Journal of Social Sciences *Vol. III, no. 4 (2020), pp. 62 - 72*
Fascicle *Social Science* *ISSN 2587-3490*
Topic *Marketing and Logistics* *eISSN 2587-3504*

DOI: 10.5281/zenodo.4296327
CZU 004:003.26 (478)

DIGITAL SIGNATURE: ADVANTAGES, CHALLENGES AND STRATEGIES

Dinu Țurcanu*, ORCID: 0000-0001-5540-4246,
Serghei Popovici, ORCID: 0000-0002-4302-6003,
Tatiana Țurcanu, ORCID: 0000-0002-8972-8262

Technical University of Moldova, 168, Stefan cel Mare Bd, Chisinau, Republic of Moldova
*Corresponding author: Dinu Țurcanu, *dinu.turcanu@adm.utm.md*

Received: 09. 28. 2020
Accepted: 11. 02. 2020

Abstract. Digital signature solutions are rapidly replacing classic signatures and have the potential to dominate signature-related processes. The concept of a digital signature is based on the transition from paper to electronic documentation and the automation of workflow systems, by reducing the processing time of documents. The digital signature offers the possibility to identify a person who has signed an electronic document. The main benefits of this technology include increased efficiency, lower costs, and increased customer satisfaction. Digital signatures must be clearly distinguished from ordinary authentication processes. While authentication is only used to verify the identity of end-users, digital signatures also ensure data integrity. The paper analyzed the importance and main arguments, challenges, and strategies for the implementation of the digital signature, as well as the role of the Information Technology and Cyber Security Service-STISC in the implementation of the digital signature in the Republic of Moldova.

Keywords: *digital signature, e-government, information technology, cybersecurity, STISC.*

Rezumat. Soluțiile de semnături digitale înlocuiesc rapid semnăturile clasice și au potențialul de a domina procesele legate de semnături. Conceptul de semnătură digitală se bazează pe trecerea de la hârtie la documentația electronică și automatizarea sistemelor de flux de lucru prin reducerea timpului de procesare a documentelor. Semnătura digitală oferă posibilitatea de a identifica o persoană care a semnat un document electronic. Principalele beneficii ale acestei tehnologii includ o eficiență sporită, costuri mai mici și o satisfacție sporită a clienților. Semnăturile digitale trebuie să fie clar distinse de procesele obișnuite de autentificare. În timp ce autentificarea este utilizată doar pentru a verifica identitatea utilizatorilor finali, semnăturile digitale asigură, de asemenea, integritatea datelor. În lucrare s-a analizat importanța și principalele argumente, provocări și strategii privind implementarea semnăturii digitale, precum și rolul Serviciului Tehnologia Informației și Securitate Cibernetică – STISC – în implementarea semnăturii digitale în Republica Moldova.

Cuvinte-cheie: *semnătură digitală, e-guvernare, tehnologii informaționale, securitate cibernetică, STISC.*

Introducere

În ultimii ani, asistam la o transformare importantă în paradigmele competitive ale companiilor, în principal datorită pauzei digitale care a atras multe companii spre succes și altele spre o spirală descendentă. Lumea a trebuit să se confrunte cu o schimbare culturală inexorabilă și continuă fundamentală pentru a răspunde nevoilor pieței și consumatorilor. O transformare similară a determinat adoptarea de noi sisteme de guvernanță, metode de proiectare și modele de achiziții, cu abordări din ce în ce mai agile și deschise.

Apariția e-guvernării și a serviciilor electronice a schimbat modul în care agențiile de stat și birourile guvernamentale locale își desfășoară activitatea. E-guvernarea sau guvernarea digitală definește generic utilizarea noilor tehnologii de comunicare și a aplicațiilor informatice de către administrația publică centrală și locală în scopul eficientizării activității aparatului administrativ și a creșterii calității serviciilor publice [1].

Ca rezultat, sistemele și procesele electronice au devenit la fel de importante ca hârtia și cerneala tradiționale. Într-un mediu de hârtie, o semnătură manuală, cunoscută și sub numele de „semnătură umedă", autorizează și autentifică conținutul unui document. O semnătură oferă un nivel de încredere și responsabilitate care ajută la desfășurarea activității. Semnăturile electronice extind funcția semnăturilor scrise de mână la documentele electronice, oferind o modalitate pentru ca două părți să-și desfășoare activitatea cu încredere într-un mediu electronic. Tehnologiile și procedurile actualizate trebuie să răspundă cererii de încredere în cazul în care semnăturile manuale nu sunt viabile. Deoarece semnăturile își obțin importanța primară din valoarea lor juridică și probatorie, aceste preocupări trebuie să conducă la selectarea tehnologiilor de semnătură electronică. În consecință, fiecare agenție va trebui să-și definească nevoile legale și probatorii în legătură cu procesele sale de afaceri înainte de a alege o cerere de semnătură electronică. În plus, aplicația de semnătură digitală selectată trebuie să se potrivească arhitecturii tehnologice a agenției pentru a crea, păstra și pune la dispoziție înregistrările sale [2].

