1 iunie 2011

DOCUMENT CONCEPT

Autentificarea şi identificarea electronică mobilă pentru sectorul public din Moldova

Introducere

Guvernul Republicii Moldova a iniţiat, în cadrul iniţiativelor de e-Transformare, crearea unei infrastructuri comune – o nouă platformă a tehnologiei e-Guvernare, ce utilizează cele mai moderne tehnologii, cum sunt cloud computing, şi oferă acces la informaţie prin canale multiple, inclusiv acces de pe aparatele de telefonie mobilă. La nivelul Platformei ca Serviciu, acest mediu dispune de mai multe servicii comune, care sunt cunoscute şi ca servicii facilitante întrucât implementarea şi operarea lor cu succes va reprezenta un imbold semnificativ pentru dezvoltarea şi utilizarea serviciilor electronice. Unul dintre serviciile facilitante este Serviciul de Autentificare şi Control al Accesului (AAC). Acest serviciu va implementa sarcinile de securitate de bază cum sunt identificarea şi autentificarea utilizatorilor, autorizarea tranzacţiilor lor şi stabilirea drepturilor lor în diversele sisteme informaţionale ale Guvernului. Prezentul document descrie detaliat situaţia actuală din mai 2011 şi opţiunile de implementare a serviciului AAC.

Noţiuni şi definiţii

Autentificare	-	Procesul de identificare a utilizatorului într-un sistem informaţional;
Autorizare	-	Procesul stabilirii drepturilor utilizatorului într-un sistem informaţional;
CRM	-	Managementul Relaţiei cu Clientul (sistem);
CTS	-	Centrul de Telecomunicaţii Speciale;
SD	-	Semnătură digitală;
Identitate electronică	-	colecţie de atribute de identitate în format electronic (definiţia STORK dată de Uniunea Europeană);
ESB	-	Enterprise Service Bus
G4B	-	Guvern pentru Business (portal);
G4C	-	Guvern pentru Cetăţeni (portal);
GIS	-	Sistem Informaţional Geografic;
HSM	-	Modulul de Securitate Hardware;
M-Cloud	-	Platforma de prestare a serviciilor bazată pe cloud computing a Republicii Moldova;
Identitate mobilă	-	Identitate electronică portabilă;
M-Pass	-	Furnizorul naţional de autentificare care se bazează pe numărul de identificare de stat în calitate de nume al utilizatorului şi parolă;
M-Point	-	Chioşc instalat în fiecare localitate din Moldova ce oferă acces la serviciile electronice;

PKI	-	Infrastructura Cheii Publice;
Semnatar	-	persoana care aplică semnătura digitală conţinutului electronic;
Directiva privind semnătura	-	Directiva 1999/93/EC a Parlamentului European şi a Consiliului privind stabilirea cadrului comunitar pentru semnăturile electronice, publicată în Monitorul Comunităţilor Europene (OJ) L 13, 19.01.2000, p. 12.
SIM	-	Modulul Identităţii Abonatului;
SLA	-	Service Level Agreement;
SSCD	-	Dispozitivul Securizat de Creare a Semnăturii;
WPKI	-	Infrastructura Wireless a Cheii Publice

Arhitectura platformei

În cadrul platformei tehnologiei e-Guvernare, Republica Moldova urmează să creeze o nouă infrastructură comună ce va permite ministerelor şi agenţiilor să găzduiască sisteme informaţionale în aceasta. Infrastructura va fi creată cu utilizarea cloud computing – o tehnologie modernă şi promiţătoare care va schimba modul de prestare a serviciilor informatice şi le va transforma într-o autofurnizare eficientă a resurselor TI îmbinate cu modele plăteşte-atât-cât-utilizezi. Pentru comoditate, în Moldova, tehnologia cloud computing va fi numită M-Cloud.

Această platformă este, în esenţă, un nor privat ce oferă trei modele principale de prestare a serviciilor – Infrastructura ca Serviciu (IaaS), Platforma ca Serviciu (PaaS) şi Software ca Serviciu (SaaS).

