

**Aprobat**  
GENERAL MANAGER  
DORU VIJIANU

## Serviciu Calificat de Validare a Semnăturii ZIPPER Declaratia “Disclosure Statement”

THE STATEMENT IS THE PROPERTY OF ZIPPER SERVICES S.R.L.  
UNAUTHORIZED COPYING IS NOT ALLOWED

Istoric editii			
Editia	Data si descriere modificare	Intocmit	Avizat
1	28.06.2023 – Prima editie	Mirela Ojog	Judit Fekete
2	24.04.2024 – Editia a II-a	Mirela Ojog	Judit Fekete

**CONTINUT**

1	INFORMAȚII DE CONTACT .....	5
2	INTRODUCERE.....	5
3	CERINȚE GENERALE .....	5
4	FORMATE ȘI NIVELURI DE CONFORMITATE A SEMNATURILOR/SIGILIILOR .....	6
5	MODEL DE VALIDARE .....	6
5.1	PROCESUL DE VALIDARE .....	6
5.2	INDICATORI DE STATE DE VALIDARE ȘI RAPORT DE VALIDARE .....	7
6	SERVICE.....	7
7	UTILIZARE.....	8
8	DREPTURILE SI OBLIGAȚIILE UTILIZATORILOR .....	9
8.1	RĂSPUNDEREA UTILIZATORULUI .....	9
8.2	OBLIGAȚIILE UTILIZATORULUI .....	9
8.3	DREPTURILE UTILIZATORULUI .....	9
8.4	OBLIGAȚII DE VERIFICARE A APLICABILITĂȚII LEGALE A UNEI SEMNĂTURI/SIGILII VALIDATE.....	9
9	GARANȚIE LIMITATĂ ȘI DECLINARE A RĂSPUNDERII/LIMITAREA RĂSPUNDERII ÎN FURNIZAREA SERVICIULUI .....	9
10	ACORDURI APLICABILE, CPS, CP .....	10
11	POLITICA/DECLARAȚIA DE CONFIDENȚIALITATE .....	10
12	POLITICA DE RAMBURSARE .....	10
13	LEGEA APLICABILĂ, PLÂNGERI ȘI SOLUȚIONAREA LITIGIILOR .....	10
14	EVALUĂRI DE CONFORMITATE, MĂRCI DE ÎNCREDERE/LOGO-URI ȘI AUDIT .....	11
15	PUNCTE DE ÎNREGISTRARE ȘI VERIFICARE A IDENTITĂȚII.....	11

Acest document este o declarație de divulgare/PDS a furnizorului de servicii de încredere (TSP) ZIPPER cu privire la serviciul de validare calificată a semnăturilor și sigiliilor electronice calificate QSVS - eIDAS (pe scurt, SERVICE).

Această declarație urmează structura Anexei A a documentului ETSI TS 319-411-1 și are caracter informativ doar pentru Utilizatorii SERVICIULUI. Acest document nu înlocuiește și nu înlocuiește Declarația de Politică și Practică a QCSP pentru SERVICIUL, conform căreia este furnizată validarea calificată a semnăturilor și sigiliilor electronice calificate.

## 1. Informații de contact

Orice întrebări referitoare la acest document pot fi adresate la:

### **ZIPPER SERVICES**

Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,  
Cluj-Napoca, 400285, România

*Punct de lucru:*

B-dul 1 Decembrie 1918 nr. 1G,  
Sector 3, Bucuresti, 032451, Romania

*Punct de lucru:*

str. Nikola Tesla, nr. 2, cod 400221  
Cluj-Napoca, 400285, Romania

Site-ul web oficial al Furnizorului: <https://ezipper.ro/en/>

E-mail: [office@ezipper.ro](mailto:office@ezipper.ro)

Telephone +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

Tel: +40 213 404 638; Email: [support.pki@ezipper.ro](mailto:support.pki@ezipper.ro)

Site web de informații PKI: <https://pki.ca.ezipper.ro/>

## 2. Introducere

Acest document este o Declarație de divulgare privind serviciul de validare calificată a semnăturilor și sigiliilor electronice calificate și a semnăturilor și sigiliilor electronice avansate însoțite de certificate calificate QSVS (pe scurt, SERVICE) ale Furnizorului de servicii de încredere calificat (QCSP) ZIPPER.

Declarația de divulgare oferă utilizatorilor informații generale despre cerințele SERVICIULUI și este conformă cu cerințele pentru acest serviciu cuprinse în Regulamentul UE 910/2014.