Semnăturile digitale au fost introduse pentru a înlocui complet semnăturile tradiționale și, ca urmare, pentru a elimina hârtia din procesele de zi cu zi, cum ar fi semnarea contractelor, integrarea clienților noi sau înregistrarea legală a consimțământului și aprobării. Motivul final pentru care companiile integrează semnăturile digitale este de a putea efectua orice tip de tranzacție comercială oriunde, oricând pe orice dispozitiv [3].

Semnătura digitală electronică (Electronic Digital Signature - EDS) este un software criptografic necesar pentru rezolvarea următoarelor sarcini:

- analiza documentului și verificarea integrității acestuia;
- ascunderea datelor confidențiale și a sistemelor de dezvoltare;
- inițializarea autorului și schimbului de informații.

Conceptul de EDS se bazează pe trecerea de la hârtie la documentația electronică și automatizarea sistemelor de flux de lucru, prin reducerea timpului de procesare a documentelor. După cum s-a menționat, EDS oferă posibilitatea de a identifica o persoană care a semnat un document electronic. Se poate spune că EDS este un analog atât al unei semnături scrise de mână, cât și al unui document semnat pe hârtie. De asemenea, este demn de remarcat faptul că o astfel de semnătură are propriul cadru de reglementare ce guvernează utilizarea semnăturilor digitale în organismele de guvernare de stat, în municipalități și în mâinile proprietarilor de afaceri private [4].

1. Din istoria semnăturii digitale

Chiar dacă se creează impresia falsă că tehnologia semnăturii digitale este un trend nou, netestat, totuși, este important a ști că semnăturile digitale există de zeci de ani și câștigă popularitate în mainstream. Cele mai importante etape din istoria tehnologiei semnăturilor digitale sunt:

- 1976: Whitfield Diffie și Martin Hellman au descris pentru prima dată ideea unei scheme de semnături digitale, dar au teorizat doar că astfel de scheme existau;
- 1977: Ronald Rivest, Adi Shamir și Len Adleman au inventat algoritmul RSA, care ar putea fi folosit pentru a produce un fel de semnătură digitală primitivă;
- În 1984: Shafi Goldwasser, Silvio Micali și Ronald Rivest au devenit primii care au definit riguros cerințele de securitate ale schemelor de semnături digitale;
- 1988: Lotus Notes 1.0, care a folosit algoritmul RSA, a elaborat primul pachet software comercializat pe scară largă care oferă semnături digitale;
- 1089: a fost lansat primul pachet software Lotus Notes 1.0. comercializat pe scară largă care a oferit semnătura digitală. S-a bazat pe algoritmul RSA. Semnăturile Lamport, semnăturile Merkle și semnăturile Rabin sunt câteva alte scheme de semnături digitale dezvoltate în curând după RSA;
- 1999: Capacitatea de a încorpora semnături digitale în documente este adăugată în format PDF;
- 2000: Legea ESIGN - act care face semnăturile digitale obligatorii din punct de vedere juridic;
- 2002: SIGNiX este fondat și devine cel mai utilizat software de semnătură digitală bazat pe cloud;
- 2008: Semnăturile digitale recunoscute ca fiind cea mai sigură modalitate de a obține documente semnate online;
- Formatul de fișier PDF devine un standard deschis pentru Organizația Internațională pentru Standardizare (ISO) ca ISO 32000. Include semnături digitale ca parte integrantă a formatului [5, 6, 7].

2. Semnătura digitală și problemele culturale

Se considera că semnăturile tradiționale nu vor fi complet înlocuite cu semnături digitale, dat fiind limitările semnăturilor digitale.

Aceste limitări includ, de exemplu, probleme de păstrare de lungă durată în ceea ce privește deteriorarea suportului de stocare asociat, perimarea formatului de date și evoluția algoritmilor criptografici, a standardelor conexe și validarea certificatelor.

Se susținea, de asemenea, că semnăturile digitale nu vor fi utilizate niciodată în evenimente ceremoniale sau istorice, deși acest lucru poate fi acceptat.

Conform altor surse, semnăturile digitale nu reușesc să îndeplinească așteptările mari pentru succesul lor, datorită defectului simplu că trec cu vederea factorii culturali. Înainte ca semnăturile digitale să poată prevala, trebuie să fie încorporat un sentiment adecvat de cultură în semnăturile digitale în ceea ce privește acceptarea utilizatorilor, stabilitatea și fiabilitatea pe termen lung.

Cultura sigiliilor din Japonia este considerată ca potrivită pentru implementarea semnăturilor digitale, deoarece conceptul de certificate sigiliu și certificate electronice sunt comparabile [8].