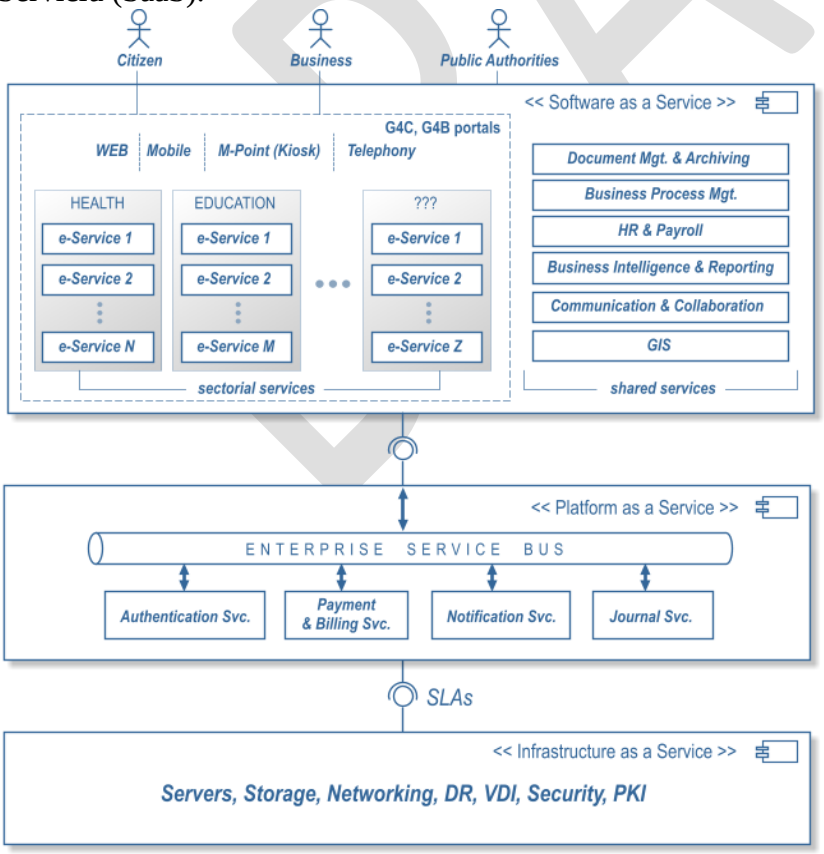

Figura. 1. Arhitectura de nivel înalt a platformei tehnologiei e-Guvernare

Serviciile la nivel de Infrastructură se vor baza în principal pe furnizarea serviciilor existente şi modernizate oferite de CTS. Utilizarea acestor servicii va permite ministerelor şi instituţiilor să-şi extindă capacitatea TI într-o perioadă scurtă de timp. Atunci când resursele solicitate nu vor mai fi necesare, instituţia va putea să le reducă volumul, funcţionând astfel pe baza modelului plăteşte-atât-cât-utilizezi.

Serviciile la nivel de Platformă vor oferi funcţionalităţi comune pentru serviciile business operate de ministere şi instituţii la nivelul Software ca Serviciu. Pentru moment, arhitectura defineşte patru servicii reutilizabile la nivel de Platformă:

- Serviciul de Autentificare şi Control al Accesului (AAC) – reprezintă o modalitate unificată de realizare a sarcinilor aplicaţiei de securitate cum sunt managementul identităţii, autentificarea, autorizarea tranzacţiei etc.;
- Serviciul de plată – reprezintă o modalitate unificată de implementare a plăţilor electronice;
- Serviciul de notificare – reprezintă o modalitate unificată de expediere a notificărilor atunci când sunt necesare, permiţând astfel interacţiunea cu cetăţenii în regim offline;
- Serviciul de jurnalizare – reprezintă o modalitate unificată de stocare şi extragere a datelor referitoare la activitatea utilizatorilor în sistemele informaţionale.

Serviciile la nivel de platformă urmează să fie utilizate de serviciile electronice curente şi viitoare pe care le pot elabora ministerele şi instituţiile.

Platforma M-Cloud cuprinde, de asemenea, şi un nivel de comunicare bazat pe enterprise service bus (ESB). Prin intermediul acestuia, serviciile vor putea să facă schimb de mesaje, ceea ce va permite crearea proceselor complexe de business care vor fi dirijate prin instrumentele de management al procesului business.

Serviciile prestate la nivelul SaaS pot fi grupate în două categorii mari – servicii sectoriale şi servicii comune.

Serviciile sectoriale sunt implementate şi menţinute de diferite sectoare, cum sunt educaţia, medicina, protecţia socială etc., ai căror consumatori direcţi sunt cetăţenii. Aceste servicii sunt accesibile printr-un portal comun. Accesul la portal va fi posibil prin diferite canale ca web, mobilul sau chioşcurile, acestea din urmă fiind numite M-Points, din motive de comoditate.

Serviciile comune la nivelul SaaS sunt serviciile care vor putea fi utilizate în comun între ministere şi instituţii. Exemple de asemenea servicii sunt sistemul de management al documentului electronic, sistemul resurselor umane şi al statelor de plată, sistemul CRM şi de raportare etc., reprezentând serviciile care vor contribui la optimizarea activităţii autorităţilor publice.

Structura serviciilor la nivel de platformă

Întrucât serviciile la nivel de platformă vor fi reutilizate de multe servicii business în contexte multiple, acestea trebuie să fie cât mai configurabile pentru a se ajusta la diferite scenarii de utilizare. Pe de altă parte, mai multe companii şi-au exprimat interesul de a oferi soluţii comerciale.

Arhitectura serviciilor la nivel de platformă se va baza pe modelul arhitectural al prestatorului, care decuplează serviciul generic de la implementarea lui specifică. În acest caz, vânzătorii vor trebui să se conformeze unor interfeţe de comunicare care acţionează în calitate de contracte tehnice între componente.

