APROVED
GENERAL MANAGER
DORU VIJIIANU

Autoritatea de Marcare Temporală Zipper Services
Politica și Codul de Practici și Proceduri

Mărci temporale calificate conform Regulamentului eIDAS și legislației naționale

.

Istoria ediției			
Ediție	**Data și descrierea modificării**	**Pregătit**	**Aprobat**
1	28.02.2022 – Ediția I	Mirela Ojog	Judit Fekete
2	06.02.2023 – Editia 2	Mirela Ojog	Judit Fekete

ZIPPER

CUPRINS

1. Introducere

Acest document constituie Politica și Codul de Practici și Proceduri Autoritatea de Marcare Temporală Zipper. Scopul documentului este de a descrie normele și procedurile operaționale adoptate de ZIPPER TSA pentru furnizarea de servicii calificate de marcare temporală în conformitate cu Regulamentul (UE) nr. 910/2014 (Regulamentul eIDAS).

Serviciile calificate de marcare temporală ale ZIPPER susțin afirmații ale dovezilor că o înregistrare electronică a existat înainte de o anumită perioadă de timp. Aceste servicii pot fi utilizate în sprijinul serviciilor de non-repudiere, pentru a dovedi că o semnătură electronică a fost generată în perioada de valabilitate a unui certificat cu cheie publică, pentru a sprijini arhivarea electronică pe termen lung etc.

Documentul curent specifică regulile generale utilizate de ZIPPER TSA pentru emiterea tokenelor de marcă temporală (TST). Acesta definește părțile implicate, responsabilitățile, drepturile și gama de aplicabilitate a acestora.

Serviciile de marcare temporală ZIPPER pot fi accesate prin intermediul http://tsa.ezipper.ro:8777/adss/tsa

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

Serviciile de marcare temporală calificate ZIPPER sunt furnizate în conformitate cu Regulamentul eIDAS, ETSI EN 319 421 și standardele EN 319 422 și sub autoritatea ZIPPER care acționează în calitate de autoritate calificată de marcare temporală.

Conducerea poate face excepții de la acest document de la caz la caz pentru a atenua impactul semnificativ, iminent asupra clienților, partenerilor, părților care se bazează și/sau altor persoane în cazul în care nu există soluții practice. Orice astfel de excepții de gestionare sunt documentate, urmărite și raportate ca parte a procesului de audit.

2. Administrarea politicilor

Organizația care administrează prezentul document:
ZIPPER SERVICES SRL
Autoritatea de marcare temporală
str. Fabricii nr. 93-103
Cluj-Napoca, 400632, România

Punct de lucru:
B-dul 1 Decembrie 1918 nr. 1G,
Sector 3, Bucuresti, 032451, Romania
Punct de lucru:
Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,
Cluj-Napoca, 400221, Romania
https://ezipper.ro/
E-mail: office@ezipper.ro

Telefon +40 21.340.4638 / +40 31.101.1020
Fax: +40 21.340.4636 / +40 31.101.1022
(Luni-Vineri 09.00. – 18:00 Ora Europei de Est)
Persoană de contact: Echipa de administrare a politicilor

3. Procedura de aprobare

Aprobarea acestui document si modificarile ulterioare se fac de catre persoanele dedicate de Zipper. Aceste persoane constituie echipa de administrare a politicilor. Managementul aprobă noi versiuni ale acestui document. Versiunile sau actualizările modificate se încarcă în depozitul ZIPPER situat la https://pki.ca.ezipper.ro/repository/policies.php

Versiunile modificate înlocuiesc orice dispoziții contradictorii ale versiunilor anterioare ale acestui document. Echipa de administrare a politicilor va determina dacă modificările aduse acestui document necesită o modificare a identificatorilor de obiect de politică TSA ai politicilor de certificat.

4. Referinţe

Următoarele referințe conțin dispoziții care sunt relevante pentru politica de certificare a autorității de marcare temporală calificată ZIPPER și declarația privind practica de certificare:

1. Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

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

3. ETSI EN 319 421: "Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care emit marcaje temporale".

4. ETSI EN 319 422: "Semnături și infrastructuri electronice (ESI); Protocol de marcare temporală și profiluri token de marcă temporală".

5. IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

6. ETSI EN 319 411-1: "Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea 1: Cerințe generale".

7. ETSI EN 319 411-2: "Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea 2: Cerințe pentru prestatorii de servicii de încredere care eliberează certificate calificate în UE".

Legislația națională aplicabilă:

8. Hotărârea Guvernului nr. 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României.

9. ORDIN nr. 449 din 30 mai 2017 privind procedura de acordare, suspendare şi retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014.