3. Scopul și utilizarea EDS

O semnătură digitală electronică îndeplinește următoarele funcții:

➲ asigurarea integrității documentului. Dacă în timpul transferului unui document electronic acesta este modificat, corectat, semnătura electronică devine automat invalidă. Acest lucru se datorează faptului că semnătura digitală se formează pe baza primei versiuni a documentului semnat;

➲ confirmarea corectă a autorului. Într-un document semnat prin semnătură digitală electronică, autorul nu poate fi schimbat. Imediat se creează un EDS, se generează o cheie privată, care este numai a autorului. Prin urmare, prezența unei semnături digitale sub document garantează identitatea proprietarului semnăturii;

➲ furnizarea de probe. Pentru a confirma disponibilitatea unei semnături digitale funcționale, autorul trebuie doar să furnizeze cheile publice și private pe care le primește în momentul creării semnăturii digitale electronice [9].

Astfel, se poate concluziona că semnătura digitală asigură un grad ridicat de protecție a datelor, ceea ce este extrem de important în realitățile moderne ale spionajului digital și existența diferitelor metode de interceptare a datelor. Prin urmare, astfel de semnături sunt deja utilizate în sistemele bancare, achizițiile publice, la înregistrarea imobilelor, în sistemul judiciar, în sistemele de tranzacționare, declarațiile vamale etc. Cu toate acestea, nu se poate să nu menționăm o caracteristică importantă - documentele cu semnătură electronică au forță juridică și sunt recunoscute ca echivalente cu documentele pe hârtie numai atunci când sunt protejate de un cadru legislativ sau sunt documentate prin acordul părților [10].

4. Autenticitatea, integritatea și nivelul de securitate

Soluțiile de semnături digitale înlocuiesc rapid semnăturile pe hârtie și au potențialul de a domina procesele legate de semnături. Principalele beneficii ale acestei tehnologii includ o eficiență sporită, costuri mai mici și o satisfacție mai mare a clienților. Semnăturile digitale trebuie să fie clar distinse de procesele obișnuite de autentificare. În timp ce autentificarea este utilizată doar pentru a verifica identitatea utilizatorilor finali, semnăturile digitale asigură, de asemenea, integritatea datelor. O combinație a acestor doi factori de securitate este esențială pentru multe tranzacții comerciale, în special pentru cele care implică date sensibile și confidențiale. Semnăturile digitale sunt o subcategorie de semnături electronice. În timp ce o semnătură electronică poate fi orice fel de date atașate unui document, cum ar fi un nume scris sub un e-mail, o semnătură digitală se bazează pe un proces matematic de protecție a documentului. Există două tipuri majore de semnături digitale, diferențiate doar de cât de sigur a fost procesată autentificarea:

- Semnătura digitală calificată (SDQ) este o semnătură creată cu un dispozitiv sigur de creare a semnăturii, altul decât dispozitivul pe care documentul este de fapt semnat, care oferă o securitate foarte ridicată;
- Semnătura digitală avansată (SDA) este o semnătură digitală în care semnătura ar putea fi creată pe același dispozitiv pe care este semnat documentul, care este ceva mai puțin sigur decât SDQ.

Semnătura digitală implică trei procese: procesul de semnare, procesul de autentificare și procesul de asigurare a integrității datelor. Procesul de creare a unei semnături digitale este același, indiferent dacă este administrat intern sau extern. Procesul de semnare începe prin furnizarea unui utilizator final a unui document care trebuie

semnat. Pentru a fi sigur că persoana semnează corect contractul, identitatea utilizatorului final este verificată prin autentificare multiplă, cum ar fi un cod PIN, o parolă și coduri de jetoane bazate pe secvențe. Odată ce identitatea este verificată, semnatarul primește un certificat care îi demonstrează identitatea și îi furnizează o pereche de chei: o cheie privată (cunoscută doar de semnatar) și o cheie publică (cunoscută publicului). Aceste chei sunt necesare pentru a semna un document și pentru a verifica identitatea semnatarului. După eliberarea certificatului, din document se creează un cod matematic unic. Acest cod matematic este apoi criptat cu cheia privată (semnare) și poate fi decriptat numai cu cheia publică corespunzătoare (verificarea semnăturii). Documentul, împreună cu codul matematic criptat, este apoi trimis destinatarului [11].

➲ Pentru a asigura autenticitatea, destinatarul cu acces către cheia publică poate decripta codul matematic și, prin urmare, este capabil să asigure autenticitatea. Cheia publică funcționează pentru decriptare numai dacă documentul a fost semnat cu cheia privată corespunzătoare, confirmând deja identitatea semnatarului.

➲ Integritatea datelor este asigurată printr-un cod matematic, care este vizibil pentru receptor după decriptare. Pentru a verifica dacă documentul nu a fost modificat de orice persoană neautorizată, receptorul își calculează propriul cod matematic din document. Dacă ambele coduri se potrivesc, integritatea datelor este asigurată. Dacă documentul ar fi schimbat în tranziție, calculatorul receptorului ar da un cod diferit.

