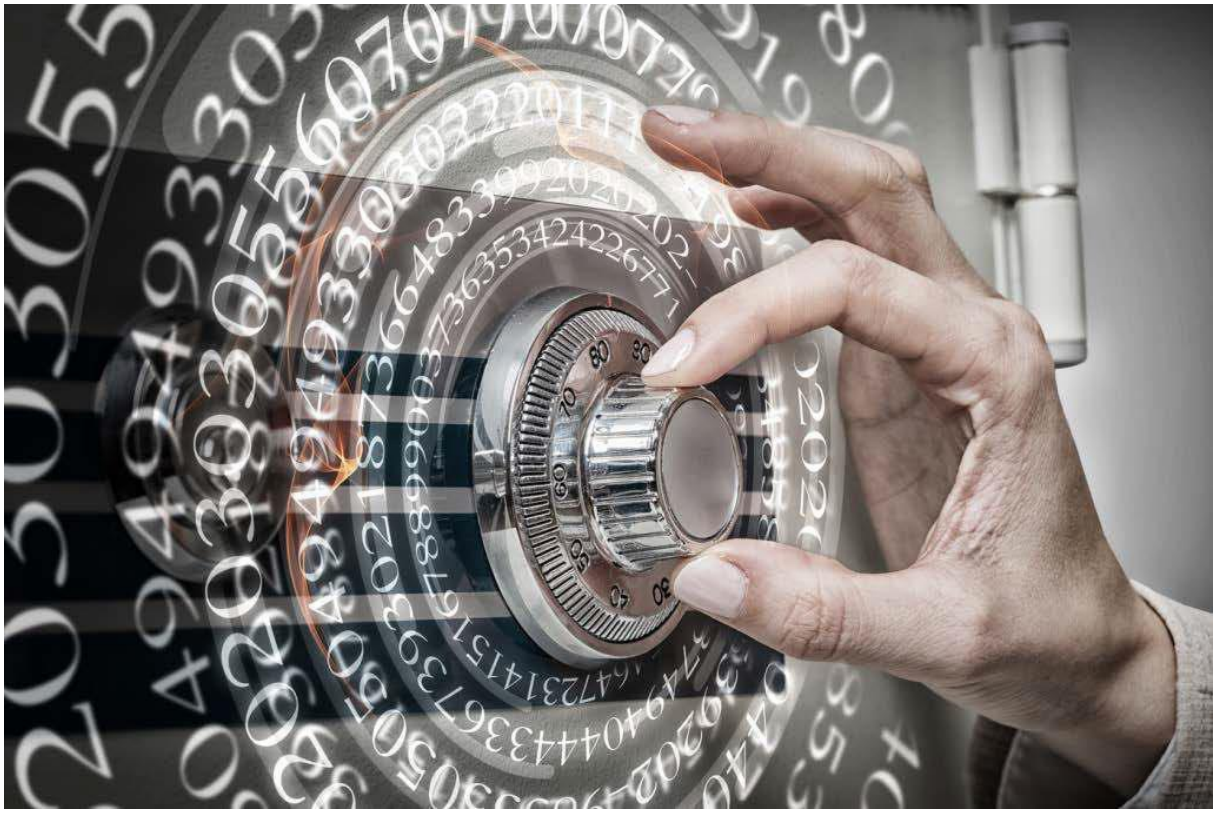


SERVICIUL CALIFICAT DE PĂSTRARE PE TERMEN LUNG

Declarație de Politici și Practici

Versiunea 1.1,

Data intrării în vigoare: 2 martie 2020

Informații generale	
OID	*1.3.6.1.4.1.39965.5.1.1.1.1.0*
Versiune	*1.1*
Clasificarea informației	*Public*
Aprobat de	*Camelia Ivan*
Data aprobării	*2.03.2020*
Data intrării în vigoare	*2.03.2020*

Istoricul Modificarilor			
Versiune	**Descriere**	**Data**	**Autor(i)**
1.0	Prima versiune	3.02.2020	Mihaela Bunea
1.1	Alinierea conținutului cu ETSI TS 119 511	2.03.2020	Mihaela Bunea

CUPRINS

1. INTRODUCERE

Este o practica obisnuita ca un Furnizor de Servicii de Incredere sa aiba in vigoare doua documente:

- Declaratie de Certificare a Practicilor (CPS)/ (DCP) care descrie practicile pe care un TSP le utilizeaza in gestionarea certificatelor (cerere, eliberare, utilizare si revocare) sau servicii de incredere;
- Politica a Certificatului (CP)/ (PC) care descrie procesele de examinare si care permite o estimare a credibilitatii si fiabilitatii serviciilor sale;

Deoarece toate serviciile de incredere calificate stau la baza acelorasi reglementari si cerinte definite in Regulamentul eIDAS, ambele documente mentionate mai sus (CPS si CP) au fost integrate intr-un singur document, aceasta Declaratie de Politici si Practici.

Acest document contine Declaratia de Politica de pastrare calificata pe termen lung si de Practica definita si operata de catre Trans Sped (denumita in continuare: Trans Sped sau Furnizorul de servicii de pastrare pe termen lung) privind serviciul de conservare calificat.

Serviciul calificat de pastrare pe termen lung indeplineste cerintele stabilite de Regulamentul eIDAS [1], serviciul furnizat in conformitate cu aceste regulamente este un serviciu de incredere calificat in UE.

Conditiile prealabile pentru furnizarea calificata de servicii de incredere si indicatia "EU Trust Mark" sunt:

- Serviciul este auditat de un organism independent de evaluare acreditat in temeiul Regulamentului eIDAS, acesta emite un raport de evaluare a conformitatii si un certificat pentru Furnizorul de servicii de pastrare pe termen lung cu privire la evaluarea reusita;
- Furnizorul de servicii de pastrare pe termen lung prezinta certificatul de evaluare a conformitatii unui Organism de supraveghere;
- Organismul de supraveghere accepta certificatul de evaluare a conformitatii depus si publica serviciul in lista nationala de incredere.

1.1. Prezentare generala

Politica de pastrare calificata pe termen lung reprezinta un set de reguli care specifica utilitatea serviciului de conservare calificata pentru o comunitate si/sau o clasa de aplicatii cu cerinte comune de siguranta.

Politica de pastrare calificata pe termen lung stabileste cerintele de baza pentru Furnizorul de servicii de pastrare pe termen lung referitor la conservarea calificata care urmeaza sa fie stabilita.

Politica de pastrare calificata pe termen lung reprezinta unul din multiplele documente emise de Furnizorul de servicii de pastrare pe termen lung, care guverneaza in mod colectiv conditiile de stocare a serviciilor asigurate de Furnizorul de servicii de pastrare pe termen lung. Alte documente importante includ Termenii si conditiile generale, Declaratiile de practica de pastrare pe termen lung si alte acorduri cu clientii si partenerii.

1.1.1. Politica de pastrare pe termen lung

Primele sapte numere ale identificatorului OID pentru Politica de pastrare calificata pe termen lung reprezinta identificatorul unic al Trans Sped, dupa cum urmeaza:

(1)	Organizatia Internationala pentru Standardizare (ISO)
(3)	Schemele de identificare a organizatiei inregistrate conform ISO / IEC 6523-2
(6)	Departamentul Apararii al Statelor Unite (DoD)/ (DA)
(1)	Internet
(4)	Proiecte private
(1)	Companii private
(39965)	Trans Sped srl

Sistemul numerelor urmatoare a fost alocat in cadrul competentei proprii Trans Sped, interpretarea fiind dupa cum urmeaza:

(1.3.6.1.4.1.39965)	Trans Sped srl
(5)	Pastrarea pe termen lung in cadrul Trans Sped
(1)	Documente
(1)	Documente Publice
(x)	Numar unic de identificare al documentului
(y)	Versiune a documentului
(z)	Subversiune a documentului

Prezentul document defineste urmatoarea Politica:

OID	DENUMIRE	PRESCURTARE
1.3.6.1.4.1.39965.5.1.1.1.1.0	Politica de pastrare calificata pe termen lung conform regulamentului eIDAS	QLTP

1.1.2. Intrare in vigoare

Aceasta Declaratie de Politici si Practici este in vigoare din februarie 2020 pana la retragere.

Prezenta Declaratie de Politici si Practici trebuie revizuita cel putin o data pe an si trebuie sa se asigure o rectificare a posibilelor solicitari si a cerintelor preliminare modificate.

Intrarea in vigoare a Declaratiei de Politici si Practici se extinde la fiecare dintre participantii mentionati in sectiunea 1.2.

1.2. Participanti LTP

1.2.1. Furnizori LTP

Furnizorul de servicii pe termen lung este un Furnizorul de servicii de pastrare pe termen lung, in cadrul caruia Serviciul de incredere se ocupa de pastrarea valabilitatii semnaturilor electronice, a sigiliilor electronice, a marcilor temporale si a certificatelor de creator ale acestora, optional incluzand si pastrarea documentelor electronice semnate si sigilate.

Cerintele prezentului document se aplica fiecarui Furnizorul de servicii de pastrare pe termen lung, care se angajeaza in Declaratia de Practica a Pastrarii pe Termen Lung sa respecte oricare dintre Politicile Calificate de Pastrare pe Termen Lung, descrise in prezentul document.

1.2.2. Abonati

Abonatii definesc domeniul de aplicare al utilizatorilor care intrebuinteaza serviciul, iar Abonatii acopera, de asemenea, taxele de servicii legate de utilizarea acestor capabilitati.

1.2.3. Beneficiari

Beneficiarii nu sunt in mod necesar intr-o relatie contractuala cu Furnizorul de servicii de pastrare pe termen lung. Declaratia privind practica de conservare pe termen lung si celelalte politici mentionate in aceasta contin recomandarile legate de functionarea acesteia.

1.3. Managementul Politicii

1.3.1. Compania care administreaza Documentul

Datele companiei care administreaza actuala Politica de pastrare calificata pe termen lung pot fi gasite in urmatorul tabel:

Numele companiei	Trans Sped srl
Adresa companiei	Strada Despot Voda, nr. 38, Sectorul 2, 020656, Bucuresti, Romania
Numar de telefon	+40212107500
Numar de fax	+40212110207
Adresa de e-mail	office@transsped.ro

1.3.2. Persoana de contact

Intrebarile legate de Declaratia actuala de politici si practici pot fi adresate in mod direct urmatoarei persoane:

Persoana de contact	Camelia IVAN
Numele companiei	Trans Sped srl
Adresa companiei	Strada Despot Voda, nr. 38, Sectorul 2, 020656, Bucuresti, Romania
Numar de telefon	+40212107500
Numar de fax	+40212110207
Adresa de e-mail	office@transsped.ro

1.3.3. Proceduri de aprobare a declaratiei de politici si practici

Furnizorul de servicii de pastrare pe termen lung va descrie procedura de acceptare a Declaratiei de practica privind pastrare pe termen lung care isi anunta conformitatea cu Politica actuala de pastrare calificata pe termen lung, in Declaratia de politici si practici privind pastrarea pe termen lung.

1.4. Definitii si Acronime

1.4.1. Definitii

Centru de Date	O resursa destinata amplasarii si functionarii sistemelor de calcul si a componentelor asociate. Aceste componente includ in mod obisnuit sisteme de telecomunicatii si conexiuni de comunicatii, surse de alimentare redundante, stocare de date, aer conditionat, protectie impotriva incendiilor si sisteme de securitate.
Organism de Supraveghere	In conformitate cu Regulamentul eIDAS
Serviciu de Incredere	Inseamna un serviciu electronic oferit in mod normal in schimbul unei remuneratii care consta in: • crearea, verificarea si validarea semnaturilor electronice, a sigiliilor electronice sau a marcilor temporale electronice, a serviciilor de livrare inregistrate electronic si a certificatelor aferente acestor servicii; sau • crearea, verificarea si validarea Certificatului de autentificare a site-ului; sau • pastrarea semnaturilor electronice, sigiliilor sau a certificatelor aferente acestor servicii; *(eIDAS [1] 3. articolul 16. punct)*
Furnizor de Serviciu de Incredere	O persoana fizica sau juridica care furnizeaza unul sau mai multe Servicii de Incredere, fie ca furnizor de servicii de incredere calificat, fie ca necalificat. *(EIDAS [1] 3. articolul 19.*

	punct
Furnizor de servicii de pastrare pe termen lung	Trans Sped S.R.L.
E-dossier	Fisierul electronic (e-dosarul) reprezinta o semnatura electronica in format container, un tip de document electronic. Un dosar electronic poate sa contina documente sau profilurile (metadate) asociate, semnaturi, contrasignaturi si marci temporale.
E-document	Un e-document este un document electronic care contine cel putin o semnatura electronica sau un sigiliul conform cu regulamentul eIDAS. In functie de tipul documentului electronic, acesta poate sa contina alte documente electronice si profilele corespunzatoare (metadatele), semnaturi, contrasignaturi si marci temporale.
Document electronic	Inseamna orice continut stocat in forma electronica, in special inregistrare text sau sunet, vizuala sau audiovizuala *(eIDAS [1] 3. articolul 35. punct)*
Marca temporala electronica	Inseamna date in format electronic care leaga alte date in format electronic de o anumita perioada de timp, furnizand dovada ca aceste date au existat in acel moment. *(EIDAS [1] 3. articolul 33. punct)*
Pachet(e) export-import	Informatie extrasa din serviciul de pastrare incluzand datele obiect, evidenta de pastrare si metadatele referitoare la serviciul de pastrare ce permite unui alt serviciu de pastrare sa o importe pentru a continua atingerea obiectivului de pastrare a acestei informatii
Abonat	O persoana sau o organizatie care semneaza contractul de furnizare a serviciului cu Furnizorul de servicii de pastrare pe termen lung pentru a utiliza unele dintre serviciile sale.
Suspendare	Rezilierea temporara a valabilitatii *Certificatului* inainte de expirarea perioadei de valabilitate indicate in *Certificat*. Suspendarea *Certificatului* nu este definitiva; valabilitatea Certificatului suspendat poate fi restabilita.

