowing where relevant data is stored, and external access to that data. A

governance framework is required. A consequence is that a Register should be made and maintained in which eArchiving providers can store for which Identity documents are archived.

C. A hybrid model in which both patterns co-exist.

Schematic overview of the TIP basic function *Archiving data*

The illustration is based around a use case in which a citizen receives an offer for a new energy contract, reviews it, signs it and returns the signed contract to the energy company. Both Actors choose to (temporarily) store documents, including their seals and signatures, and audit trails of the exchange. In this example the 'offer' probably has a short retention period since the 'signed contract' supersedes it.



This picture illustrates Pattern A in which both Actors choose an eArchiving solution provider. For Pattern B we do not know yet what the (de)central solutions for discovery and access to another eArchive look like.

The TIP basic functions are outlined in blue. These include *Signing data* and *Exchanging data* in addition to *Archiving data*. *Archiving data* is drawn outside the Acting space, but Acting space providers may choose to make it an integral offering within their Acting space.

Agreements

TIP agrees on the following requirements regarding implementation of Archiving data.

General requirements

The service archiving data MUST include services to extract or migrate the electronic archiving data.

Sharing of archived data MUST be done in one of the two ways:

- Sending the archived data by using the basic function *Exchanging data*
- Granting access to the archived data by using the basic function *Authorizing actor* and/or *Attestation of Attributes*

Users MUST be able to use the basic function *Validating Signatures* to validate the archiving.

Retention period MUST be set in advance for every document in the eArchive. Actors cannot change the Retention Period after initial storage.

Provider requirements

Providers MUST apply Publishing service or chain specifications at Level 1 (Embedded trust services) for potential integration into an Acting space.

Providers MUST verify the identity of the subscriber with a high level of assurance.

Providers MUST verify the identity of the relying party (who accesses data) with a high level of assurance.

Providers MUST use the basic function *Preserving signatures* to retain the legal effect of the archived data beyond the technical lifespan or beyond ad hoc events impacting the trust chain.

Providers MUST have described an exit procedure in their Terms and Conditions.

Providers MUST have functionality to notify, within a reasonable timeframe – ie. 3 months, all Relying Parties that data will be deleted after the Retention Period.

Interoperability

Acting Spaces MUST have functionality to transport Archived data from one eArchiving Provider to another. Relationships between electronic data and electronic documents and their audit trails must be retained.

Standards

The specification of electronic archiving under eIDAS 2.0 (article 45j) will be available May 2025. For now, the relevant standards of archiving will be mentioned. When the implementation acts for electronic archiving are released, standards can be removed from this list where needed.

> Article 45j, Requirements for qualified electronic archiving services
>
> *2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*[2]

These standards are applicable:

ISO 14641 for Electronic archiving. It focuses on:

- Electronic archiving and document management
- Preservation of electronic documents
- Design and operation of information systems for document preservation

NEN-ISO 15489-1

ISO/DIS 14721 (derived from ISO 14721:2012 (OAIS model))

In the context of preservation of general data by means of digital signatures, the following standards are applicable:

ETSI 119.511 : is a technical specification that outlines policy and security requirements for trust service providers offering long-term preservation services for digital signatures or general data using digital signature technique

ETSI 119.512 is titled "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services". This specification focuses on the protocols used by trust service providers for long-term preservation services.

Pending the implementation acts by the EU, part of the E-ARK specifications can be applicable but in the context of this document, these specifications are excessive.

[2] https://www.european-digital-identity-regulation.com/Article_45_(Regulation_EU_2024_1183).html

E-ARK specifications are a set of standards and guidelines for digital archiving and preservation. The E-ARK specifications are designed to promote wider community adoption and interoperability in digital archiving.

Best practices

Based upon the OAIS-model and other standards as mentioned in *Standards* as well as by E-ARK and the *Digital Preservation Coalition* (DPC) the following best practices are promoted:

- **Use of Open Standards**: Employ open, non-proprietary formats for digital records wherever possible. This ensures greater interoperability and facilitates long-term accessibility across different systems and platforms.
- **Comprehensive Metadata**: Capture detailed metadata for all digital records, including descriptive, administrative, and technical metadata. This helps in managing, retrieving, and understanding records in the long term.
- **Consistent Information Packages**: Implement the concept of Archival Information Packages (AIPs), which contain both digital content and the corresponding metadata. This standardizes the submission, storage, and retrieval processes.
- **Regular Data Integrity Checks**: Conduct regular checks to verify the integrity of digital records and detect any corruption or data loss over time. This typically involves using checksums or other digital signatures.
- **Emulation and Migration Strategies**: Develop strategies for emulating old software environments and migrating obsolete file formats to contemporary standards to maintain access as technology evolves.
- **Collaboration and Knowledge Sharing**: Engage with other organizations, communities, and standards bodies to share knowledge, tools, and resources. This collaboration can lead to more effective solutions for common challenges, like interoperability.
- **Risk Management**: Perform regular risk assessments to identify and mitigate potential threats to digital preservation, such as technological obsolescence or insufficient resource allocation.
- **Policy and Governance**: Establish clear policies and governance frameworks to manage records throughout their lifecycle, assigning roles and responsibilities to ensure accountability within the archiving process.

