**APROBAT**

**GUVERNANȚA PMO**
DORU VIJIIANU ZIPPER SERVICES SRL Digitally signed by ZIPPER SERVICES SRL Date: 2025.10.14 18:15:20 +03'00'
JUDIT FEKETE FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2025.10.14 18:22:37 +03'00'
MIRELA OJOG Mirela Ojog Digitally signed by Mirela Ojog Date: 2025.10.14 20:15:59 +03'00'

# -Autoritatea Zipper Services-
# Serviciul calificat de păstrare (QPS)
# pentru semnături/sigilii electronice calificate (QES)

# Politică, cod de practică și proceduri



| **Istoric ediții** | | | |
|---|---|---|---|
| **Ediție** | **Data și descrierea modificării** | **Gata** | **Aprobat** |
| 1 | 18.09.2025 – Prima ediție | Judit Fekete | Mirela Ojog |
| 2 | 08.10.2025 -Ediția a doua – recenzii minore | Judit Fekete | Mirela Ojog |
| | | | |
| | | | |
| | | | |

**Annex A. Conținut**

## 1. Introducere

**Politica, Codul de Practică și Proceduri (PCPP)** detaliază politicile, practicile și procedurile pe care Zipper Services (denumită în continuare Zipper) le aplică la serviciul de**păstrare a semnăturilor/sigiliilor electronice calificate** (denumit în continuare **QPS).**

Zipper pune la dispoziția utilizatorilor săi serviciul de păstrare calificată a semnăturilor/sigiliilor electronice calificate în conformitate cu art. 34 și art. 40 din Regulamentul (UE) nr. 910/2014 și Regulamentul (UE) 2024/1183 (eIDAS 2.0) și este înregistrat în lista de încredere a furnizorilor europeni de servicii de încredere, precum și în registrul furnizorilor de servicii de încredere din România ținut de Autoritatea pentru Digitalizarea României (ADR).

Conținutul **PCPP-QPS** este conform cu cele mai recente versiuni ale cerințelor ETSI TS 119 511 și ETSI TS 119 512.

Acest document este pus la dispoziția publicului la https://pki.ca.ezipper/policies

Cerintele tehnice si de securitate (conform art. 5 din Normele tehnice privind procedura de acreditare a administratorilor de arhiva electronica si procedura de aprobare a sistemelor de arhivare electronica, parte integranta a Ordinului 20717/2024) pe care le indeplineste sistemul de arhivare electronica sunt descrise in Planul de securitate specific sistemului de arhivare electronica v1, considerat anexa la prezentul document.

Conducerea poate face excepții de la acest document de la caz la caz pentru a atenua impactul semnificativ și iminent asupra clienților, partenerilor, părților de încredere și/sau altor persoane în absența unor soluții practice. Orice astfel de excepții de manipulare sunt documentate, urmărite și raportate ca parte a procesului de audit.

## 2. Administrarea politicilor și a practicii

Serviciul de arhivare electronică este oferit de Zipper Services în infrastructura Centrului de Date Zipper Services, autorizat de ADR pentru servicii de arhivare electronică în condițiile Legii 135/2007 (Hotărârea nr. 253 din 23.05.2024).

Organizația care administrează acest document:

**ZIPPER SERVICES SRL**

Str. Rene Jeannel, nr. 8, Imobil Novis Plaza, corp A, et. 2, 400285, Cluj-Napoca, RO

Cluj-Napoca, 400285, România

*Punct de lucru:*

Bd. 1 Decembrie 1918 nr. 1G,

Sector 3, București, 032451, România

*Punct de lucru:*

Strada Nikola Tesla, nr. 2, cod 400221, jud. Cluj

Cluj-Napoca, 400285, România

https://ezipper.ro/

E-mail: office@ezipper.ro

Telefon +40 21.340.4638 / +40 31.101.1020

Fax: +40 21.340.4636 / +40 31.101.1022

(Luni-Vineri 09.00. – 18:00 ora Europei de Est)

Contact: pki@ezipper.ro Echipa de Management al Politicilor

## 3. Procedura de aprobare

Aprobarea acestui document și modificările ulterioare sunt făcute de persoanele dedicate Zipper. Aceste persoane alcătuiesc echipa de management al politicilor. Membrii PMO GOVERNANCE aprobă noi versiuni ale acestui document. Versiunile modificate înlocuiesc orice prevederi contradictorii ale versiunilor anterioare ale prezentului document.

Abonații care nu acceptă termenii și reglementările noi, modificate ale PCPP trebuie să facă o declarație adecvată în termen de 15 zile de la data publicării noii versiuni a PCPP. Acest lucru va duce la rezilierea contractului aferent serviciilor QPS furnizate.

## 4. DENUMIREA ȘI IDENTIFICATORUL DOCUMENTULUI

Numele complet al acestui document este "Serviciul de conservare calificat pentru semnături/sigilii electronice calificate (QPSES) (Qualified preservation service) Policy, Code of Practice and Procedures (PCPP)" și identificator de obiect (OID):

| Denumirea documentului | Identificator de obiect (OID) |
|---|---|
| Serviciul de conservare calificat (QPS) pentru semnăturile/sigiliile electronice calificate (QES) - Politică, Cod de practică și proceduri (PCPP) | **1.3.6.1.4.1.57570.4.3.2**<br>4=> nod de clasificare a serviciului<br>3 => servicii de conservare (subarbore pentru politicile legate de conservare)<br>2=> **variantă de conservare** calificată |

Conform ETSI EN 319 401, este obligatoriu ca un TSP să identifice politicile de servicii pe care le acceptă. Pentru serviciile de conservare, un astfel de identificator este comunicat prin intermediul documentației furnizate abonaților și părților de bază, prin OID specific:

• ITU-T(0) Organizație-identificată(4) ETSI(0) Politici-de-serviciu(19511) Identificatori-politici(1) Calificați (2).

Zipper se asigură că nu modifică identificatorul obiectului acestui document, precum și identificatorii obiectelor politicilor, practicilor și altor documente de trimitere. Dacă există o extensie/actualizare în politică și practică care nu va afecta certificatele emise anterior, Zipper prezintă un nou identificator de obiect care acoperă certificatele noi sau cele extinse/actualizate.

## 5. Referinţe

**Legislația națională aplicabilă:**

1. Legea nr. 135 din 15 mai 2007 privind arhivarea documentelor în format electronic
2. ORDIN nr. 20.717 din 9 mai 2024 pentru aprobarea Normelor tehnice privind procedura de acreditare a administratorilor de arhive electronice și procedura de aprobare a sistemelor de arhivare electronică și pentru abrogarea Ordinului ministrului comunicațiilor și societății informaționale nr. 493/2009 privind normele tehnice și metodologice de aplicare a Legii nr. 135/2007 privind arhivarea documentelor în formă electronică
3. Ordinul ministrului MCSI nr. 489/15.06.2009 privind normele metodologice de autorizare a centrelor de date
4. Ordinul nr. 585 din 9 mai 2011 pentru completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date
5. Ordinul nr. 1167 din 25 noiembrie 2011 pentru modificarea anexei nr. 3 la Ordinul ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date.
6. Legea nr. 455/2001 privind semnătura electronică, republicată, cu modificările și completările
7. Legea Arhivelor Naționale nr. 16/1996, republicată, cu modificările și completările ulterioare;
8. Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare;
9. Hotărârea Guvernului nr. 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României, cu modificările și completările ulterioare;

10. Normele tehnice privind procedura de acreditare a administratorilor arhivei electronice și procedura de aprobare a sistemelor de arhivare electronică, aprobate prin Ordinul ministrului cercetării, inovării și digitalizării nr. 20.717/2024;

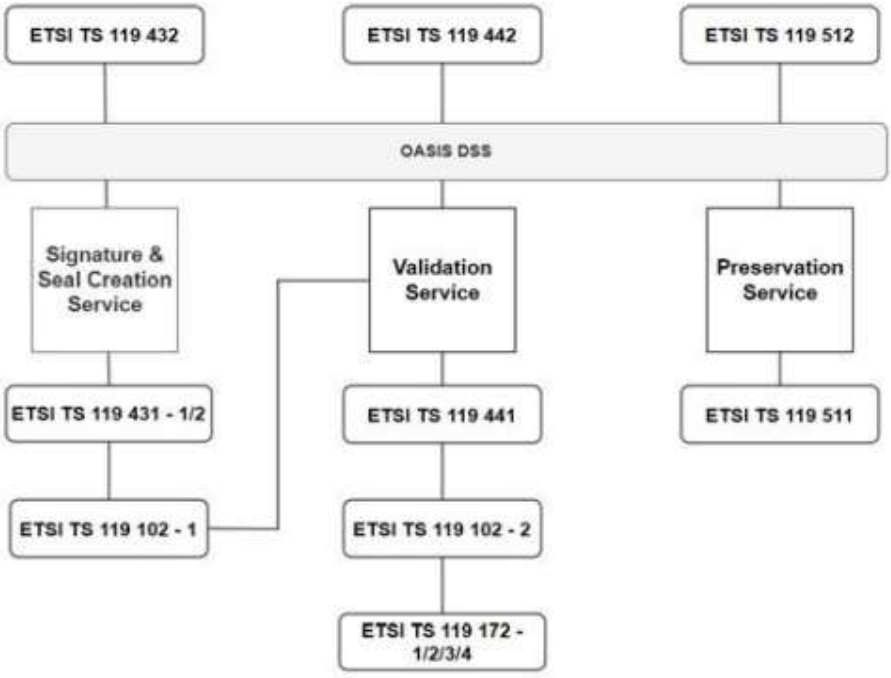
**Următoarele referințe conțin prevederi care sunt relevante pentru politica centrelor de date ZIPPER și serviciul de arhivare electronică:**

Legea nr. 190/2018 privind măsurile de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare.

REGULAMENTUL (UE) nr. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE [1];

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european de identitate digitală




ETSI TS 119 511 Semnături electronice și infrastructuri (ESI); Cerințe de politică și securitate pentru furnizorii de servicii de încredere care asigură conservarea pe termen lung a semnăturilor digitale sau a datelor generale utilizând tehnici de semnătură digitală

ETSI TS 119 512 Semnături electronice și infrastructuri (ESI); Protocoale pentru furnizorii de servicii de încredere care furnizează servicii de conservare a datelor pe termen lung

ETSI SR 019 510 Semnături electronice și infrastructuri (ESI); Studiu de scop și cadru pentru standardizarea serviciilor de conservare a datelor pe termen lung, inclusiv păstrarea / cu semnături digitale

ETSI TS 119 132-3 Semnături electronice și infrastructuri (ESI); Semnături digitale XAdES; Partea 3: Încorporarea mecanismelor de sintaxă a înregistrărilor de dovezi (ERS) în XAdES

ETSI EN 319 102 privind aprobarea semnăturilor electronice și a infrastructurilor de încredere (ESI); Proceduri de creare și validare a semnăturilor digitale AdES; Partea 1: Creare și validare

ETSI EN 319 401 Semnături electronice și infrastructuri (ESI); Cerințe generale de politică pentru furnizorii de servicii de încredere.

ETSI TS 119 312 Semnături electronice și infrastructuri (ESI); Suite criptografice;

ETSI EN 319 102-1 Semnături electronice și infrastructuri (ESI); Proceduri de creare și validare a semnăturilor digitale AdES; Partea 1: Creare și validare;

ETSI EN 319 122-1 Semnături electronice și infrastructuri (ESI); Semnături digitale CAdES; Partea 1: Blocuri de construcție și semnături de referință CAdES;

ETSI EN 319 122-2 Semnături electronice și infrastructuri (ESI); Semnături digitale CAdES; Partea 2: Semnături CAdES extinse;

ETSI TS 119 122-3 Semnături electronice și infrastructuri (ESI); Semnături digitale CAdES; Partea 3: Încorporarea mecanismelor de sintaxă a înregistrărilor de dovezi (ERS) în CAdES;

ETSI EN 319 132-1 Semnături electronice și infrastructuri (ESI); Semnături digitale XAdES; Partea 1: Blocuri de construcție și semnături de bază XAdES;

ETSI EN 319 132-2 Semnături electronice și infrastructuri (ESI); Semnături digitale XAdES; Partea 2: Semnături XAdES extinse;

ETSI EN 319 142-1 Semnături electronice și infrastructuri (ESI); semnături digitale PAdES; Partea 1: Blocuri de construcție și semnături de referință PAdES;

ETSI EN 319 142-2 Semnături electronice și infrastructuri (ESI); semnături digitale PAdES; Partea 2: Profiluri suplimentare de semnături PAdES;

ETSI EN 319 162-1 semnături electronice și infrastructuri (ESI); Containere de semnături asociate (ASiC); Partea 1: Blocuri de construcție și containere ASiC Baseline;

ETSI EN 319 162-2 semnături electronice și infrastructuri (ESI); Containere de semnături asociate (ASiC); Partea 2: Containere ASiC suplimentare;

ETSI TS 119 172-1 Semnături electronice și infrastructuri (ESI); Politici de semnătură; Partea 1: Blocuri de construcție și cuprins pentru documentele de politică privind semnăturile care pot fi citite de om;

ETSI TS 119 172-4 Semnături electronice și infrastructuri (ESI); Politici de semnătură; Partea 4: Politica de validare a semnăturilor pentru semnăturile/sigiliile electronice calificate europene care utilizează liste de încredere;

ETSI EN 319 421 Semnături electronice și infrastructuri (ESI); cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit marcaje temporale;

ETSI EN 319 422 Semnături electronice și infrastructuri (ESI); profiluri de protocol de marcare temporală și token de marcare temporală;

ETSI TS 119 511 Semnături electronice și infrastructuri (ESI); cerințe de politică și securitate pentru furnizorii de servicii de încredere care asigură conservarea pe termen lung a semnăturilor digitale

sau a datelor generale utilizând tehnici de semnătură digitală;

ETSI TS 119 512 Semnături electronice și infrastructuri (ESI); Protocoale pentru furnizorii de servicii de încredere care furnizează servicii de conservare a datelor pe termen lung;

ISO/IEC 21320-1 Tehnologia informației -- Document Container File -- Partea 1: Nucleu;

IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);

IETF RFC 3986 Uniform Resource Identifier (URI): Sintaxă generică;

IETF RFC 6283 Sintaxa înregistrării dovezilor (ERS);

IETF RFC 5280 Certificat de infrastructură cu cheie publică și profil de listă de revocare a certificatelor (CRL);

IETF RFC 5816 ESSCertIDv2 Actualizare pentru RFC 3161;

IETF RFC 6283 Sintaxa extensibilă a înregistrării de dovezi a limbajului de marcaj (XMLERS);

IETF RFC 6838 Specificații de tip de suport și proceduri de înregistrare;

IETF RFC 6960 Online Certificate Status Protocol - OCSP;

W3C Extensible Markup Language (XML) 1.0 (a cincea ediție)", Recomandarea W3C;

BSI TR-03125-F Păstrarea dovezilor documentelor, formatelor semnate criptografic (TR-ESOR-F);

ETSI TS 119 461 Semnături electronice și infrastructuri (ESI); cerințe de politică și securitate pentru componentele serviciilor de încredere care asigură verificarea identității subiecților serviciilor de încredere;

ETSI TS 119 441 Semnături electronice și infrastructuri (ESI); Cerințe de politică pentru TSP care furnizează servicii de validare a semnăturilor;

ETSI TS 119 442 Semnături electronice și infrastructuri (ESI); Profiluri de protocol pentru furnizorii de servicii de încredere care furnizează servicii de validare a semnăturii digitale AdES.

