

TRANSPARENȚA ȘI SECURITATEA INFORMAȚIEI

Nadejda VACAROV,

magistru în informatică, lector superior universitar,
Academia de Administrare Publică pe lângă
Președintele Republicii Moldova

SUMMARY

Security represents a process and a way of thinking concerning systems, networks, users and applications, which cover a set of technologies. The minimal set of requirements for an application that uses security-based systems is:

- Confidentiality: keeping information privacy;
- Integrity: the proof of non-modification of the information;
- Autenticity: the proof of identity of message sender;
- Non-rejection: assurance that the message generator cannot damn it later.

132

Administrarea publică, nr. 4, 2007

Paza bună trece primejdia rea. Zicala aceasta se potrivește extrem de bine tuturor celor care își stochează date confidențiale pe suport electronic. În prezent, una din problemele comunicării datelor o reprezintă securitatea transmisiei și recepției acestora.

Securitatea reprezintă un proces, un mod de a gândi, legat de sisteme, rețele, utilizatori și aplicații care îmbrățișează un set de tehnologii. Setul minim de cerințe pe care trebuie să le respecte o aplicație ce utilizează sistemele bazate pe securitate sînt:

- *confidențialitatea*: menținerea caracterului privat al informației;
- *integritatea*: dovada că respectiva informație nu a fost modificată;
- *autenticitatea*: dovada identității celui ce transmite mesajul;
- *non-repudierea*: siguranța că cel ce generează mesajul nu poate să-l calomnieze mai târziu.

Toate aceste proprietăți pot fi respectate prin utilizarea unor chei publice

criptografice. Criptografia este considerată o artă sau o știință de menținere a mesajelor secrete, asigurînd confidențialitatea prin criptarea unui mesaj, utilizînd chei asociate cu un algoritm. Cheia utilizată trebuie să fie secretă ambelor părți, problema reprezentînd-o managementul cheilor și menținerea lor secretă. Criptografia are la bază codificarea mesajelor, un bloc fiind substituit prin altul, respectînd anumite reguli. Codificarea se poate realiza în mai multe moduri, acestea avînd următoarele proprietăți comune:

- atît intrările, cît și ieșirile sînt reprezentate ca stram-uri de octeți;
- criptarea unei date se realizează cu ajutorul unei chei;
- decriptarea datei se realizează tot cu o cheie.

Criptarea poate fi realizată cu chei simetrice sau asimetrice. Prima se realizează cu aceeași cheie la criptare și la decriptare, iar cealaltă - cu chei diferite.

Criptarea asimetrică are avantajul că

una dintre chei (cea de criptare) poate fi făcută publică. Această cheie de criptare poate fi transmisă oricui, în timp ce cheia de decriptare este deținută de cel ce a criptat, fiind denumită cheie privată. Un alt avantaj al cheilor asimetrice este că asigură identitatea. Dacă o persoană X criptează un mesaj cu o cheie privată și, transmițându-l unei persoane Y, aceasta îl poate decripta cu o cheie publică, putem spune că Y are certitudinea că mesajul vine de la X. Această idee o au la bază *semnăturile digitale*.

Criptarea mesajelor oferă confidențialitate, dar acest lucru nu este suficient. În cazul unei transmisiuni sau recepții, trebuie să existe certitudinea că cel ce a generat mesajul este o persoană autorizată, motiv care a condus la adăugarea de noi proprietăți, cum ar fi integritatea și autentificarea, acestea fiind asigurate cu ajutorul semnăturii digitale.

Integritatea, confidențialitatea și non-reproducerea sunt asigurate prin criptografia cheilor publice. Pentru aceasta însă trebuie să se știe: *cine generează certificatul, unde este stocată cheia și unde se află certificatele?* Un certificat digital bazat pe infrastructura cheilor publice (PKI - Public Key Infrastructure) asigură rezolvarea tuturor problemelor.

Componentele PKI sunt:

- *autoritatea certificatoare (CA)*: responsabilă de generarea și revocarea certificatelor;

- *autoritatea registratoare (RA)*: responsabilă de verificarea construcției generate de cheile publice și identitatea deținătorilor;

- *deținătorii de certificate (subiecții)*: oameni, mașini sau agenți software care dețin certificate și le pot utiliza la semnarea documentelor;

- *clienții*: ei validează semnătura

digitală și certificarea de la un CA:

- *depozitele*: stochează și fac accesibile certificatele și listele de revocare a certificatelor (CRLs - Certificate Revocation Lists);

- *politicile de securitate*: definesc procesele și principiile de utilizare a criptografiei;

Dintre funcțiile realizate cu ajutorul PKI putem menționa:

- *înregistrarea*: este un proces în care cel ce dorește să obțină un certificat de la CA își prezintă atributele sale; acestea sunt verificate, iar apoi se eliberează certificatul;

- *certificarea*: este procesul în care CA eliberează certificatul ce conține cheia publică subiectului, apoi îl depune într-un depozit public;