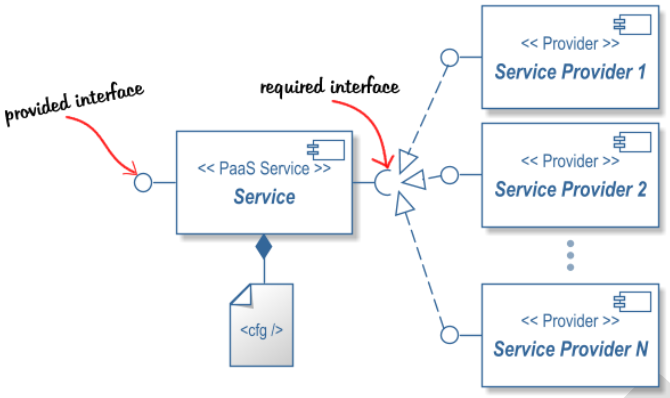

Figura. 2 Modelul de structură al prestatorului

Aplicat la funcţia de autentificare, modelul prestatorului va fi similar diagramei prezentate mai jos.

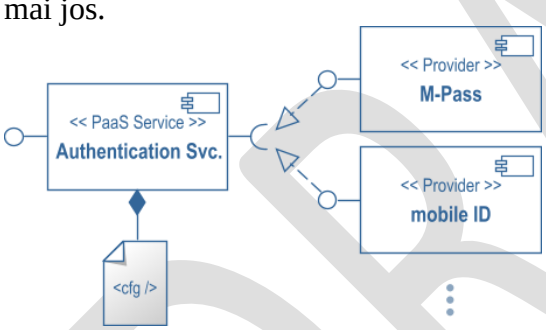

Figura. 3 Modelul prestatorului aplicat la autentificare

Conform acestei structuri, arhitectura trebuie să integreze diferiţi prestatori de autentificare/autorizare. Pentru moment, am identificat doi prestatori: M-Pass şi m-ID. M-Pass este un prestator de servicii de autentificare care acceptă credenţialele utilizatorului, adică numele utilizatorului şi parola, şi eliberează, în rezultat, un bilet de autentificare în cazul unei autentificări reuşite. M-Id este un alt prestator care autentifică utilizatorii şi autorizează tranzacţiile pe baza certificatelor digitale eliberate de autoritatea naţională de certificare.

Acest model al prestatorului oferă o flexibilitate mai înaltă la ajustarea diverselor scenarii de utilizare. De exemplu, anumite servicii pot să utilizeze M-Pass, în timp ce alte servicii, care necesită un nivel mai înalt de securitate, pot să utilizeze m-ID; de asemenea, în cadrul aceluiaşi serviciu, pentru autentificare poate fi utilizat M-Pass, în timp ce unele autorizări ale tranzacţiilor pot să utilizeze m-Id. Deşi sunt admise excepţiile, regula generală este că serviciile de comunicare unidirecţionale (ex. serverul prezintă informaţii utilizatorilor) utilizează autentificarea simplă cu ajutorul M-Pass, în timp ce serviciile de comunicare bidirecţionale vor utiliza identificarea electronică mobilă.

Identificarea mobilă

Am analizat câteva implementări ale identităţii electronice şi mobile în mai multe state europene care se conformează Directivei Parlamentului European 1999/93 privind stabilirea cadrului comunitar pentru semnăturile electronice, publicate în Monitorul Comunităţilor Europene (OJ) L 13, 19.01.2000, pagina 12.
Această directivă stipulează că statele membre UE trebuie să implementeze şi să utilizeze pe larg identitatea electronică până la mijlocul anului 2001. Chiar şi acum, un deceniu mai târziu, aşteptările înalte referitoare la utilizarea şi asimilarea semnăturilor electronice calificate nu au fost atinse. Este o situaţie curioasă, întrucât, pe de o parte, numărul atacurilor asupra datelor confidenţiale şi al furturilor de identitate este în continuă creştere[1] în timp ce, pe de altă parte, rata adoptării semnăturilor electronice calificate este foarte joasă, deşi acestea ar reprezenta soluţia cea mai potrivită pentru provocările menţionate mai sus.

Semnăturile electronice calificate sunt semnături electronice avansate care se bazează pe un certificat calificat şi care sunt create de un dispozitiv securizat de creare a semnăturii[2]. De obicei, acesta din urmă implică utilizarea unui smart-card specific. Întrucât computerele şi notebook-urile obişnuite nu conţin un dispozitiv de citire pentru utilizarea simplă a smart-card-ului, procedura ce trebuie să fie aplicată pentru a putea fi utilizat card-ul poate fi una costisitoare şi de durată. Pe lângă faptul că este necesară o procedură de înregistrare oficială pentru identificarea semnatarului[3], acesta din urmă trebuie să cumpere o componentă specifică de hardware (dispozitiv de citire a smart-card-ului), ceea ce poate complica experienţa utilizatorului şi accesibilitatea produsului, care nu este disponibil, de regulă, în magazine. În plus, pot fi necesare proceduri suplimentare de instalare pentru dispozitivul de citire a card-ului, precum şi instalarea componentelor de soft pentru aplicaţiile semnăturii. De asemenea, mai multe aplicaţii implicate ar putea să nu fie auto-explicative, cauzând astfel bariere suplimentare pentru utilizarea pe larg a produsului.