The Digital Preservation Handbook of the Digital Preservation Coalition gives an overview of best practices: https://www.dpconline.org/handbook/institutional-strategies/standards-and-best-practice

Supplier(s)

When the implementing acts are accepted, suppliers need to be on the EU trusted list for QeArch.

Administrator(s)

National level

Until adoption of the implementing act (due data 21st of May 2025), ETSI standards and other specifications where necessary there is no possibility yet to certify a service at the European level. Up to that moment, such services are listed as "non-regulatory, nationally defined trust service" with certification schemes at the national level.

Qualified trust service

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. The Rijksinspectie Digitale Infrastructuur (RDI) is the Dutch supervisory body as far as QTSPs are concerned.

Regulations

The following regulations are applicable to the basic function *Archiving Data*

eIDAS (910/2014) describes a qualified electronic archiving service (QEAS) and the requirements. For the amendments concerning eIDAS 2.0 and changes in the QEAS, see: Article 45 - eIDAS 2 text (european-digital-identity-regulation.com). The use of digital archiving services is voluntary. EIDAS provides the requirements of those services.

GDPR; art 5 (processing personal data), art 15 (right of access), art 17 (Right to erasure), art 25 (data protection by design and default), art 89 (safeguards and derogations for archiving).

Archiefwet 1995 (being modernised due to technical innovations and new version expected in 2026 Scope of this law is access and archive management of government archives for public organisations. Seems to be no relation with digital archiving in the context of TIP.

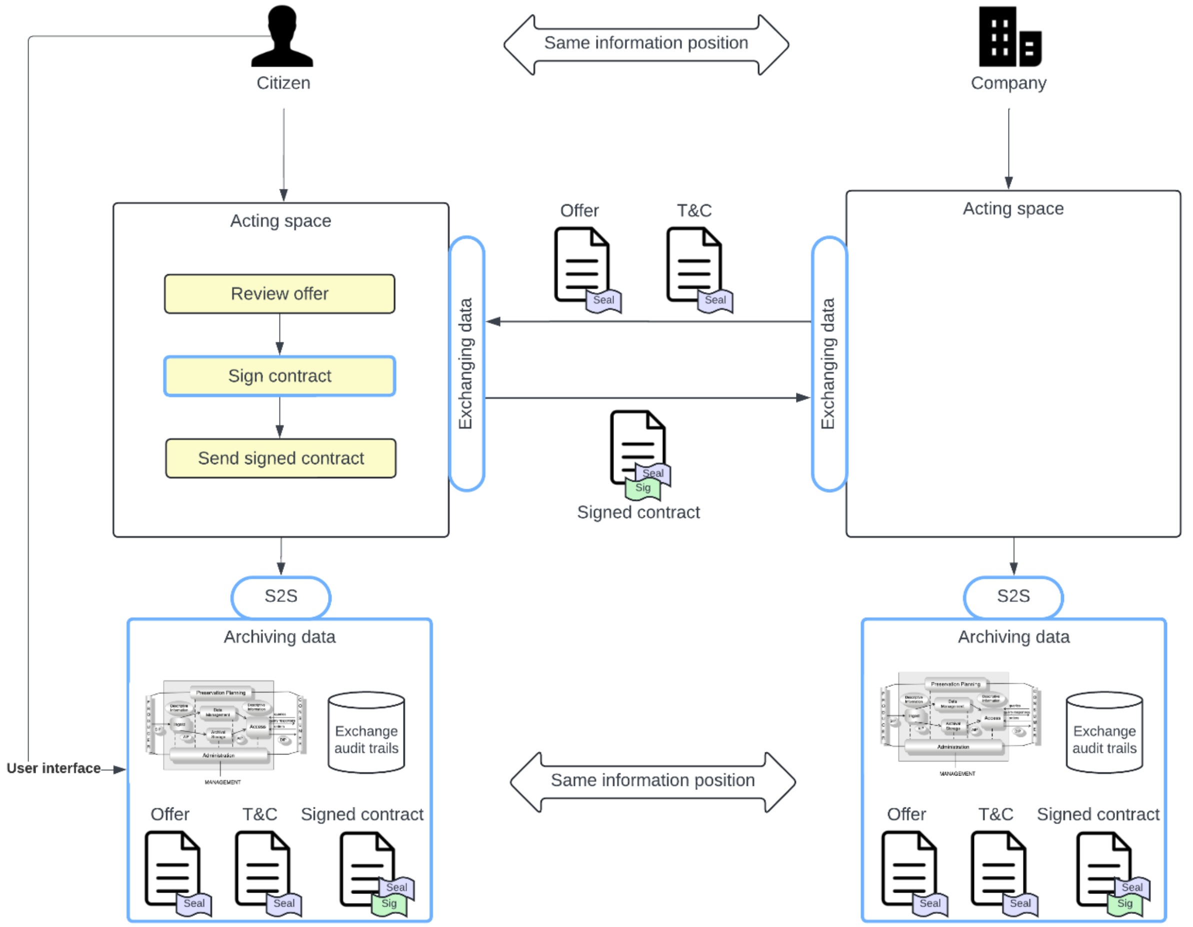
The **Belgian Digital Act** of July 21, 2016 implements the eIDAS Regulation and adds qualified electronic archiving as an additional trust service. Belgium has developed a certification scheme for qualified electronic archiving, which was finalized in April 2022.

