Politica și Codul de Practici și Proceduri
Autoritatea de Marcare Temporală DigiSign

Mărci temporale calificate

conform Regulamentului eIDAS și legislației naționale

Categorie:	**Document Public**	Limba:	**Română**
Emis de:	**Organismul de Gestionare a Politicilor DigiSign**		
Verificat de:	**Auditor Intern**	Ediția:	**1**
Aprobat de:	**General Manager**	Verisunea:	**2**

OID: **1.3.6.1.4.1.34285.3.1.1.1.1.1.0**

1.3.6.1.4.1.34285.3.1.1.2.3.1.0

Status: ***Spre abrobarea Organismului de Supraveghere***

DIGISIGN S.A.

Str. Virgil Madgearu, nr. 2 – 6, sector 1

014135, București, România

+4 031 620 12 89

+4 031 620 20 99

office@DigiSign.ro

www.DigiSign.ro

Istoria documentului

Ediție	Versiune	Descriere	Data	Emitent
1	1	Prima redactare: Politica și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign, în conformitate cu Regulamentul eIDAS și legislația națională aplicabilă	15 mai 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	2	Actualizări aduse ca urmare a auditului	15 iunie 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign

Contents

Introducere

DIGISIGN S.A. (denumită în continuare DigiSign) operează o infrastructură de chei publice (denumită în continuare PKI) în vederea furnizării de servicii de încredere, precum: semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate. DigiSign PKI utilizează o Autoritate de Certificare cu rol de rădăcină, sub care sunt emise Autorități de Certificare intermediare dedicate unei clase sau unui anumit tip de serviciu. În cadrul unei Autorități de Certificare Intermediară sunt definite mai multe profile de certificate pentru a emite un tip de certificat specific unei anumite clase sau aplicabilități.

În calitate de Autoritate de Certificare (denumită în continuare CA), DigiSign emite certificate digitale atât entităților din cadrul sectorului public, cât și celui privat, dar și persoanelor fizice, în conformitate cu regulile, principiile și practicile definte în acest document. În rolul său de CA, DigiSign operează funcții asociate cu operații criptografice care includ, dar nu se limitează la, cereri, emitere, revocare, suspendare, reînnoire de certificate digitale, emiterea și publicarea Listelor de Certificate Revocate (denumite în continuare CRL), precum și menținerea unui serviciu de verificare în timp real al certificatelor, bazat pe protocolul Online Certificate Status Protocol (denumit în continuare OCSP).

În calitatea de Autoritate de Marcare Temporală (denumită în continuare TSA), DigiSign emite mărci temporale de încredere pentru a aduce valoare adăugată semnăturilor electronice și aplicațiilor digitale care necesită să demonstreze faptul că o informație a existat într-o anumită formă la un moment anume în timp.

DigiSign este unul din principalii Prestatori de Servicii de Încredere Calificate care reușește cu succes să furnizeze servicii de încredere precum semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate, având în același timp și un rol de Terță Parte de Încredere (denumită în continuare TTP) în ceea ce privește crearea și validarea serviciilor respective.

1. Scop

Politica Autorității de Marcare Temporală DigiSign și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign au fost contopite în acest document care reprezintă o declarație publică a politicilor și practicilor urmate de DigiSign în calitate de Prestator de Servicii de Încredere Calificată, în vederea emiterii, validării și, în general, administrării cu succes a mărcilor temporale. Acest document este numit Politica și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign (în continuare CPP) și este structurat în conformitate cu RFC 3647 și standardul ETSI EN 319401. În acest document, dacă nu este specificat altfel, expresia CPP reprezintă prezentul document.

CPP conține o prezentare generala a politicilor, practicilor și a procedurilor implementate de DigiSign, pentru a functiona ca Autoritate de Marcare Temporala, în vederea emiterii Marcilor Temporale Calificate, în conformitate cu Regulamentul UE nr. 910/2014 (denumit în continuare Regulamentul eIDAS), legislația națională aplicabilă și cu standardele relevante din domeniu.

Acest document nu descrie protocoalele necesare accesării Autorității de Marcare Temporală DigiSign, ori cum pot fi evaluate cerințele identificate în prezentul document de către entități independente, ori cerințele necesare pentru a pune la dispoziția entităților independente respectivele informații, ori criteriile pe care entitățile independete trebuie să le îndeplinească pentru a obține astfel de informații.

2. Referințe

2.1. Referințe normative

- Regulamentul EU nr. 910/2014
- Legislația națională aplicabilă
- ETSI EN 319 421 – Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing Time Stamps
- ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocols and time-stamp token profiles;
- ETSI EN 319 402 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- IETF RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol
- Codul de Practici și Proceduri al Autorității de Certificare DigiSign

2.2. Referințe informative

- ITU-R TF. 460-6 (2002) – Standard-frequency and time-signal emissions
- IETF RFC 5905 – Network Time Protocol Version 4: Protocol and Algorithm Specifications
- ISO/IEC 19790:2012 – Information technology; Security techniques; Security requirements for cryptographic modules
- ISO/IEC 15408 (part 1 to 3) – Information technology; Security techniques; Evaluation criteria for IT security
- FIPS PUB 140-2 (2001) – Security requirements for cryptographic modules

3. Definiții și abrevieri

3.1. Definiții

- **Ora universală coordonată**: este o scală a timpului la secundă așa cum este definită în recomandarea ITU-R TF.460-6. În scopuri practice, este echivalentul mediei timpului solar în meridianul principal (0 °). Mai precis, UTC este un compromis între timpul atomic foarte stabil (Temps Atomique International - TAI) și timpul solar derivat din rotația neregulată a Pământului. UTC este standardul principal al timpului după care lumea reglează ceasurile și timpul.
- **Datum**: Data care a fost marcată temporal.
- **Network Time Protocol**: este un protocol de rețea pentru sincronizarea timpului sistemelor informatice prin rutarea pachetelor de rețea cu latență variabilă. Standardul de referință este IETF RFC 1305 (Network Time Protocol (NTP v3).
- **Entitate parteneră**: Destinatarul unei marcari temporale care se bazează pe acea marcare temporală.
- **Autoritate de marcare temporală:** Autoritatea administrată de un TSP care furnizează servicii de marcare temporală folosind unul sau mai multe protocoale de marcare temporală.
- **Beneficiar**: o persoană fizică sau juridică căreia îi este emisă o marcă-temporală.
- **Marcare temporală**: date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment.
- **Politica de marcare temporală**: Un set de reguli care indică aplicabilitatea unei mărci temporale pentru o comunitate și/sau o clasă de aplicații cu cerințe comune de securitate.

