Long-term Preservation of Digital Signatures: a Need-to-have or a Nice-to-have?

Ștefan-Ciprian ARSENI, Emil BUREACĂ, and Mihai TOGAN

***Abstract*—Digital signatures are one of the main components that sustain recent digitization efforts made by public and private institutions. Despite their clear advantages, digital signatures have an 'Achilles heel': they cannot be properly validated, thus trusted, after the corresponding validating certificate has expired. To resolve this issue, standardization and legislative actions have been taken for developing an optimal framework for the implementation of services that can enable users to trust a digital signature, by ensuring that its validation can be done even after multiple years. This is what long-term preservation does and in this article we try to emphasize its role in a modern public-key environment. We focus on the regulation and standards perspective and present a comparison of several implementations of long-term preservation solutions that are available on the market. Through this paper we try to show that this nice-to-have functionality, as it is considered by many vendors, should, in fact, become a need-to-have for anyone dealing with creation and management of digital signatures.**

***Index Terms*—long-term preservation, ETSI standards, digital signature validation, digital certificate validation.**

I. Introduction

Public-key cryptography, first introduced in 1976 by Martin Hellman, Ralph Merkle and Whitfield Diffie, has been at the core of secure communication protocols or privacy and trust-ensuring APIs. Digital signatures, one of the main "products" of public-key cryptography, have seen an increasing adoption in recent decades, given the rise of technology in different areas of our societies, digitization of public and private institutions or, recently, the Covid-19 pandemic. In this digitization movement, the need to ensure trust between parties and, in some cases, non-repudiation of signed data is continuously growing. Thus, digital signatures will become more and more embedded in our everyday lives. This can also be seen in the accelerated rhythm of the development of a common framework for providing digital signature services, through the assurance of standards and regulation.

Yet, digital signatures have a major drawback: by being a cryptographic construction, created using a user's private key, that is paired with a public key embedded in a digital certificate, the lifetime of the digital signature is linked to the validity of the user's digital certificate. Thus, how can a person trust a specific digital signature after its validation digital certificate is no longer valid?

As an answer to the first of the previous questions, standardization and legislative bodies have made an effort in establishing the ground rules for a service that could preserve digital signatures for longer periods of time. The long-term validation service will act as a "guardian" for digital signatures, by continuously monitoring their validity state and executing specific tasks to maintain that validity, in accordance with certain preservation policies. In this manner, any digital signature that is valid at the time of signing and is then preserved, will maintain its validity even after several decades.

In order to function properly and meet all requirements, a preservation service needs to integrate with other services, from which it retrieves specific information, such as:

- a digital certificate validation service that groups certificate validation responses from various Certificate Authorities (CAs) and returns them to the long-term preservation service;
- a digital signature validation service that returns a standardized or custom validation report which includes detailed information related to the validity of the signature and all related cryptographic material, at the time of signing. Based on this report, the long-term preservation service will decide if the signature can or cannot be preserved;
- a qualified TimeStamp Authority (TSA) that can apply timestamps on the augmented constructions made by the long-term preservation service.

Depending on how the system is designed, other services can be integrated with the long-term preservation service, as long as the final augmented preservation object is compliant with existing regulation and standards (e.g.: signing service, storage provider or archive manager, etc.).

Given that there are many digital signature providers worldwide, all implemented long-term preservation services should follow a similar guideline. This will lead to a final encapsulated structure that can be recognized by multiple long-term preservation solutions, thus ensuring interoperability between systems, or even nations. Therefore, taking into consideration all that was mentioned above, is a long-term preservation service for digital signatures a need-to-have or a nice-to-have component?

In this paper we try to answer this question, by creating an overview of both the legislative and standardization efforts that are being made by certain institutions, in order to establish a common set of rules and directions that long-term preservation services should follow when designed and implemented. The regulations perspective is completed with

This work was supported by a grant obtained within POC, Priority axe 1, Investment priority no. 1.2.1, MySMIS code 123423, Contract no. 297/03.06.2020.

Ș. C. ARSENI is with the Military Technical Academy "Ferdinand I", Bucharest, Romania (e-mail: stefan.arseni@mta.ro).