Definiții și abrevieri

Termen	Rost
Furnizor de servicii de încredere calificat (QTSP)	Un furnizor de servicii de încredere care oferă servicii de încredere calificate și este inclus în lista sigură a UE.
Relying party	Un destinatar al unei mărci temporale care se bazează pe acea marcă

	temporală.
Abonat	O persoană juridică sau fizică căreia i se eliberează o ștampilă temporală și care este obligată să respecte orice obligații de abonat.
Autoritatea de marcare temporală (TSA)	Un furnizor de servicii de încredere (TSP) care furnizează servicii de marcare temporală .
Politica TSA și codul de parctici	Politica și codul de practici ai autorității de marcare temporală: declararea practicilor pe care le utilizează un TSA în emiterea de mărci temporale.
Timbru de timp	Date în formă electronică care leagă alte date electronice la un anumit moment, stabilind dovezi că aceste date existau la momentul respectiv.
Time Stamp Token	Obiect de date care leagă o reprezentare a unui datum la un anumit moment, stabilind astfel dovezi că data a existat înainte de acel moment.
Unitate de marcare temporală	Set hardware și software care este gestionat ca unitate și are o singură marcă de timp activă la un moment dat.
TSP	Furnizor de servicii de încredere

5. Concepte generale

6.1 Servicii de marcare temporală

Serviciile de marcare temporală calificate ZIPPER constau în gestionarea infrastructurii pentru și furnizarea de token-uri time-stamping (TST). Aceste servicii sunt furnizate abonaților de către Autoritatea de marcare temporală ZIPPER (TSA) și sunt în conformitate cu Regulamentul eIDAS și cu standardele ETSI.

ZIPPER oferă servicii de marcare temporală utilizând Protocolul de marcare temporală RFC 3161 prin transport HTTP. Fiecare TST conține un identificator de politică de marcare temporală, un număr de serie unic și un certificat de unitate de marcare temporală (TSU) care conține informații de identificare ZIPPER TSA.

Serviciile calificate de marcare temporală asigură utilizarea unei surse de timp fiabile și gestionarea corectă a tuturor componentelor sistemului.

6.2 Autoritatea de marcare temporală

ZIPPER TSA este responsabil pentru furnizarea de servicii calificate de marcare temporală, așa cum este descris în acest document. Aceasta are responsabilitatea de a operatusurile de sistem de transport și de sistem relevante care sunt create și semnate în numele TSA. Persoana juridică responsabilă pentru TSA este ZIPPER S.A. care acționează ca O TSA calificată.
ZIPPER emite marcaje de timp calificate în următoarea ierarhie:

Root CA

CN = ZIPPER Root CA G1
O = ZIPPER SERVICES SRL
OU = ZIPPER Trust Services
C = RO

Time Stamping Authority CA

CN = ZIPPER TSA G1
O = ZIPPER SERVICES SRL
OU = ZIPPER Time Stamping Services
C=RO
2.5.4.97 = VATRO-16723187

Time Stamping Unit CA
CN = ZIPPER TSU 2023 A
O = ZIPPER SERVICES SRL
OU = ZIPPER Time Stamping Services
C = RO
2.5.4.97 = VATRO-16723187
Certificatele ZIPPER TSA și TSU sunt emise în conformitate cu următoarele politici de certificare:

- **OID 0.4.0.2042.1.2** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)
- **OID 0.4.0.2023.1.1**: itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

• OID tree	
1.3.6.1.4.1.57570	Numărul de identificare (OID) al Zipper Services SRL, înregistrat la IANA
1.3.6.1.4.1.57570.1	Furnizor de servicii de încredere
1.3.6.1.4.1.57570.1.1	Politica privind certificatele de servicii de încredere (CP)
1.3.6.1.4.1.57570.1.1.1	Declarație practică privind certificatul de încredere calificat pentru servicii de încredere (CPS)
1.3.6.1.4.1.57570.1.1.1.1	Servicii calificate de marcare temporală

6.3 Abonați

Abonatul este solicitantul, persoana fizica sau juridica, caruia i se pune amprenta temporala si care intra intr-o relatie contractuala cu ZIPPER.
Atunci când Abonatul este un utilizator final, utilizatorul final va fi considerat direct responsabil dacă obligațiile sale nu sunt îndeplinite în mod corect.

Abonatul poate fi o organizație formată din mai mulți utilizatori finali sau un utilizator final individual. Atunci când Abonatul este o organizație, unele dintre obligațiile care se aplică organizației respective vor trebui să se aplice și utilizatorilor finali, prin urmare organizația va notifica în mod corespunzător utilizatorii săi finali. În orice caz, organizația va fi trasă la răspundere dacă obligațiile nu sunt îndeplinite corect de către utilizatorii finali.