Certificat de baza	De asemenea, cunoscut ca si certificat de nivel superior. *Certificatul* cu auto-semnare, care este eliberat de o anumita *Unitate de Certificare* pentru el insusi, care este semnat cu o cheie privata, astfel incat poate fi verificat cu Semnatura - Date de verificare - indicate in certificat.
HSM/MSH: Modul de Securitate Hardware	Un instrument securizat bazat pe hardware care genereaza, stocheaza si protejeaza cheile criptografice si ofera un mediu securizat pentru implementarea functiilor criptografice.
Compromis	O cheie criptografica este compromisa, atunci cand persoanele neautorizate ar fi putut avea acces la ea
Unitatea de Certificare Intermediara	O *Unitate de Certificare* al carei *Certificat* a fost emis de o alta *Unitate de Certificare.*
Cheie criptografica	O serie de semnale digitale individuale care controleaza transformarea criptografica, a caror cunoastere este necesara pentru criptare, decriptare, crearea si verificarea semnaturii electronice
Gestionarea Cheii	Producerea de chei criptografice, livrarea lor catre utilizatori sau implementarea algoritmica a acestora, precum si inregistrarea, stocarea, arhivarea, revocarea si incheierea de chei care sunt strans legate de metoda de securitate folosita.
Pastrare pe termen lung	Extensie a statusului de validitate a unei semnaturi electronice peste perioade lungi de timp si/sau extensia dovezii existentei datelor pentru o perioada lunga de timp, in contextul iesirii din functiune a tehnologiilor criptografice precum: crypto-algoritmi, lungimi de chei, functii hash, compromiterea cheilor sau pierderea abilitatii de a verifica statusul de validitate a cheilor publice.
Profil de pastrare	Set de informatii unic identificat despre implementarea unui model de pastrare si unul sau mai multe obiective de pastrare care specifica cum sunt generate si validate evidentele de pastrare.

Cheie Privata	In infrastructura cheii publice, elementul pereche de cheie criptografica asimetric care face pereche cu elementul pereche pe care *Subiectul* il va pastra strict secret. In timpul emiterii *Certificatelor*, *Autoritatea de Certificare* utilizeaza cheile private ale *Unitatii de Certificare* pentru a plasa o semnatura electronica sau un sigiliu pe *Certificat* pentru a-l/a o proteja.
Serviciu de incredere calificat	Un *Serviciu de Incredere* care indeplineste cerintele aplicabile stabilite in Regulamentul eIDAS. *(eIDAS [1] articolul 3. punctul 17.)*
Furnizor calificat de servicii de incredere	Un *Furnizor de Servicii de Incredere* care ofera unu sau mai multe *Servicii de Incredere Calificate* si care beneficiaza de statutul calificat din partea Organismului de supraveghere. *(eIDAS [1] articolul 3 punctul 20)*
Cheie publica	In infrastructura cheii publice, elementul de de cheie criptografice anasimetrica pereche apartinand unui actant, care ar trebui sa fie facut public. Revelarea este, de obicei, sub forma unui *Certificat*, care leaga numele actantului cu cheia sa publica. Autenticitatea *Certificatelor* poate fi verificata cu ajutorul cheii publice a *Unitatii de Certificare*.
Infrastructura Cheii Publice, PKI/ICP	O infrastructura bazata pe criptografie asimetrica, inclusiv algoritmi criptografici, chei, certificate, standarde si legislatie aferenta, sistem institutional fundamental, o varietate de furnizori si dispozitive.
E-dosar necriptat	Un e-dosar, care include fisiere necriptate si semnaturi electronice sau sigilii electronice in ele. In dosarul electronic necriptat fisierele si semnaturile marcate, stampilate, sigiliile sunt incluse necriptate.
Situatie Operationala Deosebita	O situatie deosebita care cauzeaza perturbari in cursul functionarii furnizorului de pastrare pe termen lung, atunci cand nu este posibila continuarea functionarii normale a furnizorului de pastrare pe termen lung, intr-un termen temporar sau permanent.
Companie	Persoana juridica.

Baza de stocare a certificatului	Depozit de date care contine diverse *Certificate*. O Autoritate de certificare are o Baza de stocare de certificate in care sunt pastrate certificatele emise, dar sistemul care contine Certificatele disponibile aplicatiei pe computerul Beneficiarilor este denumit de asemenea Baza de stocare a certificatelor.
Anulare	Rezilierea valabilitatii *Certificatului* inainte de expirarea termenului de valabilitate indicat de asemenea pe *Certificat*. Revocarea *Certificatului* este permanenta, *Certificatul* revocat nu mai poate fi restabilit.
Inregistrarea statutului de revocare	Inregistrarile *Certificatelor* suspendate si revocate, care includ suspendarea sau revocarea si timpul de suspendare sau revocare mentinut de *Autoritatea de Certificare.*

1.4.2. Acronime

CRL	Lista de revocare a certificatelor
eIDAS	Identificare electronica, Autentificare si Semnatura
LDAP	Protocol de Acces facil in Director
LTP	Long Term Preservation (Pastrare pe termen lung)
SB	Organism de supraveghere
OCSP	Protocol de stare al Certificatului online
OID	Identificatorul Obiectului
PKI	Infrastructura Cheii publice
TSP	Trust Service Provider (Furnizor servicii de incredere)
VM	Virtual Machine (masina virtuala)

2. RESPONSABILITATILE DE PUBLICARE SI STOCARE

2.1. Stocare

Furnizorul de servicii de pastrare pe termen lung publica Declaratia de politici si pratici de pastrare calificata pe termen lung si alte documente care contin termenii si conditiile pe baza carora functioneaza intr-o unitate de stocare.

2.2. Publicarea informatiilor de certificare

2.2.1. Publicarea informatiilor furnizorului de pastrare pe termen lung

Furnizorul de servicii de pastrare pe termen lung trebuie sa dezvaluie electronic pe site-ul sau web conditiile contractuale si politicile sale.

Noile documente care vor fi introduse, vor fi publicate pe site-ul web cu 30 de zile inainte de intrarea in vigoare. Documentele in vigoare vor fi disponibile pe site in plus fata de toate versiunile anterioare ale tuturor documentelor.

Versiunea actuala a politicilor si a conditiilor contractuale trebuie sa poata fi citita in forma tiparita la departamentul de relatii cu clientii al Furnizorului de pastrare pe termen lung.

Furnizorul de servicii de pastrare pe termen lung va pune la dispozitia clientului Declaratia de Politici si Practici si Contractul de servicii pe un suport durabil in urma incheierii contractului.

Furnizorul de servicii de pastrare pe termen lung isi va notifica Clientul despre modificarea Termenilor si conditiilor generale.

2.3. Frecventa publicarii

2.3.1. Frecventa publicarii termenilor si conditiilor

Divulgarea Politicii de pastrare calificata pe termen lung in legatura cu noile versiuni este conforma cu metodele descrise in Sectiunea 8.12.

Furnizorul de servicii de pastrare pe termen lung dezvaluie alte reglementari, conditiile contractuale si noile lor versiuni, daca este necesar.

Furnizorul de servicii de pastrare pe termen lung va publica fara intarziere informatii extraordinare, in conformitate cu cerintele legale si in absenta acestora atunci cand este necesar.

3. SERVICIUL ELECTRONIC DE PASTRARE PE TERMEN LUNG

In cadrul serviciului electronic de pastrare pe termen lung trebuie sa fie furnizate urmatoarele sarcini:

- Abonatul sa poata incarca documente electronice semnate electronic in arhiva operata de Furnizorul de servicii de pastrare pe termen lung.
- Furnizorul de servicii de pastrare pe termen lung stocheaza in siguranta documentele electronice acceptate - fisierele incluse si materialele de validare pe termen lung si asigura pe parcursul intregii perioade de conservare urmatoarele:
  - numai persoanele autorizate au acces la datele pastrate;
  - abonatul indreptatit are acces permanent la datele pastrate;
  - datele pastrate nu pot fi modificate sau sterse fara autorizare.
- Furnizorul de servicii de pastrare pe termen lung asigura furnizarea pe termen lung a marcilor si sigiliilor electronice plasate pe documentele electronice si pe fisierele pastrate in documentele electronice. Furnizorul de servicii de pastrare pe termen lung asigura lizibilitatea pe termen lung a fisierelor in documentele electronice si in cazul formatelor de fisiere specificate in timpul perioadei de conservare.

  Perioada de pastrare este de obicei de 50 de ani, cu exceptia cazului in care perioada de valabilitate a contractului de servicii inceteaza inainte de sfarsitul acestei perioade (pentru detalii, a se vedea sectiunea 4).
- Abonatul are acces permanent la documentele electronice, semnaturile si sigiliile plasate de acestia in arhiva Furnizorului de pastrare pe termen lung si la materialul corespunzator de validare pe termen lung si le poate descarca (vezi sectiunea 3.3).
- Dupa primirea documentului electronic, Furnizorul de servicii de pastrare pe termen lung ar putea verifica semnatura/urile electronica/e sau sigiliul/ iile de pe documentul electronic, in baza unui acord individual sau de pe fisierele incluse in documentele electronice, completeaza sau compileaza materialul de validare pe termen lung, plaseaza Marca Temporala electronica de arhivare pe materialul de validare si salveaza documentul electronic acceptat (vezi sectiunea 3.2).
- La cererea Abonatului, Furnizorul de servicii de pastrare pe termen lung emite o confirmare autentica referitoare la faptul ca stocheaza documentele electronice si ca, la momentul acceptarii in arhiva, semnaturile electronice sau sigiliile de pe e-document si de pe documentele stocate in fisierele electronice au fost valabile (vezi sectiunea: 3.4).
- La solicitarea Abonatului, Furnizorul de servicii de pastrare pe termen lung sterge documentele electronice din arhiva (vezi sectiunea: 3.6).

Sarcina principala a serviciului de conservare pe termen lung este pastrarea valabilitatii documentelor semnate digital sau a sigiliului plasat pe documentul electronic.

Furnizorul de servicii de pastrare pe termen lung poate furniza Abonatului si alte servicii in afara de furnizarea atributiei de baza, de exemplu:

- pastrarea documentelor electronice cu semnatura sau sigiliul electronic, care sa asigure lizibilitatea si interpretabilitatea umana a documentelor electronice incarcate in arhiva,
- efectuarea conversiilor formatelor de fisiere care devin necesare,
- pastrarea documentelor electronice fara semnatura electronica sau sigiliu
- copii certificate ale documentelor electronice pastrate in Sistemul de pastrare pe termen lung

Prezenta Declaratie de Politici si Practici de Pastrare Calificata pe Termen Lung defineste cerintele pentru asigurarea valabilitatii pe termen lung a semnaturilor electronice si a sigiliilor.

Furnizorul de servicii de pastrare pe termen lung poate specifica si restrictiona formatul semnaturilor sau sigiliilor electronice acceptate, Autoritatile de certificare acceptate si orice alt parametru.

3.1. Incheierea unui acord de servicii

Inainte de a utiliza serviciul, Abonatul incheie un contract de servicii cu Furnizorul de servicii de pastrare pe termen lung.

Declaratia privind politicile si practicile de conservare pe termen lung si celelalte reglementari citate vor specifica in mod clar detaliile serviciului care trebuie furnizat si instrumentele necesare pentru utilizarea serviciului.

3.2. Incarcarea Documentului

Furnizorul de servicii de pastrare pe termen lung accepta documentele electronice care urmeaza sa fie arhivate numai dupa identificarea Abonatului in cadrul unei proceduri de securitate. Procedura trebuie sa asigure integritatea, confidentialitatea documentelor electronice.

Trebuie sa se precizeze in mod clar ce semnatura si ce format de fisier accepta Furnizorul de servicii de pastrare pe termen lung in documentul electronic, modul in care verifica semnaturile electronice si sigiliile si in ce conditii accepta documentele electronice.

Validitatea semnaturii (urilor) electronice sau a sigiliului (iilor) pe documentul electronic primit se verifica pe baza materialului de validare pe termen lung. Verificarea se poate baza pe materialul de validare partiala sau completa pe termen lung atasat la semnatura (uri) electronica (e) sau sigiliul (sigiliile). Orice informatie necesara in continuare pentru validare va fi colectata de catre Furnizorul de servicii de pastrare pe termen lung si acesta le va pastra pe cele legate de documentul electronic. Dupa intocmirea materialelor de validare pe termen lung, Furnizorul de servicii de pastrare pe termen lung va plasa pe fiecare material de validare pe termen lung o Marca Temporala de arhivare calificata.

Furnizorul de servicii de pastrare pe termen lung va verifica documentele electronice primite cat mai curand posibil, dar nu mai tarziu de 3 zile de la admitere si va trimite Abonatului o confirmare ca materialul de validare pe termen lung a fost compilat cu succes si ca a acceptat e-documentul. Daca procesul este intrerupt undeva, Furnizorul de servicii de pastrare pe termen lung va notifica Abonatul intr-un mesaj de eroare. Pe baza mesajului de eroare, trebuie sa se poata identifica in mod clar ce document electronic este implicat si care a fost motivul respingerii.