**5. Definiții și abrevieri**

**Audit IT** - activitatea de colectare și evaluare a probelor pentru a determina dacă sistemul IT respectă parametrii de performanță și de lucru conform cerințelor de proiectare, dacă asigură funcționalitățile necesare cerințelor de business și conformității cu legislația în domeniu, dacă este securizat, dacă menține integritatea datelor prelucrate și stocate, dacă permite realizarea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;

**Auditor IT** - persoana fizică autorizată care deține certificat de auditor IT sau persoana juridică cu

personal certificat care desfășoară o activitate de audit al sistemelor informatice, conform reglementărilor și bunelor practici în domeniu;

**Raport de audit IT** - instrumentul prin care se comunică scopul auditului, obiectivele urmărite, normele/standardele aplicate, perioada parcursă, natura, procedurile, constatările și concluziile auditului, precum și eventualele rezerve pe care auditorul IT le are cu privire la sistemul informatic auditat;

**prestator de servicii de asigurare a încrederii calificat** - în conformitate cu art. 3 punctul 20 din Regulamentul (UE) nr.910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

**backup** - activitatea de copiere a fișierelor sau bazelor de date în vederea păstrării și recuperării acestora în caz de deteriorare sau alt eveniment neprevăzut;

**Container de date:** un obiect de date care conține un set de obiecte de date și informații suplimentare care descriu obiectele de date conținute și, opțional, conținutul și relațiile dintre acestea (semnături/sigilii digitale, marcaje temporale, înregistrări de dovezi, date de validare etc.);

**Autoritate UE calificată de marcare temporală**: un furnizor de servicii de asigurare a încrederii calificat care emite marcaje temporale electronice calificate, astfel cum se prevede în Regulamentul (UE) nr. 910/2014;

**înregistrarea dovezilor**: date care pot fi utilizate pentru a dovedi existența unui obiect de date arhivat sau a unui grup de obiecte de date arhivate la un moment dat;

**QPSES (Serviciul de Conservare a Semnăturilor Electronice):** un serviciu calificat de păstrare a semnăturilor/sigiliilor electronice calificate;

**OCSP:** un protocol care furnizează informații online despre starea certificatului (OCSP sau CRL);

**Fișier ASiCArchiveManifest**: fișier container al cărui nume se potrivește cu "*ASiCArchiveManifest*.xml" care conține o instanță de element ASiCManifest

**Fișier ASiCEvidenceRecordManifest:** fișier container utilizat în ASiC-E pentru a face referire la un set de fișiere la care se aplică un ER al căror nume se potrivește cu "META-INF/ASiCEvidenceRecordManifest*.xml" și care conține o instanță de element ASiCManifest

**Fișier ASiCManifest:** fișier al cărui nume se potrivește cu "*ASiCManifest*.xml" care conține o instanță de element ASiCManifest

**container:** fișier creat conform ZIP care conține ca elemente interne fișiere cu manifest, metadate și

semnături asociate, sub o ierarhie de foldere. Un obiect de date care conține un set de obiecte de date și informații suplimentare care descriu obiectele de date conținute și, opțional, conținutul și interrelațiile acestora (semnături/sigilii digitale, marcaje temporale, înregistrări de probe, date de validare etc.);

**Container de obiecte de conservare delta**: un container de obiecte de conservare care descrie exclusiv diferența dintre un container de obiecte de conservare deja existent și un obiect de date actualizat;
**tehnici de semnătură digitală:** tehnici bazate pe semnături/sigilii digitale, marcaje temporale sau înregistrări de probe;

**Autoritate calificată a UE de marcare temporală**: un prestator calificat de servicii de asigurare a încrederii care emite marcaje temporale electronice calificate, astfel cum se prevede în Regulamentul (UE) nr. 91 0/2014;

**durata preconizată a probelor:** durata preconizată a evidențelor probelor;

**pachet de export-import:** informații extrase din serviciul de conservare, inclusiv conținut și dovezi, care pot fi importate;

**pe termen lung:** o perioadă lungă de timp în care schimbările tehnologice, cum ar fi învechirea tehnologiei criptografice, a algoritmilor cripto, dimensiunile cheilor sau a funcțiilor hash, compromiterea cheilor sau capacitatea de a verifica starea de valabilitate a certificatelor pot constitui un motiv de îngrijorare;

**conservare pe termen lung:** păstrarea pe termen lung (cu stocare), în cazul în care prelungirea stării de valabilitate a unei semnături digitale și/sau furnizarea de dovezi de existență a datelor pe o perioadă lungă de timp nu depinde de învechirea tehnologiei criptografice, a algoritmilor cripto, a dimensiunilor cheilor sau a funcțiilor hash, a compromiterilor cheilor sau a capacității de a verifica starea de valabilitate a certificatelor;

**protocol de notificare:** un protocol utilizat de serviciul de conservare pentru a notifica clientul de conservare;

**client de conservare:** un client de conservare fiind o componentă sau o bucată de software care interacționează cu un serviciu de conservare prin protocolul de conservare;

**dovezi de conservare**: dovezi de conservare furnizate de serviciul de conservare care pot fi utilizate pentru a dovedi îndeplinirea unuia sau mai multor obiective de conservare pentru un anumit obiect;
**politica de conservare a probelor:** o politică de păstrare a probelor, inclusiv un set de reguli care specifică

cerințele și procesul intern de generare și validare a oricăror dovezi de conservare;

**perioada de păstrare a probelor de conservare:** o perioadă de păstrare a probelor de conservare; **Scopul de conservare:** scopul de conservare este extinderea (augmentarea) stării de valabilitate a semnăturilor/sigiliilor digitale dincolo de statutul de validitate tehnologică, furnizarea de dovezi de existență a datelor pe perioade lungi de timp sau o combinație a celor două;

**Mecanism de conservare:** mecanism de conservare bazat pe tehnici de semnătură digitală, care este utilizat pentru a conserva obiectele de conservare și pentru a menține validitatea dovezilor de conservare**; interfață de conservare:** interfața de conservare este o componentă care implementează protocolul de conservare. Evrotrust elaborează și utilizează o interfață de programare aplicată (API) în conformitate cu cerințele ETSI TS 119 512;

**manifest de conservare:** descrierea unui obiect de date dintr-un container de conservare, referindu-se la obiectele de date de conservare sau la informații și metadate suplimentare din containerul de obiecte de conservare;

**obiect de conservare (PO):** un obiect de conservare, care este trimis, prelucrat sau preluat de la un serviciu de conservare a datelor;

**container de obiecte de conservare (POC):** un container pentru conservarea obiectelor de date, de exemplu, ASiC-S, ASiC-E sau pachete de informații OAIS;

**identificator de obiect de conservare:** un identificator unic al unui obiect de conservare; **perioada de conservare:** o perioadă de conservare are durata în care serviciul de conservare păstrează obiectele de conservare prezentate și orice dovezi asociate acestora; **profil de conservare:** un profil de conservare reprezintă un set identificat unic de detalii de implementare relevante pentru modelul de conservare și obiectivele de conservare care specifică modul în care sunt generate și validate dovezile de conservare;

**protocol de conservare:** protocol de comunicare între serviciul de conservare și client;

**schemă de conservare:** o schemă de conservare reprezintă un set de proceduri și reguli pertinente modelului de conservare și obiectivelor de conservare;

**serviciu de conservare:** un serviciu de conservare capabil să prelungească starea de valabilitate a unei semnături digitale pe o perioadă lungă de timp și/sau să furnizeze dovezi ale existenței datelor pe o perioadă lungă de timp;

**furnizor de servicii de conservare**: un furnizor care prestează un serviciu de conservare; **politica serviciului de conservare:** o politică pentru un serviciu de

conservare;

**Declarație de practică a serviciului de conservare:** o declarație de practică pentru un serviciu de conservare; **model de depozitare de conservare:** un model de depozitare (temporară, permanentă);

**transmițătorul de păstrare:** o persoană fizică sau juridică (de exemplu, clientul unei bănci) care utilizează serviciul de păstrare pentru a transmite obiectul de date;

**abonat de conservare:** o persoană fizică sau juridică (client) legată prin acord cu Zipper (de exemplu, o bancă, o companie de asigurări, o companie de utilități etc.);

**dovada existenței:** dovada existenței unui anumit obiect de date la o anumită dată/oră**; dovada marcajului temporal calificat** – marcaj temporal electronic calificat în conformitate cu articolul 3 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

**obiect de date de trimitere:** un obiect de date original furnizat de transmițător; **afirmație temporală:** un jeton cu marcaj temporal sau o înregistrare de probe;

**obiect de date de trimitere**: un obiect de date original furnizat de transmițător; afirmație de timp: un token de marcaj temporal sau o înregistrare de probe;

**nomenclatorul arhivistic** - instrument de lucru utilizat în domeniul arhivistic, care este elaborat de fiecare creator pentru organizarea și gestionarea documentelor proprii, în conformitate cu prevederile Legii Arhivelor Naționale nr. 16/1996, republicată, cu modificările și completările ulterioare;

**Păstrarea calificată pe termen lung** - serviciu calificat pentru păstrarea semnăturilor electronice calificate conform art. 34 alin. (1) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

**certificat calificat** – certificat calificat pentru semnătură electronică în conformitate cu articolul 3 alineatul (15) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

**jurnal de audit** - un registru în care sunt înregistrate toate acțiunile întreprinse asupra datelor și/sau documentelor în format electronic sau asupra sistemului propriu-zis, inclusiv informații precum data și ora acțiunii, utilizatorul implicat, tipul de acțiune (creare, modificare, ștergere etc.), precum și orice alte detalii relevante;

**Politica de păstrare a documentelor electronice** – stabilirea regulilor și procedurilor pentru păstrarea și gestionarea pe termen lung a arhivelor, inclusiv definirea perioadelor de păstrare și eliminare a documentelor în conformitate cu reglementările și politicile administratorului arhivei

**servicii de conservare cu stocare (WST)** În acest caz, datele care urmează să fie păstrate sunt stocate de serviciul de conservare, în timp ce dovezile și datele păstrate sunt livrate la cererea serviciului de conservare clientului de conservare. Serviciul de conservare stochează obiectul (obiectele) de date trimise (SubDO)) și obiectul (obiectele) de conservare (PO) și dovezile de conservare asociate. PO-urile sunt derivate din Subdo prin augmentare sau prin construirea unui container de obiecte de conservare (POC).

**Servicii de conservare cu stocare temporară (WTS)** Datele care urmează să fie păstrate sunt stocate temporar pe partea de servicii de conservare pe termen lung. Serviciul stochează temporar SubDO trimis și dovezile de conservare generate. Dovezile de conservare sunt produse sincron după primirea SubDO. Serviciul de conservare păstrează urmele acțiunilor sale pentru a putea furniza evidențe ale activităților sale.

## 6. Ancronim

**AUG** Obiectiv de augmentare

**CA** Autoritatea de certificare

**CARL** Lista de revocare a autorității de certificare

**LCR** Lista de revocare a certificatelor

**DN** Nume distins

**EUMS** Stat membru al Uniunii Europene

**OCSP** Protocol de stare a certificatului on-line

**QTSP** - Furnizor de servicii de încredere calificat;

**CSA** (Certificate Status Authority) - Autoritate de încredere pentru verificarea stării (OCSP)

**ER -** Înregistrarea probelor

**PCPP** - Politică, cod de practică și proceduri

**PO** - Obiect de conservare

**PDO** - Obiect de date de conservare

**PDS** - Păstrarea semnăturilor digitale

**PGD** - Păstrarea datelor generale

**POC** - Container de obiecte de conservare

**PRP** - Protocolul serviciului de conservare

**PRS** - Serviciu de conservare

**PSP** - Furnizor de servicii de conservare

**QC** - Certificat calificat

**QES** - Semnătură electronică calificată sau sigiliu electronic calificat

**QPS** – Serviciu de conservare calificat

**QVS** – Serviciu de validare calificat

**SubDO** - Obiect de date de trimitere

**SigS** - Serviciu de creare de semnături digitale

**TS** - Serviciu de încredere

**TL** - Lista de încredere

**TSA** - Autoritatea de marcare temporală

**TSP** - Furnizor de servicii de încredere

**UTC** - Timp universal coordonat

**ValS** - Serviciu de validare

**Zipper Services SRL** - Zipper

**WST** - serviciu de conservare cu depozitare

**WTS** - servicii de conservare cu depozitare temporară

## 6. APLICABILITATEA SERVICIULUI CALIFICAT DE CONSERVARE A SEMNĂTURILOR/SIGILIILOR ELECTRONICE CALIFICATE

Serviciul este destinat utilizatorilor care au nevoie de păstrarea pe termen lung a documentelor lor electronice sau de păstrarea pe termen lung a documentelor semnate cu semnătură electronică. Serviciul de conservare își propune să sprijine un serviciu calificat de conservare a semnăturilor/sigiliilor electronice calificate în conformitate cu Regulamentul (UE) nr. 910/2014.

Acest document tratează două aplicații principale:

1) Păstrarea pe termen lung folosind tehnici de semnătură electronică, capacitatea de a valida o semnătură electronică, capacitatea de a-i menține starea de valabilitate și capacitatea de a obține dovezi ale existenței datelor de semnătură asociate, precum și în timpul serviciului de păstrare a depunerii, chiar dacă ulterior cheia de semnătură este compromisă, valabilitatea certificatului expiră sau există un atac criptografic al algoritmului de semnătură sau al algoritmului hash utilizat în semnătură;
2) Furnizarea de dovezi ale existenței obiectelor digitale, folosind tehnici de semnătură electronică (semnături electronice, marcaje temporale, evidențe de probe).

Aceste dovezi oferă o dovadă a existenței semnăturii digitale și a datelor de validare (marcaje temporale, căi de certificare, informații de revocare), precum și o dovadă a existenței datelor semnate în cazul în care datele semnate sunt furnizate împreună cu semnătura.