- **Time-Stamping Unit**: Setul hardware și software care este gestionat ca o unitate și are o singură instanță de timp care este activată cu o cheie la fiecare intrare.
- **Prestator de servicii de încredere**: entitatea care prestează unul sau mai multe servicii de încredere.
- **TSA Disclosure Statement**: Un set de declarații publice cu privire la politicile și practicile unui Autorități de Marcare Temporală, care vin in sprijinul beneficiarilor și entitatilor partenere, de exemplu, pentru a îndeplini cerințele de reglementare.
- **TSA Practice Statement**: O declarație publică despre practicile pe care un TSA le utilizează pentru a emite o marcă temporală.
- **Sistem TSA**: Un set de produse și componente IT utilizate pentru a oferi suport pentru furnizarea de servicii de marcare temporala.
- **UTC (k)**: O scală de timp dată de laborator "k" și care are o relație apropiată cu UTC, cu scopul de a ajunge la ± 100 ns.

3.2. Abrevieri

În acest document se aplică urmatoarele abrevieri:

BIPM	Bureau International des Poids et Mesures
BTSP	Bune practici privind politica de marcare temporala
CA	Autoritate de Certificare
CAB	Organism de evaluare a conformitatii
CAR	Raport de evaluare a conformitatii
CRL	Lista certificatelor revocate
DN	Nume distinctiv
ETSI	European Telecommunications Standards Institute
GMT	Greenwich Mean Time
HSM	Modul de securitate hardware
HTTP	Hypertext Transfer Protocol
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
PKI	Infrastructura de chei publice
SB	Organism de supraveghere
TAI	International Atomic Time
TCP	Transmission Control Protocol
TSA	Autoritate de marcare temporala
TSP	Prestator de servicii de incredere
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Ora universala coordonata

4. Concepte generale

Prezentul document face referire la Codul de Practici și Proceduri al Autorității de Certificare DigiSign (denumit în continuare CA CPP), în ceea ce privește politicile generale comune serviciilor de încredere furnizate de DigiSign în calitate de Prestator de Servicii de Încredere Calificate.

Cerințele politicii stabilite în CA CPP și în acest document fac referire la infrastructurile de chei publice și sursele de timp de încredere.

Toți participanții in procesul de marcare temporală, incluzând beneficiarii și entitățile partenere interesate, sunt așteptate să consulte acest document pentru a obține detalii privind modul în care DigiSign asigură serviciul de marcare temporală, în felul asta stabilind încredere și siguranță în serviciul oferit.

4.1. Servicii de marcare temporală

Furnizarea de servicii de marcare temporală e segmentată în prezentul document în urmatoarele servicii componente, în vederea clasificării cerințelor:

- Furnizarea de servicii de marcare temporală: Serviciul component care emite mărcile temporale
- Administrarea de servicii de marcare temporală: Serviciul component care monitorizează și controlează serviciilor de marcare temporală, incluzând sincronizarea cu sursa de timp UTC de referință și care asigura faptul că serviciul furnizat este în conformitate cu prevederile prezentului document.

DigiSign TSA aderă la standardele și regulile prezentate în cap. 2 al acestui document, pentru a menține încrederea beneficiarilor și entităților partenere în serviciile de marcare temporală.

4.2. Autoritate de Marcare Temporală

DigiSign în calitate de Prestator de Servicii de Încredere Calificate administrează o Autoritate de Marcare Temporală ca parte a Infrastructurii de Cheie Publica pentru a furniza publicului servicii de marcare temporală. Autoritatea de marcare temporala din cadrul DigiSign își asumă responsabilitatea pentru furnizarea serviciilor de marcare temporală, și prin urmare Autoritatea de Marcare Temporală are responsabilitatea uneia sau mai multor unități de marcare temporală care crează și semnează mărci temporale în numele Autorității de marcare temporală. DigiSign TSA se poate folosi de alte terțe părți pentru a furniza anumite servicii adiționale serviciilor de marcare temporală, însă Autoritatea de marcare temporală își asumă toată responsabilitatea și asigură ca politica prezentată în acest document este îndeplinită.

DigiSign, ca Autoritate de Marcare Temporală este auditată la fiecare 24 de luni de Organismul de Evaluare a Conformității conform punctului 13 din Articolul 2 al Regulamentului European nr. 765/2008. Organismul de evaluare a conformității auditează Autoritate de marcare temporală DigiSign și emite un raport de evaluare a conformității pe care DigiSign îl înaintează Organismului de Supraveghere pentru a putea obține statutul de furnizor de servicii de marcare temporală calificată. În urma obținerii acestui statut pentru serviciile de marcare temporala, DigiSign va informa organismul supraveghetor cu privire la orice schimbare ce ține de furnizarea acestui serviciu.

Astfel, TSA DigiSign este identificată în certificatul unitatății de marcare temporală și ar putea opera una sau mai multe unități de marcare temporală. Fiecare unitate de marcare temporală are câte o pereche diferită de chei, însă folosirea cheii e setată pe **semnatură digitală** și folosirea cheii extinsă e setată numai pe marcare temporală. Certificatul unității de marcare temporală este valabil timp de 12 ani. În domeniul DigiSign și în conformitate cu acest CPP, niciun certificat al unității de marcare temporală nu va fi folosit în semnarea certificatelor utilizatorilor finali sau a oricarui alt tip de certificate.

Mai jos se află un tabel care conține un sumar al unitatilor de marcare temporala DigiSign și a emitenților acestora.