Auditul evaluării conformității SERVICIULUI a fost efectuat de către auditorul independent.

## 3. Cerințe generale

Serviciul de validare a semnăturii/sigiliului calificat (SERVICIUL) al Furnizorului de servicii de încredere calificat ZIPPER (furnizorul) utilizează infrastructura cheii publice (PKI) pe care o operează.

Furnizorul, prin acest SERVICIU (QS VS), validează semnătura electronică/sigiliul electronic calificat și/sau semnătura/sigiliul avansat însoțit de un certificat calificat al fiecărei părți interesate, sub rezerva unei Politici de Validare comune.

SERVICIUL validează semnăturile/ștampilele cu formate/profiluri conform Politicii Furnizorului urmând termenii și procedurile incluse în Declarația sa de practică pentru serviciu.

• Arborele OID	
1.3.6.1.4.1.57570	Numărul de identificare (OID) al Zipper Services SRL, înregistrat la IANA
1.3.6.1.4.1.57570.4.2.1.1	Serviciul de validare <b>Conform criteriilor de validare ETSI TS 119 441</b>
1.3.6.1.4.1.57570.4.2.2.3	Serviciu de validare calificat <b>Conform criteriilor de validare calificată ETSI TS 119 441</b>

Identificatorul confirmă conformitatea Politicii de validare a Furnizorului cu ETSI TS 119 441. Identificatorul 0.4.0.9441.1.2 confirmă că SERVICIUL este calificat așa cum este definit în articolele 32 și 33 din Regulamentul UE 910/2014 (EIDAS).

Conform ETSI EN 319 401, este obligatoriu ca un TSP să identifice politicile de servicii pe care le suportă. Pentru serviciile de validare, un astfel de identificator este comunicat de către SVSP prin răspunsurile și/sau rapoartele de validare și prin documentația furnizată abonaților și părților care se bazează.

#### 4. Formate și niveluri de conformitate ale semnăturii/sigiliilor

DECIZIA DE IMPLEMENTAREA (UE) 2015/1506 A COMISIEI a definit specificațiile tehnice și standardele referitoare la formatele și nivelurile de semnături electronice/sigiliile electronice calificate și avansate, pe care fiecare stat membru al Uniunii ar trebui să le susțină (semneze și valideze) și care sunt acceptate de autoritățile publice ale statelor membre, având în vedere interoperabilitatea lor transfrontalieră și nivelul necesar de securitate pentru anumite scopuri comerciale :

- XAdES Profil de bază - ETSI TS 103 171 v.2.1.1 (2012) (sau proiect ETSI EN 319 132 1, 2015);
- CAdES Profil de bază - ETSI TS 103 173 v.2.1.1 (2012) (sau proiect ETSI EN 319 122-1, 2015);
- PAdES Profil de bază - ETSI TS 103 172 v. 2.1.1 (2012) (sau proiectul ETSI EN 319 142-1, 2015).

HOTĂRÂREA (art. 1 și , 3), în conformitate cu Regulamentul 910/2014, aprobă următoarele semnături/sigilii avansate în formatele CMS, XML și PDF la nivelurile de conformitate B, T și LT, care ar trebui recunoscute între Statele membre .

HOTĂRÂREA (Articolele 2 și 4) aprobă condițiile în care se confirmă valabilitatea unei semnături/sigilii electronice avansate :

- (1) certificatul care susține semnătura electronică avansată era valabil la momentul semnării, iar când semnătura electronică avansată este susținută de un certificat calificat, certificatul calificat care susține semnătura electronică avansată era, la momentul semnării, un certificat calificat pt. semnătura electronică care respectă anexa I la Regulamentul (UE) nr. 910/2014 și că a fost emisă de un furnizor de servicii de încredere calificat;
- (2) datele de validare a semnăturii corespund datelor furnizate părții care se bazează;
- (3) setul unic de date care reprezintă semnatarul este furnizat corect părții care se bazează;
- (4) utilizarea oricărui pseudonim este indicată în mod clar părții care se bazează în cazul în care a fost folosit un pseudonim la momentul semnării;
- (5) atunci când semnătura electronică avansată este creată de un dispozitiv calificat de creare a semnăturii electronice, utilizarea oricărui astfel de dispozitiv este indicată în mod clar părții care se bazează;
- (6) integritatea datelor semnate nu a fost compromisă;
- (7) cerințele prevăzute la articolul 36 din Regulamentul (UE) nr. 910/2014 au fost îndeplinite la momentul semnării;
- (8) sistemul utilizat pentru validarea semnăturii electronice avansate oferă părții care se bazează rezultatul corect al procesului de validare și permite părții care se bazează să detecteze orice probleme relevante de securitate.