Pe baza specificațiilor ETSI 119 511, datele de validare vor fi incluse într-un raport de validare, iar serviciul de conservare va utiliza un serviciu de validare a semnăturii pentru a crea un raport de validare. ETSI EN 319 102-1 definește diferite statusuri de validare (TOTAL_VALID, TOTAL_FAILED, NEDETERMINAT). În cazul în care toate datele de validare necesare nu pot fi colectate și verificate de către serviciul de validare, EN 319 102-1, clauza 5 și clauza 5.1.3 definesc modul în care trebuie utilizate stările "TOTAL-EȘEC" și NEDETERMINAT și ce informații trebuie returnate: "procesul de validare trebuie să producă informații suplimentare pentru a explica indicația TOTAL-EȘEC/NEDETERMINAT pentru fiecare dintre constrângerile de validare care au fost luate în considerare și pentru care a apărut un rezultat negativ." Dacă rezultatul validării este NEDETERMINAT SAU TOTAL_FAILED, înseamnă că serviciul de validare a concluzionat că semnătura este categoric invalidă. Serviciul de conservare nu poate accepta semnătura ca dovadă valabilă. În aceste cazuri:

- Procesul de conservare va eșua pentru acel obiect
- Serviciul de conservare:
    - Să înregistreze eșecul în evidența probelor sale de conservare,
    - Generați un raport de validare care arată rezultatul NEDETERMINAT sau EȘUAT,
    - Opriți generarea de dovezi suplimentare pentru acea semnătură/document.

## 7. Procesul de furnizare a serviciilor

### 7.1 Concepte generale

Sarcina principală a **Serviciului de conservare pe termen lung** este de a asigura valabilitatea continuă a semnăturilor electronice calificate și a sigiliilor electronice calificate aplicate pe documentele electronice.

Acest document se referă la un serviciu de încredere furnizat de Zipper în conformitate cu art. 34 și art. 40 din Regulamentul (UE) nr. 91 0/2014 și în conformitate cu legislația română aplicabilă. Politica și practica descrie toate cerințele legate de orice proceduri și tehnologii utilizate care ar putea spori fiabilitatea semnăturii/sigiliului electronic calificat în afara perioadei sale de valabilitate tehnologică. Zipper aplică cerințele, recomandările sau autorizațiile Comisiei Europene aplicabile unui serviciu de conservare calificată pe termen lung cu stocare (serviciu de conservare cu stocare) pentru păstrarea combinată a semnăturilor digitale și cu stocare temporară (serviciu de conservare cu stocare temporară) pentru orice tip de obiecte de date.

În conformitate cu articolele 34 și 40 din Regulamentul (UE) *eIDAS 2.0*, serviciul garantează că semnăturile și sigiliile rămân **valabile și verificabile** pe perioade lungi de timp, în pofida schimbărilor tehnologice, a evoluției criptografice sau a potențialei expirări/revocări a certificatelor.

Relația dintre Zipper și utilizatorul final este guvernată de Termenii și condițiile generale ale Contractului de servicii de conservare sau, după caz, de un contract de furnizare a serviciului respectiv, Termenii generali fiind o parte inseparabilă a acestora.

Prezentul PCPP definește cerințele și angajamentele serviciului de păstrare pentru menținerea valabilității pe termen lung și a valorii probatorii a documentelor electronice semnate sau sigilate.

Furnizorul (Zipper) poate specifica și limita:

- formatele semnăturilor și sigiliilor acceptate;
- orice parametri tehnici sau operaționali suplimentari.

**Subgrupuri de conservare acoperite de prezentul document:**

- Serviciu de conservare [WST] cu depozitare;
- păstrarea [PDS] a semnăturilor digitale;
- păstrarea [PGD] a datelor generale;

• [PDS+PGD] păstrarea combinată a semnăturilor digitale și a datelor generale - serviciul de conservare va extinde starea de valabilitate a semnăturilor digitale depuse și, în același timp, va furniza o dovadă a existenței celorlalte date transmise

• [AUG] Creșterea probelor de conservare depuse.

## 7.2 Participanţii

### 7.2.1 Abonați (beneficiar)

Orice persoană fizică sau juridică care are un contract cu Zipper pentru un serviciu calificat de păstrare a semnăturilor/sigiliilor electronice calificate este abonat QERDS. Abonatul/beneficiarul este solicitantul, persoana fizică sau juridică care solicită serviciul calificat de păstrare a semnăturilor/sigiliilor electronice calificate și care intră într-o relație contractuală cu ZIPPER. Abonatul va fi tras la răspundere în mod direct dacă obligațiile sale nu sunt îndeplinite corect.

Acolo unde este practic fezabil, serviciul de certificare furnizat și produsele utilizate în livrarea QERDS sunt, de asemenea, accesibile persoanelor cu dizabilități.

### 7.2.2 Părți de încredere

Părțile de încredere (terți) sunt persoane fizice sau juridice care se bazează pe dovezile furnizate de furnizor în legătură cu QERDS. În acest caz, nu sunt utilizatori QERDS.

### 7.2.3 Alți participanți

Pentru a furniza serviciul conform acestui document, Zipper nu utilizează furnizori externi de servicii de certificare calificați.

Zipper își rezervă dreptul de a încheia contracte cu părți externe pentru furnizarea anumitor servicii de certificare (de exemplu, emitenți de certificate electronice calificați), acolo unde este necesar.

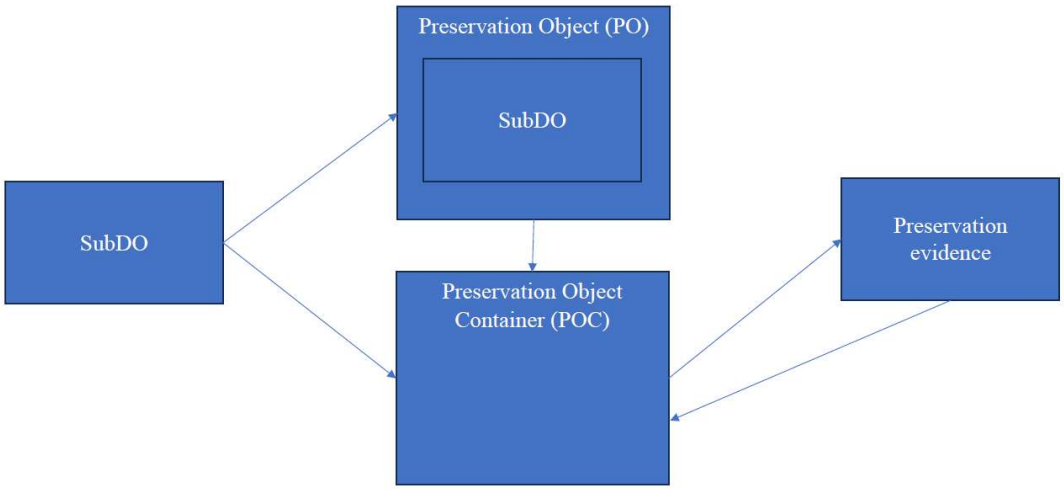
## 7.3 Perioada de conservare

În cazul unui serviciu de conservare cu depozitare [WST], perioada de conservare este durata în care serviciul de conservare păstrează obiectele de conservare (OP).

Organizațiile de producători pot consta în:

- obiectele de date transmise (SubDO) și OP-urile derivate din obiectele de date transmise prin augmentare sau
- prin construirea unui POC care să includă dovezile asociate.

Această perioadă de păstrare poate fi definită folosind o perioadă de durată (de exemplu, în lună sau ani) din momentul depunerii, de la perioadele de păstrare impuse de lege, de la un criteriu sau de la o dată.




În această perioadă, serviciul de conservare creează și îmbunătățește dovezile de conservare după cum este necesar pentru a atinge obiectivul de conservare. Modul în care sunt create dovezile se poate schimba în această perioadă, deoarece, de exemplu, certificatele expiră sau pentru că un algoritm criptografic nu mai este de încredere.

Serviciul de conservare poate utiliza surse externe de informații pentru a aprecia ce algoritmi criptografici, dimensiuni de cheie sau funcții hash nu mai sunt de încredere, de exemplu ETSI TS 119 312 și, dacă este necesar, poate emite un nou profil de conservare.

### 7.4 CERINȚE PENTRU SERVICIUL DE CONSERVARE CALIFICAT PENTRU SEMNĂTURILE/SIGILIILE ELECTRONICE CALIFICATE

*Serviciul QPSES furnizat de Zipper îndeplinește toate cerințele ETSI EN 319 401, paragraful 6.1, precum și cerințele descrise în documentul "Practica serviciilor de certificare calificate":*

> Profilurile de conservare care susțin serviciul de conservare sunt descrise în paragraful *"Profiluri de conservare*"

> Realizarea obiectivelor de conservare (PDS și PGD) este descrisă în paragraful "MODEL FUNCȚIONAL AL UNUI SERVICIU DE CONSERVARE CALIFICAT"

> Disponibilitatea SubDO și a dovezilor aferente se realizează prin controale de securitate fizice, informaționale și organizaționale, așa cum este descris în acest document;

> Organizațiile externe nu sunt implicate în funcționarea Zipper atunci când furnizează un serviciu de stocare

> Pachetele de intrare/ieșire, dovezile de stocare relevante și informațiile suplimentare necesare validării acestora sunt accesate prin utilizarea interfeței de serviciu sau prin solicitarea unei solicitări specifice de date și/sau dovezi. Acestea pot fi furnizate separat sau într-un pachet I/O care este protejat în siguranță prin criptare. În toate cazurile, acestea sunt predate numai clientului sau reprezentantului autorizat al acestuia;

> Toate informațiile privind furnizarea QPSES sunt stocate pentru o perioadă de 10 ani, în conformitate cu legislația națională. După încheierea perioadei, toate datele disponibile sunt distruse definitiv, cu excepția cazului în care s-a convenit altfel cu Abonatul;

> Zipper asigură autentificarea expeditorului;

> Trimiterea obiectelor de date este securizată de dovezi ștampilate cu marcajul temporal electronic al Evrotrust într-un mod care exclude orice posibilitate de modificare neobservată a obiectului de date;

> disponibilitatea, integritatea și confidențialitatea obiectelor de date este garantată de Zipper;

## 7.5 MODEL FUNCȚIONAL AL UNUI SERVICIU DE CONSERVARE CALIFICAT

### 7.5.1 Servicii de conservare cu depozitare [WST]

În acest caz, datele care urmează să fie păstrate sunt stocate de serviciul de conservare, în timp ce dovezile și datele păstrate sunt livrate la cerere de către serviciul de conservare clientului de conservare.

Serviciul de conservare stochează obiectul (obiectele) de date trimise (SubDO)) și obiectul (obiectele) de conservare (PO) și dovezile de conservare asociate.

OP (OP) sunt derivate din subdo (subdo):

- prin augmentare sau
- prin construirea unui container de obiecte de conservare (POC).

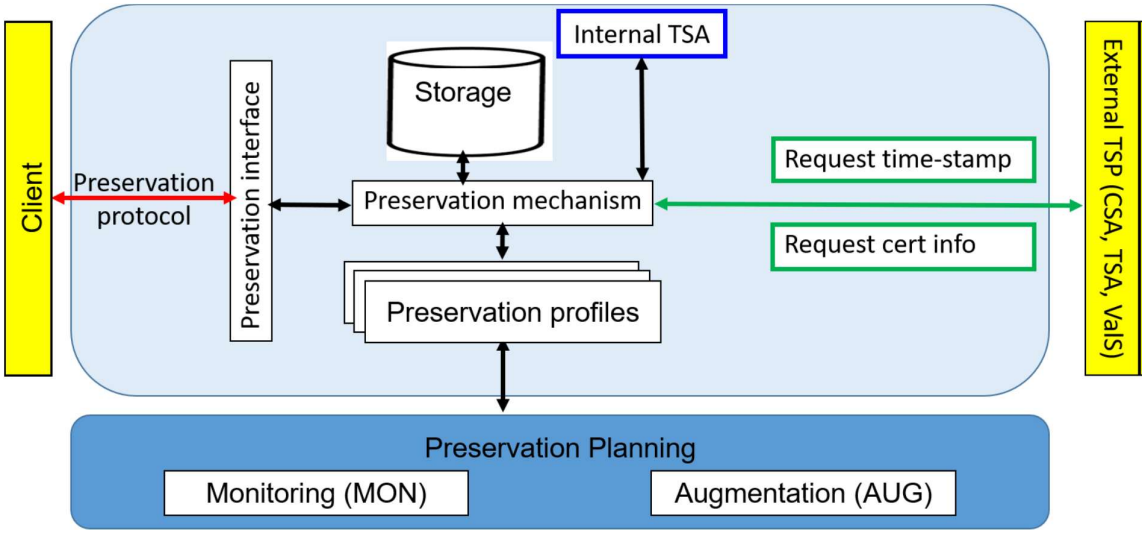



Figura: Serviciu de conservare pe termen lung cu depozitare

Solicitantul (abonatului) furnizează sistemului unul sau mai multe obiecte de date de conservare, iar serviciul de conservare trimite înapoi un identificator unic al obiectului de conservare. Apoi, în timpul perioadei de păstrare, solicitantul poate extrage la cerere una sau mai multe probe de conservare și/sau obiecte de conservare. Serviciul de conservare calificat oferă posibilitatea de a șterge orice obiecte de date păstrate, în conformitate cu legislația națională. În cazul ștergerii probelor de conservare, subsistemele respective le șterg, de asemenea, dar serviciul de conservare păstrează dovezile de conservare până la sfârșitul perioadei de conservare.

#### 7.5.1.1 Declarație de practică legată de serviciul ePreservation (eArchiving) oferit de Zipper

Fluxul de conservare/arhivare constă în:

1. Descărcarea documentului și a metadatelor asociate din arhiva operațională în aplicația RepoZip LTa în modul convenit (hot folder FTP, API). Ex. aplicația de arhivă operațională va apela, prin webservice, solicitarea de încărcare a unui document și a metadatelor asociate în arhivă.

2. În funcție de tipul documentului, RepoZip face asocierea la nomenclatorul arhivistic al companiei utilizatore și completarea metadatelor obligatorii (în baza legislației române).

3. Aplicația verifică automat semnătura electronică a documentului. Semnătura/sigiliul emitentului oficial al documentului trebuie să fie valabil și întocmit cu un certificat calificat.

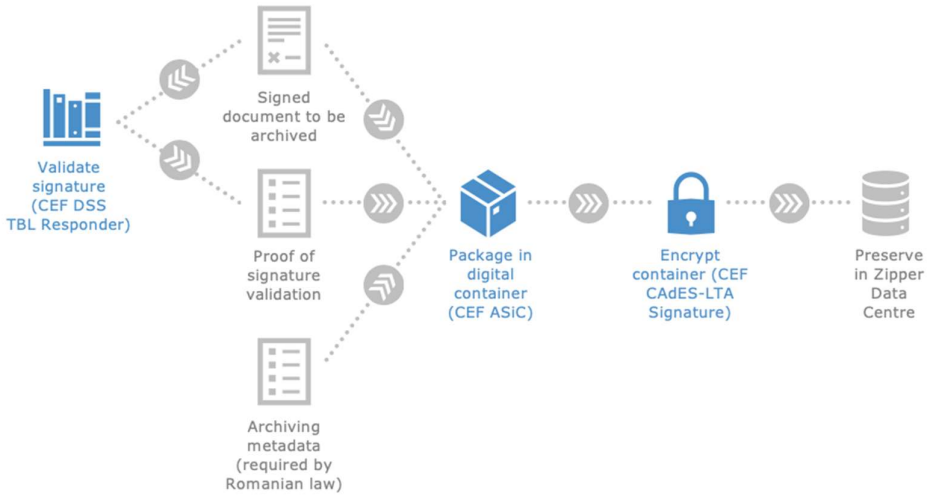
4. Generați un raport de validare bazat pe ETSI EN 319 102-1, folosind QVS Zipper 'qualified validation service' (verifică starea certificatului, revocarea, profilul de semnătură, algoritmii etc.). Raportul de validare este semnat cu un sigiliu electronic calificat (emis pentru Zipper) și TS calificat încorporat.