Astăzi există mai multe abordări tehnice şi organizaţionale referitoare la modul în care dispozitivele mobile pot să servească ca mijloace de autentificare. În urma analizei efectuate, am convenit asupra a două alternative viabile pentru implementarea acestei tehnologii: a) implementarea din partea clientului, unde materialul criptografic este stocat în Modulul Identităţii Abonatului (SIM) localizat în aparatul mobil al clientului (modelul utilizat în prezent în Estonia) şi b) din partea server-ului, unde materialul criptografic este stocat pe server în Modulul Securităţii Hardware (HSM) (modelul utilizat în prezent în Austria). Mai jos este prezentată o scurtă descriere a acestor alternative.

Identificarea mobilă din partea clientului

O abordare pentru realizarea identificării electronice mobile este aplicarea semnăturii digitale direct din aparatul telefonului, utilizând elemente securizate incorporate, elemente securizate pe card-uri SIM speciale sau elemente securizate implementate pe un hard extern conectat la aparatul mobil.
Cheia privată necesară pentru aplicarea semnăturilor este stocată securizat printre elementele securizate. Utilizarea acesteia este protejată printr-un cod PIN, cunoscut doar de proprietarul telefonului, astfel încât acesta are controlul exclusiv asupra credenţialelor sale. Rezultatul

[1] Pentru fapte şi cifre interesante, a se vedea http://www.enisa.europa.eu/act/ar/deliverables/2010/preventing-identity-theft_training-material/at_download/file sau rapoartele privind ameninţările la adresa securităţii internet-ului, elaborate de Symantec, http://www.symantec.com/business/theme.jsp?themeid=threatreport.
[2] Art. 5 par. 1 al Directivei.
[3] A se vedea în special Anexa II d.) a Directivei.

semnăturii digitale este transferat, de obicei, partenerului de comunicare, fie prin utilizarea unui canal GSM sau a altei tehnologii de comunicare cum sunt RFID, NFC sau Bluetooth.

O soluţie aprobată deja este integrarea unui modul PKI în cadrul Modulului Identităţii Abonatului (SIM). Această abordare pare evidentă întrucât SIM card-urile sunt instalate şi integrate deja în telefon, distribuţia este asigurată de operatorul de telefonie mobilă şi cheile private pot fi generate pe card, astfel încât acestea nu părăsesc mediul securizat.

SIM-ul este un modul care stochează securizat informaţia aferentă reţelei, utilizată pentru identificarea şi autentificarea abonaţilor în Reţea:

- ca orice smart card, SIM-ul oferă aşa-numitul "Card de identificare cu circuit integrat" (ICCID), un identificator internaţional unic,
- Identitatea Internaţională a Abonatului Mobil (IMSI), identificator unic utilizat de reţelele operatorilor individuali
- o cheie de autentificare utilizată pentru autentificarea SIM-ului în reţeaua mobilă.

Fiecare abonat este conectat în mod unic la SIM, care stochează în manieră inviolabilă cheia privată a utilizatorului necesară pentru autentificare pe baza semnăturilor.
Un SIM card din telefon poate fi considerat un smart card complet integrat, cu un dispozitiv de citire şi ecran, în combinaţie cu funcţiile în reţea.
Procesele de înregistrare, autentificare sau semnare pot să difere de la caz la caz, după cum este prezentat mai jos:

Procesul înregistrării utilizatorului

1. Utilizatorul primeşte de la operatorul de telefonie mobilă un SIM card ce suportă WPKI.
2. Dacă există deja chei private stocate pe card, fişierele PKCS#10 şi certificatele publice ale dispozitivului sunt stocate deja la operatorul mobil.
3. Autoritatea de înregistrare/certificare (RA/CA) verifică identitatea utilizatorului (nu în cadrul WPKI) şi expediază utilizatorului un cod de activare.
4. Utilizatorul contactează RA/CA pentru a iniţia procesul de activare. În dependenţă de numărul telefonului, RA/CA identifică operatorul de telefonie mobilă corespunzător.
5. RA/CA contactează operatorul de telefonie mobilă prin interfaţa WPKI pentru a iniţia procesul de activare. Operatorul de telefonie mobilă verifică dacă SIM card-ul utilizatorului dispune deja de chei pre-distribuite incluse. Dacă acestea nu există, este trimisă o comandă specială la SIM card-ul utilizatorului pentru a iniţia un proces de generare a cheilor pe SIM, care implică definirea codurilor PIN.
6. RA/CA primeşte certificatul dispozitivului.
7. RA/CA expediază, prin intermediul operatorului de telefonie mobilă, o solicitare de semnătură la SIM card-ul utilizatorului.
8. Utilizatorul este rugat să introducă codul de activare, pe care trebuie să-l semneze suplimentar utilizând codul PIN.
9. Codul semnat este returnat la RA/CA prin intermediul operatorului de telefonie mobilă.
10. RA/CA verifică semnătura şi codul de activare.
11. RA/CA primeşte solicitările PKCS#10 de la operatorul de telefonie mobilă.