E. BUREACĂ is with the Military Technical Academy "Ferdinand I", Bucharest, Romania (emil.bureaca@mta.ro)

M. TOGAN is with the Military Technical Academy "Ferdinand I", Bucharest, Romania (mihai.togan@mta.ro)

an analysis of various existing digital signature validation or long-term preservation systems that either exist on the market or are proposed in the scientific literature. Through these analyses, an entity that is indeterminate of whether or not to implement a long-term preservation service, could obtain an overall perspective of what this type of service means to be built and its role in the grand scheme of public-key services.

The rest of the paper is structured as follows: Section 2 presents an overview of the legislation framework that sets up boundaries for a long-term preservation service, while Section 3 introduces the standards that provide the technical means required for implementing such a service. Section 4 contains an analysis of several existing long-term preservation solutions, taking into consideration several perspectives and performance metrics. In Section 5 we end the paper and draw some conclusions regarding the overall "eco-system" to which a long-term preservation service will need to adapt.

II. Overview of Existing Legislation

Legislation in the context of preserving digitally signed documents and, thus, their applied digital signatures, is diverse and composed of several distinct regulations focusing on different aspects of the digital document. Thus, the primary scope of the general legislation was focused on preserving a signed document, in either digital or printed format, while the secondary scope, that became more and more obvious in recent years, was that of maintaining trust in a digital signed document even after the signature validation certificate expires. Both scopes are linked and dependent on each other:

- you cannot trust a digitally signed document without trusting and validating the digital signature;
- you cannot trust a digital signature without having the related document, needed to compute the cryptographic hash embedded in the signature.

Therefore, a single complex scope can be defined: preserving the digital document and its digital signature, by sealing its validation state. Even though this goal should be the same worldwide, there are similarities, but also differences, in how legislation is being created and enforced in different parts of the world.

A. Legislation framework in the European Union

In the European Union (EU), the processes of creating, validating or preserving a digital signature are regulated through the Regulation on electronic identification and trust services for electronic transactions in the internal market (Regulation No 910/2014 - eIDAS) [1]. This regulation is the foundation of the adoption of digital signatures in the EU, mainly because, besides clearly defining what a digital signature is, it also introduced several notions:

- a clear distinction between a qualified and an advanced digital signature;
- the possibility of remotely signing a document;
- electronic seals and qualified timestamps;
- the possibility of suspending qualified digital certificates;
- the qualified validation service for qualified digital signatures;
- the qualified preservation service for qualified digital signatures.

Referring to the unique scope identified at the beginning of this section, the eIDAS regulation targets only the digital signature, leaving the issue of preserving the actual document in the care of each state. Still, a solace for this issue has already been put in place, by regulating the digital archiving process. Thus, many countries and vendors have combined the nation-level archiving regulation with the eIDAS Regulation to obtain the required legal framework for implementing preservation services for digital signatures.

B. Legislation framework in the United States of America

In the United States of America (USA), digital signatures first appeared in some states and a regulation to ensure interoperability between states soon followed. The Uniform Electronic Transactions Act (UETA Act) [2] was the first regulation that appeared and set a generic boundary in which digital signatures can be used. This regulation was soon followed by a federal law, the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) [3] that complements the UETA Act, by stating the role of digital signatures and the operations done with or on them. Both these regulations offer the required legal framework for working with digital signatures but do not limit all the possible use cases, thus private companies tend to define their custom signature structures or workflows. In order to address these situations, the National Institute of Standards and Technology (NIST) has created several standards (NIST SP 800-63-3 [4], NIST SP 800-63A [5], NIST SP 800-63B [6] and NIST SP 800-63C [7]) that introduce certain constraints and define several digital signature assurance levels. Other standards from NIST, such as NIST SP 800-89 [8] or NIST SP 800-102 [9], introduce the means that one can use to achieve a valid digital signature preservation scheme.