- QVS returnează un raport de validare (VR), semnat/sigilat digital de QVS, afirmând rezultatul în acel moment.

5. Validarea va avea ca rezultat o stare TOTAL_FAILED OT TOTAL_PASSED, NEDETERMINATĂ, pe baza regulilor de constrângere Zipper.

6. Doar documentul electronic TOTAL_PASSED și NEDETERMINAT (NO-POE) va fi acceptat în arhivă pentru a fi păstrat. Un container ASIC-E este creat și este contrasemnat/sigilat de către administratorul arhivei (Zipper) folosind un certificat electronic calificat. Semnătura aplicată pe ASIC va asigura disponibilitatea și integritatea pe termen lung a materialului de validare (ER).

7. Aplicația de arhivare RepoLTA va menține păstrarea stării de valabilitate a semnăturii digitale (semnătură la nivel LTA) aplicată pe fișierul ASIC. Această operațiune se va face pentru fișierele ASIC, înainte ca marcajul de timp calificat aplicat să expire sau să existe probleme de securitate criptografică.




În cazul unui IMPORT reușit în arhivă:

1. Documentul electronic va primi un act de identitate unic (IDDoc/POID) pentru identificare în arhivă. Metadatele create automat sunt generate (de exemplu, timp de arhivare, utilizator)

2. Containerul de documente "Container de semnături asociat" este creat, stocat într-un format ZIP (extensie .asic), conform ETSI TS 102 918 V1.3.1. Containerul va conține pdf-ul original primit, metadatele primite, raportul de validare, conform ETSI EN 319 102-1

3. Se contrasemnează cu semnătura electronică a administratorului arhivei electronice și se aplică marca temporală calificată, containerul CAdES creat va avea nivelul B-LTA.

"Dosarul electronic" atașat fiecărui document arhivat va conține cel puțin următoarele informații:

Primit de la beneficiar:

a) proprietarul documentului în format electronic.

a) emitentul documentului în format electronic.

b) titularul dreptului de a dispune de document.

c) data emiterii documentului.

d) tipul de document în format electronic.

e) nivelul de clasificare a documentului în format electronic.

f) cuvinte-cheie necesare identificării documentului în format electronic.

g) perioada de păstrare a documentului (poate fi calculată în raport cu un metadat/cuvânt cheie).

h) elemente de amplasare a suportului fizic; - dacă este necesar.

Generat automat în aplicația de arhivare (după momentul arhivării electronice):

Generat de Archiver:

i) identificatorul unic al documentului în format electronic, în cadrul arhivei electronice.

j) data arhivării (data introducerii în arhivă).

k) formatul digital în care documentul este arhivat în format electronic.

l) istoricul documentului în format electronic.

m) dimensiunea documentului arhivat

Pentru a preveni accesul neautorizat al utilizatorilor, controlul accesului se realizeaza prin restrictii impuse, prin reguli de acces la documentele din arhiva. Verificarea integrității documentelor arhivate este asigurată de faptul că acestea sunt semnate de titularul dreptului de dispoziție și contrasemnate de administratorul arhivei. Verificarea integrității se face de către agenții automatizați ai sistemului de arhivare pe baza semnăturii aplicate tuturor documentelor introduse în RepoZip.

Dacă un document nu îndeplinește criteriile de integritate, acesta este marcat automat și nu poate fi arhivat. După corectare, va trebui reintrodus în sistem și, dacă trece cu succes validările, va fi arhivat.

Sunt înregistrate toate operațiunile efectuate pe arhiva electronică, înregistrările de audit care conțin data și ora evenimentului, tipul evenimentului, rezultatul (succes sau eșec) al evenimentului.

Accesul la sistemul de arhivare electronică RepoZip se realizează prin linii de comunicare securizate între Beneficiar și Furnizor (Servicii Zipper). Accesul la documentele arhivate este restricționat, un

utilizator poate prelua un document arhivat doar dacă face parte din grupul de acces stabilit de participant pentru a accesa documentul și are nivelul de securitate adecvat pentru a putea vizualiza documentul.

Modulul de verificare și semnătură a arhivatorului utilizează DSS de semnătură electronică pentru a valida mai întâi semnătura electronică a documentului primit, înainte ca documentul să fie aprobat pentru arhivare.

- Verificați dacă semnătura este calificată și ce tip de certificat a fost utilizat. Beneficiarul va fi responsabil pentru semnarea documentelor folosind un certificat calificat furnizat de un QTSP (furnizor de servicii de încredere calificat). Dacă semnarea este externalizată, aceasta trebuie făcută de un QTSP, care oferă semnare QTS (servicii de încredere calificate). Certificatele digitale AdES sunt acceptate (conform ETSI TR 119 112 V1.1.1 (2019-04) și ETSI EN 391 102-1 [i.6]) de tipul:

-> semnătură de bază (ex. CAdES-B, PAdES-B etc.)

-> Semnătură cu timp (de exemplu, CAdES-T, PAdES-B-T etc.)

-> semnături cu material de validare pe termen lung. Ex. CAdES-X, PAdES-B-LT

-> Semnături care asigură disponibilitatea și integritatea pe termen lung a materialului de validare (ex. CAdES-X-L, PAdES-B-LTA, PADES-E-LTV etc.)

Pașii de verificare sunt:

A) certificatul X.509 pentru semnătura electronică aplicată documentului de către titularul dreptului de dispunere este verificat prin:

-> comparație hash pentru integritatea documentelor;

-> certificate de cheie publică (PKC) utilizate

-> Informații despre starea revocării pentru fiecare listă de revocare a certificatelor (CRL) sau stare a certificatului (OCSP)

-> "Afirmație de timp" aplicată semnăturii (dacă există)

- Documentul care urmează să fie arhivat este apoi ambalat într-un container digital împreună cu dovada validării semnăturii, precum și alte metadate care detaliază procesul de arhivare, conform legislației române.

- În pasul următor, containerul este criptat pentru a proteja integritatea. Criptarea are loc prin aplicarea unei semnături de arhivare pe termen lung (numită și semnătură la nivel LTA) cu un furnizor de marcaj temporal calificat.

- Modulul Data Container Creation and Encryption (ASIC) se bazează, de asemenea, pe specificațiile eSignature DSS: profilul de bază ASiC (Associated Signature Container) pentru container și CMS Advanced Electronic Signature (CAdES) pentru criptare.

- ASIC: "Container de semnătură asociat" în conformitate cu ETSI TS 102 918 V1.3.1. Containerul va conține pdf-ul original primit, PDF-ul de verificare (punctul b), metadatele primite, datele de identificare a semnăturii.

Serviciul Zipper eArchiving arhivează containerele de obiecte de conservare, așa cum este descris în Politica de arhivare electronică Zipper.

POC conține:

- Obiecte de conservare (PO) — datele care trebuie păstrate. Acestea puteau fi doar date semnate
- Date de probă, validare și revocare / stare - date necesare pentru validarea semnăturilor, marcajelor temporale, căilor de revocare / valabilitate a certificatelor și, eventual, rapoarte de validare. Acestea sunt esențiale pentru a se asigura că, în viitor, starea de valabilitate (sau invaliditatea) semnăturilor poate fi reconstruită.
- Metadate despre POC în sine: identificatori (de exemplu, proprietarul documentului), marcaje temporale, valori hash, sume de control etc. Acest lucru susține integritatea, trasabilitatea, capacitatea de a verifica dacă recipientul nu a fost modificat și ajută la reconstruirea dovezilor.

**Containerul POC Zipper** are următoarele specificații:

- **Format**: Recipient ASiCE
- **Conținut: Documente** semnate + semnături + raport de validare (XML semnat) + evidențe de evidență
- **Nivel de semnătură**: BLTA (Linie de bază cu validare pe termen lung și marcaje temporale de arhivare)
- **Certificat de semnare**: Certificat calificat pentru sigiliu electronic emis de un QTSP [Furnizor] de la TL, emis către *Zipper Services*
- **Marcaj temporal**: Marcaj temporal calificat (QTS) furnizat de Zipper QTS (vezi https://pki.ca.ezipper.ro/repository/certs.php)
- **Datele de validare au inclus:** Certificate, informații de revocare (CRL-uri/OCSP) printr-un raport de validare emis de Zipper QVS.
- **Scop:** Serviciul de conservare asigură că semnătura și obiectele asociate sunt verificabile pe

termen lung, în conformitate cu cerințele ETSI TS 119511 și eIDAS.

Zipper va păstra POC-ul extinzându-l în timp:

[**Client**] → *Zipper Creează POC inițial* (nivel ASiC-E, B-LTA) → [**Serviciu de conservare** PDS+PGD+WST] -> *Validați prin SVS* → *Colectați date de validare > Generați dovezi de conservare-> Stocați POC extins (+ dovezi) cu =>* [**Serviciu de conservare-AUG] (nivel A-E, B-LTA)**

↓

*Recuperare PO* / Audit / Verificare

### 7.6 Obiective de conservare

Serviciul de conservare pe termen lung urmărește obiective distincte, dar complementare, care pot fi utilizate separat sau în combinație:

1. **Păstrarea generală a datelor (PGD)**
    - Furnizarea de dovezi ale existenței pe termen lung a unui obiect electronic de date
2. **Păstrarea semnăturii digitale/sigiliului (PDS)**
    - Asigurați-vă că semnăturile și sigiliile electronice rămân valide, verificabile și fiabile din punct de vedere juridic pentru perioade lungi de timp
    - Păstrați dovada existenței și a stării de valabilitate a datelor semnate sau sigilate asociate
    - Păstrați semnăturile/sigiliile verificabile și fiabile din punct de vedere juridic chiar și după expirarea certificatelor sau slăbirea algoritmilor criptografici
3. **Augmentare (AUG)**
    - Efectuați **re-marking periodic** atunci când algoritmii sau certificatele se apropie de sfârșitul duratei de viață
    - [WST]: În timpul perioadei de conservare, serviciul de conservare trebuie să se asigure că dovezile de conservare pot fi utilizate pentru a atinge obiectivul de conservare corespunzător

- [WTS]: În timpul perioadei de păstrare a probelor, serviciul de conservare se asigură că probele de conservare pot fi utilizate pentru a atinge obiectivul corespunzător de conservare
- NOTA 1: Acest lucru poate fi pus în pericol în cazul în care un algoritm criptografic nu mai poate fi de încredere sau informațiile de revocare nu mai pot fi primite
- [WST] [WTS]: Serviciul de conservare va spori dovezile de conservare înainte ca acestea să nu mai poată fi utilizate pentru a atinge obiectivul corespunzător de conservare
    - În cazul unei semnături digitale, augmentarea se poate face prin încorporarea la o semnătură digitală a informațiilor pentru a menține validitatea acelei semnături, deoarece există, de exemplu, marcaje temporale, date de validare etc.
    - În cazul unei înregistrări de dovezi, augmentarea se poate face prin reînnoirea marcajului de timp sau reînnoirea arborelui hash conform IETF RFC 6283 sau IETF RFC 6283
- [AUG] se efectuează numai în combinație cu PGD sau PDS

### 7.7 PACHETE DE DATE DE EXPORT-IMPORT

Zipper permite utilizatorilor serviciilor de conservare să solicite pachete de export-import cu date stocate, dovezi și toate informațiile necesare pentru validarea dovezilor. Pachetele de export-import pot fi utilizate pentru a muta datele stocate de la un serviciu de conservare la un alt serviciu de conservare. Zipper a utilizat formatul pachetului de export-import descris în ETSI TS 119 512.

Serviciul de conservare ține evidența tuturor pachetelor de export-import eliberate, inclusiv:

- Data evenimentului
- Criteriile care au fost utilizate pentru a selecta setul de obiecte de conservare care urmează să fie incluse în pachetul de export-import.

În cazul WST, pachetele de export Zipper cu dovezile de conservare produse în modul descris sunt informațiile incluse într-un format de arhivă al unei semnături AdES.

În cazul obiectelor arhivate, formatul de export va fi un format standardizat (Associated Signature Container Extended (ASiC-E) conform ETSI EN 319 162-1 -clauza 4.4).

Coletele de export sunt furnizate numai unei persoane fizice sau juridice autorizate.

### 7.8 PROTOCOALE OPERAȚIONALE DE CONSERVARE

Protocolul de conservare permite clientului de conservare să interacționeze cu interfața de conservare. Canalul de comunicare dintre utilizatorul serviciului de conservare și QPSES este securizat, adică Zipper asigură securitatea autentificării și confidențialității utilizatorului în conformitate cu cerințele ETSI TS 119 512. Protocolul utilizat este protejat împotriva utilizării neautorizate.

QPSES permite ca unul sau mai multe obiecte de date (SubDO) să fie stocate sub un profil de conservare specific prin preluarea fie a unui identificator de obiect de conservare, fie a unei dovezi de conservare (mod sincron). Identificatorul obiectului de conservare poate fi utilizat ulterior pentru a prelua obiecte PO și / sau pentru a urmări sau șterge OP-uri sau pentru a actualiza containerele de obiecte de conservare (mod asincron), așa cum este definit în ETSI TS 119 512.

Serviciul de conservare pe termen lung permite recuperarea probelor și/sau a obiectelor de conservare (OP). OP-urile pot conține dovezi (RetrievePO), astfel cum sunt definite în ETSI TS 119 512.

Serviciul permite ștergerea OP-urilor stocate. Dacă dovezile sunt șterse, SubDO este, de asemenea, șters. QPSES asigură că OP-urile stocate pot fi șterse numai înainte de sfârșitul perioadei de păstrare când este trimisă cererea de ștergere (împreună cu justificarea corespunzătoare). Fiecare justificare furnizată este înregistrată împreună cu informații despre cererea de ștergere (DeletePO), astfel cum este definită în ETSI TS 119 512.

QPSES permite necesită un set de identificatori de obiecte din stocarea datelor, care pot fi utilizați pentru a prelua sau șterge comenzi.

### 7.9 POLITICA DE CONSERVARE A DOVEZILOR

Înregistrarea de dovezi este o structură care leagă valorile hash ale documentelor semnate sau semnăturilor cu marcaje temporale de arhivă. Dovezile Zipper QPSES includ un token de marcaj temporal care este conform cu IETF RFC3161 și versiunea actualizată RFC 5816. QPSES utilizează o marcă temporală electronică care se potrivește cu protocolul de marcare temporală utilizat și profilul tokenului de marcare temporală, așa cum este definit de ETSI EN 319 422.