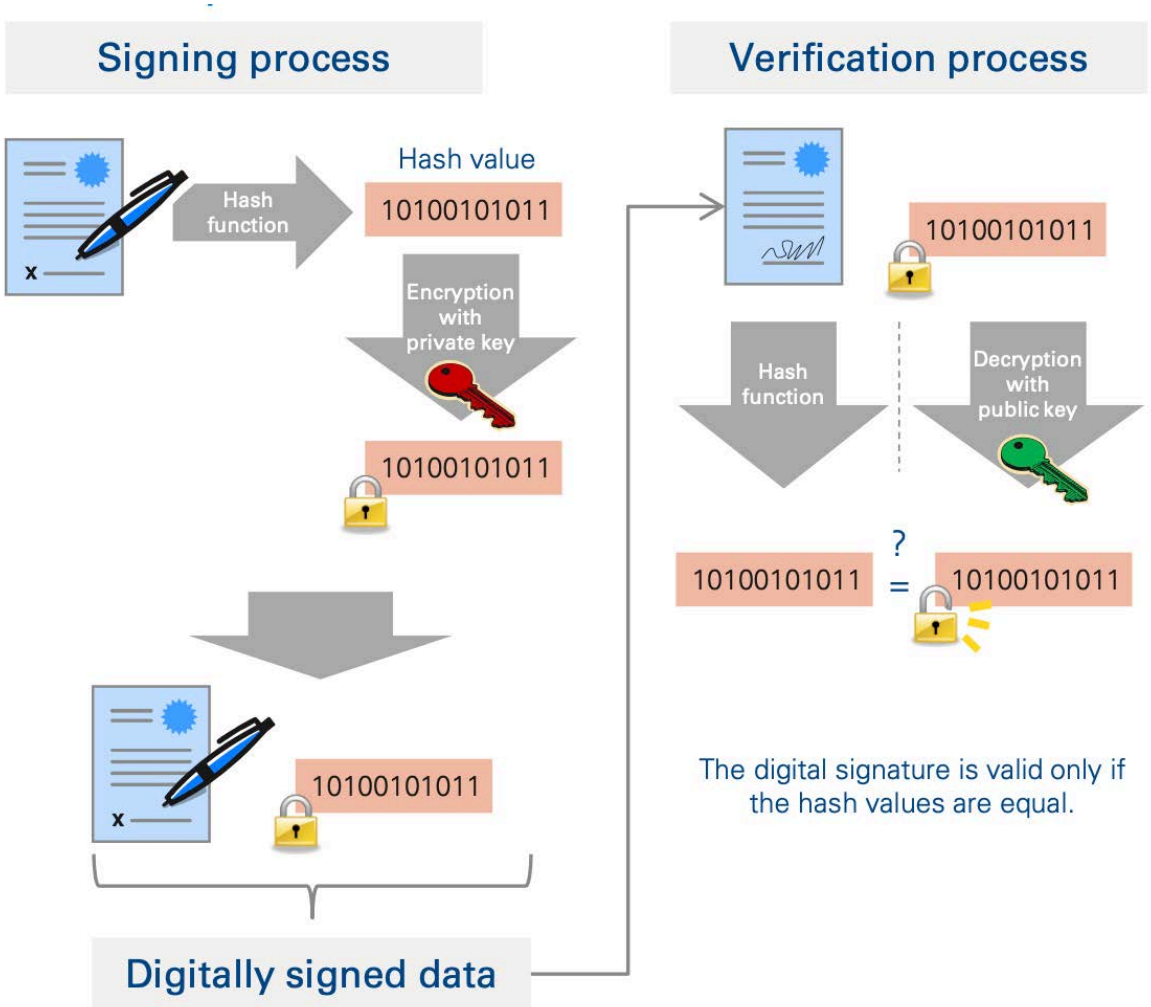

Figura 1. Procesele de semnare și verificare a semnăturii digitale.
Sursa: [12].

5. Avantajele semnăturii digitale

Semnăturile digitale pot fi implementate într-o varietate de domenii, deoarece companiile pot utiliza semnături digitale pentru procesele lor interne sau pentru comunicarea cu partenerii de afaceri și clienții. Guvernele sunt, de asemenea, o categorie importantă de clienți pentru această tehnologie, întrucât li se cere din ce în ce mai mult să implementeze procese mai noi care reduc costurile. Multe companii și guverne au realizat deja potențialul acestei tehnologii.

Un proces complet digital de semnare și trimitere a documentelor reduce orele de lucru și costurile pentru hârtie și transport. Studiile și analizele ulterioare au confirmat că adoptarea imediată a tehnologiei are potențialul de a crea un avantaj competitiv durabil, independent de industria în care operează o companie [12].

Principalul argument pentru adoptarea tehnologiei este îmbunătățirea eficienței, ceea ce conduce la reducerea costurilor și creșterea afacerii prin reducerea cheltuielilor de procesare, cum ar fi scanarea, înregistrarea, arhivarea, tipărirea și trimiterea prin poștă etc.

Procesele de afaceri sunt, de asemenea, mai eficiente prin creșterea agilității generale a întreprinderilor (cicluri reduse de proces, viteza de închidere a activității) și prin urmărirea în timp real și coordonarea afacerii.