C. Comparison between the two legislation frameworks

As it can be seen from their titles, regulations from both entities (EU and USA) were designed for electronic transactions, with the goal of simplifying administrative procedures and eliminating printed documents in certain workflows. Still, there is a certain discrepancy in how these entities project the digital signature: in the EU, a digital signature is constructed only by using a cryptographic private key that an user uniquely has, while in the USA, to digitally sign a document it is sufficient to express the intention of the signing (i.e.: through a voice recording, a name put in a document title, etc.). Also, in the USA there is a clear distinction between public and private sectors, enabling private organizations to enforce proprietary digital signature creation and verification mechanisms.

Despite these differences, all regulations enforce the idea that a digitally signed document cannot be rejected because it is present only in its digital form. Also, another similarity is the separation of digital signatures in different trust and assurance levels:

- in the *EU*: simple digital signature, advanced digital signature and qualified digital signature;
- in the *USA* - defined in NIST standards: *Identity Assurance Level* (IAL), *Authenticator Assurance Level*

 Digital Object Identifier 10.32754/JMT.2022.1.06

(AAL) and *Federation Assurance Level* (FAL). IAL and AAL are used in the private sector, while FAL is used in governmental institutions.

Overall, both in the EU and the USA, the legislation frameworks for digital signatures, seconded by legislation referring to archiving documents, enable the creation and operation of digital signatures preservation services. Still, legislation is augmented through the creation and adoption of standards that ensure system interoperability and a good level of security.

III. LONG-TERM PRESERVATION OF DIGITAL SIGNATURES FROM A STANDARDIZATION PERSPECTIVE

Before diving into the complex process of preservation, we must be aware of the necessity to verify the validity of all the linked elements, encompassing the public key certificate chains related to every signature. Moreover, several standards and technical specifications have been developed by ETSI in order to support the EU eIDAS Regulation [1]. Thus, preservation of documents can only be fulfilled by applying electronic signatures and timestamps, which imply conformity with several standards, given that the document will pass through the several phases before being considered a preserved object:

- Digital certificates validation;
- Creation and validation of digital signatures;
- Digital signature formats and profiles;
- Creation and validation of timestamps.

A. Digital certificates validation

Use of public key infrastructure (PKI) along with digital certificates accomplishes trust between the entities in the sense that it identifies a specific person or a system and assures the ownership of the associated private key. On the other hand, due to their inherent trustworthy nature, such a system has a lot of advantages derived from the ease of implementation, and distribution of digital certificates without the need of a secured transmission channel.

At EU level, the Certificate Trust List architectural model is adopted, with ETSI TS 119 612 [10] and ETSI TS 102 231 [11] providing an interoperable definition and XML format statements, describing the protocols and operations supported. Moreover, eIDAS imposes member states to publish and maintain Trust Lists and information about their Qualified Trust Service Providers (QTSPs).

As a result of higher security requirements and existent delays implicit in off-line schemes based on periodically issued Certificate Revocation Lists (CRLs), several on-line validation schemes, which provide real-time information, have been proposed:

- *Online Certificate Status Protocol (OCSP)* - Online certificate client-server validation protocol proposed in RFC 2560 [12] and RFC 6960 [13]. In comparison with CRLs, it solves the scalability problem by including in the response the revocation data only about the certificates specified in the request. Furthermore, the issue of up-to-date information is addressed by accessing data right from the certification authority database. Also, in RFC 5019 [14] an optimized version, Lightweight OCSP, is proposed;
- *Server-based Certificate Validation Protocol* (SCVP) - Another certificate validation solution, proposed in RFC 5055 [15], which offers the client the possibility to delegate the validation of the target certificate and the entire certification chain;
- *Data Validation and Certification Server Protocols* (DVCS) - Used mainly to ensure non-repudiation, represents another method for certificate validation, and is regulated through RFC 3029 [16].

B. Signatures validation

Digital signatures represent data structures generated by applying cryptographic algorithms using the signer's private key. Anyone can verify the integrity and authenticity of a digitally signed document with the help of the corresponding key pair.

Before or after executing the verification process of the validity state of the signer’s certificate and of all the certificates involved for the validation of the identified certification path, one must verify the signature value in accordance with the content of the signed document by applying inverse cryptographic operations. It involves the use of the public key from the signer’s certificate and the generation of hash information to be compared. In addition, ETSI TS 119 172 [17-20] technical specifications define several rules and constraints which can be enforced in the validation procedures. For example, one can set the admitted signature formats and levels, specify supplementary constraints on the algorithms used, define mandatory signature properties or even custom conditions.