Probele **de conservare** constau în:

- Arhivați marcaje temporale - CAdES-(LT)A, XAdES-(LT)A, PAdES-LTA cu indici hash criptografici (cum ar fi ats-hash-index-v3 pentru CAdES)
- **Rapoarte de validare** generate atunci când semnătura/sigiliul a fost verificat cu certificate, CRL-uri/OCSP-uri utilizate în timpul validării
    - Zipper QSP, peste QVS creează raportul de validare care este conform cu ETSI EN 319

102-1 ca document XML definit de ETSI TS 119 102-2. Raportul de validare conține următoarele elemente despre semnătura electronică validată:

- Element de raport de validare a semnăturii, care conține starea generală de validare a semnăturii pentru semnătură, precum și informații suplimentare privind validarea semnăturii efectuată (clauza 4.3).
- Elementul obiectelor de validare a semnăturii, care conține materialele colectate în timpul procedurii de validare, cum ar fi CRL-urile, ancorele de încredere, răspunsurile OCSP etc. și dovada existenței în cel mai timpuriu moment al existenței obiectului (clauza 4.4.)
- Elementul de informații al validatorului, care identifică entitatea care validează semnătura. (clauza 4.5.)
- Semnătura raportului de validare, care conține semnătura raportului de validare. (clauza 4.6.)

**Raportul de validare calificat** va fi stocat asociat cu pachetul de dovezi de conservare, deoarece dovedește că **la un moment dat**, semnătura/sigiliul a fost valabil conform eIDAS, conține întregul context de validare (algoritmi, lanțuri de certificate, stare de revocare) și reduce povara revalidării în viitor - serviciul de validare oferit de Zipper QVS marcă timp QVR în sine pentru a-i garanta integritatea.

*Evidenta dovezilor*

Zipper QPSES a implementat o dovadă de evidenta este în conformitate cu IETF RFC 6283 (MerkleTree).

Generarea de înregistrări de dovezi: Această înregistrare oferă dovezi criptografice că un set de obiecte de date a existat și au rămas neschimbate de la ora marcajului de timp.

Procesul de construire a înregistrării de dovezi implică calcularea hash-urilor pentru obiectele de date, construirea unui arbore hash și obținerea unui marcaj de timp pe rădăcină. De asemenea, implică repetarea reînnoirilor/re-marcării temporale în timp, pe măsură ce puterea criptografică se degradează sau certificatele expiră.

*Verificare*: Având în vedere o înregistrare de dovezi, abonatul poate verifica dacă un obiect de date a existat la un moment dat, urmărind arborele hash, marcajul temporal și lanțul de probe, verificând toți pașii criptografici. Această dovadă poate fi vizualizată pe aplicația RepoZip (MerkleTree proof).

Verificarea implică:

- Recalcularea arborelui hash pentru datele originale.

- Verificarea marcajului temporal RFC 3161 utilizând lanțul de certificate al TSA
- Verificarea faptului că fiecare etapă de reînnoire (dacă există) este valabilă și în concordanță cu dovezile anterioare

Formatul/canonizarea înregistrării de dovezi este XML (cu TimeStamp):

Ierarhia structurii XMLERS arată astfel:

(spațiul de nume XML RFC 6283=> urn:ietf:params:xml:ns:ers):

```
EvidenceRecord  (Version="1.0")
|
└── ArchiveTimeStampSequence
    |
    └── ArchiveTimeStampChain (Order="1")
        |
        ├── DigestMethod
        |     └── @Algorithm = "http://www.w3.org/2001/04/xmlenc#sha256"
        |
        ├── CanonicalizationMethod
        |     └── @Algorithm = "http://www.w3.org/2001/10/xml-exc-c14n#"
        |
        └── ArchiveTimeStamp (Order="1")
              |
              ├── HashTree
              |     ├── Sequence (Order="1")
              |     |     └── DigestValue (base64)
              |     ├── Sequence (Order="2")
              |     |     └── DigestValue (base64)
              |     ├── ...
              |     └── Sequence (Order="8")
              |           └── DigestValue (base64)
              |
              └── TimeStamp
                    └── TimeStampToken
                          ├── @Type = "RFC3161"
                          └── [Base64-encoded timestamp token]
```

*Stocare*: Înregistrarea de dovezi este stocată separat de obiectul de date și este corelată cu ObjectId (PreservationObjectId).

Această politică este listată în profilul de conservare, care o face cunoscută utilizatorilor QPSES și terților.

*Zipper QPSES a implementat o dovadă de înregistrări este în conformitate cu **IETF RFC 6283***.

Această politică este listată în profilul de conservare, care o face cunoscută utilizatorilor QPSES și terților.

### 7.9.1 Durata preconizată a probelor se aplică pentru un serviciu de conservare

Pe baza ETSI EN 319 401, punctul 4.4, durata preconizată a probelor este o durată în care sau o dată până la care serviciul de conservare se așteaptă ca o dovadă de conservare să poată fi utilizată pentru

atingerea obiectivului de conservare. Aceasta înseamnă că dovezile de conservare pot fi verificate în continuare și oferă protecție criptografică. Pentru mai multe formate de dovezi de conservare, de exemplu înregistrări de dovezi sau semnături AdES de arhivă, este suficient să se poată **valida cu succes cea mai recentă marcă temporală a întregii dovezi de conservare**.

Pentru dovezile de conservare generate folosind tehnici de semnătură digitală, trebuie luate în considerare mai multe durate:

1) perioada de valabilitate a cheii private, adică perioada de timp prestabilită în care cheia privată poate fi utilizată pentru a genera dovezi, cu excepția cazului în care certificatul asociat a fost revocat din orice motiv;

2) perioada de valabilitate a certificatului;

3) durata în care sunt gestionate cererile de revocare a certificatului, adică un certificat poate fi revocat;

4) durata în care informațiile privind revocarea rămân disponibile;

5) durata în care funcțiile hash sunt rezistente la atacurile de coliziune; și

6) durata în care cheia publică este rezistentă la atacurile criptografice. Pentru certificatele cu cheie publică conforme cu IETF RFC 5280, certificatul poate fi revocat numai în perioada de valabilitate a certificatului. Pentru certificatele cu cheie publică conforme cu IETF RFC 5280, informațiile de revocare sunt disponibile cel puțin până la sfârșitul perioadei de valabilitate a certificatului. Cu toate acestea, o autoritate de certificare poate furniza informații de revocare și după expirarea unui certificat. EXEMPLU: Pentru certificatele calificate, astfel cum sunt definite în Regulamentul (UE) nr. 910/2014, informațiile privind revocarea sunt furnizate după perioada de valabilitate a certificatului, a se vedea articolul 24 punctul 4 din Regulamentul (UE) nr. 910/2014.

O dovadă generată folosind aserțiuni de timp (marcaje temporale sau înregistrări de dovezi) trebuie validată prin construirea unei căi de certificare până la o ancoră de încredere.

O dovadă de conservare poate fi validată atâta timp cât:

1) niciunul dintre certificatele din calea de certificare nu a fost revocat din motivul "compromis cheie";

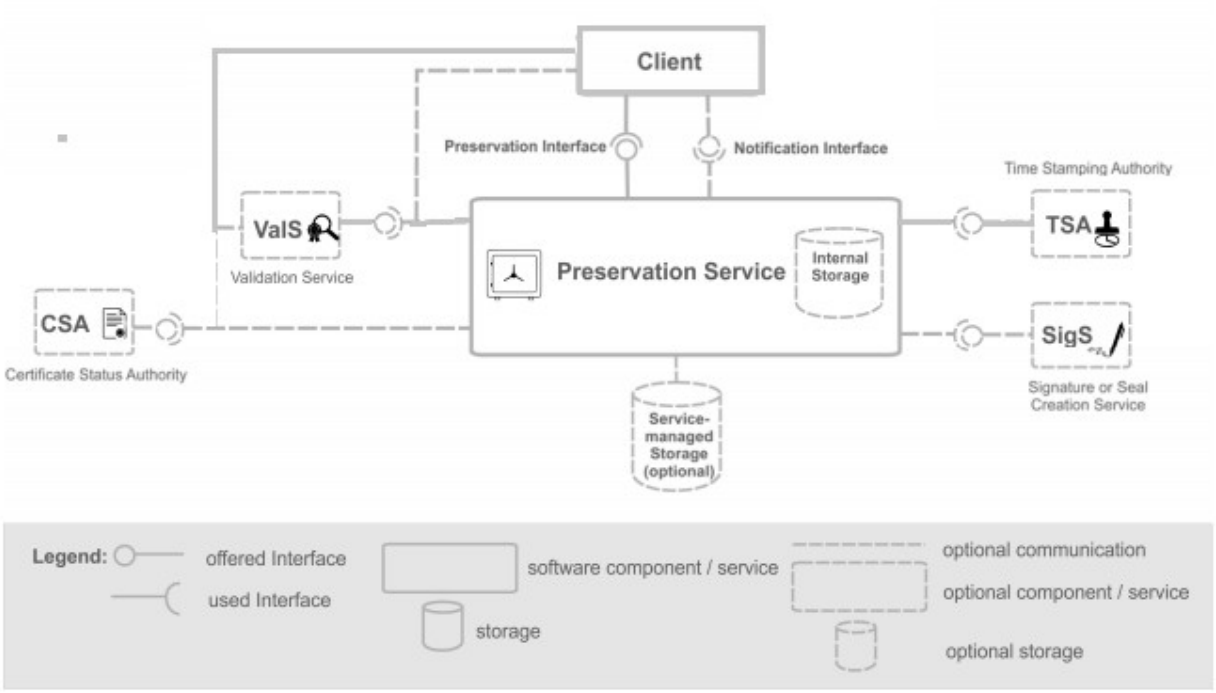
2) nicio cheie publică prezentă în datele de validare nu este supusă atacurilor criptografice; și

3) niciuna dintre funcțiile hash utilizate în datele de validare nu este supusă atacurilor de coliziune.

Punctul 1) poate fi verificat atâta timp cât sunt disponibile informații despre revocare. Dacă cheia privată și toate copiile de rezervă ale acesteia sunt efectiv distruse la sfârșitul perioadei de valabilitate

a cheii private, atunci singura modalitate de a compromite cheia privată va fi efectuarea unui atac criptografic de succes asupra cheii publice corespunzătoare sau asupra uneia dintre funcțiile hash utilizate. Durata preconizată a dovezilor reflectă o estimare a unei date pentru rezistența atât a algoritmilor de semnătură digitală, cât și a funcțiilor hash utilizate în datele de validare pentru ultimele dovezi de conservare. Perioada de valabilitate tehnologică corespunde unei perioade de timp în care o semnătură sau o dovadă poate fi validată și de încredere. Depinde de momentul în care calea de certificare poate fi verificată și până când algoritmii criptografici hashing și semnătura pot fi de încredere. Perioada de valabilitate tehnologică a semnăturii este similară cu durata preconizată a probelor de conservare bazate pe tehnici de semnătură digitală.

### 7.10 ARHITECTURA SISTEMULUI




Serviciul calificat de conservare definit în prezentul document oferă interfața de conservare așa cum este specificat în clauza 5 și utilizează Zipper Time-Stamping Authority (TSA), care emite marcaje temporale calificate conform ETSI EN 319 422. Serviciul utilizează un serviciu de validare calificat (QValS) (a se vedea ETSI TS 119 441 și ETSI TS 119 442) pentru a colecta informații despre calea de certificare și informații despre revocare sau pentru a colecta direct informații despre calea de certificare și pentru a colecta informații despre starea certificatului emise de o autoritate de stare a certificatului

(CSA).

Serviciul de conservare calificat elaborat de Zipper oferă interfețe pentru accesul la resursele sistemului sau la serviciile externe. Serviciul calificat de conservare pe termen lung folosește propriul spațiu de depozitare sub controlul Zipper. Serviciul are scopul de a păstra datele generale și de a asigura dovezi ale trimiterii obiectului de date.

Perioada în care serviciul de conservare calificat păstrează obiectele de date transmise și orice dovezi de păstrare aferente acestora prin validarea și îmbunătățirea fiabilității semnăturii electronice calificate dincolo de starea de valabilitate tehnologică sau aplicarea unei marcaje temporale, este de 10 (zece) ani și apoi sunt șterse definitiv de sistem.

În această perioadă, serviciul de conservare calificat generează și extinde dovezile de conservare necesare pentru atingerea obiectivului de conservare. Metoda de creare a dovezilor se poate schimba în această perioadă din motive, de exemplu, expirarea certificatelor sau pentru că algoritmul criptografic nu mai este fiabil.

Zipper se informează permanent cu privire la standardele ETSI (în special TS 119 312) publicate pe site-ul Comisiei Europene pentru a evalua care algoritmi criptografici, dimensiuni ale cheilor sau funcții hash probabil nu mai sunt fiabile și, dacă este necesar, emite un nou profil de conservare.

### 7.11 Schema de conservare

Schema de conservare detaliază cadrul procedural și bazat pe reguli utilizat pentru crearea și validarea dovezilor de conservare și descrie abordările și metodele generale utilizate pentru a menține integritatea și accesul la date în timp.

Un serviciu de conservare în domeniul de aplicare al acestui document poate sprijini mai multe scheme de conservare. Schema de conservare definește abordarea conceptuală generală pentru conservarea pe termen lung.

- Fiecare schemă trebuie să sprijine cel puțin un obiectiv de conservare
- Fiecare schemă funcționează în cadrul unui singur model de stocare

***Formate acceptate pentru intrare***

- semnătura digitală CAdES conform ETSI EN 319 122;
- semnătura digitală XAdES conform ETSI EN 319 132;
- semnătura digitală PAdES conform ETSI EN 319 142;

***Generarea și validarea dovezilor de conservare***

Schema de conservare actuală mărește semnătura corespunzătoare formatului de semnătură, care sunt anunțate în elementul Profile/EvidenceFormat cu următoarele URI-uri:

- http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3 conform ETSI EN 319 122-1
- http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp conform ETSI EN 319 132
- http://uri.etsi.org/ades/PAdES/document-time-stamp conform ETSI EN 319 142

Notă: ETSI EN 319 122-1 definește id-aa-ets-archiveTimeStampV3 (înregistrează în mod explicit ce elemente sunt marcate cu timp). În cazul semnăturilor CadES, pentru a sprijini arhivarea pe termen lung, informațiile vor apărea în interiorul SignerInfo.unsignedAttrs cu atributul digestAlgorithm și ats-hash-index-v3 și timeStampToken real (un TST compatibil cu RFC 3161).

Serviciul de conservare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă la semnătură și o protejează cu un marcaj temporal corespunzător formatului specific de semnătură.

Serviciul de conservare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnologiei.

Nivelul de semnătură aplicat (pentru PadES, CadES, XadES) va fi nivelul B-LTA, care prevede cerințe pentru încorporarea token-urilor time-stamp care permit validarea semnăturii mult timp după generarea acesteia. Acest nivel își propune să abordeze disponibilitatea și integritatea pe termen lung a materialului de validare. Acest nivel este adecvat în cazul în care valabilitatea tehnică a semnăturii trebuie păstrată pentru o perioadă de timp după crearea semnăturii, în cazul în care expirarea certificatului, revocarea și/sau obsolescența algoritmului reprezintă motive de îngrijorare. Nivelul B-LTA vizează disponibilitatea și integritatea pe termen lung a materialului de validare a semnăturilor digitale. Nivelul B-LTA poate ajuta la validarea semnăturii dincolo de multe evenimente care îi limitează validitatea (de exemplu, slăbiciunea algoritmilor criptografici utilizați sau expirarea datelor de validare). Utilizarea nivelului B-LTA este considerată o tehnică adecvată de conservare și transmitere a datelor semnate.