DigiSign TSU	TSU DN	TSU Issuer
DigiSign Time-Stamping Authority	CN = DigiSign Time Stamping Authority SERIALNUMBER = 200506245DT47 OU = Autoritate de Marcare Temporala - Time Stamping Authority O = DigiSign S.A. L = BUCURESTI C = RO	CN = DigiSign Qualified CA Class 3 2017 OU = DigiSign Certification Services 2.5.4.97 = VATRO-17544945 O = DigiSign S.A. C = RO

4.3. Politici și Practici ale Autorității de Marcare Temporală

Politica de Marcare Temporală („la ce se aderă") și Codul de Practici și Proceduri al Autorității de Marcare Temporală („cum se aderă") au fost contopite în acest document numit Politica și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign (denumit în continuare CPP TSA). Documentul specifică o politică și o practică pentru serviciul de marcare temporală în vederea îndeplinirii cerințelele generale pentru furnizarea serviciilor de marcare temporală de încredere în conformitate cu standardele descrise în Capitolul 2 al acestui document.

Toate politicile și declarațiile de practică ale DigiSign, precum și declarațiile de informare, sunt sub controlul Organismului de Gestionare al Politicilor DiigSign și sunt puse la dispoziția publicului la următoarea adresă: www.digisign.ro

Prezentul document stabilește regulile generale privind funcționarea DigiSign TSA. Documentele interne și confidențiale suplimentare definesc exact modul în care DigiSign îndeplinește cerințele tehnice, organizaționale și procedurale identificate în standardele relevante. Aceste documente nu vor fi furnizate publicului datorită importanței lor în ceea ce privește securitatea operațiunilor DigiSign.

Acest document este gestionat de DigiSign prin intermediul Organismului său de Gestionare a Politicilor DigiSign. Regulile descrise în Capitolul 1.4 al CPP CA se aplică și pentru prezentul document.

Pentru orice detalii suplimentare privind furnizarea de servicii de marcare temporală de către DigiSign, părțile interesate pot adresa o cerere în acest sens la:

DIGISIGN S.A.
Adresă: Str. Virgil Madgearu, nr. 2 – 6, sector 1, 014135, București, România
Telefon: +4 031 620 12 89
Fax: +4 031 620 20 99
E-mail: office@DigiSign.ro
Website: www.DigiSign.ro

4.4. Utilizatorii și entitățile partenere

Utilizatorii și entitățile partenere reprezintă principalii actori ai DigiSign PKI, deoarece aceștia reprezintă destinatarii serviciilor de marcare temporală.

4.4.1. Utilizatorii

Utilizatorii sunt entități care dețin un acord privind serviciul de marcare temporală cu DigiSign și pot fi fie un utilizator individual, fie o organizație care cuprinde unul sau mai mulți utilizatori individuali.

În cazul în care Utilizatorul este un utilizator individual (Utilizator final), el / ea este răspunzător direct de obligațiile sale atunci când acestea nu sunt îndeplinite în mod corect.

Dacă Utilizatorul este o organizație care cuprinde unul sau mai mulți utilizatori individuali, unele dintre obligațiile care se aplică acelei organizații trebuie să se aplice și utilizatorilor individuali. În orice caz, organizația este responsabilă pentru îndeplinirea corectă a obligațiilor utilizatorilor individuali și, prin urmare, organizația trebuie să informeze în mod corespunzător utilizatorii individuali despre modul corect de utilizare a mărcilor temporale emise de DigiSign TSA și condițiile din TSA CPP.

4.4.2. Entitățile Partenere

O Entitate Parteneră este o entitate care acționează în baza unei mărci temporale generate conform CPP TSA și poate sau nu să fie abonat al serviciilor de marcare temporală furnizate de DigiSign. Entitatea Parteneră este pe deplin responsabilă pentru decizia de a se baza sau nu pe respectiva marcă temporală și, prin urmare, are obligația de a identifica și de a cunoaște condițiile în care a fost emisă respectiva marcă temporală.

5. Politici

5.1. Prezentare generală

DigiSign TSA eliberează TST în conformitate cu cerințele standardului ETSI EN 319 421 și cu dispozițiile prezentului document. TST emise de TSU din cadrul DigiSign TSA, au o precizie de 1 secundă UTC sau mai bună.

DigiSign TSA emite mărci temporale folosind chei private care sunt destinate special pentru acest scop. Mărcile temporale pot fi solicitate utilizând protocolul HTTP (S), așa cum este descris în RFC 3161.

5.2. Identificare

Identificatorul acestui CPP TSA sub care DigiSign emite TSTs este: 1.3.6.1.4.1.34285.3.2.4.256.2.1.3.n. Prin includerea acestui OID în toate mărcile temporale generate de DigiSign TSA, DigiSign pretinde conformitatea cu această politică de marcare temporală.

5.3. Aria de aplicabilitate

Această politică are scopul de a îndeplini cerințele privind mărcile temporale, pentru validitatea pe termen lung (de exemplu, așa cum este definită în ETSI EN 319 122), dar este, în general, aplicabilă oricărei utilizări care are o cerință pentru o calitate echivalentă. Această politică poate fi utilizată pentru serviciile publice de marcare temporală sau pentru serviciile de marcare temporală utilizate în cadrul unei comunități închise.

Mărcile temporale DigiSign pot fi generate prin orice aplicație care are capacitatea de a încorpora o marcă temporală.

5.4. Conformitate

DigiSign face referire la identificatorul de politică descris în secțiunea 5.2. din acest document, în toate mărcile temporale pentru a indica conformitatea cu această politică. DigiSign TSA face obiectul unor evaluări interne și externe, pentru a demonstra că DigiSign TSA își îndeplinește obligațiile și a implementat controalele adecvate descrise în acest document.

6. Practici și proceduri

6.1. Evaluarea riscurilor

DigiSign TSA efectuează evaluări de risc în mod regulat pentru a asigura calitatea și fiabilitatea serviciilor de marcare temporală. Controalele de securitate sunt definite într-un cadru de securitate al serviciilor de marcare temporală și sunt supuse controlului cel puțin o dată la 12 luni pentru a asigura eficiența acestora.