6.4 Părțile care se bazează

O parte bazându-se este o persoană fizică sau o entitate care primește un document digital care este marcat în timp și acționează pe baza unui certificat și/sau a unei semnături digitale emise în temeiul TSA. O parte care se bazează trebuie să evalueze corectitudinea și validitatea documentului în sine în contextele în care este utilizat.

6.5 Alți participanți

Nu se aplică.

6.6 Utilizarea marcajelor temporale

Marcajele temporale emise de ZIPPER, astfel cum se specifică în prezentul document, sunt calificate în

sensul Regulamentului eIDAS.
Mărcile temporale se utilizează numai în măsura în care utilizarea este conformă cu legislația aplicabilă și în limitele și contextele specificate în prezentul document. Orice utilizare în afara limitelor și contextelor specificate în prezentul document sau în scopuri ilegale sau contrare interesului public sau care ar putea afecta în alt mod afacerea sau reputația ZIPPER este interzisă. Cu titlu orientativ, este interzisă utilizarea mărcilor temporale pentru documentele de marcare temporală care pot duce la consecințe ilegale.

6. Declarația privind politica și practica TSA

7.1 Scop

Această secțiune specifică cerințele de politică și securitate referitoare la practicile de operare și gestionare ale ZIPPER ca autoritate de marcare temporală (TSA) pentru emiterea de marcaje temporale calificate. Acestea pot fi utilizate în sprijinul semnăturilor electronice sau pentru orice aplicație care necesită să se dovedească existența unui datum înainte de o anumită perioadă de timp.

Acest document poate fi utilizat de entități independente ca bază pentru confirmarea faptului că ZIPPER TSA este o entitate de încredere pentru emiterea de marcaje temporale calificate în conformitate cu Regulamentul eIDAS.

Prezentul document conține detalii specifice privind mediul de operare, structura organizațională, procedurile de operare, facilitățile și mediul de calcul al TSA ZIPPER. Acesta descrie numai normele generale de emitere și gestionare a TSTS. Descrierea detaliată a infrastructurii și a procedurilor operaționale aferente sunt descrise în documente suplimentare care nu sunt disponibile publicului. Aceste documente suplimentare sunt disponibile numai personalului autorizat ZIPPER și, pe baza necesității de a cunoaște, organismului de evaluare a conformității care auditează serviciile de marcare temporală.

7. Politica TSA

8.1 Prezentare generală

Politica TSAP definește un set de reguli utilizate în timpul emiterii TSTs și reglementează nivelul de securitate pentru ZIPPER TSA. ZIPPER TSA emite TSTs în conformitate cu ETSI EN 319 422.
ZIPPER TSU emite marcaje temporale electronice calificate conform regulamentului eIDAS; ZIPPER TSU nu emite marcaje temporale electronice necalificate.
TSTs sunt emise cu o precizie de o (1) secundă.
Marcajele temporale sunt solicitate prin intermediul Hypertext Transfer Protocol (HTTP), așa cum este descris de RFC 3161.

8.2 Identificarea

Identificatorul de obiect (OID) al Declarației de politică și practică ZIPPER TSA este 57570. :

1.3.6.1.4.1.57570	Numărul de identificare (OID) al ZIPPER, înregistrat la IANA
1.3.6.1.4.1.57570.1	Furnizor de servicii de certificare
1.3.6.1.4.1.57570.1.1	Politici de certificare calificate
1.3.6.1.4.1.57570.1.1.1	Servicii calificate de marcare temporală

Acest OID este menționat în fiecare TST emis de ZIPPER, iar Politica și declarația de practică ZIPPER TSA este disponibilă atât abonaților, cât și părților care se bazează.
ZIPPER emite TSTs în conformitate cu ETSI EN 319 421 cele mai bune practici pentru politica de marcare temporală
(OID 0.4.0.2023.1.1).

8.3 Comunitatea utilizatorilor și aplicabilitatea

Nu există limitări privind eligibilitatea sau aplicabilitatea serviciilor furnizate de utilizatori. ZIPPER TSA poate furniza servicii de marcare temporală oricărui utilizator, inclusiv comunităților închise.
ZIPPER nu oferă servicii publice de marcare temporală.

8.4 Conformanța

ZIPPER TSA utilizează identificatorul din TSTs, așa cum este indicat în secțiunea "Identificare".
ZIPPER TSA asigură conformitatea serviciilor furnizate cu reglementările specificate în secțiunea "Conformitatea cu cerințele legale" și asigură fiabilitatea mecanismelor de control descrise în secțiunea "Practici TSA".