In cazul in care verificarea privind acceptarea documentului electronic nu ajunge la Abonat in termenul limita stabilit, se considera ca Furnizorul de servicii de pastrare pe termen lung nu a acceptat documentul electronic. Furnizorul de servicii de pastrare pe termen lung este singurul responsabil pentru stocarea documentului electronic si pentru asigurarea credibilitatii pe termen lung a semnaturilor si sigiliilor electronice incluse in cazul transmiterii unei confirmari pozitive.

3.3. Asigurarea disponibilitatii materialului de validare pe termen lung - Descarcare a e-documentelor

Furnizorul de servicii de pastrare pe termen lung se asigura ca Abonatul isi poate descarca documentele electronice stocate in arhiva si materialul de validare pe termen lung corespunzator pe durata perioadei de valabilitate a acordului de servicii.

Abonatul are acces numai la documentele electronice si la materialul de validare pe termen lung pastrat in arhiva Furnizorului de servicii de pastrare pe termen lung prin intermediul unui canal securizat.

Furnizorul de servicii de pastrare pe termen lung trebuie sa se asigure ca fiecare Abonat are acces doar la documentele electronice si la materialul de validare pe termen lung la care are dreptul sa aiba acces.

3.4. Emiterea confirmarii

La cererea Abonatului, Furnizorul de servicii de pastrare pe termen lung emite o confirmare in legatura cu documentul electronic. Confirmarea consta in urmatoarele:

1. Hash-ul documentului electronic, numele si identificatorul Abonatului.
2. Declaratia conform careia documentul dat are un anumit hash, astfel incat acesta este identic cu documentul electronic cu acelasi hash prezentat de catre abonat.
3. Timpul de acceptare a documentelor electronice in arhiva.
4. Dimensiunea fisierului si adresa IP a clientului
5. Declaratia conform careia semnaturile electronice avansate sau calificate, sigiliile, marcile temporale pe documentele electronice date si Certificatele corespunzatoare au fost valabile in momentul marcarii timpului si validarii dupa incarcare.

Furnizorul de servicii de pastrare pe termen lung emite confirmarea pe suport de hartie sau intr-un dosar electronic cu o semnatura electronica calificata. Confirmarea este creata de un functionar responsabil de emiterea confirmarii arhivei si, in cazul unei confirmari electronice, isi plaseaza semnatura electronica calificata, in cazul unei confirmari pe suport de hartie, autentifica confirmarea tiparita cu semnatura sa de mana.

Cunoasterea e-documentului arhivat nu este necesara pentru emiterea confirmarii, aceasta este emisa pe baza hash-ului documentului electronic necriptat, pastrata in text clar. Nu pot fi obtinute informatii din valoarea hash in raport cu continutul documentului electronic pastrat.

Solutia aplicata asigura faptul ca oficialii responsabili de emiterea confirmarii arhivei nu cunosc continutul documentului electronic necriptat in legatura cu emiterea confirmarii.

Abonatul poate solicita eliberarea confirmarii din partea Furnizorul de servicii de pastrare pe termen lung in baza unei cereri in scris semnate, pe suport de hartie depusa prin orice modalitate de livrare sau prin completarea unei cereri electronice, certificata cu cel putin o semnatura electronica avansata sau un sigiliu.

Eliberarea confirmarii poate fi solicitata de catre reprezentantul autorizat al Abonatului daca a prezentat in prealabil autorizatia Abonatului continuta intr-un document privat complet concludent.

3.5. Prezentarea Documentului

Furnizorul de servicii de pastrare pe termen lung trebuie sa puna la dispozitia Abonatului posibilitatea ca prin utilizarea software-ului si a dispozitivelor hardware ale Furnizorului de servicii de pastrare pe termen lung la o data si locatie convenita in prealabil sa isi poata vizualiza documentele electronice stocate in arhiva Furnizorului de servicii de pastrare pe termen lung.

3.6. Stergerea documentului si a materialului de validare pe termen lung

Furnizorul de servicii de pastrare pe termen lung trebuie sa puna la dispozitie stergerea selectiva a documentelor electronice si a tuturor materialelor corespunzatoare de validare pe termen lung pastrate in arhiva la cererea Abonatului. Stergerea inseamna stergerea fizica a documentului electronic pastrat si suprascrierea lui in asa fel incat sa nu poata fi restabilit ulterior (sau numai cu cheltuieli financiare nerealist de mari) din mediul de date.

Stergerea se va face in intregul sistem al Furnizorul de servicii de pastrare pe termen lung, iar pe parcursul stergerii se va distruge fiecare copie pastrata a documentului electronic.

Furnizorul de servicii de pastrare pe termen lung trebuie sa precizeze in Declaratia de politici si practici de pastrare pe termen lung modul si conditiile de acceptare si prelucrare a cererii de stergere.

3.7. Incetarea Acordului de Servicii

In cazul finalizarii contractului, Furnizorul de servicii de pastrare pe termen lung va pune la dispozitia Abonatului sau a altei persoane indreptatite documentele electronice si materialele de validare pe termen lung comandate de Abonat pentru a fi pastrate pentru descarcare.

Dupa terminarea contractului, Furnizorul de servicii de pastrare pe termen lung va sterge documentele electronice si materialul de validare pe termen lung corespunzator Abonatului.

3.8. Obiectivele pastrarii pe termen lung

Serviciile de pastrare pe termen lung urmaresc obiective precum:

- Dovada integritatii unui document electronic
- Dovada existentei unui document electronic (la un moment dat/in trecut)
- Mentenanta statusului de validitate a semnaturilor/sigiliilor electronice pe parcursul unor perioade lungi

- Disponibilitatea datelor

Integritatea datelor este verificata pe parcursul timpului de pastrare prin mijloace de asigurare a integritatii (hash, semnatura/sigiliu).

Dovada existentei indica faptul ca obiectul digital a existat la un anumit moment de timp si este implementat prin combinarea unei dovezi de integritate si a unei indicatii de timp de incredere (marca temporala calificata).

Pentru a mentine statusul validitatii unei semnaturi/sigiliu electronic, toate elementele necesare verificarii validitatii si pentru care nu se poate garanta ca vor fi disponibile in viitor, trebuie sa fie, de asemenea, pastrate. Astfel, sunt incluse certificatele, informatiile de revocare (CRL-uri, raspunsuri OCSP), liste de incredere, etc.

Disponibilitatea datelor este asigurata prin utilizarea unor echipamente de stocare dedicate in doua locatii diferite intr-o configuratie de tip “high availability” utilizand o infrastructura in cluster care asigura copii in oglinda pentru toate documentele si meta-datele asociate.

3.9. Profile de pastrare

Furnizorul de servicii de pastrare suporta urmatorul profil de pastrare:


```
  "type": "object",
  "properties": {
    "pid": {
      "type": "https://link.catre.profile.identifier"
    },
    "op": {
      "type": "array",
      "items": {
        "https://lta.transsped.ro/api/PreservePO": "PreservePO",
        "https://lta.transsped.ro/api/RetrievePO": "RetrievePO",
        "https://lta.transsped.ro/api/DeletePO": "DeletePO",
        "https://lta.transsped.ro/api/UpdatePOC": "UpdatePOC",
        "https://lta.transsped.ro/api/Search": "Search"
      }
    },
    "pol": {
      "type": "array",
      "items": {
        "http://uri.etsi.org/19512/policy/preservation-
evidence": "http://uri.etsi.org/19512/policy/preservation-evidence",
      }
    },
    "ext": {
      "type": "array",
      "items": {
        "$ref": "#\/definitions\/md-ExtensionType"
      }
    },
    "sid": {
```

```
        "type": "http://uri.etsi.org/19512/scheme/pds+pgd+wst"
      },
      "pvp": {
        "type": "object",
        "properties": {
          "vfrom": {
            "type": "string",
            "format": "01-04-2020 00:00:00.000"
          },
        }
      },
      "psm": {
        "http://uri.etsi.org/19512/scheme/wst": "WithStorage"
      },
      "pg": {
        "type": "array",
        "items": {
          "http://uri.etsi.org/19512/goal/pgd": "http://uri.etsi.org/19512/goal/pgd"
        }
      },
      "ef": {
        "type": "array",
        "items": {
          "http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp": "http://uri.etsi.org/ades/XAdES/ArchiveTim
eStamp"
        }
      },
      "eed": {
        "type": "One Year"
      }
    }
}
```


Acelasi profil de pastrare va fi aplicat pe intreaga durata de pastrare a documentului, respectiv pe durata de pastrare a evidentei.

3.10. Politica de evidenta a pastrarii

Evidenta de pastrare este creata dupa validarea semnaturilor si marcilor temporale ale documentului. Procesul de validare ia in considerare integritatea semnaturii respectiv ca se potriveste cu amprenta documentului si ca certificatul utilizat pentru semnare este parte din lista de incredere UE si nu este revocat.

Dupa validare, se creeaza un XADES-A xml ce contine toate informatiile necesare pentru a confirma in viitor ca validarea a fost realizata cu succes la momentul testarii:

- Amprenta documentului
- Timpul semnarii
- Certificatul semnarii si calea certificatului
- Semnaturile si marcile temporale

- Date de revocare din OCSP si/sau CRL

Dupa construirea XADES-A, se marcheaza temporal si se stocheaza alaturi de fisier, pregatita sa fie descarcata la cererea clientului utilizand API-ul furnizat. Furnizorul marcilor temporale calificate este Trans Sped S.R.L.

3.11. Politica de validare a semnaturii

Validarea semnaturilor este realizata utilizand Release-ul 5.5 al framework-ului DSS, creat de ESIG si furnizat sub termenii Lesser General Public License (LPGL), versiune 2.1.

Acest framework verifica documentul pentru integritatea semnaturii, conformitatea cu lista de incredere si verifica, de asemenea, serviciile de revocare. Intregul lant al certificatului este verificat. Dupa finalizare, datele sunt extrase si inserate intr-un xml XADES-A conform cu standardele ETSI.

Lista de incredere utilizata este lista de incredere europeana unde Trans Sped S.R.L. este membra.

3.12. Pachete export-import

Furnizorul de servicii de pastrare permite Abonatului sa solicite pachete de export-import continand datele pastrate, evidentele si toate informatiile necesare validarii evidentei

Cererile de export-import vor fi acceptate, dupa cum urmeaza:

- Prin e-mail: cererile trebuie sa fie transmise de la o adresa cunoscuta si aprobata in prealabil
- Prin prezenta fizica: orice persoana care are o imputernicire oficiala de a reprezenta Utilizatorul poate transmite o cerere la sediul Trans Sped

Importul unor volume extinse de documente din diferite platforme necesita o abordare diferita.

Documentele trebuie sa fie prezente in forma lor originala si insotite de un xml XADES-A. Serviciul de import trebuie sa revalideze datele si sa verifice xml-ul XADES-A pentru acuratete, dupa care aplica din nou marca temporala.

Furnizorul de servicii de pastrare poate exporta intregul continut al bazei de date si furniza documentul original, respectiv xml-ul XADES-A asociat acestuia.

4. MASURI TEHNICE DE SECURITATE

4.1. Garantii de securitate

Furnizorul de servicii de pastrare pe termen lung utilizeaza sisteme si produse fiabile protejate impotriva modificarilor. Acesta utilizeaza un sistem informatic uniform care consta in produse de securitate de incredere, evaluate din punct de vedere tehnic si certificate pentru furnizarea serviciilor sale. Furnizorul de servicii de pastrare pe termen lung utilizeaza sisteme si produse fiabile care sunt protejate impotriva modificarilor neautorizate. Atat Furnizorul de servicii de pastrare pe termen lung, cat si furnizorul de sistem si contractorii de instalare au o experienta semnificativa in ceea ce priveste construirea serviciilor de certificare si utilizarea tehnologiilor recunoscute pe plan international.

Daca Furnizorul de servicii de pastrare pe termen lung utilizeaza un serviciu de incredere al unei terte parti, acesta verifica daca respectiva terta parte respecta toate cerintele necesare. Furnizorul de servicii de pastrare pe termen lung stocheaza documentele electronice arhivate intr-un mediu protejat fizic, in conformitate cu cerintele fizice si procedurale descrise in sectiunea 5, a caror siguranta este garantata de politicile de securitate interna si de auditurile regulate interne si externe de securitate.

Furnizorul de servicii de pastrare pe termen lung asigura faptul ca documentele electronice stocate nu pot fi citite nici macar de angajatii sai. Furnizorul de servicii de pastrare pe termen lung trimite documentele electronice unei terte parti (de exemplu autoritate) numai in cazul in care Abonatul autorizeaza acest lucru sau cand este solicitat de lege.

Integritatea dosarelor electronice stocate este asigurata de protectia fizica a dosarelor electronice, precum si de tehnologiile legate de semnaturile electronice sau de criptarea datelor.

Disponibilitatea documentelor electronice este asigurata de sistemul de inalta calitate al Furnizorului de servicii de pastrare pe termen lung si de reglementarile si procedurile interne care reglementeaza sistemul, procedurile de asigurare a continuitatii activitatii si de gestionare a situatiilor de urgenta si alte proceduri de gestionare a situatiilor de urgenta.

Furnizorul de servicii de pastrare pe termen lung evita erorile aparute in timpul operarii si intretinerii prin utilizarea acestor procese si prin monitorizarea si testarea lor continua interna si externa.

Furnizorul de servicii de pastrare pe termen lung stocheaza documentele electronice arhivate in doua locatii fizice una departe de cealalta.

Furnizorul de servicii de pastrare pe termen lung distruge documentele electronice arhivate la cererea Abonatului sau in cazul incetarii contractului - in conditiile descrise in sectiunea 3.6.