6.2. Asigurarea calității

Asigurarea calității este una dintre cele mai importante valori pe care un Furnizor de servicii de încredere calificate trebuie să le aibă, tocmai pentru că trebuie să asigure încrederea în sistemul lor. Prin urmare, DigiSign a implementat o varietate de controale de securitate pentru a asigura calitatea, performanța și funcționarea serviciului de marcare temporală pe care îl oferă.

Toate controalele de securitate implementate de DigiSign TSA au fost documentate și fac obiectul unor evaluări regulate de către o entitate independentă de încredere, capabilă să verifice respectarea controalelor de securitate.

În plus, pentru a asigura conformitatea cu standardul ETSI EN 319 421, au fost implementate de DigiSign TSA o serie de măsuri descrise în acest capitol.

6.2.1. Format

DigiSign TSA emite TST conforme cu standardul RFC 3161. Serviciul de marcare temporală folosește algoritmul RSA cu o funcție hash SHA-256 și o lungime a cheii de 2048 când generează TST.

6.2.2. Acuratețea timpului

DigiSign TSA generează TST cu o precizie de o secundă de UTC sau mai bine. Sursa de timp este asigurată de sistemul informatic al MCSI care asigură sursa de timp oficială pentru România, în conformitate cu cadrul juridic național.

6.2.3. Limitări

Atâta timp cât utilizatorul are un acord încheiat cu TSA DigiSign, atunci serviciul de marcare temporală oferit de DigiSign TSA poate fi utilizat în legătură cu orice tranzacție, fără o limită, dacă nu se specifică altfel în acord.

În limitele stabilite de legislația națională aplicabilă, cu excepția fraudei sau a abaterilor intenționate, DigiSign nu va fi responsabilă pentru orice pierdere a profitului, a datelor

sau orice daune indirecte, consecvente sau punitive, rezultate din sau în legătură cu utilizarea serviciilor de încredere furnizate.

DigiSign nu își asumă nici o responsabilitate financiară pentru mărcile temporale utilizate în mod necorespunzător. Nici un utilizator sau entitate parteneră care utilizează servicii de marcare temporală furnizate de DigiSign TSA nu va putea invoca necunoașterea condițiilor acestui document.

DigiSign va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfășurării activității de marcare temporală, tuturor persoanelor care își întemeiază conduita pe efectele juridice ale mărcilor temporale calificate, până la echivalentul sumei de 100 RON pentru fiecare risc asigurat. Riscul asigurat reprezintă fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligații prevăzute de lege.

6.2.4. Obligațiile utilizatorilor

Conform condițiilor generale de furnizare a serviciilor, publicate la adresa www.digisign.ro.

6.2.5. Obligațiile Entităților Partenere

Conform condițiilor generale de furnizare a serviciilor, publicate la adresa www.digisign.ro.

6.2.6. Verificarea mărcilor temporale

Pentru a verifica o marcă temporală emisă de DigiSign TSA, următoarea activitate trebuie să fie finalizată cu succes:

I. Verificarea emitentului

Emitentul unui mărci temporale este o TSA care trebuie să utilizeze certificate electronice adecvate pentru eliberarea unei mărci temporale. Cheile publice ale certificatelor de marcare temporală sunt incluse în certificatele TSU și CA și sunt publicate pentru a permite verificarea mărcii temporale, respectiv dacă a fost semnată corect de TSA. Certificatele de TSUs din cadrul domeniului DigiSign sunt disponibile pentru verificare la: www.DigiSign.ro.

II. Verificarea revocării

DigiSign pune la dispoziția părților interesate serviciul OCSP pentru a verifica starea certificatelor utilizate de TSU pentru a semna mărci temporale. Adresa pentru accesarea serviciului OCSP este inclusă în certificatul de TSU, utilizat pentru a semna marca temporală.

III. Verificarea integrității

Pentru a verifica integritatea unui mărci temporale, trebuie verificată integritatea criptografică a mărcii temporale, precum dacă structura ASN.1 este corectă și data aparține cererii. Aceste informații pot fi verificate prin intermediul serviciului web DigiSign TSA oferit gratuit la www.digisign.ro.

6.2.7. Legea aplicabilă

DigiSign oferă servicii de marcare temporală calificată în conformitate cu prevederile legale europene și naționale aplicabile:

- Regulatamentul UE nr. 910/2014
- Legea națională aplicabilă

6.2.8. Disponibilitate

DigiSign TSA a pus în aplicare măsurile următoare pentru a asigura disponibilitatea serviciului:

- configurarea redundantă a sistemului IT,
- conexiuni redundante la Internet de mare viteză, pentru a evita indisponibilitatea serviciului,
- utilizarea de surse de alimentare și generator electric.

Cu toate că aceste măsuri asigura disponibilitatea serviciului a DigiSign TSA, acesta nu poate garantată o disponibilitate anuală de 100%. DigiSign TSA își propune să ofere disponibilitatea serviciului de peste 99% anual.

6.3. Termeni și condiții

Pentru utilizarea serviciilor de marcare temporală calificată furnizate de DigiSign TSA, utilizatorii și entitățile partenere trebuie să respecte condițiile generale de furnizare publicate la adresa www.digisign.ro, care conțin informații despre limitările serviciului, obligațiile părților și alte informații adiționale. Condițiile respective sunt completate de prevederile acestui document.

6.3.1. Implementarea unei politici

Se realizează conform cap. 5 al acestui document.

6.3.2. Reținerea logurilor

În calitate de QTSP, DigiSign păstrează jurnale de evenimente în fișierele de pe discul de sistem până când acestea ajung la capacitatea maximă permisă. După depășirea spațiului alocat, jurnalele de evenimente sunt stocate în arhive, fiind disponibile offline. Jurnalele arhivate sunt păstrate timp de cel puțin 10 ani.

6.4. Informații despre politicile de securitate

Pentru Autoritatea Marcare Temporală, DigiSign a implementat o politica de securitate a informațiilor. Toți angajații trebuie să respecte reglementările menționate în această politică și conceptele de securitate derivate. Politica de securitate a informației este revizuită în mod regulat și mai ales atunci când se produc schimbări semnificative. Managementul DigiSign, dacă este cazul, aprobă modificările privind această politică.