**Dovezile sunt incluse în semnătură. Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare.**

Notă: Politica de creare a dovezilor de conservare aplicată și o politică de validare a dovezilor de conservare sunt anunțate în elementul Profil/Politică aplicabil cu Tip egal cu următorul URI: http://uri.etsi.org/19512/policy/preservation-evidence

### 7.12 Profil de conservare

Un profil de conservare este implementarea concretă, tehnică a unei scheme de conservare. Profilurile de conservare detaliază aspectele de implementare ale conservării și specifică modul în care dovezile de conservare sunt generate, gestionate și validate în funcție de schema pe care o urmează.

Elementul Profile descrie aspectele tehnice ale unui profil de conservare care permit unui client să utilizeze interfața de conservare pentru a comunica cu QPresS.

- Un profil de conservare trebuie identificat în mod unic
- Dacă ținta de conservare este PDS, profilul de conservare se referă la informații legate de politici care abordează aspecte ale dovezilor de creare și validare și validare a semnăturii.
- Dacă ținta de conservare este PGD, datele primite de la client vor fi semnate de QPresS și apoi se vor aplica elementele definite în profilurile de conservare echivalente definite pentru ținta de conservare PDS.

| **Schema/Obiectivul de conservare** | **Focar** | **Model de depozitare** | **Înregistrări de conservare** |
|---|---|---|---|
| PGD+AUG | Accentul este pus pe *existență și integritate*, nu pe semnături<br>**Înregistrare de dovezi bazată pe marcaje temporale** (de exemplu, ERS – Sintaxa înregistrării de dovezi, RFC 6283 / RFC 6283) | WST | **Marcajul temporal al documentului** aplicat asupra obiectului de date sau a unei **înregistrări de dovezi de container** |
| PDS+AUG | Asigură nu numai existența, ci și dovada valabilității la momentul semnării | WST | **Formulare de arhivare PAdES/XAdES/CAdES cu LTV + marcaje temporale ale documentului** (dovada validității semnăturii) aplicate pe întregul |

| | | | |
|---|---|---|---|
| | | | document semnat sau lanțuri de marcaj temporal de arhivă. |

Se aplică cerințele specificate în ETSI EN 319 401, clauza 7.5.

În plus, următoarele cerințe speciale se aplică pentru gestionarea cheilor utilizate pentru generarea și validarea dovezilor:

- PSP se asigură că marcajele temporale utilizate în procesul de conservare provin de la o TSA care urmează practicile de ultimă generație pentru cerințele de politică și securitate pentru furnizorii de servicii de încredere care emit marcaje temporale. În special, TSA ar trebui să fie conformă cu ETSI EN 319 421 și, în contextul UE, profilurile de conservare pot utiliza TSA calificate.
- PSP ar trebui să utilizeze numai în procesul de conservare marcaje temporale care pot fi verificate folosind CRL-uri sau răspunsuri OCSP care includ un "cod de motiv" în cazul revocării unui certificat cu cheie publică.
- Atunci când PSP semnează (o parte din) o probă de conservare, PSP ar trebui să selecteze un certificat de semnare emis de o autoritate de certificare de încredere care implementează ETSI EN 319 411-1 sau ETSI EN 319 411-2.
- Atunci când PSP semnează (o parte din) o probă de conservare, cheia de semnare privată a PSP trebuie păstrată și utilizată într-un modul criptografic care este un sistem de încredere care este asigurat la EAL 4 sau o versiune ulterioară în conformitate cu ISO/IEC 15408 sau cu criterii de evaluare echivalente recunoscute la nivel național sau internațional pentru securitatea IT.
- Atunci când PSP semnează (o parte din) o probă de conservare, dispozitivul criptografic securizat necesar

**Valabilitatea pe termen lung a ASiC-E**

Pe baza ETSI EN 319 162-1 și ETSI TS 102 918 V1.3.1, valabilitatea pe termen lung a ASiC-E este obținută pentru diferitele tipuri de containere, după cum urmează:

1) Pentru un container ASiC-E cu semnături XAdES, mecanismele specificate în standardele de bază și extinse ale semnăturilor XAdES ETSI EN 319 132-1 și ETSI EN 319 132-2 sau specificația de

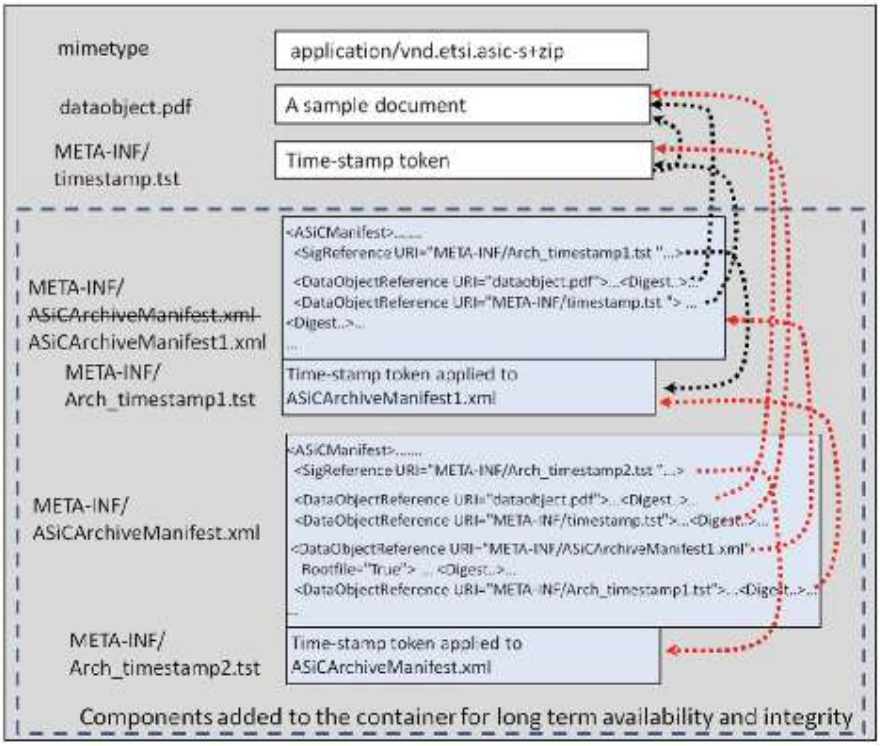
înregistrare a dovezilor IETF RFC 6283 și IETF RFC 6283 vor fi utilizate pentru obținerea validității pe termen lung. Acest lucru se aplică tuturor semnăturilor prezente în containere.

2) Pentru containerele ASiC-E cu CAdES - aserțiuni de timp fie:

a) unul sau mai multe fișiere ASiCArchiveManifest și tokenul de marcaj temporal aferent vor fi adăugate în container urmând regulile specificate în clauza A.7; sau

b) unul sau mai multe fișiere ASiCEvidenceRecordManifest se aplică tuturor fișierelor de date și/sau de semnătură și/sau token de semnătură și/sau marcaj temporal care necesită suport de validare pe termen lung.

3) Pentru containerele ASiC-E cu EvidenceRecord, va fi utilizat mecanismul intern al IETF RFC 6283 și IETF RFC 6283.




### 7.12.1 Profil de conservare F1 - Schema de conservare cu stocare pe baza de evidențe

#### 1. F.1.1 SchemaIdentificator

Schema de conservare cu evidențe de stocare și de evidență a probelor este identificată prin următoarele URI:

- http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers

Profilul de serviciu F1 este publicat pe http://pki.ezipper.ro/PreservationProfileF1

Descriere:

[**PDS] care extinde pe perioade lungi de timp starea de valabilitate a semnăturilor digitale + [PGD] furnizarea de dovezi ale existenței datelor pe perioade lungi de timp + [AUG] creșterea dovezilor depuse cu stocare**

**2. F.1.2 Obiectiv(e) de conservare**

Schema actuală de conservare susține următoarele trei obiective de conservare:

• extinderea pe perioade lungi de timp a stării de valabilitate a semnăturilor digitale, care este indicată de URI:

- http://uri.etsi.org/19512/goal/pds

• furnizarea de dovezi ale existenței datelor pe perioade lungi de timp, care este indicată de URI:

- http://uri.etsi.org/19512/goal/pgd

• completarea dovezilor depuse, care este indicată de URI:

- http://uri.etsi.org/19512/goal/aug

**3. F.1.3 Modelul de depozitare a conservării**

Schema de conservare actuală acceptă modelul de stocare de conservare "cu stocare" care corespunde valorii ***WithStorage*** din elementul PreservationStorageModel

**4. F.1.4 Operațiuni acceptate**

Profilul de conservare acceptă următoarele operațiuni:

- Păstrați PO conform clauzei 5.3.3.
- Recuperarea PO conform clauzei 5.3.4.
- Ștergeți PO conform clauzei 5.3.5. (în conformitate și cu reglementările naționale)

**5. F.1.5 Generarea și validarea dovezilor de conservare**

Schema de conservare actuală generează dovezi de conservare sub formă de înregistrări de dovezi conform IETF RFC 6283 și/sau IETF RFC 6283, care sunt anunțate în elementul Profile/EvidenceFormat ca:

- **urn:ietf:rfc:6283; și/sau urnă:ietf:rfc:6283**

În acest scop, funcția PreservePO a actualei scheme de conservare distinge două tipuri de SubDO:

- SubDO cu una sau mai multe semnături digitale (SubDOwithDS); și
- SubDO fără semnături digitale (SubDOwoDS).

Pentru SubDOwithDS, serviciul de conservare va efectua o validare a semnăturii în conformitate cu o politică adecvată de validare a semnăturii și va colecta și stoca materialul de validare necesar într-un loc adecvat într-un ***raport de validare încorporat într-un container de obiecte de conservare***.

De îndată ce toate SubDO au fost pregătite în consecință, acestea sunt hashate cu un algoritm hash adecvat, inserate într-un arbore hash Merkle, așa cum este specificat în IETF RFC 6283 și protejate de un marcaj temporal inițial de arhivă, folosind autoritatea de marcare a timpului calificată Zipper conform politicii specificate.

Validarea înregistrărilor de dovezi produse poate fi efectuată utilizând o politică de validare

adecvată, care specifică în special setul de ancore de încredere și alte constrângeri de validare.

Politica de creare a dovezilor de conservare aplicate și o politică de validare a dovezilor de conservare recomandate pot fi anunțate în elementul Profil/Politică aplicabil cu Tip egal cu următorul URI:

- http://uri.etsi.org/19512/policy/preservation-evidence

6. **F.1.6 Creșterea dovezilor de conservare**

Pe baza monitorizării adecvării algoritmilor criptografici pe baza unei politici criptografice adecvate, serviciul de conservare va efectua reînnoiri ale marcajelor temporale, așa cum este specificat în IETF RFC 6283 și IETF RFC 6283.

7. **F.1.7 Cerințe privind profilurile de conservare**

a. Serviciul acceptă formate de **dovezi de conservare**:

- Marcajul de timp al arhivei CAdES V3 conform ETSI EN 319 122;

b. Nu sunt acceptate formate de ieșire suplimentare

c. Valoare care specifică ora la care profilul este considerat activ:

   - ValidFrom=01.12.2025,

d. Perioada de păstrare a probelor

- **10 ani**, cu excepția cazului în care acordul cu clientul prevede altfel sau există o altă perioadă stabilită printr-un act normativ (la nivel național sau UE).

e. Politici tehnice aplicabile:

- PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.3.2
- ValidationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.2.2.2

### 7.12.2 Profil de conservare F3 - Schema de conservare cu mărire a semnăturii și cu stocare

Profilul de serviciu de conservare calificat F3.1 respectă schema F3 descrisă mai sus:

2. **F3.1 SchemaIdentificator:**

- http://uri.etsi.org/19512/scheme/pds+wst+aug

Profilul de serviciu F3 este publicat pe http://pki.ezipper.ro/PreservationProfileF3

Descriere:

**[PDS] extinzând pe perioade lungi de timp starea de valabilitate a semnăturilor digitale + + [AUG] augmentarea dovezilor depuse cu Stocare**

3. **F3.2 Obiectiv de conservare (date semnate electronic):**

Schema de conservare actuală susține următoarele obiective de conservare:

• prelungirea pe perioade lungi de timp a stării de valabilitate a semnăturilor digitale, care este indicată de URI: http://uri.etsi.org/19512/goal/pds

• completarea dovezilor depuse, care este indicată de URI:

- http://uri.etsi.org/19512/goal/aug

4. **F3.3 Model de conservare (cu stocare):fișier**
   - ***CuStocare***
5. **F3.4 Lista operațiunilor acceptate de protocolul de conservare:**
   - ConservePO;
   - Recuperați-PO;
   - Ștergeți PO (în conformitate și cu reglementările naționale)
6. **F3.5 Serviciul acceptă formate pentru intrare:**
   - http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3 semnătura digitală CAdES conform ETSI EN 319 122;
   - http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp semnătură digitală XAdES conform ETSI EN 319 132;
   - http://uri.etsi.org/ades/PAdES/document-time-stamp semnătura digitală PAdES conform ETSI EN 319 142;

7. **F3.6 Creșterea dovezilor de conservare**

   Pe baza monitorizării adecvării algoritmilor criptografici pe baza unei politici criptografice adecvate, serviciul de conservare efectuează o majorare a semnăturii în funcție de formatul specific de probă.

8. **Informații generale**

   a. F3.7 Serviciul acceptă formate de **dovezi de conservare**:
   - Marcajul de timp al arhivei CAdES V3 conform ETSI EN 319 122;
   - Marcajul de timp al arhivei XAdES conform ETSI EN 319 132;
   - Marcajul temporal al documentului PAdES conform ETSI EN 319 142.

   b. Nu sunt acceptate formate de ieșire suplimentare

   c. Valoare care specifică ora la care profilul este considerat activ:
      - ValidFrom=01.12.2025,

   d. Perioada de păstrare a probelor
      - **10 ani**, cu excepția cazului în care acordul cu clientul prevede altfel sau există o

altă perioadă stabilită printr-un act normativ (la nivel național sau UE).

e. Politici tehnice aplicabile:

- PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.3.2
- ValidationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.2.2.2

## 8. PROTECȚIA DATELOR DE STOCARE ÎMPOTRIVA RISCULUI DE PIERDERE, FURT, DETERIORARE SAU MODIFICĂRI NEAUTORIZATE

**Datele constând în software, arhive de date sau informații de audit sunt păstrate în siguranță într-o infrastructură specială în Zipper Data Center cu control implementat al accesului.**

**Centrele de date îndeplinesc următoarele condiții:**

**(a)** asigură securitatea și integritatea datelor, la nivelul securității fizice și al accesului prin mijloace informatice;

b) disponibilitatea serviciului de arhivare electronică și copierea de rezervă a informațiilor stocate.

