



certSIGN

eIDAS 2.0 Provocări și confirmări

Constantin Burdun | Deputy CEO certSIGN



eIDAS 2.0

- Comisia Europeană a propus o nouă versiune a Regulamentului 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.
- În prezent este în dezbatere la nivelul Parlamentului European.
- eIDAS 2.0 vine cu o serie de provocări, prin faptul că vine cu noi concept și servicii de încredere necesare pentru dezvoltarea unui mediu digital de încredere.
- Dar, în același timp, eIDAS 2.0 vine și cu confirmări a direcțiilor fundamentale stabilite la nivelul Regulamentului 910 în vigoare în prezent, unele dintre aceste direcții fiind, din păcate interpretate greșit la nivel național.



Portofel european de identitate digitală (European Digital Identity Wallet - DIW)

- eIDAS 2.0 impune statelor membre, la articolul 6 a, să elibereze un **portofel european de identitate digital** (European Digital Identity Wallet - DIW) în cadrul unui sistem eID notificat conform unor standarde tehnice comune și în urma evaluării obligatorii a conformității și a certificării voluntare într-un cadru european de certificare a securității cibernetice, astfel cum este stabilit prin Directiva privind securitatea cibernetică (Directiva NIS 2)
- Statele Membre au termen de **un an** pentru a implementa cel puțin un sistem pentru emiterea portofelului european de identitate.
- Un astfel de sistem poate fi pus la dispoziție și de o **entitate privată**, nu numai de o organizație publică dintr-un stat Membru (art.6 a, 2.c).

IDENTITY

Portofel european de identitate digitală (European Digital Identity Wallet - DIW)

- Rolul portofelului european de identitate digitală este să asigure că persoanele fizice și juridice vor avea posibilitatea:
 - ✓ să solicite și să obțină în siguranță,
 - ✓ să stocheze,
 - ✓ să combine și
 - ✓ să utilizeze
- datele lor de identificare și atestări electronice ale atributelor lor pentru:
 - ✓ a le permite **accesul la servicii publice și private online sub controlul exclusiv utilizatorului**
 - ✓ a facilita cetățenilor semnarea utilizând semnătura electronică calificată.



Mijloacele de identificare electronică

- În scopul punerii la dispoziție a mai multor mijloace de identificare electronică disponibile pentru utilizarea transfrontalieră și îmbunătățirii eficienței procesului de recunoaștere reciprocă a sistemelor de identificare electronică notificate, **notificarea a cel puțin unui sistem de identificare electronică de către statele membre devine obligatorie la articolul 7 (în maxim un an de la data intrării în vigoare).**
- În plus, se adaugă dispoziții pentru **a facilita** și pentru **a asigura identificarea unică și persistentă a persoanelor fizice la nivel european** la articolul 11a. Aceasta se referă la cazuri în care legea impune identificarea, cum ar fi în domeniul sănătății, în domeniul finanțelor pentru a îndeplini obligațiile de combatere a spălării banilor sau pentru uz judiciar.
- În acest scop, statelor membre li se va solicita să includă un identificator unic și persistent în setul minim de date de identificare a persoanei.
- Posibilitatea statelor membre de a se baza pe **certificarea mijloacelor de identificare electronică pentru a asigura conformitatea cu regulamentul**, înlocuindu-se astfel procesul de evaluare de tip “peer review” (cum este în versiunea în vigoare a Regulamentului), îmbunătățește eficiența recunoașterii reciproce.

Acceptarea portofelului de identitate digitală

- Secțiunea 3 a eIDAS2.0 prezintă noi dispoziții privind dependența transfrontalieră de portofelul european de identitate digitală pentru a se asigura că utilizatorii se pot baza pe utilizarea portofelelor europene de identitate digitală pentru a accesa serviciile online furnizate de organismele din sectorul public și de furnizorii de servicii privați care necesită autentificarea utilizatorului.
- Astfel furnizorii publici de servicii online care necesită un mijloc de autentificare pentru acces trebuie să accepte și DIW.
- La fel, furnizorii de servicii electronice privați din domeniile transport, energie, bancar și servicii financiare, securitate socială, sănătate, apă potabilă, servicii poștale, infrastructuri digitale, educație și telecomunicații, care necesită autentificare puternică pentru access, trebuie să accepte și DIW, dacă posesorul dorește să îl folosească.
- Platformele online mari (definite în DSA) trebuie să accepte și identificarea și autentificarea electronică cu DIW, bineînțeles, dacă posesorul dorește acest lucru.