8. Obligații și răspundere

Acest capitol include toate obligațiile, datoriile, garanțiile și responsabilitățile ZIPPER TSA, ale abonaților săi și ale utilizatorilor TST (abonați și părți care se bazează). Aceste obligații și responsabilități sunt reglementate de acorduri acceptate de toate părțile.
ZIPPER operează ZIPPER TSA și își asumă responsabilitatea că sunt puse în aplicare cerințele secțiunii "Practici TSA" din acest document, precum și prevederile eIDAS.
Acordurile ZIPPER cu abonații și părțile care se bazează descriu obligațiile și responsabilitățile reciproce, inclusiv responsabilitățile financiare. Declarația de politică și practică ZIPPER TSA (acest document) face parte integrantă din aceste acorduri.

9.1 Obligațiile TSA și garanțiile față de abonați

ZIPPER garantează disponibilitatea a 99,00 % din serviciile de marcare temporală 24/7, cu excepția pauzelor tehnice programate, în ceea ce privește conservarea echipamentelor și a sistemului.
ZIPPER isi asuma urmatoarele obligatii fata de Abonati:

- Să funcționeze în conformitate cu prezenta Declarație de politică și practică ZIPPER TSA (acest document) și cu alte politici și proceduri operaționale relevante;
- Pentru a se asigura că OTS menține o precizie minimă a orei UTC de ± 1 secundă;
- Mentinerea unei echipe competente si experimentate care sa poata asigura continuitatea Serviciilor de Pontaj;
- Asigurarea permanentă a securității fizice și logice, precum și a integrității materialelor, software-ului și bazelor de date necesare funcționării corecte a serviciilor de marcare temporală;
- Să monitorizeze și să controleze serviciile de marcare temporală și întreaga infrastructură TSA, pentru a preveni sau limita orice perturbare sau indisponibilitate a serviciilor de marcare temporală;
- Să se supună unor revizuiri interne și externe pentru a asigura conformitatea cu legislația relevantă și cu politicile și procedurile interne ZIPPER;
- Pentru a oferi acces cu disponibilitate ridicată la sistemele ZIPPER TSA, cu excepția cazului întreruperilor tehnice planificate și al pierderii sincronizării timpului.

9.2 Obligațiile abonaților

Abonații trebuie să verifice semnăturile create de ZIPPER TSA pe TST.
Această verificare cuprinde:

- Verificați dacă semnătura TSA de pe TST este validă.
- Verificarea certificatului TSA:
  - Verificarea căii de încredere până la certificatul rădăcină de încredere și pentru fiecare dintre certificatele din lanț (inclusiv certificatul TSA în sine)
  - Verificarea faptului dacă certificatul nu este expirat în momentul semnării TSA

- Verificați dacă certificatul nu a fost revocat în momentul semnării TSA.

Abonații trebuie să utilizeze funcții criptografice securizate pentru solicitările de marcare temporală. Alte obligații ale Abonatului pot fi, de asemenea, definite în Termenii și condițiile ZIPPER pentru serviciile de marcare temporală.

9.3 Obligațiile părții care se bazează

Părțile bazându-se ar trebui să verifice semnăturile create de ZIPPER TSA pe TST.
Această verificare cuprinde:

- Verificați dacă semnătura TSA de pe TST este validă.
- Verificarea certificatului TSA:
  - Verificarea căii de încredere până la certificatul rădăcină de încredere și pentru fiecare dintre certificatele din lanț (inclusiv certificatul TSA în sine)
  - Verificarea faptului dacă certificatul nu este expirat în momentul semnării TSA
  - Verificați dacă certificatul nu a fost revocat în momentul semnării TSA.

Părțile care se bazează ar trebui să țină seama de orice limitări privind utilizarea mărcii temporale indicate de Declarația de politică și practică ZIPPER TSA. În cazul în care verificarea are loc după încheierea perioadei de valabilitate a certificatului, părțile care se bazează ar trebui să urmeze orientările notate în anexa D la ETSI EN 319 421.

Bazându-se părțile sunt de așteptat să utilizeze o listă sigură pentru a stabili dacă TSU și marca de timp sunt calificate. Dacă cheia publică a TSU este listată în Lista sigură și serviciul pe care îl reprezintă este un serviciu calificat de marcare temporală, atunci marcajele temporale emise de acest TSU pot fi considerate calificate. QcStatement "esi4-qtstStatement-1", astfel cum este definit în clauza 9.1 ETSI EN 319 422, este utilizat ca o indicație că marca de timp este calificat.

9.4 Răspunderea

Răspunderea ZIPPER care acționează în calitate de TSA și a abonaților și a părților bazându-se în legătură cu serviciile de marcare temporală este specificată în acordul relevant sau este cea prevăzută în legislația aplicabilă.