Disponibilitatea datelor este asigurată prin utilizarea dispozitivelor de stocare dedicate în două locații diferite într-o configurație de înaltă disponibilitate, folosind un backend clusterizat care oferă copii în oglindă ale tuturor documentelor și metadatelor asociate.

## 9. AUTORITATEA PENTRU EMITEREA MARCAJULUI TEMPORAL ELECTRONIC CALIFICAT

Zipper oferă un serviciu calificat de verificare a timpului TSS. Zipper TSA acceptă interogări pentru emiterea de marcaje de timp electronice calificate pentru a verifica ora exactă în dovezile generate.

O descriere detaliată este furnizată în documentul "Declarația de politică și practică a autorității de marcare temporală (TSA)", pe https://pki.ca.ezipper.ro/repository/TSAPDS-EN.pdf

## 10. Autoritatea de stare a certificatului (QSVP)

Zipper este un furnizor calificat de servicii de validare a semnăturii (QSVP) și ar trebui să efectueze validarea semnăturii/sigiliului digital, iar rezultatul acestei proceduri este un raport de validare a semnăturii.

O descriere detaliată este furnizată în documentul "Politica și practica pentru serviciul de validare calificată a semnăturilor/sigiliilor electronice calificate" (Politica și practica pentru serviciul de validare a semnăturilor).

## 11. Reguli generale privind cerințele tehnice, organizatorice și procedurale ale ZIPPER

Această secțiune stabilește regulile generale privind cerințele tehnice, organizatorice și procedurale ale ZIPPER. Zipper Services SRL dispune de un centru de date, format din 2 containere, pe o arhitectură redundantă, performanță ridicată și disponibilitate a serviciilor, într-o structură distribuită.

Mai jos sunt descrise politicile și procedurile de asigurare a confidențialității datelor, integritatea și disponibilitatea documentelor arhivate în formă electronică, pe toată perioada legală de păstrare a acestora.

**Aplicația RepoZip LTA oferă aplicația de arhivare pentru Abonați și include modulul de validare și modulul de conservare. Datele electronice și documentele electronice transmise serviciului de arhivare electronică conțin semnături/sigilii electronice calificate, iar serviciul utilizează proceduri și tehnologii de păstrare și validare capabile să le extindă fiabilitatea pe perioada de păstrare a acestor date. Pentru a crea probe de conservare în cazul în care se utilizează semnături electronice, sigilii electronice sau marcaje temporale electronice, se vor utiliza servicii de încredere calificate.**

În aplicația internă RepoZip LTA situată în infrastructura centrului de date, vor fi asigurate:

**Confidențialitate** - asigurarea accesului la documente (metadate asociate) printr-un canal securizat, doar prin autentificarea persoanei, în conformitate cu permisiunile rezultate din setarea grupului și a rolului (pe baza Nomenclatorului în vigoare trimis arhivatorului Zipper). Soluția permite:

- Autentificare cu mai mulți factori (MFA)
- Control granular al accesului: Permisiunile sunt gestionate dinamic pe baza grupurilor și rolurilor definite în Nomenclatura arhivistică. Accesul poate fi restricționat la nivelul acțiunii permise (de exemplu, citire, descărcare).
- Criptare end-to-end: Canalele de comunicare dintre utilizator și arhivă sunt criptate cu protocoale TLS 1.3, iar obiectele arhivate sunt stocate criptate (AES-256).

**Integritate** - interzicerea modificării prin ștergerea sau adăugarea neautorizată a documentelor (metadate asociate), prin punerea amprentei documentului și semnarea cu semnătura electronică extinsă a Arhivistului

- Generarea amprentei digitale (hash): Fiecare document este asociat cu un hash unic (de exemplu, SHA-512) calculat înainte de import
- Semnătură electronică calificată cu marcaj temporal inclus: Aplicată de arhivist pe obiectul arhivat în momentul importului în sistem, semnătura garantează integritatea acestuia și nemodificarea ulterioară
- Pistă de audit și înregistrare: Orice operațiune pe document este înregistrată într-un jurnal

**Disponibilitate** - asigurarea condițiilor necesare pentru recuperarea și utilizarea ușoară, ori de câte ori este necesar, cu respectarea strictă a condițiilor de confidențialitate și integritate a documentelor (metadate asociate):

- Redundanță și replicare: Arhiva este stocată în două locații geografice (geo-redundanță) pentru a preveni pierderea datelor
- Backup periodic și automat: Efectuat zilnic, cu politici stricte de restaurare
- Interfață de recuperare rapidă: Oferă funcționalitate de căutare bazată pe metadatele asociate

**Autenticitate** - asigurarea posibilității verificării identității persoanei/entității, care a semnat/sigilat documentul cu un certificat calificat, în calitate de titular cu drept de a dispune de document. Această verificare se face prin serviciul de validare a semnăturii/sigiliului calificat (acreditare Zipper Services):

- Certificate calificate eIDAS: Sunt acceptate doar semnăturile/sigiliile bazate pe certificate calificate, emise de furnizori acreditați, iar raportul de verificare, semnătura
- Validare automată: Sistemul integrează serviciile de validare (OCSP, CRL) furnizate de Zipper Services pentru a verifica valabilitatea semnăturilor și sigiliilor titularilor dreptului de dispoziție.
- Marcarea identității semnatarului: Se păstrează metadatele cu datele semnatarului și ale autorității emitente a certificatului

**Nerepudiere** - măsură prin care se asigură că, după importul în RepoZip LTA, acel document exista la acel moment. Această dovadă este asigurată de măsurile aplicate procedural, arhivistul aplicând și o marcă temporală calificată pentru a demonstra ulterior existența acesteia.

- Import înregistrat cu marcaj temporal calificat: La momentul importului, obiectului arhivat i se aplică o marcă temporală conform Regulamentului eIDAS, certificată de furnizorul QTSP Zipper
- Lanț de încredere: Fiecare obiect arhivat este însoțit de un sigiliu calificat al Arhivatorului și de o marcă temporală încorporată în semnătură, formând un lanț criptografic care poate fi verificat în instanță

### 11.1 PROPRIETARUL DOCUMENTULUI ÎN FORMAT ELECTRONIC

Proprietarul documentului în formă electronică este definit la nivel de aplicație sub numele de Client și va defini tipurile de documente, metadate, grupuri și utilizatori aparținând acestui Client.

Titularul dreptului de a dispune de document este proprietarul sau, după caz, emitentul documentului,

care are dreptul de a stabili și modifica regimul de acces la document, conform legislației în vigoare.

### 11.2 METADATE DOCUMENTE

În cadrul aplicației se creează informații descriptive de conservare pentru informațiile arhivate, respectiv cuvinte-cheie necesare identificării documentului în formă electronică.

Cuvintele cheie, denumite în continuare metadate, vor permite grupurilor de utilizatori să descopere și să identifice documentul de interes.

### 11.3 VALIDAREA SURSEI

Cererea are un proces pentru a se asigura că documentul acceptat provine dintr-o sursă cunoscută și acceptabilă.

Arhiva poate demonstra că are acces la instrumentele și resursele necesare pentru a stabili contextul tehnic al obiectelor digitale pe care le conține. Arhiva înregistrează informațiile de reprezentare (inclusiv formatul) primite în arhivă. Arhiva are mecanisme de monitorizare și notificare atunci când informațiile de reprezentare (inclusiv formatul) se apropie, atunci când devin depășite sau nu mai sunt valabile.

### 11.4 POLITICA DE ACCES LA DOCUMENTE

Soluția are mecanisme adecvate pentru a detecta coruperea sau pierderea datelor. Există o procedură internă de raportare a tuturor incidentelor de corupție sau pierdere de date și a pașilor întreprinși pentru a restaura sau elimina datele corupte sau pierdute.

Soluția dispune de mecanisme adecvate pentru a asigura integritatea documentelor arhivate. Integritatea este definită ca absența modificărilor neintenționate ale conținutului arhivei, a metadatelor descriptive necesare rămânând asociate corespunzător, verificarea numărului de copii, sincronizarea copiilor, verificarea completitudinii acordurilor de arhivare, validarea urmelor de audit pentru toate accesările.

Soluția are mecanisme adecvate pentru a asigura confidențialitatea și confidențialitatea informațiilor stocate. Toate informațiile stocate vor fi obținute, stocate și prelucrate în conformitate cu legile în vigoare, în special cu Legea română privind protecția datelor cu caracter personal. Există o declarație de politică privind protecția datelor cu caracter personal, care va fi anexată la acest document.

Accesul la date va fi în concordanță cu clasificarea datelor, a grupului și a rolului utilizatorului. Regimul de acces la un document în format electronic, modificarea și termenul de păstrare a acestuia se stabilesc exclusiv de titularul dreptului de a dispune de documente.

Drepturile fiecărui utilizator sunt stabilite la nivel de client, grup și rol (nivel de acces), asigurând astfel accesul utilizatorului doar la documentele și datele clientului căruia îi aparține grupul.

Parolele tuturor utilizatorilor sunt păstrate criptate în sistemul RepoZip LTA. Un cont de utilizator care nu a fost utilizat pentru o perioadă de timp (poate fi definit pentru fiecare abonat, pe baza cerințelor contractuale de securitate) este dezactivat, necesitând o cerere de reactivare din partea Beneficiarului.

Beneficiarul este obligat să întreprindă toate acțiunile posibile pentru a proteja identificarea, numele și parola necesare utilizării serviciilor furnizate. Beneficiarul este responsabil pentru orice eveniment sau fapte care au avut loc prin utilizarea numelui său de identificare și a parolei de acces, cu excepția cazului în care evenimentul sau acțiunea a avut loc din motive care pot fi atribuite Arhivistului.

### 11.5 POLITICA PRIVIND DISPOZITIVELE CRIPTOGRAFICE UTILIZATE

Deținătorul unui dispozitiv criptografic trebuie să își îndeplinească sarcinile și obligațiile în mod responsabil în orice situație posibilă.

Următoarele elemente sunt luate în considerare la elaborarea politicii privind controalele criptografice:

- modul în care conducerea abordează utilizarea controalelor criptografice, inclusiv principiile generale care stau la baza protecției informațiilor comerciale;

- Abordarea de gestionare a cheilor, inclusiv metode de recuperare a informațiilor criptate în caz de pierdere, compromitere sau distrugere a cheilor;

- roluri și responsabilități pentru:

- punerea în aplicare a politicii;

- managementul cheilor;

Un deținător de dispozitiv criptografic trebuie să-și notifice emitentul în caz de furt, pierdere, dezvăluire neautorizată sau compromitere a securității imediat după incident.

Un deținător de dispozitiv criptografic nu este responsabil pentru neîndeplinirea sarcinilor/obligațiilor sale din motive imposibil de controlat pentru el.

Deținătorul dispozitivului criptografic este responsabil pentru neglijarea obligațiilor sale de a notifica emitentul cu privire la dezvăluirea sau încălcarea securității ca urmare a greșelilor, neglijenței sau

iresponsabilității sale.

### 11.6 POLITICA PRIVIND MIJLOACELE DE CONTROL ȘI SECURITATE A DOCUMENTELOR ȘI A BAZELOR DE DATE

Aplicatia RepoZip LTA asigura controlul si securitatea accesului la aplicatie prin limitarea accesului la:

- internal mesh Zipper
- rețeaua/IP-urile beneficiarului

*Controlul și securitatea accesului la documente:*

-Este securizat, prin indicarea unui nume de utilizator și a unei parole.

- Regimul de acces la un document în format electronic, modificarea și termenul de păstrare a acestuia sunt stabilite exclusiv de titularul dreptului de a dispune de documente. Furnizorul este obligat să respecte regimul de acces la documentele electronice.

-Drepturile fiecarui utilizator sunt stabilite la nivel de client, grup si rol (nivel de acces), asigurand astfel accesul utilizatorului doar la documentele si datele clientului la care apartine grupul are acces.

- Parolele tuturor utilizatorilor sunt păstrate criptate în sistemul RepoZip LTA.

- Un cont de utilizator neutilizat pentru o perioadă de 1 an este dezactivat, necesitând o cerere de reactivare din partea Beneficiarului.

- Beneficiarul este obligat să întreprindă toate acțiunile posibile în vederea protejării numelui de identificare și a parolei necesare utilizării serviciilor furnizate. Beneficiarul este responsabil pentru orice eveniment sau fapte care au avut loc prin utilizarea numelui său de identificare și a parolei de acces, cu excepția cazului în care evenimentul sau acțiunea a avut loc din motive care pot fi atribuite Furnizorului.

### 11.7 Controlul și securitatea accesului la baza de date

-La cererea Beneficiarului, exista si posibilitatea utilizarii unui server virtual separat exclusiv pentru aplicatia clientului (se utilizeaza o clona a aplicatiei si o baza de date care contine exclusiv datele clientului) pentru un nivel sporit de securitate.

- Orice acces la baza de date a Beneficiarului este înregistrat într-un fișier de acces (denumit jurnal de

procesare automată). Informațiile privind adăugarea, modificarea sau ștergerea datelor de afaceri ale Beneficiarului sunt salvate

### 11.8 Autentificarea utilizatorului

Orice activitate care poate duce la acțiuni asupra datelor sensibile ale afacerii (de exemplu, descărcare)

Jurnalul unui eveniment Log va conține următoarele date: ID utilizator, marcaj temporal și tip de operațiune

Jurnalul va fi disponibil pentru consultare de către utilizatorii cu drepturi în acest sens.

## 12. Obligații și răspundere

Acest capitol include toate obligațiile, răspunderile, garanțiile și răspunderile ZIPPER LTA, ale abonaților și utilizatorilor săi (abonați și părți de încredere). Aceste obligații și responsabilități sunt guvernate de acorduri acceptate de toate părțile.

ZIPPER își asumă responsabilitatea pentru implementarea cerințelor secțiunii "Practici LTA" a acestui document, precum și a prevederilor legislației naționale.

Acordurile ZIPPER cu abonații și părțile pe care se bazează descriu reciproc obligațiile și responsabilitățile, inclusiv responsabilitățile financiare. Declarația de politică și practică ZIPPER (acest document) face parte integrantă din aceste acorduri.

### 12.1 Obligații și garanții pentru abonați

ZIPPER garanteaza disponibilitatea a 99,5% din infrastructura si aplicatia de arhivare electronica 24/7, cu exceptia pauzelor tehnice programate, in ceea ce priveste mentenanta echipamentelor si sistemelor.

ZIPPER își asumă următoarele obligații față de Abonați:

- Să opereze în conformitate cu această declarație de politică și practică ZIPPER LTA (acest document) și cu alte politici și proceduri operaționale relevante;
- să se asigure că OTS menține o precizie minimă a orei UTC de ± 1 secundă;
- Menținerea unei echipe competente și experimentate care să asigure continuitatea serviciilor de infrastructură;
- Asigurarea permanentă a securității fizice și logice, precum și a integrității serverelor, software-ului și bazelor de date necesare bunei funcționări a serviciilor de arhivare electronică

- Monitorizează întreaga infrastructură LTA pentru a preveni sau limita orice întrerupere sau indisponibilitate a serviciilor
- Urmează revizuiri/audituri interne și externe pentru a asigura conformitatea cu legislația relevantă și cu politicile și procedurile interne ale ZIPPER;
- Oferă acces de înaltă disponibilitate la sistemele LTA ZIPPER, cu excepția întreruperilor tehnice planificate și a pierderii de sincronizare a timpului.