Pe lângă considerațiile privind eficiența, adoptarea soluțiilor de semnătură digitală reprezintă o imagine progresivă atât a utilizatorului, cât și a furnizorului de astfel de tehnologii. De asemenea, soluțiile de semnături digitale au potențialul de a spori confortul clienților. De exemplu, o bancă poate oferi clienților săi soluții multicanal pentru a semna un contract de împrumut. Semnăturile digitale oferă un nivel mai ridicat de securitate decât metodele tradiționale de trimitere a documentelor, atunci când sunt implementate corespunzător cu proceduri criptografice cu certificate calificate:

- Integritatea datelor poate fi asigurată, deoarece contrafacerea este practic imposibilă, în timp ce un document pe hârtie poate fi modificat după ce a fost semnat de o persoană neautorizată;
- Probabilitatea de a pierde o copie digitală este mult mai mică în comparație cu documentele pe hârtie;
- Toate tipurile de date, cum ar fi fotografiile sau fișierele audio, pot fi semnate digital, ceea ce protejează drepturile de autor asupra acestor materiale;
- O semnătură de timp poate fi atașată la semnătura digitală, asigurându-se că documentul a fost semnat la o anumită dată.

Fluxul de lucru al semnăturii digitale este centrul transformării care a început deja, care, odată cu remotizarea ultimelor luni, s-a deplasat și mai mult în centrul afacerilor din diferite sectoare.

Semnătura digitală, ca un anumit tip de semnătură calificată, garantează identitatea autorului, integritatea și imuabilitatea documentelor pe care este aplicată.

Modul de semnătură digitală bazat pe utilizarea serviciilor telematice la distanță, care nu implică utilizarea de dispozitive precum carduri inteligente sau chei, garantează același grad de securitate și aceleași efecte juridice ca și semnătura digitală tradițională, dar ultima oferă mai multe avantaje specifice: de exemplu, nu necesită instalarea de hardware sau software dedicat și permite generarea semnături digitale în orice moment și în orice loc, chiar și de pe mobil [13].

6. STISC – instituție publică în domeniul tehnologiilor informaționale

Pe măsură ce soluțiile de semnătură digitală devin mai acceptate pe scară largă, furnizorii de software încearcă să asigure cota de piață prin a se distinge de concurenții lor. Acestea fac lucrul respectiv, concentrându-se pe un aspect specific al procesului de semnare digitală. Unii furnizori oferă o experiență multicanal și aplicații pentru smartphon și tabletă pentru semnarea digitală. Alții sunt mai preocupați de crearea unei experiențe de utilizare intuitivă pentru utilizatorii lor. În timp ce alți furnizori au ales să iasă în evidență prin respectarea standardelor stricte de securitate.

Instituţia publică „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” (STISC) este o instituţie publică creată în temeiul Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, ca urmare a reorganizării prin transformare a Întreprinderii de Stat „Centrul de Telecomunicaţii Speciale” și absorbției Întreprinderii de Stat „Centrul Informaţional Agricol”. Statutul acesteia a fost aprobat prin Hotărârea Guvernului nr. 414/2018.

STISC are drept scop asigurarea administrării, menţinerii şi dezvoltării infrastructurii de tehnologie a informaţiei, sistemului de telecomunicaţii a autorităţilor administraţiei publice, precum şi implementarea politicii statului în domeniul securităţii cibernetice. Domeniile de competenţă ale STISC sunt:

- administrarea infrastructurii de tehnologie a informaţiei şi a Sistemului de telecomunicaţii al autorităţilor administraţiei publice ca parte a reţelei de comunicaţii speciale;
- administrarea şi menţinerea sistemelor informaţionale de stat;
- securitatea cibernetică;
- gestionarea infrastructurii unice a cheii publice (PKI) a Guvernului;
- implementarea tehnologiilor informaționale în sectorul public.

În calitate de operator al sistemului informaţional de telecomunicaţii al Guvernului, STISC coordonează şi exercită controlul asupra funcţionării şi asigurării securităţii sistemelor informaţionale şi de telecomunicaţii ale autorităţilor administraţiei publice [14].

STISC și infrastructura unică a cheii publice. STISC gestionează infrastructura unică a cheii publice (PKI) a Guvernului (Centrul unic de certificare al Guvernului), conform Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat.

Pe măsură ce facilităţile tehnologiei informaţiei, comunicaţiilor şi a serviciilor informaţionale performante din prezent evoluează, creşterea bunăstării populaţiei este inevitabilă. Accesul extins la rețeaua de internet și capacitatea solicitării serviciilor online au favorizat considerabil utilizarea documentelor electronice, astfel încât în ultimii ani, semnătura electronică a devenit un instrument indispensabil în activitățile cotidiene, inclusiv în Republica Moldova.