6.5. Obligații

În calitate de QTSP, DigiSign operează o Autoritate de marcare temporală și își asumă responsabilitatea în conformitate cu prevederile acestui document, precum și cu prevederile regulamentului eIDAS și ale legislației naționale aplicabile.

DigiSign acționează ca parte a acordurilor și obligațiilor reciproce dintre TSA, utilizatori și entități partenere. CPP CA și CPP TSA în vigoare fac parte integrantă din contractele de servicii încheiate între DigiSign S.A. și utilizatori.

6.5.1. Obligațiile DigiSign

DigiSign TSA își asumă următoarele obligații:

- Să opereze în conformitate cu acest document, cu CPP CA și alte politici și proceduri operaționale relevante, pentru a se asigura că TSU-urile mențin o precizie minimă a timpului UTC de ± 1 secundă,
- Să efectueze revizuiri interne și externe pentru a asigura conformitatea cu legislația și politicile și procedurile interne relevante,
- Să furnizeze acces la sisteme cu disponibilitate ridicată, cu excepția cazurilor de întreruperi tehnice planificate, pierderi de sincronizare temporală și cauze care exclud responsabilitatea.

Conformitatea cu cerințele menționate în acest document este asigurată de DigiSign TSA. Un organism independent de evaluare a conformității verifică eficiența procedurilor.

În plus, DigiSign garantează că:

- Activitatea sa comercială este asigurată pe baza unor echipamente și aplicații software fiabile,
- Activitățile și serviciile furnizate sunt conforme cu legislația aplicabilă și, în special, nu încalcă proprietatea intelectuală, licențele și alte drepturi conexe,
- Serviciile furnizate sunt conforme cu normele general acceptate,
- TST emise de DigiSign TSA nu conțin date sau greșeli false,
- Menține o echipă competentă și experimentată care să asigure continuitatea serviciilor de marcare temporală,
- Asigură în permanență securitatea fizică și logică, precum și integritatea materialelor, software-urilor și bazelor de date necesare pentru funcționarea corectă a TSA, așa cum este descris în acest document,
- va monitoriza și va controla infrastructura TSA, pentru a preveni sau a limita orice perturbare sau indisponibilitate a TSA care rezultă din atacuri deliberate,
- Va lua toate măsurile necesare conform normelor general acceptate pentru a-și asigura serviciile,
- Va pune la dispoziție o infrastructură de rezervă care poate fi utilizată în cazul întreruperii serviciului infrastructurii principale.

6.5.2. Obligațiile utilizatorilor

Obligațiile utilizatorilor privind utilizarea serviciilor de marcare temporală sunt descrise în Termenii și condițiile publicate la www.DigiSign.ro și se referă la:

- Utilizatorul este obligat să verifice semnătura TST și să se asigure că cheia privată utilizată pentru semnarea TST nu a fost revocată,
- Utilizatorul este obligat să utilizeze funcții criptografice securizate pentru solicitări de marcare,
- Utilizatorul este obligat să informeze utilizatorii finali (de exemplu, Entitățile Partenere) despre utilizarea corectă a mărcilor temporale în conformitate cu CPP TSA.

6.5.3. Obligațiile Entităților Partenere

Obligațiile Enităților Partenere sunt definite în Termenii și condițiile publicate la www.DigiSign.ro. Înainte de a se baza pe o marca temporală emisă de DigiSign TSA, Entitățile Partenere trebuie:

- Sa verifice dacă TST a fost semnat corect cu cheia corespunzătoare certificatului TSU și sa se asigure că cheia privată utilizată pentru a semna TST nu a fost revocată,

- Sa ia în considerare orice limitări privind utilizarea TST indicată de politica de marcare temporală aplicabilă,
- Sa ia în considerare orice alte măsuri de precauție definite în acorduri sau alte documente relevante.

Întrucât obligația principală a unei entități partenere este de a verifica TST și semnătura electronică care îi aparține, această verificare cuprinde:

- Verificarea dacă semnătura pe TST este valabilă,
- Verificarea certificatului TSU utilizat pentru semnarea TST, după cum urmează:
  - Verificarea căii de încredere a certificatului rădăcină de încredere și pentru fiecare dintre certificatele din lanț (inclusiv certificatul TSU);
  - Verificarea dacă certificatul nu a expirat la momentul semnării,
  - Verificarea faptului dacă certificatul nu a fost revocat sau suspendat la momentul semnării - această verificare se efectuează preferențial prin cererea OCSP prin intermediul link-ului menționat în AIA al certificatului de TSA sau, alternativ, prin căutare CRL cu software adecvat sau accesând Registrul public al DigiSign sau orice altă metodă de validare propusă de DigiSign.

Entiatea Parteneră se poate baza pe un TST în care certificatul TSU a expirat doar atunci când există o dovadă care nu poate fi repudiată (de ex. Un alt TST) care garantează existența TST înainte de expirarea certificatului și că TST nu s-a schimbat de atunci. Acest lucru are o importanță deosebită atunci când funcțiile criptografice sau lungimea cheii certificatului TSU nu mai sunt considerate sigure în momentul în care partea intenționează să se bazeze pe TST.

Rețineți că DigiSign are un număr de certificate TSU diferite, semnate de diferite CA-uri DigiSign. Este important ca părțile invocate să facă referire la depozitarul acestor certificate pentru a determina TSU relevant, deoarece acest lucru poate afecta, de asemenea, nivelul de încredere.

În plus, deoarece DigiSign TSA pretinde conformitatea cu standardul ETSI EN 319 421 și deoarece acest standard conține câteva cerințe suplimentare pentru mărcile temporale electronice calificate (QTS) conform regulamentului eIDAS, toate părțile interesate ar trebui să ia notă de următoarele:

DigiSign funcționează în prezent în cadrul măsurilor tranzitorii definite la articolul 51 din Regulamentul eIDAS. Cheia publică a TSU-urilor DigiSign nu este prezentă pe lista de încredere europeană. Cu toate acestea, CA-urile emitente ale certificatelor DigiSign TSU sunt enumerate în Lista de încredere europeană.