- *generarea cheilor*: în multe cazuri subiectul generează o pereche de chei în mediul său, înainte de a transmite cheia publică la CA pentru certificare; dacă CA răspunde de generarea cheilor, acestea sunt oferite subiectului ca un fișier criptat;

- *recuperarea cheilor*: în unele implementări PKI necesită ca toate cheile schimbate și/sau criptate să fie depuse într-un depozit securizat; sunt recuperabile dacă subiectul pierde cheia, acest lucru revenind lui CA sau sistemului de recuperare;

- *actualizarea cheilor*: toate cheile-perechi și certificatele lor asociate trebuie actualizate la un interval regulat. În acest sens există două situații care necesită acest lucru: *data care este specifică în certificat ca data de expirare este depășită și se actualizează*. Dacă cheia privată a uneia din entități din PKI este compromisă, în acest caz PKI trebuie să anunțe că vechiul certificat nu mai este valabil și urmează să-l înlocuiască. Una din chei este de regenerare și stocare securizată a perechilor de chei pentru astfel de situații, acțiune ce duce la informarea fiecărui

utilizator de acest lucru. *Altă cale este metoda "out-of-band"* unde cu ajutorul telefonului, faxului, scrisorii se transmite cheia respectivă;

- *certificarea încrucișată*: permite utilizatorilor dintr-un domeniu administrativ să utilizeze certificate generate de un CA operațional în alt domeniu. Procesul implică un CA (CA_1) ce oferă o certificare pentru alt CA (CA_2). Acest certificat conține cheia publică CA asociată cu cea privată pe care CA_1 o utilizează, lucru ce permite subiecților certificați prin CA_2 să accepte certificatele generate de CA_1 sau orice CA subordonat;

- *revocarea*: apare în momentul

expirării perioadei de validitate care poate apărea când subiectul își schimbă numele, angajatul părăsește compania, cheia privată este compromisă. Pentru a revoca un certificat se utilizează lista revocărilor certificatelor (CRL - Certificate Revocation List). Această listă identifică certificate și sînt semnate de CA.

Din cele expuse se observă că în cazul dezvoltării aplicațiilor ce utilizează Internetul sau Intranetul, cerințele unei bune securități sînt confidențialitatea, integritatea, autentificarea și non-repudierea. Toate acestea se realizează prin utilizarea cheilor publice criptografice în certificate digitale.

BIBLIOGRAFIE

Cadrul juridico-normativ

1. Decretul Președintelui Republicii Moldova nr.1743-III din 19.03.2004 privind edificarea societății informaționale în Republica Moldova.
2. Legea nr.467-XV din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat.
3. Legea nr.264 din 15.07.2004 cu privire la documentul electronic și semnătura digitală.
4. Legea nr.284-XV din 22.07.2004 privind comerțul electronic.
5. Legea nr.1069-XIV din 22.06.2000 cu privire la informatică.
6. Legea nr.982-XIV din 11.05.2000 privind accesul la informație.
7. Tratatul internațional ce țin de drepturile omului la care Republica Moldova este parte.
8. Hotărîrea Guvernului nr.255 din 09.03.2005 privind Strategia Națională de edificare a societății informaționale – "Moldova electronică".
9. Hotărîrea Guvernului nr. 733 din 28.06.2006 cu privire la Concepția guvernării electronice.
10. Hotărîrea Guvernului nr.320 din 28.03.2006 pentru aprobarea Regulamentului privind modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice.
11. Hotărîrea Guvernului nr.632 din 08.06.2004 despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova.
12. Hotărîrea Guvernului nr.272 din 06.03.2002 despre măsurile privind crearea sistemului informațional automatizat "Registrul de stat al unităților de drept".
13. Hotărîrea Guvernului nr.333 din 18.03.2002 pentru aprobarea Concepției

sistemului informațional automatizat "Registrul de stat al populației" și Regulamentului cu privire la Registrul de stat al populației.

14. Hotărîrea Guvernului nr.668 din 19.06.2006 privind paginile oficiale ale autorităților administrației publice în rețeaua Internet.

15. Hotărîrea Guvernului nr.765 din 05.07.2006 privind pagina oficială a Republicii Moldova în rețeaua Internet.

LITERATURĂ

1. Vasiu, L., Vasiu, I. *Informatică juridică și drept informatic*. Ed. Albastră, - Cluj-Napoca, 2005.

2. Vasiu, I. *Criminalitatea informatică*, Ed. Nemira, - București, 2001.

3. Patriciu, V., Vasiu, I., Patriciu, G. *Internetul și Dreptul*, Ed. All Beck, - București, 1999.

4. Vasiu, I., Vasiu, L. Frauda informatică, *Revista Română de Drept Penal*, nr. 1, 2005.

5. Revista „NET Report”, nr. 100, Ianuarie 2001.

6. <http://www.mdi.gov.md/img/mejsoir/ActionPlanEUMeng.pdf>.

7. <http://www.mfa.md/Ro/PlanulActiuniRM UE.pdf>

Prezentat: 23 noiembrie 2007.

Recenzent: Oleg BULGARU, doctor în științe fizico-matematice, conferențiar universitar.

E-mail: vnt15@yahoo.com