Serviciul de validare a semnăturii este compatibil cu următoarele profiluri de bază:

XAdES	CADES	PADE	JADES
XAdES-B-B	CAdES-B-B	PAdES-B-B	JAdES-B-B
XAdES-B-T	CAdES-B-T	PAdES-B-T	JAdES-B-T

XAdES-B-LT	CAdES-B-LT	PAdES-B-LT	JAdES-B-LT
XAdES-B-LTA	CAdES-B-LTA	PAdES-B-LTA	JAdES-B-LTA

## 5. Model de validare

### 5.1 Proces de validare

Procesul de validare calificată a QES/ QESeal sau AdES / AdESeal cu un certificat calificat urmează modelul de validare în conformitate cu ETSI EN 319 102-1.

Procesul de validare primește o semnătură electronică/sigiliu electronic și, în conformitate cu Politica de validare (setul de constrângeri), îl validează prin generarea unui indicator de stare și a unui raport de validare interpretat de Utilizator (partea care se bazează) în ceea ce privește aplicabilitatea semnătura/sigiliului.

Pentru validarea unuia dintre formatele de semnătură/sigiliu specificate în secțiunea 4, în cadrul SVA (proces de validare pentru un format/nivel selectat) se execută mai multe subprocese: verificarea formatului, verificarea certificatului calificat, verificarea criptografică etc. indicatorul de stare al fiecărui astfel de proces este **PASSED, FAILED or INDETERMINATE**

Indicatorul de stare furnizat după validarea anumitor format/nivel în conformitate cu ZIPPER de validare Politica este:

- TOTAL-PASSED - verificările tuturor caracteristicilor/parametrilor criptografici ai semnăturii/sigiliului au succes, iar cele în conformitate cu Politica (constrângeri); **Utilizatorul/Partea care se bazează acceptă semnătura/sigiliul ca fiind valabile din punct de vedere tehnic, dar aceasta nu înseamnă că este aplicabilă scopului comercial specific;**
- TOTAL-FAILED - verificările tuturor caracteristicilor/parametrilor criptografici ai semnăturii/sigiliului sunt nereușite sau semnătura/sigiliul a fost creat după revocarea QC, sau formatul nu se potrivea cu unul dintre formatele de referință specificate în secțiunea 4 ; **Utilizatorul/Partea care se bazează acceptă semnătura/sigiliul ca fiind invalidă din punct de vedere tehnic;**
- INDETERMINATE - rezultatele verificărilor individuale/single nu permit evaluarea semnăturii/sigiliului ca TOTAL-PASSED sau TOTAL-FAILED; **acceptarea semnăturii/sigiliului este apanajul Utilizatorului/Parții care se bazează.**

### 5.2 Starea de validare-indicatori și raport de validare

Procesul de validare a semnăturii/sigiliului se încheie cu:

- Indicator de stare de validare (TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE);
- Identificatorul politicii de validare (sau descrierea constrângerilor );
- Data și ora validării și datele de validare (certificat de semnătură/sigiliu ;
- Procesul de validare selectat (conform profilului semnăturii/sigiliului);
- Raport de validare.

SERVICIUL furnizat de QS VA ZIPPER SERVICES implementează modelul procesului de validare, specificat în secțiunea 5.1, aplicabil validării calificate a QES/ QESeal sau AdES / AdESeal cu un certificat calificat în conformitate cu Regulamentul 910/2014, în conformitate cu Practica și Politica Furnizorului pentru acest serviciu.

## 6. SERVICIU

SERVICIUL folosește schimbul de cereri/răspunsuri cu Utilizatorii. Schimbul este securizat prin autentificarea SERVICE (server), iar autentificarea clientului poate fi acceptată . Protocolul de validare corespunde specificației tehnice ETSI EN 119 442 .

În conformitate cu ETSI TS 319 172-1, SERVICIUL realizează procesul de validare în următorii pași:

**Pasul 1** : Utilizatorul (interfața browser sau program) generează și trimite o cerere de validare care conține documentul semnat.