Directly related with digital signatures validation process, ETSI developed two standards:

- ETSI TS 102 853: Signature verification procedures and policies - It offers a general view with regard to the validation process requirements, the type of the responses resulting from the validation, as well as the elements of the validation report;
- ETSI EN 319 102 and ETSI TS 119 102: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation; Part 2: Signature Validation Report - All of these are, in fact, an update or a replacement for the previous technical specification, which targets the compliance with the eIDAS Regulation. Alongside defining the procedures for creation and validation of AdES electronic signatures, if a TSP wishes to obtain Qualified TSP (QTSP) status, then the following of this standard is a compulsory requirement.

C. Long-term preservation

In order to prolong the lifetime of digitally signed documents, mechanisms have been defined which help extend the verifiability status for long periods of time, even if the signer’s key becomes expired or revoked, issuer Certification Authority (CA) no longer exists, or if the algorithms and cryptographic keys that were used to create the signature become obsolete. As described in [21], signature augmentation is the “*process of adding, to a digital signature, information aiming to maintain the validity over the near term and/or the long term*”.

Besides the previously enumerated technical specifications and standards, in Fig. 1, other fundamental pieces to preservation along with their interrelationship are encompassed:

- The creation of signatures is done by a signature / seal generation service which complies with ETSI TS 119 431-1 [22] and ETSI 119 431-2 [23]. Likewise, the interaction with the signature applications is performed according to ETSI TS 119 432 [24] which incorporates OASIS DSS-X 2.0.
- The signature validation process can be performed in its entirety by a signature validation service implemented in accordance with ETSI 119 441 [25]. Additionally, the service is accessed through the protocol specified in ETSI 119 442 [26].
- Preservation of signatures is accomplished by a preservation service in compliance with ETSI TS 119 511 [27] standard while the interaction between the preservation service and the preservation application shall be performed in accordance with the protocol described in ETSI TS 119 512 [28].

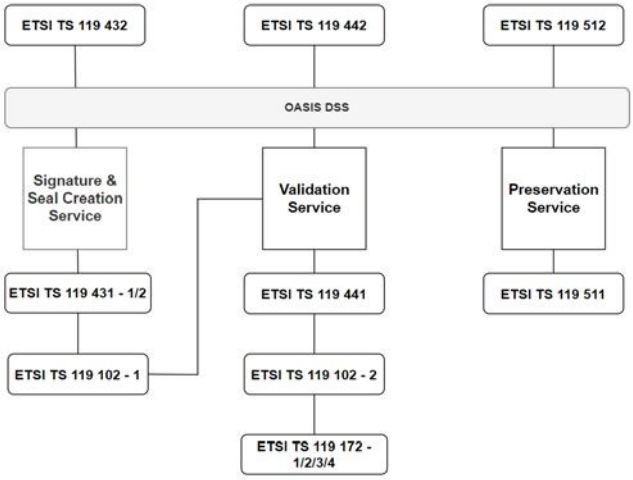

Figure 1. Long-term preservation in the context of ETSI standards

IV. Analysis of Existing Long-term Preservation Solutions

In the analysis of existing providers of long-term preservation services for digital signatures, we took into consideration mainly providers based in EU states. This choice was made given the consistent standardization context created around the eIDAS Regulation [1] and its continuous improvement. The main focus of the analysis is put on long-term preservation solutions, divided into three distinct categories, each with its own comparison metrics.

For managing trust service providers (TSPs) the EU has put in place the European Union Trusted Lists (EUTL). This registry contains a collection of all the TSPs that have been certified in the EU as being trustworthy, thus their services could be consumed by clients without questioning their reliability. Querying the EUTL for providers of certificates and digital signatures will result in over 250 uniquely identifiable entities, while a query for providers of long-term preservation result in ten times fewer entities. These fewer entities are also included in the first category, given that the majority of long-term preservation solutions are offered as an optional service by providers of digital certificates, digital signatures or electronic archiving.