6.6. Răspunderea

DigiSign se angajează să opereze TSA în conformitate cu prevederile CPP TSA, CPP CA și termenii acordurilor cu abonații. DigiSign își declină orice responsabilitate în ceea ce privește utilizarea necorespunzătoare a TST-urile pe care le furnizează și semnează.

DigiSign își asumă răspunderea specifică pentru daunele aduse Utilizatorilor și Entităților Partenere în legătură cu certificatele electronice calificate valabile utilziate, în conformitate cu legile și reglementările naționale specifice.

Răspunderea DigiSign față de uilizator este stipulată în acordurile semnate cu aceștia. DigiSign nu este responsabilă pentru greșelile de verificare a valabilității mărcilor temporale sau pentru concluziile greșite condiționate de omisiuni sau pentru consecințele unor astfel de concluzii greșite. DigiSign nu își asumă nicio răspundere pentru pierderea valorii dovezii de confirmare a valabilității din cauza forței majore.

7. Controale operaționale

Acest capitol descrie controalele implementate de DigiSign TSA pentru a furniza servicii de non-repudiere de încredere, cum ar fi mărcile temporale calificate (QTST).

7.1. Introducere

DigiSign a implementat un sistem de management al securității informațiilor pentru a menține securitatea serviciilor de marcare temporală pe care le oferă.

Furnizarea unui TST ca răspuns la o cerere este la discreția DigiSign TSA, în funcție de acordul incheiat cu utilizator.

7.2. Organizare internă

Structura, politicile, procedurile și controalele organizaționale ale DigiSign sunt aplicabile pentru DigiSign TSA, fiind descrise în CPP CA.

Procedurile organizatorice respectă regulile și reglementările definite în secțiunea 2.1. - Referințe normative ale acestui document.

7.3. Personal de încredere

Practicile definite în secțiunea 5.2. și 5.3. din CPP CA se aplică pentru controalele de personal.

În ceea ce privește personalul care administrează TSA în domeniul DigiSign, acestea răspund acelorași cerințe ca și persoanele care administrează DigiSign CA, respectiv să fie de încredere și fără conflicte de interese care ar putea prejudicia imparțialitatea operațiunilor TSA.

7.4. Alte controale

Practicile identificate în secțiunea 5.1. ale CPP CA, se aplică și pentru controalele fizice de securitate privind TSA.

Toate sistemele (software și hardware) utilizate de serviciul de marcare temporală sunt identificate, clasificate și înregistrate în mod clar într-o bază de date de gestionare a activăților. Toate mediile sunt manipulate în siguranță și datele de pe mediile eliminate sunt șterse în siguranță, fie prin ștergerea electronică a datelor, fie prin distrugerea fizică a materialelor eliminate.

7.5. Controlul accesului

Practicile definite în secțiunea 5.2. – și 5.1. ale CPP CA, se aplică și pentru controalele fizice de securitate ale TSA.

Diferitele straturi de securitate în legătură cu accesul fizic și logic asigură o funcționare sigură a serviciului de marcare a timpului (de exemplu firewall-uri, mediu fizic securizat etc.). În cazul în care o persoană care efectuează operațiuni pentru serviciile de marcare temporală, se modifică sau părăsește organizația, tot accesul privind securitatea pe care acea persoană il avea sunt retrase imediat.

7.6. Controale criptografice

Acest capitol definește regulile în care DigiSign TSA generează și gestionează perechea de chei criptografice a TSU, precum și cerințele tehnice asociate.

7.6.1. Generearea

Generarea perechii de chei a unui TSU este un proces critic dat fiind faptul că modul în care este generată o pereche de chei este esențială pentru siguranța întregului sistem PKI. DigiSign TSA asigură că orice cheie criptografică TSU este generată în circumstanțe controlate și în conformitate cu cele mai bune practici din domeniu pentru ciclul de viață cheie, lungimea cheii și algoritmii.

DigiSign generează pereche de chei criptografice utilizate în serviciile sale TSA sub controlul M în afara controlului de către personalul autorizat într-un mediu fizic securizat, într-un mod de securitate hardware (HSM) care este certificat ca fiind compatibil cu standardul FIPS 140-2 Level 3 sau cu standardul ISO 15408 Common Criteria EAL 4+.

Astfel, perechea de chei este generată și există pe toată durata vieții într-un mediu protejat fizic și electromagnetic. Cheia privată este păstrată permanent într-un format criptat pe dispozitivul HSM și niciodată nu este lasată într-un format necriptat.

Toate acțiunile întreprinse atunci când se generează perechea de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul ceremoniei. Înregistrările sunt păstrate din motive de audit sau pentru verificări periodice ale sistemului.

După ce perechea cheilor este generată și cheia privată este activată în HSM, ea poate fi utilizată în operații criptografice până la expirarea perioadei de validitate sau până când este compromisă.

TSA din domeniul DigiSign utilizează perechi de chei RSA cu o lungime de 2048 de biți, iar cheia privată este utilizată numai pentru semnarea TST.

7.6.2. Protecția

Practicile de protecție, stocare, salvare și recuperare cheie TSU sunt descrise în secțiunea 6.2. ale CPP CA.

Cheia privată TSU trebuie să fie susținută și stocată pentru un eveniment improbabil de pierdere de tip cheie din cauza unei întreruperi neașteptate a alimentării sau a unei defecțiuni hardware. În timpul ceremoniei de generare a cheilor trebuie obținută o copie de rezervă. Salvarea cheii private este păstrată în secret, integritatea și autenticitatea acesteia fiind păstrată într-o cutie sigură.

7.6.3. Cheia publică

DigiSign TSA garantează integritatea și autenticitatea cheilor de verificare a semnăturilor TSU, după cum urmează:

- Cheia publică TSU este disponibilă pentru părți interesate la www.DigiSign.ro,
- TSU nu eliberează o marcă temporală înainte de verificarea lanțului certificatului,
- Fiecare TSU are o cheie privată,
- Perioada de valabilitate a unui certificat TSU este actualizată periodic, iar serviciile CRL sau OCSP sunt disponibile cu referințele din certificatele.

DigiSign TSA emite mărci temporale calificate conform Regulamentului eIDAS, iar certificatul TSU este emis de DigiSign CA Class 3 2017 conform politicii certificatelor ETSI EN 319 411-2.