Furnizorul de servicii de pastrare pe termen lung monitorizeaza dezvoltarea tehnologiei si daca detecteaza ca o cheie nu mai este sigura sau algoritmul nu mai poate fi utilizat inlocuieste imediat cheia sau cheile afectate.

4.2. Masuri de precautie pentru securitatea computerului

Furnizorul de servicii de pastrare pe termen lung utilizeaza sisteme si solutii IT fiabile, tehnologii si dezvolta un sistem redundant. Doua instante functioneaza pentru toate componentele critice

ale sistemului furnizorului de servicii, iar in cazul unei defectiuni la oricare dintre aceste unitati, cealalta unitate preia operatiunea.

Sistemul IT al Furnizorul de servicii de pastrare pe termen lung este protejat de un sistem de firewall in mai multe etape. Fiecare firewall are doua copii, in caz de defectare a unei unitati, o alta instanta a aceleiasi unitati isi preia functia utilizand un cluster.

4.3. Masuri tehnice de precautie legate de ciclul de viata

Pentru a indeplini cerintele inalte de securitate in toate proiectele de dezvoltare a sistemului Furnizorului de pastrare pe termen lung, cerintele ridicate trebuie luate in considerare in procesul de dezvoltare generala (chiar si in faza de planificare si de definire a cerintelor).

Produsele utilizate pentru furnizarea de servicii sunt aplicate luand in calcul considerentele de securitate legate de ciclul de viata.

4.4. Monitorizarea continua a tehnologiei

Furnizorul de servicii de pastrare pe termen lung este liber sa decida in orice moment sa modifice seturile de algoritmi criptografici utilizati si parametrii lor, in cazul unui algoritm si a unui parametru care este depreciat sau ar putea aduce probleme de securitate.

4.5. Acceptarea furnizorilor de certificare si de marcare temporala

Furnizorul de servicii de pastrare pe termen lung poate specifica in ce conditii accepta Certificatele unei Autoritati de certificare date si ce Autoritati de certificare accepta, impreuna cu criteriile pentru ca Autoritatile de certificare sa fie incluse in aceasta lista sau sa fie excluse din aceasta, in cadrul serviciului de conservare pe termen lung. In principiu, Furnizorii de servicii de incredere calificati pentru semnaturi electronice si marci temporale, publicate pe Listele de incredere ale UE, sunt acceptate.

4.6. Mentinerea lizibilitatii si interpretabilitatii documentelor electronice

Furnizorul de servicii de pastrare pe termen lung trebuie sa stabileasca in mod clar in Declaratia de politici si practici de pastrare pe termen lung sau intr-un alt document ce tip de format de fisier si lizibilitate electronica a documentelor asigura in cadrul serviciului de conservare pe termen lung.

4.7. Disponibilitatea anumitor elemente ale serviciului electronic de pastrare pe termen lung

Disponibilitatea anuala a urmatoarelor elemente electronice de conservare pe termen lung este de 98%, iar intreruperile ocazionale de servicii nu trebuie sa depaseasca 3 zile:

- descarcarea electronica a documentelor electronice arhivate si a lanturilor de valori;
- cautarea documentelor arhivate;

- primirea cererilor de stergere;
- primirea solicitarilor de stergere temporizata (cu ajutorul carora Abonatul poate specifica cat timp este arhivat un anumit e-document de catre Furnizorul de servicii de pastrare pe termen lung) si modificarea cererilor anterioare de stergere temporizata;
- solicitarea de informatii privind starea solicitarilor depuse anterior.

Furnizorul de servicii de pastrare pe termen lung are dreptul sa suspende serviciul de incarcare a documentelor electronice.

5. RESURSE, MANAGEMENT SI COMENZI OPERATIONALE

Furnizorul de servicii de pastrare pe termen lung aplica masurile de precautie fizice, procedurale si de personal care respecta standardele recunoscute, impreuna cu procedurile administrative si de guvernanta implicite pe care le pun in aplicare.

Furnizorul de servicii de pastrare pe termen lung tine o evidenta a unitatilor de sistem si a resurselor legate de furnizarea de servicii si efectueaza o evaluare a riscurilor asupra acestora. Sunt utilizate masuri de protectie proportionale cu riscurile legate de elementele individuale.

Furnizorul de servicii de pastrare pe termen lung monitorizeaza cerintele privind capacitatea si se asigura ca puterea adecvata de procesare si stocarea sunt disponibile pentru furnizarea serviciului.

5.1. Controale fizice

Furnizorul de servicii de pastrare pe termen lung se asigura ca accesul fizic la serviciile critice este controlat si pastreaza la minimum un risc fizic al bunurilor legate de serviciile critice.

Scopul masurilor de precautie fizica este de a impiedica accesul nelegitim, pagubele si accesul neautorizat la informatiile oferite de Furnizorul de servicii de pastrare pe termen lung si in zonele fizice.

Serviciile care proceseaza informatii critice si sensibile sunt implementate in locatii sigure. Protectia furnizata este proportionala cu amenintarile identificate ale analizei de risc pe care a efectuat-o Furnizorul de servicii de pastrare pe termen lung.

5.1.1. Localizarea spatiului si Constructia

Sistemul informatic al Furnizorului de servicii de pastrare pe termen lung este amplasat si operat intr-un Centru de Date corespunzator, protejat fizic si logistic, care impiedica accesul ilegal. Solutiile defensive - cum ar fi, de exemplu, paza, incuietori de securitate, sisteme de detectare a intruziunilor, sisteme de supraveghere video, sistem de control al accesului - sunt instalate pe parcursul localizarii si infiintarii Centrului de Date care sunt construite la distanta una de cealalta si interdependente si impreuna asigura un sistem puternic de protectie a sistemelor IT care participa la furnizarea serviciilor si la pastrarea datelor confidentiale stocate de furnizor.

5.1.2. Accesul fizic

Furnizorul de servicii de pastrare pe termen lung protejeaza dispozitivele si echipamentele care participa la furnizarea de servicii in fata unui acces fizic neautorizat pentru a preveni manipularea dispozitivelor.

Furnizorul de servicii de pastrare pe termen lung se asigura ca:

- fiecare stocare de informatii in Centrul de date este inregistrata;
- intrarea in Centrul de date se poate realiza dupa identificarea simultana a doua persoane autorizate dintre membrii personalului cu roluri de incredere - si cel putin un membru al

personalului este administrator al sistemului;

- persoanele fara autorizatie independenta pot ramane in Centrul de date numai in cazuri justificate, pentru timpul necesar si insotite de personal cu drepturi corespunzatoare;
- jurnalele de intrare sunt arhivate in mod continuu si evaluate saptamanal.

Datele de activare (parolele, codurile PIN) ale dispozitivelor nu vor fi stocate in mod deschis nici macar in Centrul de date.

In prezenta unor persoane neautorizate:

- suporturile de date care contin informatii sensibile nu sunt disponibile din punct de vedere fizic;
- terminalele cu sesiuni deschise nu vor fi lasate nesupravegheate;
- nu se efectueaza niciun proces de lucru in timpul caruia sa se poata dezvalui informatii confidentiale.

La iesirea din sala de calculatoare, administratorul verifica daca:

- fiecare echipament al Centrului de date se afla intr-o stare de functionare sigura;
- nici un terminal nu este lasat conectat;
- dispozitivele de stocare fizica sunt blocate corespunzator;
- sistemele, dispozitivele care asigura protectia fizica functioneaza corespunzator;
- sistemul de alarma a fost activat.

Au fost desemnati oameni responsabili pentru a efectua evaluari periodice de securitate fizica. Rezultatele examinarilor se inregistreaza in intrarile corespunzatoare din jurnal.

5.1.3. Energie si aer conditionat

Furnizorul de servicii de pastrare pe termen lung a dotat Centrul de date cu o unitate de alimentare neintreruptibila care:

- are o capacitate adecvata de a asigura alimentarea cu energie a sistemelor informatice ale Centrului de date si a instalatiilor subsidiare;
- protejeaza echipamentele IT de fluctuatiile de tensiune din reteaua externa, de intreruperile de alimentare, oscilatii de tensiune si alte evenimente;
- in caz de intrerupere de durata a alimentarii cu energie electrica acesta are propriul echipament de generare a energiei electrice, care, permitand realimentarea cu combustibil, este capabil sa furnizeze energia necesara pentru orice perioada de timp.

Puritatea aerului Centrului de Date este controlata cu un sistem adecvat de filtrare pentru a detecta o varietate de contaminanti din aer (praf, poluanti si materiale corozive, substante toxice sau inflamabile). Sistemul de ventilatie furnizeaza cantitatea necesara de aer proaspat cu filtrare adecvata pentru conditiile sigure de lucru ale operatorilor.

Umiditatea este redusa la nivelul solicitat de sistemele informatice.

Sistemele de racire cu performante adecvate sunt folosite pentru a asigura temperatura necesara de functionare, pentru a preveni supraincalzirea dispozitivelor informatice.

5.1.4. Expuneri la apa

Centrul de date al Furnizorului de servicii de pastrare pe termen lung este protejat in mod corespunzator de intruziuni si inundatii.

5.1.5. Prevenirea si protectia impotriva incendiilor

Detectoarele de fum si de incendiu se instaleaza in Centrul de date al Furnizorului de servicii de pastrare pe termen lung care alerteaza automat departamentul de pompieri. Extinctoare manuale de stingere de tipul adecvat si in cantitatea corespunzatoare, care respecta reglementarile relevante sunt amplasate intr-un loc vizibil in fiecare camera.

Extinctoarele automate de incendiu sunt instalate in Centrul de date.

5.1.6. Stocare media

Furnizorul de servicii de pastrare pe termen lung trebuie sa isi protejeze unitatile cu date media de accesul neautorizat si deteriorarea accidentala. Toate datele de audit si arhiva vor fi create in dublu exemplar. Cele doua copii trebuie sa fie stocate separat fizic una de cealalta, in locatii aflate la o distanta sigura una de cealalta. Unitatile de stocare media trebuie sa fie protejate impotriva efectelor nocive ale mediului cum ar fi temperaturile scazute sau ridicate, murdaria, umiditatea, lumina soarelui, campurile magnetice puternice, radiatiile puternice.

5.1.7. Eliminarea deseurilor

Furnizorul de servicii de pastrare pe termen lung se asigura de distrugerea dispozitivelor sale, depozitele media devenind inutile in conformitate cu reglementarile de mediu.

Astfel de dispozitive si unitatile de stocare media vor fi sterse definitiv sau facute inutilizabile, in conformitate cu metodele larg acceptate, sub supravegherea personala a angajatilor Furnizorului de servicii de pastrare pe termen lung.

5.1.8. Copie de rezerva in afara site-ului

Furnizorul de servicii de pastrare pe termen lung creeaza o copie de rezerva saptamanala, din care intregul serviciu ar putea fi restabilit in cazul unei erori majore. Backup-urile, inclusiv cel putin ultima copie completa de rezerva, sunt stocate intr-o locatie externa, iar protectia fizica si operationala este identica cu cea a site-ului primar. Se asigura transmisia securizata de date de la locatiile primare la cele de rezerva.

5.2. Controale procedurale

Furnizorul de servicii de pastrare pe termen lung se asigura ca sistemele sale functioneaza in siguranta, in conformitate cu normele si cu un risc minim de defecte.

Masurile de precautie procedurale au ca obiectiv sa completeze si, in acelasi timp, sa intensifice eficacitatea serviciilor de paza fizica, impreuna cu cele aplicabile personalului, prin mijloace de numire si izolare a rolurilor de incredere, documentarea responsabilitatilor diferitelor roluri, precum si precizarea efectivului de personalului si posturile de excludere necesare pentru diferitele sarcini, si in plus identificarea si autentificarea asteptate in diferitele posturi.

Sistemul de guvernanta interna al furnizorului de pastrare pe termen lung asigura respectarea atat a reglementarilor legale, cat si a reglementarilor interne. Persoane responsabile sunt repartizate in mod clar pentru fiecare unitate de sistem si proces dat.

Persoanele responsabile pentru un element de sistem sau proces sunt atribuite fara echivoc fiecarui element de sistem si fiecarui proces din sistemul sau. Activitatile legate de dezvoltare si operatiuni sunt foarte segregate in sistemul Furnizorul de servicii de pastrare pe termen lung. Activitatea de audit a auditorului independent al sistemului si a auditorului intern al Furnizorul de servicii de pastrare pe termen lung asigura functionarea adecvata a sistemului.

5.2.1. Roluri de incredere

Furnizorul de servicii de pastrare pe termen lung a stabilit roluri de incredere pentru indeplinirea sarcinilor sale. Drepturile si functiile sunt impartite intre diversele posturi de incredere, astfel incat un singur utilizator sa nu poata ocoli masurile de protectie si securitate.

Furnizorul de servicii de pastrare a definit urmatoarele roluri:

- manager cu responsabilitate generala pentru sistemele informatice;
- ofiter de securitate: persoana cu responsabilitate generala pentru securitatea serviciului;
- administrator de sistem: persoana care realizeaza instalarea, configurarea si intretinerea sistemului informatic;
- operator: persoana care efectueaza operarea, backupul si restaurarea continua a sistemului informatic;
- auditor independent al sistemului: persoana care efectueaza auditul setului de date logate, precum si arhivate ale furnizorului, responsabil pentru verificarea aplicarii masurilor de control pe care furnizorul le pune in aplicare in interesul operarii conforme cu reglementarile, si in plus pentru auditul si monitorizarea continua a procedurilor existente.
- ofiter de pastrare pe termen lung: este capabil sa decripteze un document electronic cu cooperarea a doi ofiteri de conservare pe termen lung. Ofiterii de pastrare pe termen lung sunt responsabili pentru gestionarea sigura a documentului electronic decriptat si pentru distrugerea ulteriora a acestuia dupa utilizare.
- ofiter responsabil pentru emiterea declaratiei de pastrare pe termen lung: datoria sa consta in eliberarea si certificarea declaratiilor de pastrare pe termen lung.