Constrângerile de validare sunt stabilite implicit/imperativ de software-ul SERVICE și procesul de validare le execută conform formatului/profilului semnăturii/sigiliului livrat în cerere.

**Pasul 2** : SERVICIUL efectuează validarea semnăturii/sigiliului; implementarea acestui pas presupune utilizarea unor servicii interne suplimentare de încredere ale Furnizorului sau, dacă este necesar, ale altor furnizori externi.

**Pasul 3** : SERVICIUL generează, pregătește și trimite un raport de validare ca răspuns la o solicitare de validare a semnăturii/sigiliului ; raportul de validare detaliat conține indicatorul de stare (DA/NU) din validarea fiecărei constrângeri și efectele acesteia în funcție de procesul de validare selectat a SERVICIULUI și urmează specificația tehnică ETSI TS 119 102-2 .

Raportul de validare este sigilat/certificat de SERVICIU cu un QESal ( [profil BASELINE\\_LTA](#) ).

Raportul de validare este generat pentru fiecare semnătură/sigiliu a documentului.

**Pasul 4** : Se depune raportul de validare; clientul web transmite/vizualizează raportul de validare în formatul corespunzător care poate fi scos/tipărit. Pe baza raportului de validare, Utilizatorul/Partea care se bazează acceptă sau respinge valabilitatea tehnică a semnăturii/sigiliului .

SERVICIUL realizează următoarele procese de validare, în funcție de profilul semnăturii/sigiliului depus :

- **Procesul de validare pentru semnăturile de bază (-B)** (a se vedea ETSI EN 319 102-1 clauza 5.3): ar trebui aplicat pentru semnături în care momentul validării se află în perioada de valabilitate a certificatului de semnare și certificatul de semnare nu a fost revocat.
- **Procesul de validare pentru semnăturile cu timp (-T) și semnăturile cu material de validare pe termen lung (-LT)** (a se vedea ETSI EN 319 102-1 clauza 5.5). SVA este capabil să utilizeze datele de validare stocate în semnătură pentru validare.
- **Proces de validare pentru semnăturile care oferă disponibilitate pe termen lung și integritatea materialului de validare (-LTA)** (a se vedea ETSI EN 319 102-1 clauza 5.6).

SERVICIUL se încheie cu o indicație de stare după cum urmează:

- **PASSED** - verificările semnăturii criptografice/sigiliului (inclusiv toate valorile hash) au succes, precum și toate verificările împotriva constrângerilor, implicite (directe) către SERVICIUL (în conformitate cu această Politică) ;
- **FAILED** - verificările semnăturii/sigiliului criptografic (inclusiv toate valorile hash) au eșuat sau generarea semnăturii/sigiliului este după revocarea certificatului sau semnătura/sigiliul nu se potrivește cu unul dintre formatele/profilurile acceptabile pentru SERVICIU ;
- **INDETERMINATE** - rezultatul verificării nu permite SERVICIULUI să certifice că semnătura/tipărirea este PASSED sau FAILED .

Indicatorul de stare este însoțit de informații suplimentare conținute în:

- Un raport de sinteză privind procesul de validare (solicitat prin opțiunea „VERIFICARE” a SERVICIULUI);
- Un raport detaliat asupra procesului de validare (solicitat prin opțiunea „VERIFICARE DETALIATĂ” a SERVICIULUI);

Raportul sumar de validare pentru fiecare semnătură/sigiliu validat include:

- Politica de validare (descriere generală) ;
- stare-indicare;
- identificatorul semnăturii;
- Data și ora creării semnăturii/sigiliului;
- Semnătura/formatul sigiliului/profilul validat (adică procesul de validare selectat) ;
- Deținătorul/Creatorul semnăturii/sigiliului;
- Domeniul de aplicare al semnăturii/sigiliului ;
- Informații despre documentul semnat/sigilat (nume, număr de semnături) .

Raportul detaliat include informații complete pentru a verifica toate constrângerile din Politica privind atributele/caracteristicile obiectelor din structura semnăturii/sigiliului (conform formatului/profilului acesteia .

Ambele tipuri de rapoarte de validare sunt furnizate printr-un client web în browserul utilizatorului/parte de încredere în format PDF și format XML. Rapoartele sunt sigilate/certificate cu QESal cu QC ( CAdES -B-LTA) iar formatul XML este semnat separat, sigilat/certificat cu QESal cu QC ( X AdES -B-LTA) al SERVICIULUI care atestă proveniența acestora, datele intacte și momentul sigilării .