ZIPPER este responsabil pentru eventualele daune determinate direct, intenționat sau din neglijență, oricărei persoane fizice sau juridice, ca urmare a nerespectării obligațiilor prevăzute în prezentul document și în Regulamentul eIDAS.

Termenii și condițiile ZIPPER pentru serviciile de marcare temporală limitează răspunderea ZIPPER. Limitările răspunderii includ o excludere a daunelor indirecte, speciale, incidentale și pe cale de consecință. Acestea includ, de asemenea, un plafon de răspundere privind răspunderea agregată combinată a ZIPPER față de oricare și toate persoanele cu privire la serviciile de marcare temporală, care este limitată la o sumă care nu o depășește pe cea a contractului respectiv pentru serviciul de marcare temporală și un maxim total de 500.000EUR, indiferent de natura răspunderii și de tipul, valoarea sau amploarea oricăror daune suferite. Limitările de răspundere sunt aceleași, indiferent de numărul de mărci temporale sau de creanțe legate de astfel de marcă temporală sau serviciu de marcare temporală.

ZIPPER TSA nu este în nici un fel responsabil pentru utilizarea TSTs pe care le oferă și semne.

9. Declarație de practică TSA

Această secțiune stabilește regulile generale privind cerințele tehnice, organizatorice și procedurale ale operațiunii ZIPPER TSA. ZIPPER TSA implementează controale care îndeplinesc cerințele ETSI EN 319 421 și ETSI EN 319 422.

Certificatele de marcare temporală sunt valabile timp de cinci (5) ani, dar necesită re-generare în fiecare an. De aceea, jurnalele și înregistrările pentru marcarea temporală sunt păstrate timp de un (1) an după expirarea certificatului TSU.

Se efectuează în mod regulat o evaluare a riscurilor pentru a evalua activele comerciale și amenințările la adresa acestor active, pentru a determina controalele de securitate și procedurile operaționale necesare care au fost luate.

Termenii și condițiile ZIPPER pentru utilizarea serviciilor de marcare temporală sunt dezvăluite și puse la dispoziția tuturor abonaților și părților care se bazează, astfel cum se specifică în prezentul document.

Echipa de administrare a politicilor ZIPPER are responsabilitatea de a menține, actualiza și revizui toate politicile, practicile și procedurile în conformitate cu termenii secțiunii "Administrarea politicilor" din acest document. Conducerea are responsabilitatea de a se asigura că aceste politici, practici și proceduri sunt aprobate și puse în aplicare în mod corespunzător.

10.1 Ciclul de viață al managementului cheilor

10.1.1 Generația cheilor TSA

Personalul în roluri de încredere sub control dublu efectuează generarea cheilor de semnare TSU într-un mediu securizat fizic. Personalul autorizat să îndeplinească această funcție se limitează la cele care trebuie să facă acest lucru în conformitate cu practicile TSA.

Generarea cheilor de semnare TSU se realizează în cadrul dispozitivelor criptografice securizate, care îndeplinesc cerințele identificate în FIPS 140-2 nivel 3.

Perechile cheie sunt generate folosind algoritmi și parametri securizați pe baza cercetărilor actuale și a standardelor din industrie, urmând recomandările ETSI TS 319 312.
Activitățile desfășurate în fiecare generație-cheie sunt înregistrate, datate și semnate de toate persoanele implicate. Aceste înregistrări sunt păstrate în scopuri de audit și urmărire pentru o perioadă de timp considerată adecvată de către ZIPPER Management.

10.1.2 Protecția cheilor private TSU

ZIPPER ia măsuri specifice pentru a se asigura că cheile private TSU rămân confidențiale și își mențin integritatea.

Cheile private TSU sunt stocate într-un modul de securitate hardware securizat pentru a efectua operațiuni de semnare a cheilor, care respectă cel puțin FIPS 140-2 nivel 3 sau echivalent EAL 4+ sau mai mare în conformitate cu specificațiile ISO / IEC 15408. Există controale speciale pentru a se asigura că hardware-ul nu a fost modificat și funcționează corect.
Cheile private TSU nu pot fi extrase sub nicio formă și nu sunt accesibile în afara modulului de securitate hardware.
ZIPPER creează copii de rezervă ale cheilor private TSU, în scopuri de recuperare de rutină și recuperare în caz de dezastru. Astfel de chei sunt stocate în formă criptată în module criptografice hardware. Modulele criptografice utilizate pentru stocarea cheilor private îndeplinesc cerințele acestui CPS.

Cheile private sunt copiate în module criptografice hardware de rezervă. Restaurarea cheilor de rezervă TSU necesită control dublu într-un mediu securizat fizic.