Pentru desemnarea de posturi de incredere, managerul insarcinat cu securitatea Furnizorul de servicii de pastrare pe termen lung numeste oficial angajatii Furnizorul de servicii de pastrare pe termen lung. Numai persoanele care sunt in relatii de munca cu Furnizorul de servicii de pastrare pe termen lung pot detine un post de incredere. Posturile de incredere nu sunt detinute in contextul unui contract de comision.

5.2.2. Identificarea si autentificarea pentru fiecare post

Utilizatorii care administreaza sistemul informatic al Furnizorului de servicii de pastrare pe termen lung detin date de identificare unice, care permit identificarea sigura si autentificarea utilizatorilor.

Utilizatorii pot accesa numai sistemele IT critice din punct de vedere al furnizarii serviciului de certificare dupa identificare si autentificare.

Datele de identificare si autentificare sunt revocate fara intarziere in cazul incetarii drepturilor utilizatorilor.

5.2.3. Roluri care necesita separarea sarcinilor

Angajatii Furnizorului de servicii de pastrare pe termen lung pot detine simultan mai multe posturi de incredere, insa Furnizorul de servicii de pastrare pe termen lung este obligat sa se asigure ca:

- ofiterul de securitate si ofiterul de inregistrare nu detin postul de auditor independent al sistemului;
- administratorul de sistem nu detine postul de auditor independent al sistemului si cel de ofiter de securitate;
- managerul cu responsabilitate globala pentru sistemele informatice nu detine postul de ofiter de securitate si postul de auditor independent al sistemului.

5.3. Controale la nivel de personal

Furnizorul de servicii de pastrare pe termen lung se asigura ca politica sa de personal si practicile sale aplicabile angajarii membrilor personalului intensifica si sprijina fiabilitatea operarii Furnizorului de servicii de pastrare pe termen lung. Obiectivul masurilor de precautie aplicabile personalului este de a reduce riscului de erori umane, furt, frauda si cazuri de utilizare incorecta.

Furnizorul de servicii de pastrare pe termen lung abordeaza securitatea personalului care se afla deja in timpul etapei de angajare, inclusiv incheierea contractelor, precum si validarea acestora atunci cand sunt angajati.

In cazul tuturor posturilor de incredere, solicitantii trebuie sa aiba un certificat valabil care sa demonstreze ca nu au cazier judiciar in momentul depunerii cererii. Fiecare angajat intr-un post de incredere si partile externe care intra in contact cu serviciile Furnizorului de servicii de pastrare pe termen lung trebuie sa semneze un acord de confidentialitate.

In acelasi timp, Furnizorul de servicii de pastrare pe termen lung va asigura angajatilor sai obtinerea dar si dezvoltarea in continuare a cunostintelor generale de baza, impreuna cu cunostintele profesionale de specialitate necesare pentru realizarea diverselor indatoriri.

5.3.1. Calificari, experienta si cerinte de lichidare

Fiecare angajat al Furnizorul de servicii de pastrare pe termen lung trebuie sa aiba educatia necesara, practica si experienta profesionala pentru asigurarea domeniului sau de activitate. Chiar si in timpul recrutarii, trebuie sa se acorde o atentie speciala trasaturilor de personalitate atunci cand se selecteaza potentiali angajati si pot fi angajate numai persoane fiabile pentru posturi de incredere.

Posturile de incredere pot fi detinute in cadrul companiei Furnizorul de servicii de pastrare pe termen lung numai de catre persoane care nu au influenta externa si poseda expertiza necesara validata de Furnizorul de servicii de pastrare pe termen lung.

Managerul cu responsabilitate generala pentru sistemul IT nu poate fi decat o persoana care are:

- diploma de specialitate (matematica, liceu de fizica sau diploma universitara sau diploma de liceu / universitara dobandita la un departament de inginerie apartinand domeniului tehnic al stiintei);
- cel putin trei ani de expertiza in experienta profesionala de lucru in domeniul securitatii informatiilor.

5.3.2. Proceduri de verificare a datelor din trecut

Furnizorul de servicii de pastrare pe termen lung trebuie sa angajeze doar angajati pentru posturi de incredere sau de conducere, care:

- nu au cazier judiciar si nu exista nicio actiune in desfasurare impotriva acestora care ar putea afecta impunitatea.
- nu sunt subiectul unor descalificari profesionale care interzic sa exercite servicii legate de semnaturile electronice.

La momentul numirii, angajatul care detine postul pe termen lung, angajatul Furnizorului de servicii de pastrare pe termen lung da o declaratie si prezinta un certificat de buna conduita cu un termen de valabilitate mai mic de 3 luni care justifica cazierul judiciar curat.

Furnizorul de servicii de pastrare pe termen lung verifica autenticitatea informatiilor relevante prezentate in CV-ul solicitantului in timpul procesului de angajare.

5.3.3. Cerinte de formare

Furnizorul de servicii de pastrare pe termen lung instruieste noii angajati recrutati, pe parcursul carui proces dobandesc:

- cunostinte de baza despre PKI;
- specificul si modul de gestionare a sistemului informatic al Furnizorului de servicii de pastrare pe termen lung;
- cunostintele speciale necesare pentru indeplinirea domeniului de activitate;
- procesele si procedurile definite in regulamentele publice si interne ale Furnizorul de servicii de pastrare pe termen lung;
- consecintele juridice ale activitatilor individuale;
- reglementarile aplicabile in materie de securitate IT in masura necesara pentru domeniul specific al activitatilor;
- normele privind protectia datelor.

Doar angajatii care au trecut de modulul de formare vor avea acces la sistemul informatic de productie al Furnizorului de servicii de pastrare pe termen lung.

5.3.4. Frecventa de instruire si Cerinte

Furnizorul de servicii de pastrare pe termen lung se asigura in mod continuu ca angajatii au cunostintele necesare, astfel incat, daca este necesar, sa se desfasoare o formare suplimentara sau repetata.

Instruirea ulterioara se desfasoara in cazul in care exista o schimbare in cadrul operatiunilor sau al sistemului informatic al Furnizorului de servicii de pastrare pe termen lung.

5.3.5. Succesiunea si Frecventa de Rotatie a postului

Nicio stipulare.

5.3.6. Sanctiuni pentru Masuri Neautorizate

Furnizorul de servicii de pastrare pe termen lung reglementeaza intr-un contract de munca posibilitatile de urmarire penala ale angajatilor in caz de defectiuni, erori, daune accidentale sau intentionate. Daca angajatul - din neglijenta sau intentionat - isi incalca obligatiile, Furnizorul de servicii de pastrare pe termen lung poate da sanctiuni impotriva lui si aceasta le stabileste tinand cont de infractiune si de consecintele acesteia. Sanctiunile pot include proceduri disciplinare, concediere, revocare a numirii, raspundere penala.

5.3.7. Cerinte ale contractantului independent

Lucratorilor angajati cu relatii contractuale li se aplica aceleasi reguli cu cele referitoare la restul angajatilor.

Persoana care detine postul de incredere trebuie sa se afle intr-o relatie de munca cu Furnizorul de servicii de pastrare pe termen lung.

5.4. Proceduri de inregistrare a auditului

Pentru a mentine un mediu IT sigur, Furnizorul de servicii de pastrare pe termen lung va implementa si va opera un sistem de control si de inregistrare a evenimentelor care sa acopere intregul sau sistem informatic.

5.4.1. Tipurile de evenimente inregistrate

Furnizorul de servicii de pastrare pe termen lung inregistreaza toate evenimentele legate de securitate care pot furniza informatii despre evenimente, schimbari survenite in sistemul IT sau in mediul sau fizic, in conformitate cu practica generala acceptata de securitate a informatiilor. In cazul fiecarei inregistrari in jurnal, se pastreaza urmatoarele date:

- ora evenimentului;
- tipul evenimentului;
- succesul sau esecul implementarii;
- identificarea utilizatorului sau a sistemului care a declansat evenimentul.

Toate jurnalele de evenimente esentiale vor fi puse la dispozitia auditorilor independenti ai sistemului, care examineaza conformitatea functionarii Furnizorul de servicii de pastrare pe termen lung.

Cel putin urmatoarele evenimente vor fi inregistrate:

- PASTRAREA PE TERMEN LUNG
  - informatii referitoare la incarcarea e-dosarelor si la validarea semnaturilor electronice din cadrul acestora;
  - informatii referitoare la disponibilitatea datelor, conservarea integritatii, conservarea autenticitatii si non-repudierii, mentinerea lizibilitatii si stergerii informatiilor;
  - informatii legate de descarcarea dosarului electronic, completarea cererii de declaratie si predarea arhivei unui alt furnizor;
- AUTENTIFICARE
  - oprirea, repornirea sistemului de autentificare sau a unora dintre componentele acestuia;
  - modificarea oricarui parametru al setarilor de inregistrare, de exemplu, frecventa, pragul de alerta si evenimentul care trebuie sa fie examinat;
  - modificarea sau stergerea datelor de autentificare stocate;
  - activitatile desfasurate din cauza avariei sistemului de autentificare.
- AUTENTIFICARI IN SISTEM:
  - inregistrari reusite, incercari de conectare nereusite pentru posturi de incredere;
  - in cazul autentificarii bazate pe parola:
  - schimbarea numarului de incercari nereusite permise;
  - atingerea limitei numarului permis de incercari de conectare nereusite in cazul unei autentificari a unui utilizator;
  - reautentificarea utilizatorului blocat din cauza incercarilor de conectare nereusite;
  - modificarea tehnicii de autentificare (de exemplu, din parola bazata pe PKI).
- MANAGEMENTUL CHEILOR:
  - toate evenimentele pentru intregul ciclu de viata al cheilor de servicii (generare de chei, incarcare, salvare, etc.);
- FLUX DE DATE:
  - orice tip de date critice privind siguranta introduse manual in sistem;
  - date relevante pentru siguranta, mesaje primite de sistem;
- HSM:
  - instalarea unui HSM;
  - eliminarea unui HSM;

- dispunerea, distrugerea unui HSM;
- livrarea unui HSM;
- curatarea (resetarea) unui HSM;
- incarcarea cheilor, certificate catre HSM

- SCHIMBARE A CONFIGURARII:
  - hardware;
  - software;
  - sistem de operare;
  - patch;
- ACCESUL FIZIC, SECURITATEA LOCATIEI:
  - intrarea si iesirea unei persoane din zona de securitate care detine componentele CA;
  - acces la o componenta a sistemului CA;
  - o incalcare cunoscuta sau suspectata a securitatii fizice;
  - firewall sau trafic de ruter
- ANOMALII OPERATIONALE:
  - defectiune de sistem, eroare de hardware;
  - eroare de software;
  - eroarea de validare a integritatii software-ului;
  - mesaje incorecte sau adresate incorect;
  - atacuri de retea, incercari de atac;
  - defectarea echipamentului;
  - defectiuni electrice;
  - eroare de alimentare neintreruptibila;
  - o eroare de acces esentiala la serviciul de retea;
  - incalcarea politicilor si practicilor de pastrare pe termen lung;
  - stergerea ceasului sistemului de operare
- ALTE EVENIMENTE:
  - numirea unei persoane intr-un post de securitate;
  - instalarea sistemului de operare;
  - instalarea aplicatiei PKI;
  - initierea unui sistem;
  - incercarea de autentificare in aplicatia PKI;

- modificarea parolei, incercarea de setare;
- salvarea bazei de date interioare si restaurarea dintr-o copie de rezerva;
- operatii cu fisiere (de exemplu creare, redenumire, mutare);
- acces la baza de date

5.4.2. Frecventa prelucrarii jurnalului de audit

Furnizorul de servicii de pastrare pe termen lung asigura evaluarea regulata a jurnalelor create.

Fisierele cu jurnale zilnice create vor fi evaluate in urmatoarea zi lucratoare daca este posibil, dar nu mai tarziu de 1 saptamana.

Evaluarea fisierelor de jurnal va fi efectuata de un auditor independent de sistem cu experienta, privilegii de sistem si programare prealabila.

Furnizorul de servicii de pastrare pe termen lung utilizeaza instrumente automatizate pentru a sustine evaluarea jurnalelor electronice.

In cursul evaluarii, se asigura autenticitatea si integritatea jurnalelor examinate. In timpul evaluarii, sistemul analizeaza mesajele de eroare generate de sistem.

Modificarile semnificative ale traficului sunt analizate prin metode statistice. Desfasurarea auditului, rezultatele auditului si masurile luate pentru eliminarea oricaror deficiente constatate sunt documentate in mod corespunzator.

5.4.3. Perioada de mentinere a jurnalului de audit

Inainte de stergerea din sistemul on-line, jurnalele trebuie sa fie arhivate, iar pastrarea lor securizata sa fie asigurata pentru perioada de timp definita in Sectiunea 5.5.2.

5.4.4. Protectia Jurnalului de audit

Furnizorul de servicii de pastrare pe termen lung va proteja jurnalele create pentru timpul de conservare necesar. In timpul intregului timp de conservare, se asigura urmatoarele proprietati ale datelor din fisiere:

- protectia impotriva divulgarii neautorizate: numai persoanele autorizate - in primul rand auditorii independenti ai sistemului - vor accesa jurnalele;
- disponibilitate: persoanelor autorizate li se permite accesul la jurnale;
- integritate: orice modificare a datelor, stergerea in fisierele de jurnal si schimbarea in ordinea inregistrarilor, etc. trebuie prevenite.