12. RA/CA generează certificatele utilizatorului.
13. Utilizatorul este informat despre reuşita procesului de activare.

Procesul de autentificare

1. Utilizatorul doreşte să se autentifice la partea împuternicită cu autentificarea. Partea responsabilă de autentificare solicită numărul de telefon. Utilizatorul introduce numărul de telefon.
2. Partea împuternicită cu autentificarea efectuează o căutare prin contactarea fiecărei autorităţi de înregistrare/certificare (RA/CA) prin intermediul interfeţei de căutare WPKI. În cazul în care căutarea pentru un anumit număr de telefon se soldează cu mai multe rezultate (utilizatorul poate fi înregistrat la mai multe RA/CA), utilizatorul trebuie să aleagă o singură RA/CA.
3. Partea împuternicită cu autentificarea afişează informaţia ce urmează să fie semnată pe „canalul informativ" (de exemplu browser-ul utilizatorului), inclusiv instrucţiunea că utilizatorul trebuie să semneze utilizând canalul securizat (telefonul lui mobil). De asemenea, poate fi afişat un cod de control opţional.
4. SIM card-ul utilizatorului primeşte solicitarea de semnătură.
5. Dacă a fost utilizat un cod de control, utilizatorul trebuie să introducă codul de control respectiv în telefon mobil. Utilizatorul semnează textul afişat prin introducerea PIN-ului.
6. Operatorul de telefonie mobilă trimite mesajul semnat la partea împuternicită cu autentificarea şi acesta verifică semnătura şi validează certificatul trimiţând o solicitare OCSP la RA/CA.
7. RA/CA returnează statutul certificatului.

Procesul de semnare

1. Utilizatorul vrea să folosească un serviciu care solicită autentificare.
2. Utilizatorul introduce numărul telefonului mobil în formatul web al serviciului în care vrea să se autentifice.
3. Telefonul mobil primeşte de la prestatorul de servicii un mesaj SMS special pregătit în acest scop, ce include textul ce urmează să fie semnat.
4. Utilizatorul contraverifică textul mesajului.
5. Utilizatorul semnează mesajul prin introducerea PIN-ului format din patru cifre.
6. Mesajul este semnat utilizând funcţionalitatea PKCS#1 a cardului SIM.
7. Mesajul semnat este expediat înapoi împreună cu ICCID-ul unic al cardului SIM.
8. Autoritatea de verificare verifică semnătura. Certificatul ce conţine cheia publică necesară pentru verificarea semnăturii poate fi obţinut prin intermediul ICCID-ului transmis de semnatar.
9. Utilizatorul este autentificat acum la prestatorul de servicii.

Identificarea mobilă prin intermediul serverului

Această abordare inovativă, care a fost prezentată publicului în cadrul Conferinţei Ministeriale cu privire la Guvernarea Electronică, desfăşurată la Malmö la sfârşitul anului 2009, permite utilizarea semnăturilor electronice calificate fără instalarea unui soft

suplimentar şi utilizarea unor elemente hardware cum sunt dispozitivele de citire a smart-card-urilor.
În contrast cu soluţiile „mobile eID" aplicate din partea clientului, semnătura telefonului mobil aplicată din partea serverului nu se bazează pe SIM-card-uri specifice, întrucât datele de creare a semnăturii sunt stocate la distanţă. Astfel, dispozitivul securizat de creare a semnăturii, necesar pentru semnăturile electronice calificate nu se conţine în aparatul de telefonie mobilă, ci într-un HSM aflat la distanţă. Modelul identificării prin intermediul serverului permite utilizarea oricărui telefon mobil şi a oricărei reţele de telefonie mobilă întrucât nu este necesar un SIM card specific şi nu este necesar ca utilizatorul să-şi schimbe SIM-card precedent. Singura cerinţă tehnică este ca aparatul de telefonie mobilă să poată expedia şi primi mesaje SMS.

Similar multor soluţii utilizate de bănci pentru e-banking, după tipărirea numărului de telefon (în calitate de nume al utilizatorului) şi a parolei, utilizatorul primeşte un SMS la numărul de telefon mobil înregistrat, ce conţine un cod temporar de unică folosinţă (TAN). Introducerea codului TAN declanşează semnătura electronică calificată prin utilizarea certificatului calificat şi a datelor de creare a semnăturii, stocate într-un Modul de Securitate Hardware (HSM) care se păstrează securizat la prestator.