### 12.2 Drepturile abonaților

Abonații beneficiari au următoarele drepturi:

a) stabilirea regimului de acces la documentul arhivat, precum și modificarea acestuia, în condițiile art. 14 din Legea nr. 135/2007;

b) atestarea valorii originale sau de copie a documentului arhivat;

c) accesul online la registrul electronic al arhivei electronice;

d) accesul online la dosarul electronic atașat fiecărui document introdus în arhiva electronică, conform regimului de acces stabilit;

e) Accesul online la documentele arhivate care nu au acces public și la dosarele electronice ale acestora este considerat asigurat atunci când persoanele care au drept de acces la documente și la

Fișierele lor electronice pot fi consultate printr-o rețea privată (care nu este conectată la Internet). Este necesar consimțământul scris al beneficiarului cu privire la utilizarea rețelei respective.

Abonații trebuie să verifice pachetul de date POC arhivat de ZIPPER LTA.

Această verificare include:

- Verificați dacă pachetul de date conține documentul original arhivat, înregistrarea electronică a documentului și raportul de validare a semnăturii, contrasemnat de arhivist
- Verificarea certificatului de arhivist:
    - Verificarea căii de încredere până la certificatul rădăcină de încredere și pentru fiecare dintre certificatele din lanț (inclusiv certificatul cu care este semnat)
    - Verificați dacă certificatul nu a expirat în momentul semnării
    - Verificați dacă certificatul nu a fost revocat în momentul semnării

Alte obligații ale Abonatului pot fi, de asemenea, definite în Termenii și condițiile ZIPPER pentru serviciile de arhivare electronică.

### 12.3 Răspunderea Zipper

Răspunderea ZIPPER care acționează în calitate de administrator al arhivei pentru abonații săi este specificată în acordul dintre părți sau este cea prevăzută de legea aplicabilă.

ZIPPER este răspunzător pentru orice daune cauzate direct, intenționat sau din neglijență, oricărei persoane sau entități, ca urmare a nerespectării obligațiilor prevăzute aici.

Termenii și condițiile ZIPPER pentru serviciile de arhivare electronică limitează răspunderea ZIPPER. Limitările de răspundere includ excluderea daunelor indirecte, speciale, incidentale și consecutive. Acestea includ, de asemenea, un plafon de răspundere pentru răspunderea agregată combinată a ZIPPER față de toate persoanele în ceea ce privește serviciile de arhivare electronică, care este limitat la o sumă care nu depășește cea a contractului respectiv pentru serviciul de marcare temporală și la un maxim total de 300.000 EUR, indiferent de natura și tipul răspunderii, de valoarea sau amploarea oricărui prejudiciu suferit.

ZIPPER LTA nu este în niciun fel responsabil pentru utilizarea frauduloasă a serviciului.

## 13. Declarație de bune practici

### 13.1 Managementul și operarea infrastructurii

#### 13.1.1 Managementul securității

ZIPPER asigură existența unor proceduri administrative și de gestionare adecvate care corespund celor mai bune practici recunoscute.

ZIPPER îndeplinește toate funcțiile EE folosind sisteme fiabile care îndeplinesc cerințele ZIPPER ISMS.

#### 13.1.2 Clasificarea și gestionarea activelor

ZIPPER menține un inventar al tuturor activelor și atribuie o clasificare a cerințelor de protecție acelor active în conformitate cu analiza de risc.

#### 13.1.3 Securitatea personalului

ZIPPER menține controale adecvate ale personalului care îndeplinesc cele mai bune practici de securitate și cerințele standardelor relevante.

Personalul de conducere și operațional are abilitățile și cunoștințele adecvate privind marcarea temporală, semnăturile digitale și serviciile de încredere, precum și procedurile de securitate pentru personalul cu responsabilități de securitate, securitatea informațiilor și evaluarea riscurilor.

ZIPPER implementează politica de roluri de încredere pentru toți acei angajați care au acces sau controlează operațiunile criptografice. Persoanele și rolurile de încredere includ, dar nu se limitează la:

- Personalul operațiunilor de afaceri cripto,
- Personalul de securitate,
- personal de administrare a sistemului;
- Personalul ingineresc desemnat și
- Directori care sunt desemnați să gestioneze credibilitatea infrastructurii.

Înainte de a intra într-un rol de încredere, ZIPPER efectuează verificări de antecedente care pot include, ca orientare, următoarele:

- Verificarea identității
- Verificarea angajării anterioare și a referințelor profesionale;
- Confirmarea celei mai înalte sau celei mai relevante diplome de studii obținute;
- Verificarea faptului că nu există o condamnare penală;
- Verificarea înregistrărilor financiare.

ZIPPER cere ca personalul care dorește să devină persoane de încredere să furnizeze dovezi ale pregătirii, calificărilor și experienței necesare pentru a-și îndeplini în mod competent viitoarele responsabilități profesionale, așa cum sunt specificate în contractul de muncă și fișa postului, înainte de a îndeplini orice funcții operaționale sau de securitate.

Contractele de muncă semnate de angajați includ prevederi de confidențialitate pentru informațiile aduse la cunoștința acestora în timpul îndeplinirii acestora.

ZIPPER se asigură că personalul a obținut statutul de încredere și că aprobarea departamentului a fost acordată înainte ca acest personal să fie:

- Dispozitive de acces eliberate și acces la facilitățile necesare;
- A emis acreditări electronice pentru a accesa și îndeplini funcții specifice pe ZIPPER LTA sau alte sisteme IT.

Conturile de utilizator sunt create pentru personalul cu roluri specifice care necesită acces la sistemul în cauză. Toți utilizatorii trebuie să se conecteze cu un cont dedicat, iar comenzile administrative sunt

disponibile numai cu permisiune explicită. Permisiunile sistemului de fișiere și alte caracteristici disponibile în modelul de securitate al sistemului de operare sunt utilizate pentru a preveni orice utilizare ulterioară. Conturile de utilizator sunt blocate cât mai curând posibil atunci când schimbarea rolului dictează.

### 13.1.4 Securitatea fizică și de mediu

ZIPPER implementează Politica de securitate fizică, care acceptă cerințele de securitate ale acestei politici LTA și declarație de practică.

Operațiunile ZIPPER LTA se desfășoară într-un mediu protejat fizic care descurajează, previne și detectează utilizarea, accesul sau dezvăluirea neautorizată a informațiilor și sistemelor sensibile.

ZIPPER întreține, de asemenea, facilități de recuperare în caz de dezastru pentru operațiunile sale de servicii de arhivare electronică. Facilitățile de recuperare în caz de dezastru ale ZIPPER sunt protejate de mai multe niveluri de securitate fizică comparabile cu cele ale instalației principale ZIPPER.

Sistemul de securitate fizică include straturi pentru securitatea gestionării cheilor, care servește la protejarea stocării online și offline a unității de semnare criptografică (OSC) și a materialelor de chei.

Zonele utilizate pentru crearea și stocarea materialelor criptografice necesită control al accesului. Accesul la organizațiile societății civile și la materialele cheie este restricționat în conformitate cu cerințele de separare a sarcinilor. Deschiderea și închiderea dulapurilor sau containerelor la aceste niveluri este înregistrată în scopuri de audit.

Operațiunile ZIPPER sunt protejate prin controale fizice de acces, făcându-le accesibile doar persoanelor autorizate în mod corespunzător. Accesul în zonele securizate ale clădirilor necesită utilizarea unui card de "acces" și/sau a datelor biometrice. Utilizarea cardului de acces este înregistrată de sistemul de securitate al clădirii.

Jurnalele cardului de acces sunt revizuite în mod regulat.

Spatiile securizate Zipper sunt echipate cu sisteme primare și de back-up:

- Sisteme de alimentare cu energie electrică pentru a asigura accesul continuu și neîntrerupt la energie electrică și
- Sisteme de încălzire/ventilație/aer condiționat pentru controlul temperaturii și umidității relative.

ZIPPER a luat măsuri de precauție rezonabile pentru a minimiza impactul expunerii la apă asupra instalațiilor sale, precum și pentru a preveni și stinge incendiile sau alte expuneri dăunătoare la flacără sau fum.

Toate mediile care conțin software de producție și date, informații de audit, arhivare sau backup sunt stocate în facilități de depozitare securizate în afara locației, cu controale de acces fizice și logice adecvate, concepute pentru a limita accesul personalului autorizat și pentru a proteja aceste suporturi de daune accidentale.

ZIPPER stochează în siguranță toate suporturile amovibile și hârtia care conține informații sensibile legate de operațiunile sale în containere securizate. Documentele și materialele sensibile sunt mărunțite înainte de eliminare. Suportul utilizat pentru colectarea sau transmiterea informațiilor sensibile devine ilizibil înainte de eliminare. Dispozitivele criptografice sunt distruse fizic înainte de a fi îndepărtate.

### 13.1.5 Managementul operațiunilor

ZIPPER LTA asigură că procedurile, procesele și infrastructura trebuie să respecte managementul operațional, cerințele procedurale de securitate, managementul accesului la sistem, implementarea și întreținerea fiabilă a sistemului, managementul continuității afacerii și managementul incidentelor, așa cum sunt definite în ETSI EN 319 421.

Procedurile de management al operațiunilor pentru ZIPPER LTA sunt încorporate în procedurile generale de gestionare a operațiunilor interne ale ZIPPER.

### 13.1.6 Compromiterea serviciilor de încredere Zipper

Zipper a dezvoltat proceduri pentru a gestiona continuitatea operațiunilor sale. În cazul întreruperilor serviciului, se străduiește să minimizeze aceste întreruperi pentru a nu afecta activitatea clientului/clientului. Zipper a creat și menține un plan de continuitate în caz de dezastru. În caz de dezastru, inclusiv compromiterea unei chei de semnare private, operațiunile sunt reluate în termenul stabilit în planul de continuitate. Cauzele dezastrului sunt luate în considerare și se stabilesc măsuri rezonabile pentru a elimina cauza întreruperii procesului, precum și măsuri de prevenire a unor astfel de dezastre în viitor.

Compania a creat, documentat, implementat și întreținut planuri, proceduri și mecanisme de control în conformitate cu standardul internațional ISO 22301 pentru a asigura nivelul necesar de continuitate a afacerii și continuitatea securității informațiilor în cazuri adverse.

Zipper oferă:

a) o structură de management adecvată disponibilă pentru a pregăti, atenua și răspunde la un eveniment distructiv, utilizând personal cu autoritățile, experiența și competența necesare;

b) dezvoltarea și aprobarea planurilor și procedurilor de răspuns și recuperare care descriu în detaliu modul în care compania va gestiona un eveniment distructiv și va menține continuitatea securității informațiilor;

c) mecanisme de control al securității informațiilor în cadrul procedurilor, sistemelor și instrumentelor pentru menținerea continuității și redresării în caz de dezastre;

d) mecanisme compensatorii pentru controlul securității informațiilor mecanisme de control care nu pot fi menținute într-un eveniment advers.

Planul de continuitate include backup-ul sistemelor critice. Backup-ul este stocat în cele două locații, care se află la 300 km distanță geografic. Condițiile speciale respectă standardele, recomandările și reglementările aplicabile în domeniul securității informațiilor. Compania verifică la intervale regulate orice mecanisme create pentru a controla continuitatea securității informațiilor, astfel încât să poată asigura efectul și eficacitatea acestora în cazuri nefavorabile. Zipper face în mod regulat copii de rezervă a informațiilor și software-ului important și garantează că toate informațiile și software-ul de bază pot fi recuperate după un dezastru sau în caz de pierdere a arhivei. Mecanismele de recuperare sunt verificate periodic, astfel încât să se poată garanta că îndeplinesc cerințele planului de continuitate a muncii.

Stocarea pentru recuperarea afacerii în caz de incident sau dezastru este menținută și stocată în locații sigure și securizate. Zipper are obligația de a informa abonații și orice terțe părți despre incidentele apărute în activitatea de furnizare a serviciilor.

### 13.1.7 Încetarea serviciului de încredere

Serviciul de încredere se încheie:

- cu o decizie a Consiliului de Administrație al ZIPPER;
- printr-o decizie a autorității care exercită supravegherea serviciilor de încredere;
- printr-o hotărâre judecătorească;
- la lichidarea sau încetarea operațiunilor ZIPPER.

ZIPPER se asigură că potențialele perturbări pentru abonați și părți sunt reduse la minimum ca urmare a încetării serviciilor ZIPPER și, în special, asigură menținerea continuă a informațiilor necesare pentru

verificarea corectitudinii serviciilor.

Dacă este necesar ca ZIPPER să înceteze funcționarea, ZIPPER va depune eforturi rezonabile din punct de vedere comercial pentru a notifica abonații și părțile aflate în întreținere cu privire la o astfel de reziliere înainte de încetarea Serviciului.

### 13.2 Păstrarea dovezilor privind notificarea sau comunicarea

- ✓ Perioada de păstrare a eșantioanelor colectate este în conformitate cu legislația națională și este în conformitate cu recomandările ETSI TS 119 312;
- ✓ Confidențialitatea și integritatea înregistrărilor curente și arhivate ale funcționării Serviciului sunt păstrate și arhivate în conformitate cu practica comercială a Zipper;
- ✓ Timpul utilizat pentru înregistrarea evenimentelor, așa cum este necesar în jurnalul de jurnal, este sincronizat cu UTC cel puțin o dată pe zi;
- ✓ Evenimentele sunt înregistrate într-un mod care nu poate fi șters sau distrus cu ușurință;
- ✓ Același profil de conservare se aplică pe toată perioada de conservare a eșantionului;
- ✓ Perioada de valabilitate a eșantioanelor este prelungită prin utilizarea unor algoritmi criptografici siguri și fiabili;
- ✓ Formatul de dovezi din această politică respectă cerințele IETF RFC 6283, precum și CAdES ETSI EN 319 122, XAdES ETSI EN 319 132 și PAdES ETSI EN 319 142.

Dacă este necesar, Zipper extinde valabilitatea dovezilor la arhivă. În timpul perioadei de arhivare, serviciul de arhivare verifică dacă dovezile pot fi utilizate pentru a atinge scopul corespunzător de conservare. Acest lucru poate fi amenințat dacă algoritmul criptografic nu mai poate fi de încredere sau certificatul administratorului arhivei este revocat. În astfel de cazuri, Zipper extinde dovezile înainte ca acestea să poată fi folosite pentru a atinge scopul arhivării.

### 13.3 Fiabilitate organizațională

ZIPPER LTA se asigură că organizația sa este fiabilă în conformitate cu ETSI EN 319 421. ZIPPER are stabilitatea financiară și resursele necesare pentru a funcționa în conformitate cu această declarație de politică și practică.