5.4.5. Proceduri de backup a jurnalului de audit

Fisierele zilnice ale jurnalului vor fi create din intrarile continuue generat in jurnal in timpul operarii in fiecare sistem.

Fisierele zilnice ale jurnalului vor fi arhivate dupa evaluare in doua copii si vor fi stocate fizic la distanta una de cealalta, in locuri separate pentru timpul solicitat.

Procesul exact al backup-urilor este definit in procedurile interne de back-up.

5.4.6. Sistemul de colectare a auditului (Intern vs Extern)

Furnizorul de servicii de pastrare pe termen lung precizeaza functionarea proceselor sale de inregistrare in Declaratia de politici si practici de conservare pe termen lung.

Furnizorul de servicii de pastrare pe termen lung poate utiliza sisteme automate de audit si inregistrare daca se poate asigura ca acestea sunt active in momentul lansarii sistemului si functioneaza continuu pana la inchiderea sistemului.

Daca exista vreo anomalie in sistemele automate de audit si de inregistrare, functionarea Furnizorul de servicii de pastrare pe termen lung va fi suspendata pana la rezolvarea incidentului.

5.4.7. Notificarea referitoare la subiectul care cauzeaza evenimente

In cazul erorilor detectate, Furnizorul de servicii de pastrare pe termen lung, la discretia sa, poate decide daca notifica persoana, postul, dispozitivul sau aplicarea erorii care a provocat-o.

5.4.8. Evaluari ale vulnerabilitatilor

Evaluarea vulnerabilitatilor este efectuata in fiecare an de catre Furnizorul de servicii de pastrare pe termen lung pentru a ajuta la descoperirea potentialelor amenintari interne si externe, care pot duce la acces neautorizat. Probabilitatea aparitiei evenimentului si daunele asteptate vor fi de asemenea estimate.

Se vor evalua in mod regulat procesele implementate, masurile de siguranta, sistemele informatice, astfel incat sa poata face fata adecvat amenintarilor detectate.

Dupa evaluarea erorilor detectate, daca este necesar, sistemele de aparare vor fi modificate pentru a preveni astfel de erori in viitor.

5.5. Arhiva inregistrarilor

5.5.1. Tipuri de inregistrari arhivate

Furnizorul de servicii de pastrare pe termen lung va fi pregatit pentru arhivarea sigura pe termen lung a documentelor electronice si a celor pe suport de hartie.

Furnizorul de servicii de pastrare pe termen lung arhiveaza urmatoarele tipuri de informatii:

- orice document legat de acreditarea Furnizorului de servicii de pastrare pe termen lung;
- toate versiunile emise ale Declaratiei privind politicile de certificare si declaratiile privind practicile de conservare pe termen lung;
- toate versiunile emise de Termeni si conditii;
- contracte legate de functionarea Furnizorului de servicii de pastrare pe termen lung;
- fiecare inregistrare electronica si pe suport de hartie

5.5.2. Perioada de mentinere pentru arhiva

Furnizorul de servicii de pastrare pe termen lung este obligat sa pastreze datele arhivate pentru perioadele de timp de mai jos:

- Declaratia de Politici si Practici: 10 ani si 6 luni de la revocare.

5.5.3. Protectia arhivei

Furnizorul de servicii de pastrare pe termen lung este obligat sa stocheze toate datele arhivate in doua exemplare, in locuri fizice separate unul de cealalt. Un document de hartie sau o copie electronica pot fi facute in conformitate cu legea aplicabila de pe singura copie autentica pe suport de hartie a documentului disponibil.

Fiecare dintre cele doua locatii trebuie sa indeplineasca cerintele pentru securitatea arhivarii si a altor cerinte.

In timpul pastrarii datelor arhivate, se asigura ca:

- integritatea lor este pastrata;
- sunt protejate impotriva accesului neautorizat;
- sunt disponibile;
- pastreaza autenticitatea

Datele electronice arhivate trebuie sa fie furnizate cu cel putin o semnatura electronica avansata sau un sigiliu si o Marca temporala calificata.

5.5.4. Proceduri de back-up a arhivei

Duplicatul datelor arhivate este stocat intr-o locatie separata fizic de amplasarea site-ul Furnizorului de servicii de pastrare pe termen lung in conformitate cu cerintele din Sectiunea 5.1.8.

5.5.5. Cerinte pentru marcarea temporala a inregistrarilor

Fiecare intrare din jurnalul electronic este prevazuta cu un semn temporal pe care, cu o precizie de cel putin o secunda, este indicat timpul sistemului asigurat.

Furnizorul de servicii de pastrare pe termen lung se asigura ca, in sistemele sale de furnizor de servicii, ceasul sistemului este cel mult diferit fata de timpul de referinta cu o secunda. Timpul sistemului utilizat pentru generarea semnalului temporal trebuie sincronizat cu ora UTC cel putin o data pe zi.

Fisierele de jurnale zilnice trebuie sa fie prevazute cu o Marca temporala.

In timpul pastrarii datelor arhivate, daca este necesar (de exemplu schimbarea algoritmului o data cu expirarea Marcii temporale originale), se va asigura autenticitatea datelor.

5.5.6. Sistemul de colectare a arhivei (Intern sau Extern)

Inregistrarile in jurnal vor fi generate in sistemul informatic protejat al Furnizorului de servicii de pastrare pe termen lung si numai fisierele de jurnal care sunt semnate electronic il pot parasi.

5.5.7. Proceduri de obtinere si verificare a informatiilor din arhiva

Furnizorul de servicii de pastrare pe termen lung poate crea fisierele de jurnal manual sau automat. In cazul sistemului automat de inregistrare, fisierele de jurnal certificate vor fi generate zilnic.

Fisierele arhivate vor fi protejate impotriva accesului neautorizat.

Accesul controlat la datele arhivate trebuie sa fie disponibil persoanelor eligibile:

- Clientii sunt eligibili pentru a vedea datele stocate despre ei;
- in litigii juridice, pentru a asigura dovezi, trebuie furnizate datele necesare.

5.6. Recuperare dupa compromitere si dezastru

In caz de dezastru, Furnizorul de servicii de pastrare pe termen lung ia toate masurile necesare pentru a minimiza daunele rezultate din deficienta serviciului si restabileste serviciile cat mai repede posibil.

Pe baza evaluarii incidentului care a avut loc, acesta va lua masurile necesare, decizii corective pentru a preveni aparitia incidentului in viitor.

Odata ce problema a fost rezolvata, evenimentul va fi raportat autoritatii de supraveghere.

5.6.1. Proceduri de abordare a incidentului si a evenimentului compromis

Furnizorul de servicii de pastrare pe termen lung a implementat un plan de continuitate a activitatii.

Furnizorul de servicii de pastrare pe termen lung stabilieste si mentine un sistem de rezerva complet functional, care se afla la o distanta sigura de locatia primara, amplasat geografic intr-un loc diferit si care este independent capabil sa furnizeze intreaga gama de servicii.

Furnizorul de servicii de pastrare pe termen lung testeaza in permanenta functionarea sistemului de rezerva si revizuieste anual planurile de continuitate a activitatii.

In caz de dezastru, disponibilitatea serviciilor trebuie restabilita cat mai repede posibil.

5.6.2. Resursele de calcul, software-ul si / sau datele sunt compromise

Sistemele informatice ale Furnizorului de servicii de pastrare pe termen lung sunt construite din componente hardware si software fiabile. Functiile critice sunt puse in aplicare utilizand elemente de sistem redundante, astfel incat, in cazul unei defectiuni a unui element, acestea sa poata functiona in continuare.

Furnizorul de servicii de pastrare pe termen lung efectueaza o copie de siguranta zilnica completa a bazelor sale de date si a evenimentelor din jurnalul generat.

Furnizorul de servicii de pastrare pe termen lung efectueaza copii de siguranta complete atat de frecvent cat este necesar pentru a putea restabili intregul serviciu in caz de dezastru.

Planul de continuitate a activitatii Furnizorului de servicii de pastrare pe termen include cerinte exacte pentru sarcinile care trebuie indeplinite in caz de defectare a componentei esentiale a sistemului.

Odata ce problema a fost rezolvata si integritatea restabilita, Furnizorul de servicii de pastrare pe termen lung isi va reporni serviciile cat mai curand posibil.

5.6.3. Capacitatea de continuitate a afacerii dupa un dezastru

Sarcinile care trebuie indeplinite in caz de nerespectare a serviciului ca urmare a dezastrelor naturale sau de alta natura sunt definite in planul de continuitate a afacerii al Furnizorului de servicii de pastrare pe termen lung. In caz de dezastru, reglementarile prevazute intra in vigoare si se demareaza managementul daunelor si restabilirea serviciilor.

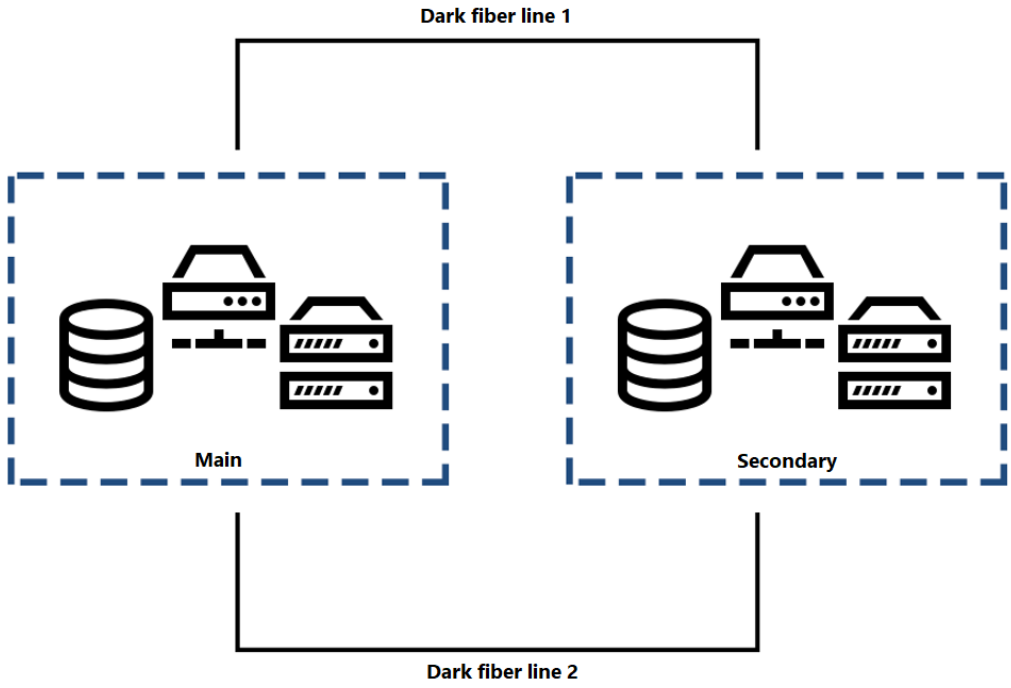
Site-ul secundar al serviciilor este plasat astfel incat un dezastru probabil sa nu poata ajunge simultan in ambele locatii.

Furnizorul de servicii de pastrare pe termen lung se obliga sa notifice utilizatorii afectati cat mai repede posibil in caz de dezastru.

Dupa restaurarea serviciilor, Furnizorul de servicii de pastrare pe termen lung va restabili cat mai repede posibil dispozitivele deteriorate in timpul dezastrului dar si nivelul original de securitate al serviciului.

5.6.4. Masuri de asigurare a disponibilitatii datelor

Furnizorul de servicii de pastrare pe termen lung foloseste o infrastructura care este plasata in doua centre de date care sunt interconectate prin intermediul a doua linii de tip “Dark fiber” asigurand un canal de comunicatii extrem de securizat intre cele doua centre de date.



Sistemul de pastrare pe termen lung este distribuit in doua centre de date intr-o topologie active - standby. Toate serverele virtuale care gazduiesc componente ale sistemului de pastrare pe termen lung sunt inrolate intr-un mecanism de back-up zilnic cu o perioada de retentie a copiilor de back-up de 30 de zile, dupa cum urmeaza:

- In sediul principal – utilizand un echipament de stocare dedicat localizat in centrul de date principal
- In afara sediului – utilizand un echipament de stocare dedicat localizat in centrul de date secundar al Trans Sped

Toate serverele virtuale care gazduiesc componente ale sistemului de pastrare pe termen lung sunt replicate zilnic din centrul de date principal in centrul de date secundar.

Sistemul de pastrare pe termen lung este implementat intr-o configuratie de inalta disponibilitate (high availability) in infrastructura cluster care asigura copii in oglinda ale tuturor documentelor si ale metadatelor asociate.

Componentele aplicatiei ruleaza pe servere virtualizate gazduite in cluster in configuratie activ – standby.

Documentele stocate sunt pastrate in oglinda pe doua echipamente de stocare distincte din punct de vedere fizic.

Aplicatiile si datele sunt salvate si replicate pe o infrastructura dedicata in centrul de date secundar. Procedurile de replicare sunt executate prin linii de tip “Dark Fiber” intre cele doua centre de date.

5.7. Incetarea serviciului de pastrare pe termen lung

Furnizorul de servicii de pastrare pe termen lung respecta cerintele prevazute de legislatie in cazul incetarii serviciului.

In timpul incetarii, sarcinile prioritare sunt:

- Partile de incredere si Abonatii vor fi instiintati in timp util despre incetarea planificata;
- Furnizorul de servicii de pastrare pe termen lung trebuie sa depuna toate eforturile pentru a se asigura ca, cel tarziu pana la finalizarea serviciului, un alt furnizor preia inregistrarile si obligatiile de serviciu;
- Dupa finalizarea serviciului, se va efectua o copie de rezerva completa si o arhivare a sistemului;
- Datele arhivate vor fi inmanate furnizorului care preia serviciile.