10.1.3 Distribuția cheilor publice TSU

Cheile publice ZIPPER TSU sunt puse la dispoziție într-un certificat digital.
Certificatele ZIPPER TSU sunt disponibile pentru descărcare securizată prin intermediul site-ului zipper Repository https://pki.ca.ezipper.ro/repository/certs.php Poate fi, de asemenea, găsit în lista sigură a UE.

10.1.4 Regenerarea cheii TSU'

Perioada de funcționare pentru perechile de chei TSU este definită prin setarea unei perioade de utilizare a cheii private în certificatul de cheie publică al TSU.

TST-urile ZIPPER sunt semnate cu certificate ZIPPER TSU cu valabilitate de cinci (5) ani. Certificatele

ZIPPER TSU de valabilitate cinci (5) ani sunt utilizate numai pentru a semna TSTs în timpul unei perioade de utilizare de un (1) an.

Procedura de regenerare a cheii ZIPPER TSU se executa la expirarea perioadei de utilizare (1 an) a certificatului TSU. Cheile publice sunt arhivate pentru o perioadă de cel puțin zece (10) ani de la data expirării certificatului.

10.1.5 Sfârșitul ciclului de viață cheie TSU

ZIPPER TSA se asigură că cheile private de semnare TSU nu sunt utilizate dincolo de sfârșitul ciclului lor de viață. În special, există proceduri operaționale și tehnice pentru a se asigura că o nouă cheie este pusă în aplicare înainte de expirarea perioadei cheie de utilizare a unei TSU și că cheile private TSU sau orice parte, inclusiv orice copii sunt distruse, astfel încât cheia privată să nu poată fi recuperată.
Sistemul de generare a TST respinge orice încercare de a emite un TST dacă cheia privată de semnare a expirat sau dacă perioada de utilizare a cheii private de semnare a expirat.

10.1.6 Gestionarea ciclului de viață al modulului criptografic utilizat pentru semnarea marcajelor temporale

ZIPPER TSA asigură securitatea HSM pe tot parcursul ciclului său de viață.
ZIPPER dispune de proceduri pentru a se asigura că:

- Modulele de securitate hardware nu sunt modificate în expediere sau stocare.
- Testarea acceptării se efectuează pentru a verifica dacă hardware-ul criptografic funcționează corect.
- Instalarea, activarea și duplicarea cheilor de semnare ale TSU în HSM-uri se face numai de către personalul cu roluri de încredere, într-un mediu sigur din punct de vedere fizic.
- Cheile private de semnare TSU stocate pe HSM sunt șterse la retragerea dispozitivului în conformitate cu instrucțiunile producătorului.

10.2 Marcarea temporală

10.2.1 Token de marcă temporală

ZIPPER dispune de proceduri tehnice pentru a se asigura că TST-urile sunt emise în siguranță și includ timpul corect. Fiecare TST include:

- o reprezentare a datei fiind ștampilată în timp, astfel cum a fost furnizată de solicitant
- un număr de serie unic pentru a identifica un anumit TST
- un identificator unic al politicii, astfel cum este descris în prezentul document

- o semnătură electronică generată utilizând o cheie utilizată exclusiv pentru marcarea temporală
- un identificator pentru TSA și TSU.
- valoarea dată și oră care poate fi urmărită la valoarea orei UTC reale
- algoritmul de semnătură utilizat în TST.

ZIPPER TSUs menține jurnalele de audit pentru toate calibrările față de referințe utc.

10.2.2 Sincronizarea ceasului cu UTC

ZIPPER TSA se asigură că timpul său este sincronizat cu UTC în precizia declarată cu mai multe surse de timp independente. ZIPPER TSA încorporează timpul în TST cu precizia descrisă la punctul 8.1 din prezentul document.
Înregistrările de audit și calibrare a sincronizării sunt menținute de ZIPPER. ZIPPER TSA se asigură că:

- în cazul în care timpul indicat într-un TST derivă sau sare din sincronizarea cu UTC, acest lucru va fi detectat.
- în cazul în care timpul TSU derivă în afara preciziei declarate și recalibrarea nu reușește, TSA nu va emite marcaje temporale până când nu se restabilește ora corectă.

ZIPPER implementeaza controale de securitate care impiedica functionarea neautorizata, avand ca scop calibrarea timpului TSA.

10.2.3 A doua procedură de manipulare salt

Un salt al doilea este o ajustare la UTC sărind peste sau adăugând o secundă în plus în ultima secundă a unei luni UTC. Prima preferință este acordată la sfârșitul lunii decembrie și iunie, iar a doua preferință este acordată la sfârșitul lunii martie și septembrie.
ZIPPER monitorizează că sincronizarea este menținută atunci când apare un salt secundă.