## 7. Utilizare

SERVICIUL **nu** validează Utilizatorului/Parții care se întemeiază aplicabilitatea semnăturii/sigiliului validat; validează **doar valabilitatea tehnică a semnăturii/sigiliului**.

Atunci când o semnătură/sigiliu validată cu succes conține identificatorul Politicii de semnătură, Partea care se bazează poate evalua aplicabilitatea semnăturii/sigilii validate la scopul comercial specific după ce s-a familiarizat cu această politică comună și cu Politica de semnare (dacă un astfel de document este disponibil) .

Atunci când semnătura/sigiliul pentru nu include un identificator de Politică de semnătură, Utilizatorul/Partea care se bazează poate evalua aplicabilitatea unei semnături/sigilii validate cu succes în conformitate cu Politica sa de aplicabilitate sau după Politica de certificate indicată.

În practică, aplicabilitatea legală a unei semnături/sigilii validate pentru un anumit scop comercial se află în întregime în prerogativele Utilizatorului/Parții de bază. Formatul și profilul semnăturii validate sunt indicate în raportul de validare, adică funcționalitatea care se realizează cu această semnătură/sigiliu și, în consecință, relevanța acesteia pentru un anumit scop(e) de afaceri.

Regulile privind aplicabilitatea legală a semnăturii electronice/sigiliului în scopuri comerciale sunt în afara domeniului de validare, acestea ar trebui să fie pregătite de Utilizatori/Parțile care se bazează pe semnătura electronică/sigiliul electronic sunt proprietatea acestora. Aceste reguli pot fi documentate sau pregătite pentru verificare automată (de exemplu, pe baza Raportului de validare) după utilizarea SERVICIULUI și înainte de acceptarea finală a semnăturii electronice/sigilii electronice de către Partea care se bazează în scopuri comerciale definite.

SERVICIUL este plătit de către Utilizator/Partea care se bazează în condiții contractuale cu Furnizorul pentru livrarea și utilizarea acestuia.

## 8. Drepturile și Obligațiile Utilizatorilor

### 8.1 Răspunderea Utilizatorului

Răspunderea Utilizatorului este determinată de Contractul de Servicii de încredere și de anexele acestuia (inclusiv termenii și condițiile).

### 8.2 Obligațiile Utilizatorului

Este responsabilitatea Utilizatorului să acționeze în conformitate cu termenii contractuali și cu Politica și Practica Furnizorului atunci când folosește SERVICIUL.

Obligațiile Utilizatorului sunt determinate de termenii și procedurile Practicii pentru Serviciul Calificat, Contractul

de Servicii de Încredere și termenii și condițiile standard ale acestuia, care fac parte integrantă din Politica Generală a Furnizorului.

### 8.3 Drepturile Utilizatorului

Utilizatorii au dreptul de a utiliza SERVICIUL în conformitate cu Politica și Practica Furnizorului pentru validarea calificată a semnăturilor și ștampilelor.

### 8.4 Obligații de verificare a aplicabilității legale a unei semnături/sigilii validate

Conform secțiunii 7 a acestui document.

## 9. Garanție limitată și declinare a răspunderii/Limitarea răspunderii în furnizarea SERVICIULUI.

QCSP ZIPPER SERVICES declară și garantează următoarele:

- cerințele și procedurile operaționale ale SERVICIULUI sunt în conformitate cu Politica și Practica Furnizorilor pentru acesta;
- să valideze doar formatele/profilurile specificate de semnături/sigilii;
- Indicatorii de Stare și Rapoartele de Validare emise de Serviciu corespund stării semnăturii/sigiliului la momentul validării și nu la momentul aplicării/utilizării pentru un anumit scop comercial;
- respectă cerințele de confidențialitate a informațiilor dintr-un document/dosar semnat;
- acceptă disponibilitatea 24x7 a SERVICIULUI;
- Efectuează proceduri de verificare a certificatelor și ștampilelor temporale ale Furnizorilor externi calificați, folosind autoritățile/sursele acestora (CRL/OCSP, TSA, TLB).

ZIPPER SERVICES nu va fi răspunzătoare în cazul:

- indisponibilitatea SERVICIULUI din cauza dezastrelor naturale, războiului, tulburărilor de telecomunicații/energetice etc.;
- Aplicabilitatea ilegală a semnăturilor/sigiliilor validate din punct de vedere tehnic de către SERVICE pentru scopuri comerciale specifice (aplicații).