6. CONTROALE TEHNICE DE SECURITATE

Furnizorul de servicii de pastrare pe termen lung utilizeaza sisteme si echipamente fiabile protejate impotriva modificarilor pentru gestionarea intregului ciclu de viata al documentelor electronice.

Cerintele privind capacitatea sunt monitorizate in mod continuu si se realizeaza estimari viitoare asupra cerintelor de capacitate, astfel incat sa fie asigurata disponibilitatea solicitata a procesarii si a necesitatilor de stocare.

6.1. Date de activare

6.1.1. Generarea si instalarea de date de activare

Cheile private ale Furnizorul de servicii de pastrare pe termen lung sunt protejate in conformitate cu procedurile, cerintele definite in ghidul de utilizare a HSM-ului (Hardware Security Module) si in documentele de certificare.

In cazul utilizarii datelor de activare bazate pe parole, parolele sunt stabilite astfel incat sa fie suficient de complexe pentru a asigura nivelul necesar de protectie.

6.1.2. Protejarea datelor de activare

Dispozitivele si datele de activare necesare pentru activarea cheii private sunt stocate in siguranta de catre angajatii Furnizorului de servicii de pastrare pe termen lung, iar parolele sunt stocate numai codat.

6.1.3. Alte aspecte ale datelor de activare

Nicio stipulare.

6.2. Controale de securitate IT

6.2.1. Cerinte tehnice de securitate

In timpul configurarii si operarii sistemelor informatice ale Furnizorului de servicii de pastrare pe termen lung se asigure respectarea urmatoarelor cerinte:

- identitatea utilizatorului este verificata inainte de acordarea accesului la sistem sau la aplicatie;
- rolurile sunt atribuite utilizatorilor si utilizatorii au doar permisiuni adecvate pentru rolurile lor;
- pentru fiecare tranzactie este creata o inregistrare in jurnal si intrarile din jurnal sunt arhivate;
- pentru procesele critice din punct de vedere al securitatii se asigura ca domeniile interne ale retelei Furnizorului de servicii de pastrare pe termen lung sunt suficient protejate impotriva accesului neautorizat;

- sunt implementate proceduri adecvate pentru a asigura recuperarea serviciului dupa pierderea unei chei sau a unei defectiuni de sistem.

6.2.2. Evaluarea securitatii IT

Pentru a asigura securitatea IT si calitatea serviciilor, Furnizorul de servicii de pastrare pe termen lung a implementat sisteme de control prin metodologii acceptate pe plan international, iar caracterul adecvat al acestora este demonstrat printr-un certificat emis de un organism independent de certificare (de exemplu, certificarea ISO 27001).

6.3. Controale tehnice la nivelul ciclului de viata

6.3.1. Controale cu privire la dezvoltarea sistemelor IT

Furnizorul de servicii de pastrare pe termen lung utilizeaza numai aplicatii si dispozitive in sistemul sau IT de productie care:

- sunt software-uri comerciale la pachet, concepute si dezvoltate printr-o metodologie documentata de proiectare;
- sunt solutii personalizate de hardware si software dezvoltate de un partener de incredere pentru Furnizorul de servicii de pastrare pe termen lung, in timpul a caror realizare s-au utilizat metode structurate si un mediu de dezvoltare controlat;
- sunt solutii open source care respecta cerintele de securitate si adecvarea acestora este asigurat de verificarea software-ului si de dezvoltarea structurata si de gestionarea ciclului de viata.

Achizitia se desfasoara intr-un mod care exclude modificarea componentelor hardware si software.

Componentele hardware si software aplicate pentru furnizarea de servicii nu pot fi utilizate in alte scopuri.

Furnizorul de servicii de pastrare pe termen lung, cu ajutorul masurilor adecvate de protectie, ia toate masurilor sa impiedice accesarea malitioasa a software-ului pentru a accesa dispozitivele utilizate in serviciul de certificare.

Inainte de prima utilizare si, ulterior, componentele hardware si software sunt verificate in mod regulat de cod malitios.

Furnizorul de servicii de pastrare pe termen lung actioneaza cu aceeasi precautie in cazul achizitiilor de actualizare a programului, dar si la achizitionarea primei versiuni.

Instalarea software- ului si a hardware-ului se realizeaza de catre personal de incredere si instruit corespuzator.

Furnizorul de servicii de pastrare pe termen lung poate instala doar software-ul pe echipamentul sau IT necesar pentru a asigura furnizarea serviciului.

Furnizorul de servicii de pastrare pe termen lung dispune de un sistem de control al versiunii, in care fiecare schimbare este documentata.

Furnizorul de servicii de pastrare pe termen lung implementeaza proceduri pentru detectarea unei modificari neautorizate.

6.3.2. Controalele pentru managementul securitatii

Furnizorul de servicii de pastrare pe termen lung trebuie sa implementeze procesele de documentare, operare, verificare, monitorizare si intretinere a sistemelor utilizate in serviciu, inclusiv modificarea si dezvoltarea lor ulterioara. Sistemul de control al versiunii trebuie sa detecteze orice tip de modificari neautorizate, introducerea datelor care afecteaza sistemul, firewall-ul, routerele, programele si alte componente utilizate in serviciu. Instalarea programului folosit in serviciul asigurat de Furnizorul de servicii de pastrare pe termen lung va asigura ca programul care urmeaza sa fie instalat reprezinta versiunea corespunzatoare si ca este securizat in fata oricarei modificari neautorizate. Furnizorul de servicii de pastrare pe termen lung verifica in mod regulat integritatea software-ului in sistemul sau utilizat in serviciu.

6.3.3. Controalele de securitate la nivelul ciclului de viata

Furnizorul de servicii de pastrare pe termen lung trebuie sa asigure protectia Modulelor de securitate a hardware-ului utilizat pe parcursul intregului lor ciclu de viata.

- Modulele criptografice (HSM) utilizate detin certificari corespunzatoare de securitate;
- La primirea Modulului criptografic, se verifica daca protectia dispozitivelor impotriva modificarilor fizice a fost asigurata in timpul transportului;
- Se asigura protectia Modulului criptografic impotriva modificarilor fizice in timpul stocarii;
- In timpul operarii, se respecta in mod continuu cerintele aplicarii securitatii Modulelor criptografice, ghidul de utilizare si raportul de certificare.
- Cheile private stocate in Modulele criptografice sunt sterse intr-un mod in care este imposibila restaurarea cheilor.

6.4. Comenzile de securitate la nivel de retea

Furnizorul de servicii de pastrare pe termen lung pastreaza sub control strict configuratia sistemelor IT si documenteaza orice modificare, dezvoltare si, de asemenea, orice actualizare de software. Furnizorul de servicii de pastrare pe termen lung implementeaza proceduri adecvate pentru detectarea oricarei modificari de hardware sau software, a instalarii sistemului si a intretinerii efectuate in sistemul informatic. Furnizorul de servicii de pastrare pe termen lung verifica autenticitatea si integritatea fiecarei componente software la prima rulare.

Furnizorul de servicii de pastrare pe termen lung aplica masuri adecvate de securitate a retelei, precum:

- Dezactivarea porturilor de retea neutilizate si serviciile nefolosite;
- Rularea aplicatiilor de retea necesare exclusiv pentru functionarea adecvata a sistemelor informatice.

Furnizorul de servicii de pastrare pe termen lung efectueaza periodic scanari ale vulnerabilitatilor la nivelul adreselor IP publice si private:

- in decurs de o saptamana de la primirea unei solicitari de la Forumul CA / Browser;
- dupa orice modificare de sistem sau de retea pe care CA le stabileste ca fiind semnificative;
- cel putin o data pe trimestru.

6.5. Marcarea Temporala

Furnizorul de servicii de pastrare pe termen lung foloseste marcile temporale oferite de un furnizor calificat de marci temporale enumerate pe lista de incredere a unuia dintre statele membre ale Uniunii Europene pentru protejarea integritatii fisierelor de jurnal si a altor fisiere electronice care urmeaza sa fie arhivate.

7. Auditul de conformitate si alte evaluari

Functionarea Furnizorului de servicii de pastrare pe termen lung este supravegheata de un Organism de supraveghere (SB) in conformitate cu reglementarile Uniunii Europene (Regulamentul eIDAS). Furnizorul de servicii de pastrare pe termen lung efectueaza o verificare a operatiunilor sale prin intermediul unui Organism acreditat de evaluare a conformitatii si transmite raportul detaliat al auditului in termen de 3 zile de la primirea lui. In cursul examinarii se stabileste daca functionarea Furnizorului de servicii de pastrare pe termen lung indeplineste cerintele Regulamentului eIDAS [1] si cerintele politicilor si practicilor serviciului calificat de pastrare pe termen lung.

Evaluarea si metodologia evaluarea respecta urmatoarele documente normative:

- REGULAMENTUL (UE) Nr. 910/2014 AL PARLAMENTULUI EUROPEAN SI AL CONSILIULUI din 23 Iulie 2014 privind serviciile de identificare electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna si abrogarea Directivei 1999/93/CE [1]
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [9]
- ETSI EN 319 401 V2.2.1 (2018-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8]
- ETSI TS 119 511 V1.1.1 (2019-06); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- Ordinul 449/2017 privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 emis de catre Ministerul Comunicatiilor si Societatii Informationale.

Rezultatul evaluarii este un document confidential accesibil numai persoanelor autorizate. Certificatul de conformitate eliberat in concordanta cu raportul de evaluare a conformitatii este publicat pe pagina web a Furnizoruuil de servicii de pastrare pe termen lung.

Furnizorul de servicii de pastrare pe termen lung isi rezerva dreptul de a inspecta in orice moment, implicand un expert independent, functionarea furnizorilor care opereaza in concordanta cu prezentul document pentru a verifica conformitatea cu cerintele prevazute.

7.1. Frecventa sau circumstantele de evaluare

Furnizorul de servicii de pastrare pe termen lung trebuie sa efectueze evaluarea conformitatii la fiecare doi ani, in conformitate cu Regulamentul eIDAS.

7.2. Identitatea / Calificarile evaluatorului

Furnizorul de servicii de pastrare pe termen lung poate efectua auditurile interne cu ajutorul angajatilor sai care ocupa postul de auditor independent al sistemului.

Evaluarea conformitatii cu eIDAS si ETSI este efectuata de o organizatie care este acreditata de catre o Organizatie nationala de acreditare a unui stat membru al UE, in conformitate cu prevederile eIDAS.

7.3. Relatia evaluatorului cu entitatea evaluata

Auditul extern poate fi efectuat numai de catre o persoana care:

- este independent de proprietarii, conducerea si operatiunile Furnizorului de servicii de pastrare pe termen lung examinat.
- este independent de organizatia examinata, si anume nici el, nici rudele sale imediate nu au nicio relatie de munca sau relatii de afaceri cu Furnizorul de servicii de pastrare pe termen lung.

7.4. Subiectele acoperite de evaluare

Evaluarea trebuie sa cuprinda cel putin urmatoarele domenii:

- respectarea legislatiei in vigoare;
- respectarea standardelor tehnice;
- respectarea politicilor si practicilor de pastrare pe termen lung;
- gradul de adecvare ;
- documentatie;
- siguranta fizica;
- gradul de adecvare a personalului;
- securitatea IT;

- respectarea normelor privind protectia datelor.

7.5. Actiuni intreprinse ca urmare a deficientei

Auditorul independent va rezuma rezultatul examinarii intr-un raport de screening detaliat care acopera componentele sistemului testat, procesele si contine dovezile utilizate in procesele de screening si in declaratiile auditorului. Discrepantele constatate in cursul examinarii si termenele stabilite pentru corectarea acestora se consemneaza intr-un capitol separat al raportului.

Auditorul independent poate inregistra, pe baza severitatii, diferentele si discrepantele constatate in timpul examinarii:

- sugestii de modificare care trebuie luate in considerare optional;
- derogari care trebuie evitate in mod obligatoriu.

Auditorul independent trebuie sa raporteze fara intarziere derogarile grave descoperite catre Organismul de supraveghere corespunzator care este autorizat sa ia masurile necesare.

Furnizorul de servicii de pastrare pe termen lung trebuie sa raspunda in scris la problemele declarate de auditorul independent si sa raporteze masurile luate pentru a le evita cu ocazia urmatoarei revizuiri a autoritatii.

7.6. Comunicarea rezultatelor

Furnizorul de servicii de pastrare pe termen lung publica raportul de sinteza privind evaluarea. Discrepantele identificate vor fi tratate ca informatii confidentiale.

8. ALTE ASPECTE JURIDICE SI DE AFACERI

8.1. Taxe

Taxele aplicate de Furnizorul de servicii de pastrare pe termen lung sunt publicate in conformitate cu reglementarile aplicabile.

8.1.1. Politica de rambursare

Nicio stipulare.

8.2. Responsabilitatea financiara

Pentru a facilita increderea, Furnizorul de servicii de pastrare pe termen lung isi asuma responsabilitatea financiara pentru a-si indeplini toate obligatiile definite in cadrul prezentului document si a Contractului de servicii incheiat cu Clientul.

8.2.1. Acoperirea asigurarii

Pentru a acoperi costurile aferente incetarii activitatii de servicii si pentru a mentine fiabilitatea, Furnizorul de servicii de pastrare pe termen lung indeplineste cerintele legale pentru furnizorii de servicii de incredere calificati.