Identificarea de la distanță echivalentă cu prezența fizică

- În ceea ce privește cerințele aplicabile serviciilor de încredere, inclusiv furnizorii de servicii de încredere calificați, articolele 17, 18, 20, 21 și 24 sunt modificate pentru a se alinia la normele aplicabile securității rețelelor și informațiilor în UE (Directiva NIS2.0).
- În legătură cu metodele care trebuie utilizate de furnizorii de servicii de încredere calificați pentru a verifica identitatea persoanelor fizice sau juridice cărora li se eliberează certificatele calificate, dispozițiile privind utilizarea mijloacelor de identificare la distanță au fost armonizate și clarificate pentru ca să se asigure că aceleași reguli sunt aplicate în întreaga UE.
- **Astfel, echivalența cu prezența fizică a unui mijloc de identificare la distanță (identificarea video) nu mai trebuie să fie reglementat la nivel național, va fi reglementat prin Regulament, inclusiv din punct de vedere tehnic, iar echivalența cu prezența fizică se va certifica de către un auditor care trebuie să îndeplinească cerințele specificate de Regulament.**



Semnătura electronică la distanță. Autentificarea serverelor Web

- Capitolul III prezintă un nou articol 29a pentru a defini cerințele pentru un **serviciu calificat pentru gestionarea dispozitivelor de creare a semnăturilor electronice la distanță, pentru a exista cerințe armonizate la nivel European.**
- Pentru a se asigura că utilizatorii pot identifica cine se află în spatele unui site web, articolul 45 este modificat pentru a solicita furnizorilor de browsere web (Mozilla, Firefox, Safari etc.) **să faciliteze utilizarea certificatelor calificate pentru autentificarea site-ului web.**



Atestările electronice de atribute

- Noua secțiune 9 introduce dispoziții privind efectele juridice ale atestărilor electronice de atribute, utilizarea acestora în sectoare definite și cerințele pentru atestări calificate de atribute.
- Pentru a asigura un nivel ridicat de încredere, la articolul 45d este introdusă o prevedere privind verificarea atributelor pe bază de surse autentice (de încredere).
- Astfel, se prevede că, pentru o listă minimă de atribute (prevăzute în Anexa VI), ale căror sursă sunt instituții de stat, acele instituții de stat sunt obligate să permită prestatorilor de servicii de atestare de atribute să poată verifica aceste atribute.
- De asemenea, **prestarea de servicii de atestare ale atributelor nu poate fi făcută de entitatea care gestionează direct datele aferente acestor atribute (Art.45 f.4).**



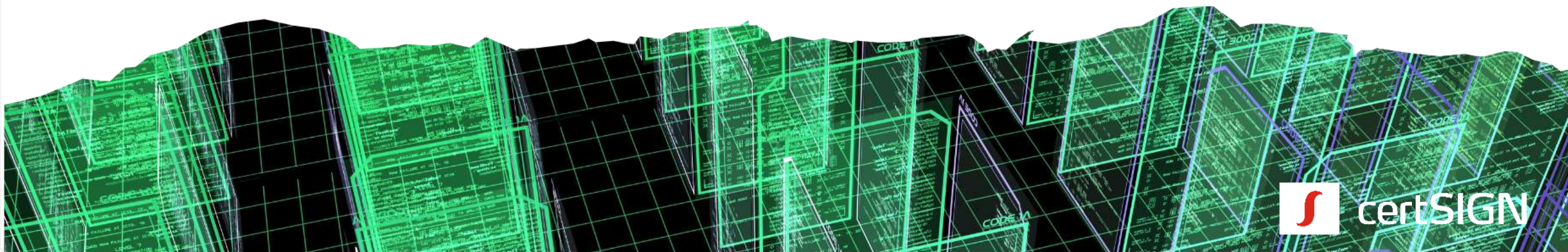
Lista minimă a atributelor (Anexa VI)

1. adresa
2. vârsta
3. genul
4. starea civilă
5. componența familiei
6. cetățenia
7. calificări educaționale, titluri și licențe
8. calificări profesionale, titluri și licențe
9. autorizații publice și licențe
10. date financiare și date privind societatea comercială.