10.3 Gestionarea și funcționarea TSA

10.3.1 Managementul securității

ZIPPER TSA se asigură că se aplică proceduri administrative și de gestionare adecvate și care corespund celor mai bune practici recunoscute.
ZIPPER îndeplinește toate funcțiile TSA folosind sisteme de încredere care îndeplinesc cerințele ZIPPER ISMS.

10.3.2 Clasificarea și gestionarea activelor

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

10.3.3 Securitatea personalului

ZIPPER menține controale adecvate ale personalului care îndeplinesc cele mai bune practici de securitate și cerințele standardelor relevante.
Personalul de conducere și operațional deține competențele și cunoștințele corespunzătoare privind marcarea temporală, semnăturile digitale și serviciile de încredere, precum și procedurile de securitate pentru personalul cu responsabilități de securitate, securitatea informațiilor și evaluarea riscurilor.
ZIPPER implementează Politica privind rolurile de încredere pentru toți acei angajați care au acces la sau controlează operațiuni criptografice. Persoanele și rolurile de încredere includ, dar nu se limitează la:

- Personalul operațiunilor de afaceri criptografice,

- Personalul de securitate,
- personalul de administrare a sistemului;
- Personal de inginerie desemnat și
- Directori care sunt desemnați să gestioneze credibilitatea infrastructurii.

Înainte de începerea angajării într-un rol de încredere, ZIPPER efectuează verificări ale antecedentelor care pot include, cu titlu orientativ, următoarele:

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

ZIPPER solicită ca personalul care dorește să devină persoane de încredere să prezinte dovada pregătirii, calificărilor și experienței necesare pentru a-și îndeplini în mod competent responsabilitățile viitoare ale postului, astfel cum se specifică în contractul de muncă și în fișa postului, înainte de a îndeplini orice funcții operaționale sau de securitate.
Contractele de muncă semnate de angajați includ dispoziții de confidențialitate pentru informațiile care le sunt aduse la cunoștință în cursul executării lor.
ZIPPER se asigură că personalul a obținut un statut de încredere și că aprobarea departamentală a fost acordată înainte ca acest personal să fie:

- A emis dispozitive de acces și a acordat acces la facilitățile necesare;
- A emis acreditări electronice pentru a accesa și a efectua funcții specifice pe ZIPPER TSA sau alte sisteme IT.

Conturile de utilizator sunt create pentru personalul cu roluri specifice care necesită acces la sistemul în cauză. Toți utilizatorii trebuie să se conecteze cu un cont dedicat, iar comenzile administrative sunt disponibile numai cu permisiune explicită. Permisiunile sistemului de fișiere și alte caracteristici disponibile în modelul de securitate al sistemului de operare sunt utilizate pentru a preveni orice altă utilizare. Conturile de utilizator sunt blocate cât mai curând posibil atunci când schimbarea rolului dictează.

10.3.4 Securitatea fizică și de mediu

ZIPPER implementează Politica de securitate fizică, care sprijină cerințele de securitate ale acestei declarații de politică și practică TSA.

Operațiunile ZIPPER TSA se desfășoară într-un mediu protejat fizic care descurajează, previne și detectează utilizarea neautorizată, accesul la sau divulgarea de informații și sisteme sensibile.

ZIPPER menține, de asemenea, facilități de recuperare în caz de dezastru pentru operațiunile sale de servicii de marcare a timpului. Instalațiile ZIPPER de recuperare în caz de dezastru sunt protejate de mai multe niveluri de securitate fizică comparabile cu cele ale instalației primare ZIPPER.

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

Zonele utilizate pentru crearea și stocarea materialelor criptografice impun controlul accesului. Accesul la OSC-uri și la materiale de chei este restricționat în conformitate cu cerințele privind segregarea sarcinilor. Deschiderea și închiderea dulapurilor sau containerelor de pe aceste niveluri este înregistrată în scopuri de audit.

Operațiunile ZIPPER sunt protejate prin intermediul controalelor de acces fizic, ceea ce le face

accesibile numai persoanelor autorizate în mod corespunzător. Accesul în zonele securizate ale clădirilor necesită utilizarea unui card de "acces" și/sau a elementelor biometrice. Utilizarea cardului de acces este înregistrată de sistemul de securitate al clădirii.

Jurnalele cardurilor de acces sunt revizuite în mod regulat.

Facilitățile securizate zipper sunt echipate cu primar și de rezervă:

- Sisteme de alimentare pentru asigurarea accesului continuu și neîntrerupt la energia electrică și
- Sisteme de încălzire/ventilație/aer condiționat pentru controlul temperaturii și umidității relative.