Sporirea accesibilității semnăturii electronice și creșterea continuă de tranzacții face să înțelegem că urmăm o cale de dezvoltare în sfera tehnologiilor informaționale și că exercitarea atribuțiilor de operator tehnico-tehnologic al serviciilor electronice guvernamentale sunt o prioritate. Întrucât Serviciul Tehnologia Informației și Securitate Cibernetică gestionează infrastructura unică a cheii publice a Guvernului (Centrul unic de certificare al Guvernului), acesta își asumă pe deplin toate obligațiunile și responsabilitățile

cuvenite în domeniul protecţiei criptografice şi tehnice a informaţiei. Centrul unic de certificare al Guvernului din cadrul STISC prestează servicii de certificare a cheilor publice autorităților administrației publice, persoanelor juridice și fizice cu diverse forme de activitate. Facilitățile pe care le oferă semnătura electronică au condus la creșterea numărului de tranzacții și de utilizatori activi astfel, încât în prezent Serviciul Tehnologia Informației și Securitate Cibernetică numără aproximativ peste 140 mii de utilizatori activi ai semnăturii electronice, iar în perioada ultimului an au fost înregistrate circa 2500000 tranzacții cu semnătură mobilă prin intermediul partenerilor operatorii de telefonie mobile și circa 20000000 tranzacții cu semnătură tradițională (tabelul 1). În același context, e de menționat că STISC a asigurat eliberarea a 64 mii semnături electronice avansate calificate subiecților declarării averii şi a intereselor personale din cadrul organizațiilor publice, conform HG nr.673/2017 pentru implementarea Legii nr.133/2016 privind declararea averii şi a intereselor personale, 10 mii de semnături prestatorilor de servicii medicale de asistență medicală primară şi specializată de ambulator în contextul HG nr.164/2019 privind modul de autentificare în Sistemul informațional automatizat "Asistenţa medicală primară", precum și peste 245 mii semnături electronice mobile prin intermediul operatorii de telefonie mobilă din Republica Moldova, Orange Moldova și Moldcell [15].

Tabelul 1

Servicii de e-semnături prestate de STISC

Numărul de utilizatori activi ai e-semnăturii	140000
Numărul de e-semnături avansate eliberate în cadrul organizațiilor publice	64000
Numărul de e-semnături prestate serviciilor medicale	10000
Numărul de e-semnături mobile (prin intermediul operatorilor de telefonie mobilă din RM)	245000
Numărul de tranzacții cu semnătură mobilă în ultimul an	2500000
Numărul de tranzacții cu semnătură tradițională	20000000

Sursa: [15].

7. Provocări în implementarea semnăturii digitale

În ciuda potențialului tehnologiei, implementarea soluțiilor de semnături digitale conduce, de asemenea, și provocări (figura 1). Majoritatea companiilor au sisteme și procese concepute în jurul metodelor tradiționale de comunicare contractuală. De la biroul unui angajat până la arhivarea documentelor semnate, adaptarea aplicațiilor sau a sistemelor existente este considerată o problemă majoră în cadrul interviurilor.

Companiile și instituțiile interesate de adoptarea tehnologiei sunt, prin urmare, extrem de dependente de soluții de încredere, convenabile și ușor de implementat, care nu măresc complexitatea fluxurilor de lucru. Furnizorii capabili să ofere acest amestec important de caracteristici vor avea probabil un avantaj competitiv substanțial pe piață pentru semnătura digitală. Mai mult, există și problema privind acceptarea partenerilor de afaceri / clienților (figura 1).

Cu toate acestea, acceptarea depinde în mare măsură de soluțiile oferite clienților, ceea ce înseamnă că o gamă vastă de cazuri de utilizare, ce garantează ușurința utilizării, va crește acceptarea partenerilor naturali și de afaceri.