8.3. Confidentialitatea informatiilor de business

Furnizorul de servicii de pastrare pe termen lung gestioneaza datele Clientilor in conformitate cu reglementarile aplicabile.

8.3.1. Informatii care nu se incadreaza in domeniul Informatiilor Confidentiale

Furnizorul de servicii de pastrare pe termen lung poate lua in considerare drept date publice oricare alte date care nu sunt marcate drept date confidentiale.

8.3.2. Responsabilitatea de a proteja Informatiile Confidentiale

Furnizorul de servicii de pastrare pe termen lung este responsabil de protectia datelor confidentiale pe care le administreaza.

Furnizorul de servicii de pastrare pe termen lung isi obliga angajatii, subcontractorii, partenerii afiliati sa protejeze toate datele confidentiale prin semnarea declaratiei de confidentialitate sau prin contract.

Situatiile in care Furnizorul de servicii de pastrare pe termen lung poate dezvalui datele confidentiale trebuie sa fie stabilite de la caz la caz in Declaratia de Politici si Practici pentru serviciul de pastrare pe termen lung.

8.4. Confidentialitatea Informatiilor Personale

Furnizorul de servicii de pastrare pe termen lung are in vedere protectia datelor cu caracter personal pe care le administreaza. Operarea si reglementarile furnizorului de pastrare pe termen lung respecta cerintele Regulamentelor privind protectia datelor si ale legislatiei nationale.

8.4.1. Planul de confidentialitate

Furnizorul de servicii de pastrare pe termen lung a implementat o Politica de Confidentialitate pentru prelucrarea datelor care contine cerinte detaliate pentru gestionarea datelor cu caracter personal. Politica de confidentialitate pentru prelucrarea datelor este publicata pe pagina web a Furnizorului de servicii de pastrare pe termen lung.

8.4.2. Informatii care sunt considerate private

Furnizorul de servicii de pastrare pe termen lung protejeaza toate datele cu caracter personal legate de persoana vizata sau sau care contin concluzii privind persoana vizata, care nu pot fi accesate in mod public de la sursa publica de date.

Furnizorul de servicii de pastrare pe termen lung colecteaza date ale abonatului doar cu consimtamantul prealabil explicit si numai in masura in care este necesar pentru furnizarea serviciului.

8.4.3. Informatii care nu sunt considerate private

Furnizorul de servicii de pastrare pe termen lung nu trateaza ca informatii confidentiale datele personale care pot fi accesate dintr-o sursa publica.

8.4.4. Responsabilitatea de a proteja informatiile private

Furnizorul de servicii de pastrare pe termen lung stocheaza in siguranta si protejeaza datele personale pe care le administreaza. Datele sunt protejate prin masuri adecvate, in special impotriva accesului neautorizat, a modificarii si a dezvaluirii.

Furnizorul de servicii de pastrare pe termen lung este, in general, responsabil cu respectarea cerintelor descrise in Politica sa de confidentialitate, iar raspunderea sa se extinde si la activitatile desfasurate de subcontractanti.

8.4.5. Notificarea si consimtamantul de a folosi Informatiile Private

Furnizorul de servicii de pastrare pe termen lung va folosi datele personale ale Clientului doar in masura in care este necesar sa contacteze Clientul pentru furnizarea de servicii.

8.4.6. Dezvaluirea informatiilor in cadrul proceselor judiciare sau administrative

In cazurile definite in legislatia relevanta, Furnizorul de servicii de pastrare pe termen lung poate dezvalui datele personale stocate despre Client fara notificarea Clientului.

8.4.7. Alte circumstante de dezvaluire a informatiilor

Nicio stipulare.

8.5. Drepturi de proprietate intelectuala

In timpul operatiunii sale, Furnizorul de servicii de pastrare pe termen lung nu trebuie sa aduca atingere drepturilor de proprietate intelectuala ale unei terte persoane.

Prezentul document este proprietatea exclusiva a Furnizorului de servicii de pastrare pe termen lung. Clientul, Subiectii si alte parti invocate sunt indreptatite sa utilizeze documentul numai in conformitate cu cerintele prezentei Declaratii de Politici si Practici si orice alta utilizare in scopuri comerciale sau in alte scopuri este strict interzisa.

Prezentul document poate fi distribuit in mod liber, in forma neschimbata, in intregime si cu indicatia de origine.

8.6. Reprezentari si Garantii

Furnizorul de servicii de pastrare pe termen lung indeplineste cerintele definite in sectiunea (2) a articolului din regulamentul eIDAS [1].

Obligatiile de baza ale Furnizorul de servicii de pastrare pe termen lung constau in faptul ca acesta va furniza serviciile in conformitate cu aceasta Declaratie de Politici si Practici si cu alte reglementari din domeniul public, termenii si conditiile contractuale si mai mult, norme interne legate de corporatie si de securitate. Aceste obligatii de baza sunt urmatoarele:

- stabilirea cadrului legal, de reglementare, material, contractual, etc. adecvat serviciului;
- sa asigure servicii de standarde inalte si sigure in conformitate cu reglementarile aplicabile;
- sa opereze si sa controleze in mod continuu organizatiile asociate cu serviciile (organismul de certificare, serviciul pentru clienti, etc.);
- respectarea procedurilor recomandate in reglementari si evitarea sau eliminarea oricarei operatiuni incorecte care ar putea aparea;
- sa asigure serviciile pentru fiecare solicitant care accepta termenii si conditiile specificate in reglementari;
- sa pastreze inregistrarile publice si de proprietate, precum si sa le puna permanent la dispozitia oricarui organism prin intermediul internetului.

8.6.1. Reprezentari si garantii ale Abonatului

Responsabilitatea abonatului

Responsabilitatea Abonatului este stabilita de contractul de servicii si de anexele sale (inclusiv de termeni si conditii).

Obligatiile abonatului

Responsabilitatea Abonatului este de a actiona in conformitate cu termenii contractuali si reglementarile Furnizorului de servicii de pastrare pe termen lung in timpul utilizarii serviciului.

Obligatiile abonatului sunt determinate de aceasta Declaratie de Politici si Practici, de contractul de servicii si de anexele sale - in special termenii si conditiile generale.

8.6.2. Reprezentari si garantii ale Beneficiarilor

Beneficiarii iau decizii in baza discretiei si/sau a politicilor lor privind modul de acceptare si utilizare a Certificatelor si a Marcilor Temporale. In timpul verificarii valabilitatii pentru mentinerea nivelului de securitate garantat de Furnizorul de servicii de pastrare pe termen lung, este necesar ca beneficiarul sa actioneze cu prudenta, astfel ca se recomanda in special:

- sa respecte cerintele, reglementarile definite in prezenta Declaratie de Politici si Practici;
- utilizarea unui mediu IT si aplicatii fiabile;
- sa verifice informatiile in baza raspunsului CRL sau OCSP actual;
- sa ia in considerare orice restrictie in ceea ce priveste utilizarea care este inclusa in Declaratia de Politici si Practici.

8.6.3. Reprezentari si Garantii ale altor Participanti

Nicio stipulare.

8.7. Note cu privire la Garantii

Furnizorul de servicii de pastrare pe termen lung exclude raspunderea sa daca:

- nu este in masura sa furnizeze informatii sau sa-si indeplineasca obligatiile de comunicare din cauza problemelor de conexiune la Internet sau a unei parti a acestuia.
- dauna provine dintr-o vulnerabilitate sau o eroare a algoritmilor criptografici acceptati de clienti.

8.8. Limitari ale raspunderii

Nicio stipulare.

8.9. Despagubiri

8.9.1. Despagubiri platite de catre Furnizorul de servicii de pastrare pe termen lung

Normele detaliate privind despagubirile achitate de Furnizorul de servicii de pastrare pe termen lung sunt specificate in Declaratia de Politici si Practici, in contractul de servicii sau in contractele incheiate cu Clientii.

8.9.2. Despagubiri platite de catre Abonati

Furnizorul de servicii de pastrare pe termen lung stabileste termenul de revendicare a daunelor de la Abonati in Declaratia de Politici si Practici si in contractul de servicii.

8.9.3. Despagubiri platite de catre Beneficiari

Furnizorul de servicii de pastrare pe termen lung stabileste in Declaratia de Politici si Practici termenul cererii sale de despagubire de la beneficiari.

8.10. Termen si incheiere

8.10.1. Termen

Data de intrare in vigoare a Politicii de conservare pe termen lung este specificata pe pagina 2 a documentului.

8.10.2. Incheiere

Declaratia de Politici si Practici a serviciului calificat de pastrare pe termen lung este valabila fara o limita de timp pana la retragere.

8.10.3. Efectul incheierii

In cazul retragerii Declaratiei de Politici si Practici, Furnizorul de servicii de pastrare pe termen lung publica pe pagina sa web regulile detaliate ale retragerii si drepturile si obligatiile care persista dupa aceasta actiune.

8.11. Notificari individuale si comunicari cu participantii

Furnizorul de servicii de pastrare pe termen lung trebuie sa opereze un serviciu de relatii cu clientii pentru a mentine contactul cu Clientii sai.

8.12. Modificari

Furnizorul de servicii de pastrare pe termen lung isi rezerva dreptul de a modifica Declaratia de Politici si Practici a serviciului calificat de pastrare pe termen lung intr-un mod controlat in cazul modificarii actelor normative, a cerintelor de siguranta, a conditiilor pietei sau a altor circumstante.

In cazuri exceptionale (de exemplu, necesitatea luarii unor masuri critice de securitate), modificarile pot fi puse in aplicare cu efect imediat.

8.12.1. Procedura de modificare

Furnizorul de servicii de pastrare pe termen lung revizuieste anual Declaratia de Politici si Practici a serviciului calificat de pastrare pe termen lung sau in cazul unei cereri exceptionale de modificare cu prioritate si efectueaza modificarile necesare. Documentul va primi un nou numar

de versiune chiar si dupa cea mai mica schimbare si tinand seama de timpul necesar procesului de aprobare, se va determina si data planificata a intrarii in vigoare.

Documentul acceptat va fi publicat pe pagina web a Furnizorul de servicii de pastrare pe termen lung cu 30 de zile inainte de data planificata a intrarii in vigoare si va fi trimis Organismului de supraveghere.

8.12.2. Circumstantele in care OID trebuie schimbat

Furnizorul de servicii de pastrare pe termen lung emite un nou numar de versiune in cazul celei mai mici modificari a Politicii de conservare pe termen lung calificata, care face parte din identificatorul documentului (OID), astfel incat orice modificare a documentului va avea ca rezultat o modificare OID , si anume doua documente - care au intrat in vigoare - cu continut diferit nu pot avea acelasi OID.

8.13. Dispozitii privind solutionarea litigiilor

Furnizorul de servicii de pastrare pe termen lung va urmari solutionarea pasnica si negociata a litigiilor care decurg din functionarea sa. Acordul trebuie sa respecte principiul abordarii treptate.

8.14. Legea aplicabila

Furnizorul de servicii de pastrare pe termen lung opereaza in orice moment in conformitate cu Regulamentul eIDAS.

8.15. Conformitatea cu normele legislative aplicabile

Prezenta Politica de conservare pe termen lung este conforma cu urmatoarele regulamente.

- REGULAMENTUL (UE) Nr. 910/2014 AL PARLAMENTULUI EUROPEAN SI AL CONSILIULUI din 23 iulie 2014 privind serviciile de identificare electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna si abrogarea Directivei 1999/93/CE [1];
- ETSI EN 319 401 V2.2.1 (2018-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8]

8.16. Dispozitii diverse

8.16.1. Intregul acord

Nicio stipulare.

8.16.2. Atribuirea

Furnizorii care opereaza in conformitate cu aceasta Politica de conservare calificata pe termen lung pot sa aloce legi si obligatii doar unei terte parti cu acordul prealabil scris al Furnizorului de servicii de pastrare pe termen lung.

8.16.3. Anulabilitatea

In cazul in care unele dintre prevederile prezentului document devin invalide din orice motiv, dispozitiile ramase vor ramane in vigoare neschimbate.

8.16.4. Executarea (Tarifele Avocatilor si Renuntarea la drepturi)

Furnizorul de servicii de pastrare pe termen lung este indreptatit sa solicite plata pentru despagubiri si taxe de avocat pentru rambursarea daunelor, pierderilor, cheltuielilor cauzate de partenerii sai. Daca, intr-un caz particular, Furnizorul de servicii de pastrare pe termen lung nu isi exercita cererea de despagubire acest lucru nu inseamna ca in cazuri similare in viitor sau in cazul incalcarii altor dispozitii ale prezentului document, aceasta ar renunta la executarea cererilor de despagubire.

8.16.5. Forta majora

Furnizorul de servicii de pastrare pe termen lung nu este responsabil pentru indeplinirea defectuoasa sau intarziata a cerintelor stabilite in Politica de conservare calificata pe termen lung si Declaratia privind practica de conservare pe termen lung, in cazul in care motivul eseculi sau intarzierii a fost un eveniment care se afla in afara controlul Furnizorului de servicii de pastrare pe termen lung.

8.17. Alte prevederi

Nicio stipulare.

REFERINTE

[1] 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 abrogarea Directivei 1999/93 / CE.

[2] REGULAMENT nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

[3] ETSI EN319 401V2.2.1 (2018-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[4] ETSI EN 319 403 V2.3.0 (2019-11) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;

[5] ETSI TS 101 533-1 V1.3.1 (2012-04) Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security.

[6] ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques`

[7] ETSI TS 119 512 V1.1.1 (2020-01) Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

[8] Ordinul 449/2017 privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 emis de catre Ministerul Comunicatiilor si Societatii Informationale.