The **Data Act** (2023/2854) sets regulation on harmonised rules on fair access to and use of data. Rules are set within the regulation that customers should be able to freely switch from service providers without any obstacles. Export in commonly used and machine readable format.

Costs

The basic function *Archiving data* is 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*.

The costs for the basic function *Archiving data* can be subscription based or pre-paid for a certain period. In accordance with the Data Act, Costs for transferring data to another Qualified Trust Service Provider within TIP should be included in the standard price.



List of observations to be evaluated in next version

Nr	Title	Remarks
01	Bankruptcy	How do we organize the assurance that, in the event of a bankruptcy of an archiving service provider, all stakeholders can safely, reliably and within a reasonable time migrate their data to another provider? Something for a working group Governance? (eHerkenning solution as an example) FR: "Termination of service clause" is een verplicht onderdeel van de Practice statment
02	Portability of data	In an open market it is desirable that customers can switch providers. Do the European standards take into account data portability? Op hoofdlijnen beschreven, E-ARK specs meest relevant voor het formaat.
03	Data lifecycle	How do the eIDAS regulation and the ETSI standards view the data lifecycle? There is talk about long-term storage. But a lot of data may also be relevant for a shorter period. For example, after 3 new annual energy contracts, can older contracts be removed? Short lifecycle: uittreksel belastingdienst bijv 3 maanden. Voorbeeldstadsarchief: "afschriften" bijv scans van documenten, die kennen korte geldigheid (bijv 3 maanden).
04	MDTO relevant?	MDTO (Metadata for Sustainable Accessible Government Information) is a standard for defining and exchanging clear metadata to enable the sustainable accessibility of government information.https://www.nationaalarchief.nl/archiveren/mdto MDTO seems to only apply to Dutch government in their archiving obligations. We leave this out of scope since the role of providing a public archive as a government organization extends way beyond the scope and objectives of eArchiving in eIDAS 2.0. MDTO produces a "sidecar file" containing metadata in XML structure. The eArchive draft standard specifies that there is a metadata file which can also reference other metadata files, such as an MDTO.
05	OAIS relevant?	The Reference Model for an Open Archival Information System (OAIS) was developed for use in facilitating a broad, discipline independent, consensus on the requirements for an archive or repository to provide long-term, preservation of digital

		information. It was also intended to support the development of additional digital preservation standards. http://www.oais.info/ Comment: *is now included in Standards: ISO/DIS 14721 (derived from ISO 14721:2012 (OAIS model))*
06	Metadata scheme by TIP?	Perhaps defining a basic set of elements as a best practice (or requirement) with the possibility to expand where necessary is a good idea. If we can reach an agreement among ourselves, it would be beneficial. It's an important pillar for interoperability.
07	What will the Implementing Act related to eArchiving say?	Are we waiting to further detail this document until the Implementing Act?
08	Transferring data from archiving data	What if data is transferred to new QTSP archiver, but after a while the original QTSP-er made mistakes and is deleted from trusted list?
09	Transferring data from archiving data	Exit and export procedure needs to be described to be able to switch from one eArchive provider to another. Qualified proof has to be exported in such a manner that this will remain intact when switching from providers. This has to be done in a predescribed manner to ensure interoperability.
10	Exporting documents as packages with signatures/seals	Do we need a retrieval / export functionality for selected data to use as evidence. Or is mandating (temporarily) access to the selected data sufficient?