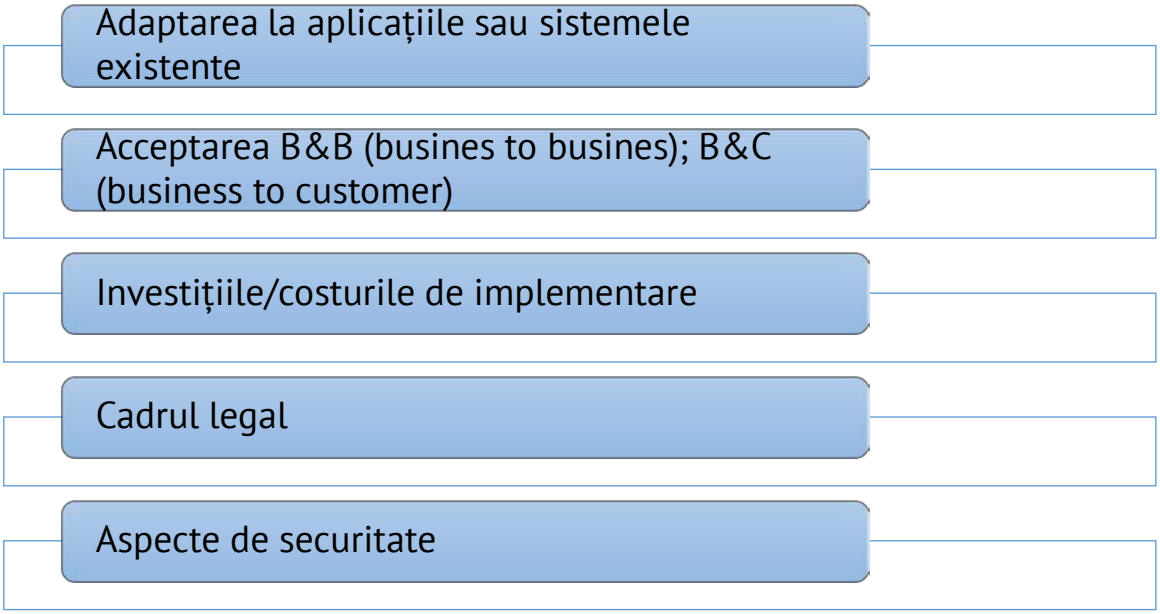

Figura 2. Provocări majore în implementarea e-semnăturii.

S-ar putea crea, de asemenea, impresia că implementarea soluțiilor de semnătură digitală va atrage un cost ridicat al investiției. Acest argument este aplicabil pe termen scurt, dar costurile reduse compensează costul investiției în general într-un timp redus. Costul unei anumite soluții depinde de tipul de implementare. Soluțiile cloud conduc la costuri mai mici de implementare. Cu toate acestea, costul general depinde de modelul de preț al soluției și de frecvența de utilizare.

E-mailul certificat ar putea fi un risc pentru semnăturile digitale. E-mailul certificat este un serviciu care urmărește, de asemenea, să asigure un transfer sigur de date între expeditor și destinatar, permițând criptarea e-mailurilor de către expeditor și decriptarea acestuia de către receptor. Pentru a face acest lucru, expeditorul și destinatarul trebuie să aibă un cont de e-mail certificat cu un furnizor de e-mail certificat și un software care să poată cripta și decripta e-mailurile. Dacă autenticitatea expeditorului joacă un rol important în tranzacția în cauză, e-mailul certificat poate fi, de asemenea, semnat digital (cu o semnătură digitală calificată) [16]. O problemă majoră de securitate a e-mailurilor certificate constă în faptul că nu se bazează pe un proces de criptare end-to-end, ceea ce înseamnă că fiecare e-mail care a fost criptat de către expeditor este decriptat de ambii furnizori de e-mail autorizați (e-mailul poate fi citit sau modificat), reprezentând o problemă de securitate care ar putea fi utilizată de părți neautorizate. Există posibilitatea de a activa criptarea end-to-end, dar numai cu software de criptare suplimentar.

În comparație cu soluțiile clasice de semnături digitale, e-mailul are dezavantaje de securitate și comoditate, deoarece modelul standard nu se bazează pe criptare end-to-end și pentru că atât expeditorul, cât și receptorul trebuie să aibă un cont de e-mail certificat [12]. Obstacolele tehnice creează mari provocări în conservarea pe termen lung a semnăturilor digitale [16].

8. Cadrul normativ

Legislația europeană se bazează în principal pe Directiva 1999/93 / CE, care stipulează obligații comune pentru furnizorii de servicii de certificare și norme comune privind răspunderea și mecanismele de cooperare pentru a asigura recunoașterea

transfrontalieră a semnăturilor și certificatelor în întreaga Comunitate Europeană. Directiva abordează trei forme de semnături digitale: semnătura digitală simplă, avansată și calificată. Regulamentul UE privind serviciile de identificare electronică și de încredere pentru tranzacțiile electronice pe piața internă a fost implementat în 2014, pentru a consolida utilizarea identificării digitale și a semnăturilor în întreaga Uniune Europeană. Pietrele de temelie esențiale ale reglementări UE includ eliminarea barierelor existente în calea furnizării unui cadru transfrontalier și intersectorial cuprinzător pentru tranzacții electronice sigure, de încredere și ușor de utilizat, precum și potențialul de a permite semnăturilor cloud să atingă cele mai înalte nivelul de securitate. Semnăturile complete bazate pe cloud vor putea fi calificate după îndeplinirea unor cerințe finale [12].

În Republica Moldova, cadrul normativ care stabileşte regimul juridic al semnăturii electronice şi al documentului electronic, inclusiv cerinţele principale faţă de valabilitatea acestora şi cerinţele principale faţă de serviciile de certificare, este stipulat prin Legea nr.91 din 27.06.2014 privind semnătura electronica și documentul electronic, care ulterior a fost modificată prin Legea nr.317 din 30.11.18 (**pentru modificarea articolului 11 din Legea nr.91/2014 privind semnătura electronică şi documentul electronic**) [17, 18].

Deși ar părea că legile, atât la nivel european, cât și la nivel national, sunt clar definite, acestea nu sunt încă suficient de transparente pentru publicul larg, creând provocări pentru potențialul tehnologiei.

Concluzii

➲ Tehnologia semnăturii digitale va fi prezentă în multe domenii ale vieții noastre de zi cu zi în care este implicată confidențialitatea.