After scouting the market in the hope of identifying valid candidates for this analysis, 16 solutions were identified. In order to create a better perspective of how these solutions comply with different standards or regulations and implement the requirements of a generic long-term preservation service, as presented in [27,28], the following analysis directions were determined:

- *general characteristics* - compliance with standards and regulations, types of supported digital signatures, location of the company, inclusion in EUTL;
- *architectural characteristics* - integration with external services, storage type, exposed interfaces for client integration;
- *implemented functionalities* - custom components that implement the workflows defined in [28].

Figures accompanying each analysis direction provide a summary, by using the following notations:

- *green dot* - feature exists;
- *red dot* - feature does not exist;
- *black dash* - not sufficient information in public material to draw a conclusion.

A. General characteristics

As presented in Fig. 2, the majority of long-term preservation providers are located in the western and northern part of the EU, with a few exceptions located in the eastern part (Hungary, Bulgaria and Romania) and southern part (Malta). This is primarily an effect of the well-developed financial markets and the large-scale adoption of technology. Despite this aspect, almost all of the solutions are included in the EUTL, thus clients can trust their provided services. Directly linked to the inclusion in EUTL is the compliance with eIDAS that, as presented in Fig. 2, is a mirrored image of the EUTL inclusion, with one exception (Ascertia Signing Long-Term Validation), that also offers compliance with regulation from the USA.

From the perspective of digital signature formats, PAdES is the common one, found in almost all analyzed solutions, since PDF files are the most used documents when using digital signatures. CAdES and XAdES signature formats, embedding digital signatures for a generic file or a XML, are also desirable and are implemented in more than 75% of the analyzed solutions.

B. Architectural characteristics

The next set of characteristics that the analysis focuses on, are some architectural traits that are specific to a long-term preservation service, as shown in Fig. 3.

Even though all solutions provide functional long-term preservation services, not all of them allow clients to change some of the required external connections, such as: CA, TSA, digital certificate validation service (CRL, OCSP or SCVP). Half of the analyzed solutions enable the update of connections to such external services, while the remaining half, constrain clients at using only the pre-configured connections. This trend of integrated resources can be seen also when discussing the storage type.

 Digital Object Identifier 10.32754/JMT.2022.1.06

No.	Solution name	Company location	Included in EUTL	Legislative domain		Supported signature standards					
				eIDAS	*Other*	*PAdES*	*CAdES*	*XAdES*	*ASiC*	*PDF/A*	*Other*
1.	Ascertia E-Notarisation & Secure Archiving	UK and Ireland	●	●	-	●	●	●	●	●	*IETF LTANS, PEPPOL*
2.	Ascertia Signing Long Term Validation	UK and Ireland	●	●	*US E-Sign Act, HIPAA, SOX, UETA, GPEA, FDA 21 CFR*	●	●	●	●	●	-
3.	B-TRUST Qualified Long Term Preservation Service	Bulgaria	●	●	-	●	●	●	●	●	-
4.	CDC Arkhineo	France	●	●	-	●	●	●	●	●	*NF 461*
5.	EDICOM Long Term Archiving	France	●	●	*NOM 151 SCFI 2016*	●	●	●	●	●	-
6.	EuroSign Long Term Archiving Service	France	●	●	-	●	●	●	●	●	-
7.	E-Witness Digital Conservation System	Malta	●	●	-	●	●	●	●	●	*ISO OAIS, UNI SInCRO*
8.	FutureTrust PresS	EU	●	●	-	●	●	●	●	●	*BSI TR 03125-F, RFC 4998, RFC 6283*
9.	LuxTrust Solutions COSI	Luxembourg	●	●	*EU PSD-2*	●	●	●	●	●	-
10.	Microsec/E-Szigno Qualified Long Term Electronic Archiving	Hungary	●	●	-	●	●	●	●	●	-
11.	Namirial StrongDox	Italy	●	●	*US E-Sign Act*	●	●	●	●	●	*ISO OAIS*
12.	Nets E-Archive	Denmark	●	●	-	●	●	●	●	●	-
13.	Signicat Preservation Archive	Norway	●	●	-	●	●	●	●	●	-
14.	Software602 Long Term Docs	Czech Republic	●	●	-	●	●	●	●	●	-
15.	Start-Storage SEAL	Romania	●	●	-	*Data not available*					
16.	Trans Sped LTP	Romania	●	●	-	*Data not available*					