Procesul înregistrării utilizatorului

Procesul tehnic de generare a datelor de creare a semnăturii este realizat complet în HSM în cursul procesului de înregistrare iniţială:

1. Identitatea semnatarului este verificată de prestatorul serviciului de certificare conform prevederilor legale. În timpul procesului de înregistrare, semnatarul trebuie să indice numărul telefonului mobil pe care vrea să-l utilizeze pentru a declanşa procesul de semnare în viitor şi să aleagă o parolă secretă.
2. Posesiunea reală a numărului de telefon mobil specificat este verificată prin expedierea imediată la aparatul respectiv a unui SMS ce conţine un cod temporar de unică folosinţă (numărul tranzacţiei TAN).
3. Semnatarul trebuie să introducă codul TAN în format web.
4. După verificarea codului TAN de către serviciu, noile date de creare a semnăturii sunt generate în HSM, în acelaşi loc unde cheia privată generată este cifrată imediat cu o altă cheie care este derivată din numărul telefonului mobil şi parola utilizatorului. Prin acest procedeu, cheia privată cifrată poate fi utilizată mai târziu doar dacă parola secretă este disponibilă pentru descifrare. De asemenea, pentru a asigura că utilizarea cheii private este posibilă doar în cadrul HSM-ului certificat, cheia privată cifrată este cifrată din nou – de această dată cu o cheie cunoscută doar de HSM. Aceste date de creare a semnăturii cifrate dublu pot fi stocate chiar şi în afara HSM-ului certificat, într-o bază de date a cheilor.

Procesul de autentificare

Un proces tipic de autentificare poate fi efectuat după cum urmează:

1. Utilizatorul vrea să se autentifice la prestatorul de servicii.
2. Prestatorul de servicii redirecţionează utilizatorul la autoritatea de autentificare.
3. Utilizatorul îşi introduce numărul de telefon şi parola. Parola este necesară pentru a preveni utilizarea abuzivă a serviciului.

4. Autoritatea de autentificare transmite, printr-un SMS la telefonul clientului, un cod TAN valabil doar pentru o perioadă scurtă de timp, opţional împreună cu o valoare hash a mesajului de autentificare ce urmează să fie semnat.
5. Utilizatorul verifică mesajul de autentificare pe care urmează să-l semneze online, şi compară valoarea hash a acestuia cu valoarea pe care a primit-o.
6. Dacă valorile corespund, utilizatorul introduce în format web codul TAN împreună cu codul PIN aferent cheii private.
7. Serverul semnează mesajul de autentificare utilizând HSM şi codul PIN oferit.
8. Rezultatul semnăturii este expediat prestatorului de servicii.
9. Prestatorul de servicii verifică semnătura şi validează certificatul.
10. Dacă verificarea a fost reuşită, prestatorul de servicii acceptă autentificarea utilizatorului.

Procesul de semnare

Utilizarea ulterioară a datelor pentru crearea semnăturii în vederea creării semnăturii este similară procesului de înregistrare descris:

1. Dacă utilizatorul doreşte să semneze un document, el iniţiază solicitarea de semnătură a aplicaţiei ce este utilizată (o aplicaţie web sau softul instalat local). Solicitarea de semnătură include documentele/datele ce urmează să fie semnate şi este adresată prestatorului semnăturii pe telefonul mobil.
2. Atunci când solicitarea este primită de HSM, utilizatorul trebuie să introducă numărul telefonului mobil (în calitate de nume al utilizatorului) şi parola secretă. Toate datele introduse sunt procesate prin canale de comunicaţie securizate direct în aplicaţia web a semnăturii pe telefonul mobil.
3. După ce se examinează dacă numărul respectiv corespunde unui semnatar înregistrat, documentul/datele ce urmează să fie semnate, împreună cu parola şi numărul telefonului, sunt imediat expediate la HSM, care calculează ulterior o valoare hash (amprentă digitală) a documentului/datelor şi un cod temporar aleatoriu de unică folosinţă (TAN). Ambele sunt expediate printr-un SMS la telefonul mobil specificat. În paralel, aplicaţia web a serviciului semnăturii pe telefonul mobil îi oferă semnatarului posibilitatea să vadă şi să verifice încă o dată datele ce urmează să fie semnate. În acelaşi timp, valoarea hash scurtă este fişată de aplicaţia web.
4. Semnatarul primeşte SMS-ul şi are posibilitatea să compare valoarea hash primită prin SMS cu valoarea hash afişată de aplicaţia web. Prin introducerea codului TAN primit, direct în serviciul de semnătură al telefonului mobil, se asigură că semnatarul este într-adevăr în posesia telefonului mobil înregistrat.
5. Rezultatul pozitiv al verificării face ca HSM să extragă datele cifrate de creare a semnăturii din baza de date a cheilor şi să le descifreze cu cheia secretă a HSM. La etapa următoare, datele de creare a semnăturii, care mai sunt cifrate, sunt descifrate prin utilizarea unei derivaţii de la parola secretă a utilizatorului. Doar acum cheia privată este disponibilă în HSM certificat.
6. Semnătura este creată în HSM şi documentul/datele semnate sunt transmise semnatarului.