➲ Tehnologia aduce o eficiență mai mare a afacerii și economii de costuri și va fi adoptată din ce în ce mai mult ca instrument de comunicare de către partenerii de afaceri, clienți și autoritățile publice.

➲ În ceea ce privește fiecare tehnologie relativ nouă, trebuie depășite obstacolele cum ar fi ușurința integrării și alinierea la fluxurile de lucru existente, calculul cazului de afaceri, precum și lipsa de transparență și adesea neînțelegerea situației juridice.

➲ Regulamentul UE promovează validitatea legală generală, precum și acceptarea soluțiilor bazate pe cloud. Există deja semne foarte promițătoare că autoritățile și industria furnizorilor depășesc aceste provocări.

➲ Deoarece piața solicită o rentabilitate rapidă a investiției și o soluție care facilitează fluxurile de lucru, se așteaptă ca soluțiile bazate pe cloud complet sau parțial să ia o parte majoră a pieței soluțiilor de semnături digitale în viitor.

➲ Cei care realizează potențialul unor astfel de soluții vor putea să creeze un avantaj semnificativ din punct de vedere al costurilor, precum și să-și mențină și să-și extindă mai bine baza de clienți datorită comodității mai mari a acestor soluții.

Referințe bibliografice

1. Studiu privind implementarea Guvernării Digitale în România. [accesat 17.09.2020]. Disponibil: https://www.arb.ro/wp-content/uploads/Studiu-e-Guvernare.pdf
2. Electronic and Digital Signatures. [accesat 15.09.2020]. Disponibil: https://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ElectronicandDigitalSignatures-v5-march2012_000.pdf
3. Digital signatures (re-) invented with EIDAS. [accesat 17.09.2020]. Disponibil: https://connective.eu/digital-signatures-re-invented/ .

4. Dzhangarov D.I. and M A Suleymanova. Electronic digital signature. IOP Conf. Series: Materials Science and Engineering 862 (2020) 052054 doi:10.1088/1757-899X/862/5/052054. [accesat 15.09.2020]. Disponibil: https://www.researchgate.net/publication/341711383_Electronic_digital_signature
5. The history of digital signature. [accesat 19.09.2020]. Disponibil: https://visual.ly/community/Infographics/technology/history-digital-signatures
6. Singh, Ankita. 2018. Digital Signature | DSC | History | Work | Creation | Need | Security | Comparison | Example. [accesat 15.09.2020]. Disponibil: https://msatechnosoft.in/blog/digital-signature-dsc-history-working-need-security-create-example/
7. Maxie, Emili. Infographic: the history of digital signature technology. [accesat 20.09.2020]. Disponibil: https://www.signix.com/blog/bid/108804/infographic-the-history-of-digital-signature-technology
8. Vicky Liu, William Caelli, Ernest Foo, Selwyn Russell. 2004. Visually Sealed and Digitally Signed Documents. [accesat 15.09.2020]. Disponibil: https://www.researchgate.net/publication/27464718
9. Housley, R., W. Ford, T. Polk and D. Solo (2002): Internet X.509 Pulbic Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. Internet Request for Comments 3280
10. Furqan Shahid, Abid Khan. 2020. Smart Digital Signatures (SDS): A Post-quantum Digital Signature Scheme for Distributed Ledgers. Preprint submitted to Future Generation Computer Systems April 26, 2020. [accesat 15.09.2020]. Disponibil: https://www.researchgate.net/publication/340934583
11. Merkle, R. C., A certified digital signature, in: G. Brassard (Ed.), Ad- vances in Cryptology — CRYPTO' 89 Proceedings, Springer New York, New York, NY, 1990, pp. 218–238. doi:10.1007/0-387-34805-0_21.
12. Arthur D. Little. Digital Signatures. *Paving the Way to a Digital Europe*. Copyright © Arthur D. Little 2014. All rights reserved. [accesat 21.09.2020]. Disponibil: www.adl.com/DigitalSignature
13. An Introduction to DIGITAL SIGNATURES For the AEC. Global Sign Industry. [accesat 15.09.2020]. Disponibil: https://www.globalsign.com/en/resources/digital-signatures-for-aec-guide.pdf
14. Stisc_ direcții de activare. [accesat 15.09.2020]. Disponibil: https://stisc.gov.md/ro/directii-de-activitate
15. STISC-Serviciul Tehnologia informației și securitate cibernetică. Semnătura digitală-o creștere continuă de tranzacții. [accesat 15.09.2020]. Disponibil: https://stisc.gov.md/ro/semnatura-electronica-o-crestere-continua-de-tranzactii
16. Electronic and Digital Signatures. Electronic Records Management Guidelines. [accesat 15.09.2020]. Disponibil:https://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ElectronicandDigitalSignatures-v5-march2012_000.pdf
17. Legea nr.91. din 27.06.2014, privind semnătura electronică și documentul electronic. [accesat 22.09.2020]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=112497&lang=ro
18. Lege nr.317 din 30.11.2018 pentru modificarea articolului 11 din Legea nr. 91/2014. [accesat 22.09.2020]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110783&lang=ro