Figure 2. General characteristics of long-term preservation solutions

Except one provider, that offers only the possibility of storing preserved objects at the client location, as seen in Fig. 3, all other providers offer the possibility of saving the preserved objects in the Cloud, namely in a private Cloud that is managed by that provider. There are two more exceptions: one provider offers the possibility of Cloud and on-premise storage, while another provider has the options of Cloud and 3rd party storage location.

Another key point, besides how the solutions can be updated to integrate other external services, refers to how clients can interact with these solutions. From this perspective, all analyzed solutions, except one, offer at least one type of connection (e.g. SOAP, REST or Web API) or a generic protocol using a specific type and format of data (e.g. XML or JSON).

No.	Solution name	Supported external services	Storage type			Provided API	Client interface			
			Local	*Cloud*	*3rd party*		*Web*	*Desktop*	*Smartphone*	*Other*
1.	Ascertia E-Notarisation & Secure Archiving	CA, TSA, OCSP	●	●	●	XML/SOAP	●	●	*Data not available*	Integration with the email server through *Secure Email Server*
2.	Ascertia Signing Long Term Validation	CA/RA, TSA, OCSP/SCVP	● *(on-premise service)*	●	●	REST	●	●		-
3.	B-TRUST Qualified Long Term Preservation Service	CA, CRL/OCSP, TSA, BG-TL	●	●	●	SOAP	●	●		-
4.	CDC Arkhineo	-	●	●	●	Web API	●	●	●	Integration with *Salesforce* and *DocuSign*
5.	EDICOM Long Term Archiving	-	●	●	●	*Yes, but no details are provided*	●	●	●	-
6.	EuroSign Long Term Archiving Service	-	●	●	●	JSON *(only for signatures)*	●	●	●	-
7.	E-Witness Digital Conservation System	-	●	●	●	-	●	●	●	-
8.	FutureTrust PresS	CA, TSA, OCSP, TL	●	●	●	REST	●	●	●	-
9.	LuxTrust Solutions COSI	TSA, CA	●	●	●	Web API	●	●	●	-
10.	Microsec/E-Szigno Qualified Long Term Electronic Archiving	TSA, SS	●	●	●	Command line	●	●	●	-
11.	Namirial StrongDox	CA, TSA	●	●	●	SOAP 1.2, SDK	●	●	●	-
12.	Nets E-Archive	-	●	●	●	REST	●	●	●	Integration with *Nets E-Signing* and *Nets Share*
13.	Signicat Preservation Archive	TSA	●	●	●	REST, SDK	●	●	●	Supports *MFA*
14.	Software602 Long Term Docs	TSA	●	●	●	REST	●	●	●	-
15.	Start-Storage SEAL	-	●	●	●	REST, CMIS	●	●	●	Multiple integrations: *Outlook, Sharepoint, Office*
16.	Trans Sped LTP	TSA, CA, OCSP	●	●	●	REST	●	●	●	-

Figure 3. Architectural characteristics of long-term preservation solutions

Another way of interaction comes under the form of a specific application, designed by the provider to enable clients to access and configure, based on specific constraints, the long-term preservation service: a web UI (portal), a desktop or a smartphone application. Given the reliability and easiness of a Web UI, this method is used by almost all analyzed solutions. Moreover, some solutions also provide integration with different workplace applications, such as email servers or *SalesForce*.

C. Implemented functionalities

The final focus is put on identifying how many functionalities specific to a long-term preservation service are implemented in the analyzed solutions. There are eight functionalities, specified in [28] as operations that a long-term preservation service should implement, depending on the storage model it uses (WithStorage, WithTemporaryStorage or WithoutStorage):

- *PreservePO* - preserves a digitally signed document and its digital signature, by augmenting it;
- *RetrievePO* - download the preserved object;
- *DeletePO* - delete the preserved object;
- *UpdatePOC* - update the signed document in the preserved object with a new version;
- *ValidateEvidence* - validate a preservation evidence issued at the moment of preserving a signed document;
- *Search* - identify preserved objects that match a certain search criteria;
- *RetrieveTrace* - obtain information about the actions made on a specific preserved object;
- *RetrieveInfo* - obtain information regarding the available preservation profiles.