## 10. Acorduri aplicabile, CPS, CP

Documentul POLITICA DE VALIDARE A SEMNĂTURII ȘI DECLARAȚIA DE PRACTICĂ DE VALIDARE A SEMNĂTURII AL SERVICIULUI DE VALIDARE CALIFICAT ZIPPER FURȚAT DE poate fi găsit în depozitul de documente ZIPPER la <https://pki.ca.ezipper.ro/validation>

În consecință, Acordul pentru abonatul serviciilor de încredere, Termenii și condițiile privind Deținătorii/părțile care se bazează pe SERVICIUL pot fi găsite pe adresa web de mai sus.

## 11. Politica/Declarația de confidențialitate

Angajamentul de a respecta confidențialitatea explică toate aspectele privind prelucrarea datelor cu caracter personal și asigură respectarea tuturor principiilor legate de prelucrare stabilite de legislația în vigoare, în special de Regulamentul (UE) 679/2016 (GDPR), activitățile desfășurate de companie. în calitate de Persoană Autorizată a Operatorului (pentru perioada de executare a contractelor cu clienții săi.

ZIPPER prelucrează datele cu caracter personal în conformitate cu legislația aplicabilă privind protecția datelor în vigoare. Pentru mai multe detalii, vă rugăm să consultați Declarația de confidențialitate ZIPPER

<https://pki.ca.ezipper.ro/repository/compliance.php>

Toate informațiile care au devenit cunoscute în timpul furnizării de servicii și care nu sunt destinate dezvăluirii sunt confidențiale. Abonatul are dreptul de a obține informații de la ZIPPER despre prelucrarea datelor sale cu caracter personal în conformitate cu legislația în vigoare.

ZIPPER are dreptul de a dezvălui informații despre Abonat unei terțe părți care, conform legii relevante sau unei



hotărâri judecătorești, are dreptul să primească astfel de informații. 10.5 ZIPPER poate publica date statistice nepersonalizate despre serviciile sale.

## **12. Politica de rambursare**

ZIPPER se străduiește să ofere cel mai înalt nivel de calitate al serviciilor de încredere pe care le oferă și le oferă. ZIPPER depune eforturi pentru a asigura cel mai înalt nivel de calitate al serviciilor sale. Cu toate acestea, Abonatul are dreptul de a se retrage din contractul de cumpărare din orice motiv, în cazul în care achiziția Serviciului de Validare se efectuează prin internet sau prin telefon a Abonatului.

Exercitarea acestui drept se va face în scris de către Abonatul la ZIPPER, prin trimiterea unui email la suport.pki@ezipper.ro în termen de 14 zile de la data cumpărării.

Sub rezerva secțiunii anterioare, ZIPPER poate gestiona rambursări de la caz la caz.

## **13. Legea aplicabilă, plângeri și soluționare a litigiilor**

Orice litigii legate de serviciile de încredere furnizate în baza acestor termeni vor fi guvernate în toate privințele și interpretate în conformitate cu legile din România.

În măsura permisă de lege, părțile vor căuta inițial să soluționeze orice litigiu pe cale amiabilă, iar dacă litigiul nu este soluționat în termen de treizeci (30) de zile de la cererea inițială, Tribunalele din București, România vor avea competență exclusivă să judece și să soluționeze. aceasta.

Orice solicitări sau revendicări pentru dispute trebuie trimise la informațiile de contact furnizate în acești Termeni și condiții.

## **14. Evaluări de conformitate, mărci de încredere/logo-uri și audit**

Audituri de verificare a conformității cu prevederile procedurale și legale, în special conformitatea documentului POLITICA DE VALIDARE A SEMNĂTURII ȘI DECLARAȚIA PRACTICĂ DE VALIDARE A SEMNĂTURII A SERVICIULUI DE VALIDARE CALIFICAT ZIPPER PRESTATAT DE ZIPPER SERVICES sunt efectuate la fiecare 24 de luni de către o Autoritate de Evaluare a Conformității, în baza art. 20 din REGULAMENTUL 910/2014 UE ( eIDAS ).

## **15. Puncte de înregistrare și verificare a identității**

ZIPPER înregistrează și încheie Acorduri de servicii de încredere. Mai multe informații despre acordurile de servicii de încredere pot fi găsite la adresa de web: <https://pki.ca.ezipper.ro/>