7.6.4. Reînnoirea

Durata de viață a certificatelor TSU nu depășește perioada de timp în care algoritmul ales și lungimea cheii sunt recunoscute ca fiind potrivite scopului.

Un singur certificat este emis pentru orice cheie specifică TSU. Certificatele TSU nu sunt reînnoite.

7.6.5. Expirarea

DigiSign TSA asigură faptul că cheile private de semnare TSU nu sunt utilizate după sfârșitul ciclului lor de viață. În special, există proceduri operaționale și tehnice pentru a asigura introducerea unei noi chei în momentul expirării perioadei cheii de utilizare a TSU și cheia privată a TSU sau a oricărei părți, inclusiv a copiilor, să fie distrusă astfel încât cheia privată să nu poată fi recuperată. Sistemul de generare TST respinge orice încercare de a emite un TST dacă expiră cheia privată de semnare sau dacă termenul de utilizare a cheii private de semnare a expirat.

7.6.6. Modulele criptografice

DigiSign dispune de proceduri pentru a se asigura că modulele de securitate hardware destinate serviciilor de non-repudiere nu sunt manipulate necorespunzător în timpul transportului sau al depozitării. Acceptarea testelor este efectuată pentru a verifica dacă hardware-ul criptografic funcționează corect. Instalarea și activarea sunt efectuate numai de personal autorizat, prin control M din N, în roluri de încredere, iar dispozitivele funcționează într-un mediu securizat fizic. Cheile private sunt șterse din module atunci când sunt scoase din uz în conformitate cu instrucțiunile producătorului. Informații suplimentare sunt furnizate la punctul 6.6. - Controlul tehnic al ciclului de viață al CPP CA.

7.6.7. Autoritatea de Certificare Rădăcină

DigiSign TSA este operat de Infrastructura publică a DigiSign, care este alcătuită din mai multe Autorități de Certificare și un serviciu de validare prin OCSP.

CA ROOT sunt operate offline, toate aspectele legate de securitatea fizică și tehnică sunt detaliate în CPP CA, publicat la www.DigiSign.ro.

7.7. Marcarea Temporală

7.7.1. Emitentul

DigiSign TSA dispune de instrumente tehnice pentru a se asigura că TST-urile sunt emise în siguranță și includ timpul corect. În conformitate cu cerințele menționate în secțiunea 2 a prezentului document, fiecare TST include:

- reprezentare (de exemplu, valoarea hash) a datei care este marcată temporal, așa cum a fost furnizată de solicitant;
- un număr de serie unic care poate fi folosit atât pentru solicitarea TST, cât și pentru identificarea TST specifice;
- un identificator pentru politica de marcare temporală utilizată;
- timpul calibrat la o secundă de UTC, trasabil la o sursă UTC (k);
- semnătura electronică generată folosind o cheie folosită exclusiv pentru marcarea temporală;
- un identificator pentru TSA și TSU.

7.7.2. Sincronizarea cu UTC

DigiSign TSA asigură faptul că ceasul său este sincronizat cu UTC cu o precizie de 1 secundă sau mai mult, utilizând protocolul NTP.

DigiSign TSA monitorizează sincronizarea ceasului și se asigură că, dacă timpul indicat într-un TST se deplasează sau sare din sincronizare cu UTC, acest lucru este detectat. În cazul în care ceasul TSA scade din precizie, nu se emit mărci temporale până când sincronizarea ceasului nu este asigurată din nou.

În mod specific, sunt acoperite următoarele subiecte:

- Calibrarea continuă a ceasului TSU
- Monitorizarea preciziei ceasului TSU
- Analiza împotriva atacurilor asupra ceasului
- Comportament în timpul săririi sau adăugării unei secunde „leap”
- Comportament în timpul departarii de mai mult de 1 secunde de la UTC

7.8. Securitatea fizică

Se aplică practicile identificate în capitolele 5 și 6 ale CPP CA.

Sistemele informatice, terminalele și resursele informaționale ale operatorilor DigiSign sunt plasate într-o zonă dedicată, protejate fizic împotriva accesului neautorizat, distrugerii sau întreruperii activității. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrata în jurnalul de evenimente (jurnale de sistem); Stabilitatea surselor de energie și a temperaturii sunt, de asemenea, monitorizate și controlate.

7.9. Securitatea operațiilor

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice operatiilor. Măsurile de securitate au fost luate la toate nivelurile, începând de la nivelul fizic și până la nivelul cererii.

Controalele care aparțin DigiSign TSA au următoarele măsuri de securitate:

- autentificare obligatorie la nivel de sistem de operare și aplicații
- controlul securizat al accesului,
- posibilitatea de a fi auditat din punct de vedere al securității,
- calculatorul este accesibil numai personalului autorizat cu roluri de încredere în DigiSign,
- segregarea sarcinilor, în funcție de rolul lor în cadrul sistemului,

- identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- împiedicarea reutilizării unui obiect printr-un alt proces după ce acesta este eliberat de autoritatea autorizată,
- protecția criptografică a schimburilor de informații și protecția bazelor de date,
- operațiile de arhivare a jurnalului efectuate pe un computer și auditul necesar datelor,
- cale sigură care permite identificarea și autentificarea rolurilor și a personalului
- îndeplinirea acestor roluri,
- metode de restaurare cheie (numai în cazul modulelor de securitate hardware), aplicația și sistemul de operare,
- monitorizarea și alertarea în cazul accesului neautorizat la resursele de calcul.

Se aplică și practicile identificate în capitolele 5 și 6 ale CPP CA.

7.10. Securitatea rețelei

Terminalele de încredere și stațiile de lucru aparținând DigiSign sunt conectate printr-o rețea LAN, împărțită în mai multe subrețele, cu acces controlat. Accesul de pe Internet către orice segment este protejat de un firewall inteligent. Verificările de securitate sunt dezvoltate pe baza firewall-ului și a filtrelor de trafic aplicate la nivelul routerelor și proxy-urilor. Evenimentele (jurnalele) sunt înregistrate în jurnalele de sistem și permit supravegherea utilizării corecte a serviciilor furnizate de DigiSign.