These functionalities have been customely implemented by each vendor, thus an operation can be found under a different name or integrated in a larger data flow. As presented in Fig. 4, the analyzed solutions have similar notations for their implemented functionalities:

- *Signature augmentation* - functionality mainly implemented by vendors that also offer digital signature services. There are two exceptions to this statement, namely *Namirial StrongDox* and *Nets E-Archive* that create custom structures derived from the documents and information that clients deliver.
- *Upload and Download* - functionalities that are found in all analyzed solutions, ensure the first layer of interaction between clients and the long-term preservation services, by enabling clients to feed documents for preservation or download their preserved format.
- *Preservation confirmation* - functionality that enables clients to receive a signed report from the long-term preservation service, containing information regarding the preserved document. Even though this report is custom-made for each vendor, all of them are legally valid.
- *Data update* - found only in two of the analyzed solutions, the functionality allows clients to update the document they have sent for preservation. Still, there are specific constraints that each vendor imposes (e.g.: updates are allowed only before the expiration date of the first preservation seal).

No.	Solution name	Implemented functionalities							
		Signature augmentation	*Upload*	*Download*	*Preservation confirmation*	*Data update*	*Signature update*	*Delete*	*Index search*
1.	Ascertia E-Notarisation & Secure Archiving	●	●	-	-	-	●	-	-
2.	Ascertia Signing Long Term Validation	*Implements signature validation services, but integrates with long term preservation services that exist in the Ascertia organization.*							
3.	B-TRUST Qualified Long Term Preservation Service	●	●	●	●	●	●	●	-
4.	CDC Arkhineo	-	●	●	●	●	●	-	●
5.	EDICOM Long Term Archiving	●	●	-	-	-	●	-	-
6.	EuroSign Long Term Archiving Service	●	●	-	-	●	●	-	-
7.	E-Witness Digital Conservation System	●	●	●	●	●	●	●	-
8.	FutureTrust PresS	●	●	-	●	●	●	●	-
9.	LuxTrust Solutions COSI	-	●	-	-	-	-	-	-
10.	Microsec/E-Szigno Qualified Long Term Electronic Archiving	●	●	●	●	●	-	●	●
11.	Namirial StrongDox	● *(proprietary format)*	●	●	●	●	-	-	-
12.	Nets E-Archive	● *(proprietary format)*	●	●	●	-	-	●	●
13.	Signicat Preservation Archive	●	●	●	-	-	●	-	●
14.	Software602 Long Term Docs	●	●	●	●	●	-	●	●
15.	Start-Storage SEAL	●	●	●	-	●	-	-	-
16.	Trans Sped LTP	●	●	●	●	●	●	●	-

Figure 4. Implemented functionalities of long-term preservation solutions

 Digital Object Identifier 10.32754/JMT.2022.1.06

- *Signature update* - functionality linked to the implementation of a mechanism that ensures the re-augmentation of signatures in the preserved document, at specific intervals and for a specific period of time. Even though all analyzed solutions should implement this functionality, public information offered by each vendor is not sufficient, thus the results are inconclusive.
- *Delete* - another mandatory functionality that is not sufficiently documented for a part of the analyzed solutions. It enables clients to remove their documents and, respectively, the preservation objects constructed over those documents.
- *Index search* - functionality directly linked to *Delete*, existent in a part of the analyzed solutions. It enables clients to search for a specific preservation object and retrieve its specific ID that can later be used for other operations, such as *Download*, *Data update* or *Delete*.

Overall, the main operations stipulated in [28] are implemented in almost all of the analyzed solutions. We also need to point out that the operations in [28] are directly linked to the storage model that a long-term preservation service implements, thus not all of them are mandatory. This is also a reason why some of the analyzed solutions do not have one or more operations implemented.