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

Toate suporturile care conțin software de producție și date, informații de audit, arhivă sau de rezervă sunt stocate în instalații zipper sau în instalații de stocare securizate în afara locației, cu controale de acces fizice și logice adecvate, concepute pentru a limita accesul personalului autorizat și pentru a proteja aceste suporturi împotriva deteriorării accidentale.

ZIPPER stochează în siguranță toate suporturile amovibile și hârtia care conțin informații sensibile legate de operațiunile sale în containere securizate. Documentele și materialele sensibile sunt mărunțite înainte de eliminare. Suporturile utilizate pentru colectarea sau transmiterea informațiilor sensibile devin imposibil de citit înainte de eliminare. Dispozitivele criptografice sunt distruse fizic înainte de eliminare.

10.3.5 Gestionarea operațiunilor

ZIPPER TSA se asigură că procedurile, procesele și infrastructura trebuie să respecte gestionarea operațională, cerințele procedurale de securitate, gestionarea accesului la sistem, implementarea și întreținerea fiabilă a sistemelor, gestionarea continuității activității și gestionarea incidentelor, astfel cum sunt definite în ETSI EN 319 421.

Procedurile de gestionare a operațiunilor pentru ZIPPER TSA sunt încorporate în procedurile generale de gestionare a operațiunilor interne ZIPPER.

10.3.6 Compromiterea serviciilor TSA

În cazul compromiterii unei chei de semnare TSU, ZIPPER va revoca certificatul relevant și îl va adăuga la CRL ZIPPER. TSU nu va emite marcaje temporale dacă cheia sa privată nu este validă.
În cazul unei pierderi de calibrare a ceasului, ZIPPER nu va emite marcaje temporale până când nu se iau măsuri pentru a restabili calibrarea timpului.

10.3.7 Încetarea TSA

TSA se încheie:

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

ZIPPER se asigură că potențialele perturbări ale abonaților și părților bazându-se sunt reduse la minimum ca urmare a încetării serviciilor ZIPPER și, în special, asigură menținerea continuă a informațiilor necesare pentru a verifica corectitudinea serviciilor.

În cazul în care este necesar ca ZIPPER TSA să înceteze funcționarea, ZIPPER depune eforturi rezonabile din punct de vedere comercial pentru a notifica Abonații și părțile care se bazează cu privire la o astfel de reziliere înainte de încetarea TSA.

ZIPPER TSA revocă certificatele TSU la încetarea serviciilor sale.

10.3.7 Respectarea cerințelor legale

ZIPPER asigură conformitatea cu cerințele legale și de reglementare aplicabile, și anume următoarele:

- Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (Regulamentul eIDAS);
- Legislația privind datele cu caracter personal [inclusiv Regulamentele (UE) 2016/679 ale Parlamentului European și ale Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Standarde europene:
    - ETSI EN 319 401 Semnături și infrastructuri electronice (ESI); Cerințe generale de politică pentru furnizorii de servicii de încredere;
    - ETSI EN 319 411-1 Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea 1: Cerințe generale;
    - ETSI EN 319 411-2 Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea 2: Cerințe de politică pentru autoritățile de certificare care eliberează certificate calificate;
    - ETSI EN 319 421: "Semnături și infrastructuri electronice (ESI); Politica și cerințele de securitate pentru furnizorii de servicii de încredere care emit marcaje temporale".
    - ETSI EN 319 422 Semnături și infrastructuri electronice (ESI); Protocolul de marcare a timpului și profilurile tokenului de marcă temporală

ZIPPER care acționează în calitate de furnizor de servicii de încredere calificat face obiectul auditurilor de conformitate pentru serviciile sale de TSA și de marcare temporală pentru a se asigura că acestea îndeplinesc cerințele Regulamentului eIDAS.

10.3.8 Înregistrare privind serviciile de marcare temporală

ZIPPER TSA se asigură că toate informațiile relevante privind operațiunile serviciilor de marcare temporală ZIPPER sunt înregistrate pentru o perioadă definită, în special pentru furnizarea de probe în scopul procedurilor judiciare. Se păstrează următoarele înregistrări:

- Sincronizarea ceasurilor utilizate în marcarea în timp
- Detectarea pierderii sincronizării
- Solicitări de marcaje temporale și marcaje temporale create
- Evenimente legate de ciclul de viață al cheilor și certificatelor TSU

ZIPPER ține evidența tuturor informațiilor relevante privind funcționarea TSA ZIPPER pentru perioada de timp specificată în secțiunea 10.1.4.

10.3.9 Fiabilitatea organizațională

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