Serviciul calificat de arhivare electronică. Serviciul calificat de registre electronice

- Noua secțiune 10 permite furnizarea de servicii calificate de arhivare electronică la nivelul UE
- Articolul 45g privind serviciile de arhivare electronică calificate completează articolele 34 și 40 privind serviciile calificate de prezervare pe termen lung pentru semnături electronice calificate și sigilii electronice calificate
- Noua secțiune 11 stabilește un cadru pentru serviciile de încredere în ceea ce privește crearea și întreținerea registrelor electronice (electronic ledger) și a registrelor electronice calificate
- Un registru electronic combină marcarea temporală a datelor și secvențierea acestora cu certitudine, similar cu semnarea electronică, cu avantajul suplimentar de a permite o guvernare mai descentralizată, care este potrivită în cazul cooperării mai multor părți (tehnologia din spate este de fapt blockchain)
- Registrele electronice ajută companiile să economisească costuri, făcând coordonarea diverselor părți mai eficientă, mai sigură și facilitează supravegherea reglementară



Serviciul calificat de registre electronice

- Registrele electronice ajută companiile să economisească costuri, făcând coordonarea diverselor părți mai eficientă, mai sigură și facilitează supravegherea reglementară.
- În cazul în care registrele electronice sunt utilizate pentru a sprijini emiterea și / sau tranzacționarea de obligațiuni sau pentru activele criptografice, cazurile de utilizare ar trebui să fie compatibile cu toate regulile financiare aplicabile, de exemplu cu Directiva privind piețele din instrumentele financiare, Directiva privind serviciile de plată și cu viitoarele piețe din Regulamentul privind activele criptografice.
- **În absența unei reglementări europene, există riscul ca legislatorii naționali să stabilească standarde naționale divergente.**
- **Pentru a preveni fragmentarea, este necesar să se definească un cadru paneuropean unic care să permită recunoașterea transfrontalieră a serviciilor de încredere care susțin funcționarea registrelor electronice.**
- **Acest standard paneuropean pentru operatorii de noduri (de blockchain) se va aplica fără a aduce atingere altor legislații secundare ale UE.**



Concluzii

- Proiectul eIDAS 2.0 continuă demersurile actualului Regulament de a stabili reguli comune pentru toate statele membre, în vederea dezvoltării unui mediu digital sigur și de încredere.
- **Cuvintele cheie sunt armonizarea, facilitarea, clarificarea, prevenirea fragmentării la nivelul statelor membre.**
- Un alt aspect important care se evidențiază și subliniază o dată în plus și prin intermediul eIDAS 2.0 este faptul că **atât portofelele europene de identitate digitală, cât și mijloacele de identificare electronică pot fi emise atât de organisme publice, cât și entități private iar la nivelul fiecărui stat membru pot exista în același timp mai multe soluții disponibile cetățenilor.**
- În prezent, sunt multe state membre care deja au notificat mai multe mijloace de identificare electronică emise atât de organisme publice, cât și de entități private.



Concluzii

- Conform precizărilor Memorandumului explicativ care însoțește draftul noii forme a Regulamentului 910/2014, deși serviciile de încredere sunt clar reglementate, există practici naționale distincte care aduc un risc mare de fragmentare a pieței digitale europene.
- Din păcate, astfel de practici, interpretări “originale” ale prevederilor Regulamentului eIDAS, există și în România pentru anumite spețe.
- De aceea, o practică uniformă la nivelul tuturor statelor membre va consolida piața unică, permițând cetățenilor, altor rezidenți și întreprinderilor să se bazeze pe un ecosistem îmbunătățit pentru servicii de încredere și de identitate electronică recunoscute și acceptate peste tot în Uniunea Europeană.
- Faptul că unul dintre cele două obiective ale portofelului european de identitate digitală este de **a facilita cetățenilor să semneze electronic utilizând semnătura calificată (Art. 6a, punctul 3)**, confirmă, fără echivoc, că utilizarea la scară largă a semnăturilor electronice calificate a fost, încă de la început, obiectivul central al Regulamentului eIDAS și în niciun caz încurajarea altor abordări, păguboase și nesusținute cu argumente tehnice, de concentrare a efortului în dezvoltarea de alternative la semnătura calificată.

Mulțumesc!

Constantin Burdun

Deputy CEO certSIGN