7.11. Managementul incidentelor

Practicile definite în secțiunea 5.6.1. a CPP CA se aplica procedurilor de tratare a incidentelor.

7.12. Evidențe

La momentul detectării unui incident de securitate, s-ar putea să nu fie evident dacă incidentul de securitate este supus unor investigații suplimentare. Prin urmare, este important ca orice dovadă, statutul sistemului IT sau al informațiilor să fie salvat în siguranță înainte de a deveni inutilizabile sau distruse.

Dosarele TSP sunt păstrate accesibile pentru o perioadă corespunzătoare, inclusiv după încetarea activităților. Toate informațiile relevante privind datele emise și primite de către TSP sunt păstrate pentru a furniza probe în procedurile judiciare și pentru a asigura continuitatea serviciului. In mod deosebit:

- Se păstrează confidențialitatea și integritatea înregistrărilor curente și arhivate cu privire la funcționarea serviciilor.
- Înregistrările privind gestionarea serviciilor sunt confidențiale și pastrate în conformitate cu practicile comerciale descrise.
- Înregistrările privind gestionarea serviciilor, dacă este necesar, sunt puse la dispoziție pentru a dovedi funcționarea corectă a serviciilor pentru procedurile judiciare.
- TSP înregistrează evenimentele semnificative de mediu, gestionarea cheilor și sincronizarea ceasurilor. Timpul utilizat pentru înregistrarea evenimentelor, după cum este necesar în jurnalul de audit, este sincronizat continuu cu UTC.
- Înregistrările privind serviciile sunt păstrate pentru o perioadă după expirarea valabilității cheilor de semnare sau a oricărui serviciu pentru a asigura încrederea, în probele juridice necesare în conformitate cu prezentul document.
- Evenimentele sunt înregistrate într-un mod care nu poate fi șters sau distrus (cu excepția cazului în care acestea pot fi transferate în mod credibil pe suporturi pe termen lung).

7.13. Continuarea afacerii

Backupurile bazelor de date ale tuturor TST-urilor emise de DigiSign TSA sunt păstrate într-un spațiu de stocare în afara amplasamentului. În cazul în care cheia privată a TSU este compromisă sau suspectată a fi compromisă, DigiSign TSA va informa abonații și părțile interesate și va înceta să utilizeze cheia compromisă. În cazul revocării certificatului TSU, acțiunile necesare se efectuează în conformitate cu planul de recuperare.

În cazul pierderii sincronizării ceasurilor, DigiSign TSA își suspendă operațiunile pentru a preveni daune suplimentare. Planul de recuperare este activat pentru a restabili sincronizarea și serviciul.

Serviciul de marcare temporala se află într-un mediu fizic securizat care minimizează riscul dezastrelor naturale (de exemplu incendii).

Cheile private ale TSU sunt stocate într-un modul criptografic securizat de tip HSM.

În cazul în care cheile private sunt compromise, arhiva marcilor temporale salvate ajută la diferențierea marcilor corecte de cele false.

HSM este izolat de rețeaua publică și, dacă este necesar, se iau următoarele măsuri:

- notificarea Administratorului de Securitate pentru a coordona măsurile care trebuie luate.
- Inceperea unei evaluari de securitate a cheilor private rămase (verificări de integritate, analiză fișier jurnal).
- notificarea incidentului părților interesate.
- În cazul dezastrelor naturale (de ex. Incendii, cutremure, furtuni), în cazul în care provoacă o pierdere a instalației, serviciul de marcare temporală ar putea fi suspendat până la activarea instalației de recuperare în caz de dezastru.

7.14. Planul de terminare

Practicile identificate în secțiunea 5.7. a CPP CA se aplică de asemenea. În plus:

- În cazul în care DigiSign TSA își încetează operațiunile din orice motiv, acesta notifică organismul național de supraveghere înainte de reziliere.
- Trebuie furnizată o notificare în timp util tuturor abonaților și părților interesate, pentru a minimiza orice întrerupere cauzată de încetarea serviciilor.
- În plus, în colaborare cu Organismul de Supraveghere, DigiSign va coordona măsurile necesare pentru a asigura păstrarea tuturor înregistrărilor arhivate relevante înainte de încetarea serviciului.
- În plus, DigiSign va menține un plan de terminare actualizat și înainte de a termina serviciile de marcare a timpului, vor fi aplicate următoarele proceduri:

a. DigiSign va informa toți abonații și alte entități cu care are acorduri sau alte forme de relații stabilite,
b. DigiSign va înceta autorizația tuturor subcontractanților de a acționa în numele său în îndeplinirea oricăror funcții legate de procesul de emitere a TST,
c. DigiSign va transfera către o entitate fiabilă, într-un timp rezonabil, obligațiile sale de a păstra toate informațiile necesare pentru a dovedi operațiunile sale, cu excepția cazului în care se poate demonstra că DigiSign nu este proprietarul acestor informații,
d. Cheile private DigiSign TSA, inclusiv copii de rezervă, vor fi distruse sau retrase din utilizare, astfel încât cheile private să nu poată fi preluate,
e. DigiSign TSA va lua măsurile necesare pentru revocarea certificatelor TSU,

f. Când este posibil, DigiSign va utiliza un sistem care permite transferul serviciilor furnizate clientului său unui alt furnizor de servicii de încredere calificat.

- De asemenea, DigiSign dispune de un aranjament care să acopere costurile pentru îndeplinirea acestor cerințe minime în caz de faliment sau din alte motive prin care DigiSign nu este în măsură să acopere costurile în sine, în măsura posibilă, în limitele impuse de legislația aplicabilă privind faliment.
- DigiSign va menține sau va transfera către o entitate fiabilă obligațiile de a-și pune la dispoziția părților învinuite cheia publică sau TST pentru o perioadă rezonabilă de timp.

7.15. Conformitate

DigiSign oferă servicii de marcare temporală calificată în conformitate cu prevederile legale europene și naționale aplicabile:

- Regulatamentul UE nr. 910/2014
- Legea națională aplicabilă

Conformitatea este asigurată prin audituri interne și externe, realizate cel puțin o dată la 24 de luni.