Atât descifrarea datelor de creare a semnăturii, cât şi crearea semnăturii propriu-zise sunt realizate exclusiv în cadrul HSM-ului certificat, iar mecanismele de descifrare selectate asigură că acest lucru este posibil din punct de vedere tehnic doar aici. Din această perspectivă, securitatea semnăturii create este egală cu cea a soluţiei bazate pe smart-card. Procesul este comparabil şi din perspectiva semnatarului: procesul de semnare este declanşat prin două componente: divulgarea parolei secrete (factorul „cunoaştere") şi a numărului telefonului mobil şi verificarea posesiunii de fapt a telefonului mobil (factorul „posesiune"). Factorul „cunoaştere" este verificat de HSM în procesul descifrării datelor de creare a semnăturii. Verificarea factorului „posesiune" este efectuată de aplicaţia semnăturii securizate a semnăturii, care include şi conectarea la elementele periferice, cum sunt SMS gateway sau web front end.

Cerinţele legale pentru semnăturile electronice

Conform Directivei UE, semnătura electronică calificată este o semnătură avansată, bazată pe un certificat calificat şi creată de un dispozitiv securizat de creare a semnăturilor. În contextul actual, cerinţele legale pentru semnătura electronică avansată sunt[4] :

a) Să facă trimitere exclusiv la semnatar;
b) Să permită identificarea semnatarului;
c) Să fie creată prin mijloace pe care semnatarul le poate menţine sub controlul său exclusiv
d) Să fie corelată la datele la care se raportează astfel încât orice modificare ulterioară a datelor să poată fi depistată.

Legislaţia actuală a Republicii Moldova cu privire la semnătura digitală, şi anume Legea Nr. 264 din 15.07.2004 cu privire la documentul electronic şi semnătura digitală, include parţial cerinţele legale menţionate mai sus. În special art. 22 al. 2 stipulează că mijloacele semnăturii digitale trebuie să asigure:

a) unicitatea cheii private şi cheii publice create;
b) dificultatea de calcul necesară la deducerea cheii private şi a semnăturii digitale;
c) confidenţialitatea cheii private.

Art. 21 al. 5 stipulează: Cheia privată este păstrată şi utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea a altei persoane.
În prezent există un proiect de lege cu privire la semnătura digitală şi documentul electronic care va înlocui legea în vigoare nr. 264-XV. Noua lege reprezintă, de fapt, o aliniere la Directiva Uniunii Europene 1999/93 şi include cerinţele explicite pentru semnătura digitală care au fost descrise mai sus.

Analiza alternativelor identităţii mobile

După cum s-a menţionat mai sus, identificarea mobilă din partea clientului este implementată cu succes în Estonia, în timp ce opţiunea din partea serverului este implementată cu succes în Austria. Din fericire, am avut posibilitatea să discutăm cu echipele de implementare din ambele ţări şi chiar am avut o şedinţă comună la care am clarificat diversele aspecte ale acestor două alternative, cum sunt securitatea, uşurinţa implementării, asimilarea de către utilizatori, etc.

[4] Art. 2.2 al Directivei

În rezultatul consultărilor cu operatorii locali de telefonie mobilă, cu reprezentanţii autorităţii naţionale de certificare şi cu echipele de dezvoltatori, am ajuns la următoarele concluzii:

1. Din punct de vedere tehnic sunt viabile ambele soluţii – ele soluţionează problema semnăturii şi autentificării mobile.
2. Pentru a selecta o alternativă în vederea implementării ulterioare, se vor utiliza o serie de criterii prezentate mai jos. Aceste criterii au o relevanţă diferită pentru contextul actual al ţării şi pot fi cântărite în urma unei analize pe o scară de la 1 (cel mai puţin relevante) până la 10 (relevanţă critică)

#	Criteriu	Descriere
1.	Costul implementării	Cât va costa statul să implementeze sistemul?
2.	Costul mentenanţei	Cât va trebui să plătească statul anual pentru a menţine sistemul în funcţiune?
3.	Perioada de implementare	Cât va dura implementarea sistemului? Când va putea fi lansat?
4.	Asimilarea de utilizatorul final: utilitatea	Cât de confortabilă va fi folosirea noului sistem pentru utilizatorii finali? - Cât de uşor va putea fi emis un set SD? - Cât de uşor va putea fi extins/înlocuit certificatul după expirarea perioadei lui de valabilitate? - Cât de uşor va putea fi utilizată SD cu modelul?
5.	Asimilarea de utilizatorul final: cheltuieli	Cât îi va costa pe utilizatori să folosească acest model: - Cât vor trebui să plătească aceştia pentru înregistrare/activare? - Cât vor trebui să plătească pentru prestarea obişnuită a serviciilor? - Care sunt cheltuielile indirecte pe care vor trebui să le suporte (ex. Cumpărarea unui nou telefon mobil pentru că cel vechi nu este compatibil cu modelul SD)?
6.	Utilitatea administrativă	Cât de uşor va putea fi administrat procesul: - De emitere a SD; - Corelarea cu persoana fizică; - Revocare a certificatului; - Extindere/înlocuire a certificatului
7.	Suport tehnic	Ce suport vor primi utilizatorii la folosirea SD? Cine va oferi acest suport?