V. Conclusion

Digital signature provision services have seen a continuous growth in recent years, due to large scale adoption of digital signatures as an easy and reliable method of signing documents and delivering trust. Their main problem, that of an "expiration date", linked to the validating certificate validity has been approached and a possible solution has been given: the long-term preservation service.

Regulations and standards have been continuously created and updated at the international level, as presented in Sections II and III of the paper, with the EU having a well-defined framework put in place. Still, even in this environment, companies are considering long-term preservation as a nice-to-have feature and not a need-to-have one. This is also sustained by the small number of entities that provide this type of service relative to the considerable number of entities that provide digital signature creation services. Yet, as presented in Section IV, the majority of these long-term preservation solutions that we analyzed are following the guidelines presented in ETSI standards. This is a valid demonstration that the standardized long-term preservation service requirements can be satisfied and the creation of a reliable and interoperable service is possible. Thus, this feature of long-term preservation should soon become mainstream, for PKI-related entities, given that it is a need-to-have, rather than a nice-to-have one, because of the way it complements and adds value to digital signature services.

From the regulation perspective, long-term preservation evidence issued for preserved documents after they pass several validation stages, are considered valid and can be used in legal activities. Combined with the easiness of archiving digital documents instead of physical ones, the long-term preservation service will become a default feature of any digital signature management solutions.

References

[1] *Regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, REGULATION (EU) No 910/2014, 2014.

[2] *Uniform electronic transactions act*, 1999.

[3] *Electronic signatures in global and national commerce act*, PUBLIC LAW 106–229, June 2000.

[4] *Digital Identity Guidelines*, NIST Special Publication 800-63-3, 2017, doi: 10.6028/NIST.SP.800-63-3.

[5] *Digital Identity Guidelines - Enrollment and Identity Proofing*, NIST Special Publication 800-63A, 2017, doi: 10.6028/NIST.SP.800-63a.

[6] *Digital Identity Guidelines - Authentication and Lifecycle Management*, NIST Special Publication 800-63B, 2017, doi: 10.6028/NIST.SP.800-63b.

[7] *Digital Identity Guidelines - Federation and Assertions*, NIST Special Publication 800-63C, 2017, doi: 10.6028/NIST.SP.800-63c.

[8] *Recommendation for Obtaining Assurances for Digital Signature Applications*, NIST Special Publication 800-89, 2006, doi: 10.6028/NIST.SP.800-89.

[9] *Recommendation for Digital Signature Timeliness*, NIST Special Publication 800-102, 2009, doi: 10.6028/NIST.SP.800-102.

[10] *Electronic Signatures and Infrastructures (ESI); Trusted Lists*, ETSI TS 119 612 V2.1.1, 2015.

[11] *Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information*, ETSI TS 102 231 V3.1.2, 2009.

[12] *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, RFC 2560, 1999.

[13] *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, RFC 6960, 2013.

[14] *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*, RFC 5019, 2007.

[15] *Server-Based Certificate Validation Protocol (SCVP)*, RFC 5055, 2007.

[16] *Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*, RFC 3029, 2001.

[17] *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents*, ETSI TS 119 172-1 V1.1.1, 2015.

[18] *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies*, ETSI TS 119 172-2 V1.1.1, 2019.

[19] *Electronic Signatures and Infrastructures (ESI); Part 3: ASN.1 format for signature policies*, ETSI TS 119 172-3 V1.1.1, 2019.

[20] *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists*, ETSI TS 119 172-4 V1.1.1, 2021.

[21] *Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*, ETSI TS 119 102-1 V1.2.1, 2018.

[22] *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev*, ETSI TS 119 431-1 V1.1.1, 2018.

[23] *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation*, ETSI TS 119 431-2 V1.1.1, 2018.

[24] *Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation*, ETSI TS 119 432 V1.1.1, 2019.

[25] *Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services*, ETSI TS 119 441 V1.1.1, 2018.

[26] *Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services*, ETSI TS 119 442 V1.1.1, 2019.

[27] *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*, ETSI TS 119 511 V1.1.1, 2019.

[28] *Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services*, ETSI TS 119 512 V1.1.1, 2020.

 Digital Object Identifier 10.32754/JMT.2022.1.06