8.	Asimilarea de sectorul privat/bancar	În ce măsură va utiliza sectorul privat acest sistem naţional de autentificare pentru soluţiile lor? Câte potenţiale companii/bănci vor fi dispuse să utilizeze din nou această soluţie?
9.	Securitate	Cât de sigură este stocarea şi transportarea datelor? Cum percepe utilizatorul securitatea sistemului? Ce şanse sunt să fie pierdute informaţii sensibile şi care este impactul acestei pierderi?
10.	Siguranţa modelului	Cât de sigur este sistemul ca un tot întreg? Câţi actori sunt implicaţi în proces? Ce se întâmplă dacă un segment cade, ex. un utilizator îşi pierde telefonul mobil – cât de repede poate acesta să utilizeze sistemul din nou?
11.	Nediscriminare	Permite acest model o competiţie corectă pe piaţă? Este acesta un model deschis în care poate intra oricine?

3. O analiză preliminară a cadrului normativ al Republicii Moldova cu privire la semnătura digitală relevă că pentru ambele opţiuni trebuie să fie operate unele modificări legislative pentru a implementa identitatea mobilă. În cazul implementării identificării mobile din partea clientului, operatorii vor avea dreptul să coreleze identităţile digitale la persoanele fizice, în timp ce în cazul implementării din partea serverului, legislaţia va trebui să interpreteze clar sintagma "semnătura va fi supusă controlului exclusiv al semnatarului" astfel încât aceasta să însemne că semnătura trebuie să fie iniţiată exclusiv de titularul acesteia indiferent de locul unde este păstrată fizic identitatea electronică. Aceasta este ceea ce stipulează de fapt noul proiect de lege. Având în vedere modificările inevitabile ale cadrului normativ pentru ambele opţiuni, acest criteriu plasează ambele alternative pe poziţii egale.

Riscuri

Au fost identificate următoarele riscuri majore:

1. Operarea modificărilor legislative poate dura mai mult decât se aştepta.
2. Deşi punctajul poate arăta că opţiunea identificării din partea serverului este mai convenabilă pentru implementare, sectorul privat (în special unele bănci) ar putea să nu o accepte din cauza perceperii ei ca fiind mai puţin sigură.

Paşii următori

1. Consultarea sectorului privat, în special a băncilor comerciale (începând cu iunie 2011) cu privire la următoarele:
    a. Ar fi interesaţi să utilizeze în mod repetat un serviciu de autentificare oferit de Guvern?
    b. Ce opţiune este preferabilă, avându-se în vedere în special perioada necesară pentru implementare şi cost-eficienţa?
2. Organizarea unei serii de întrevederi cu părţile interesate pentru a evalua ambele opţiuni, utilizând o serie de criterii predefinite (începând cu iunie 2011).
3. Identificarea modificărilor necesare ale cadrului normativ şi a modului în care trebuie să fie adoptate modificările (mijlocul lunii iunie 2011).
4. Identificarea actorilor din soluţia selectată şi elaborarea unui model business corespunzător (mijlocul lunii iunie 2011).
5. Elaborarea unui plan de implementare având în vedere opţiunea selectată şi feedback-ul colectat în timpul consultaţiilor (sfârşitul lunii iunie 2011).
6. Implementarea planului (până în noiembrie 2011).

Referinţe

1. Directiva 1999/93/EC a Parlamentului European şi a Consiliului privind stabilirea cadrului comunitar pentru semnăturile electronice, publicată în Monitorul Comunităţilor Europene (OJ) L 13, 19.01.2000, vezi http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:EN:PDF
2. Legea Nr. 264 XV din 15/07/2004 cu privire la documentul electronic şi semnătura digitală. http://www.mtic.gov.md/img/pdf/264_2004-07-15_md.pdf
3. Proiectul legii cu privire la semnătura digitală şi documentul electronic, 2010.
4. Raportul proiectului STORK, STORK Work Item 3.3.6 Mobile eID
5. Austrian Mobile Phone Signature – o semnătură electronică calificată, uşor de utilizat ca modalitate de cultivare a încrederii şi securităţii, siguranţei şi autenticităţii pentru guvernarea electronică şi dincolo de aceasta, Peter REICHSTÄDTER, Peter KUSTOR,Austira