ANEXA 1

Elemente de criptografie, autentificare şi semnături digitale

Elementele de securitate care sunt prezentate pe scurt în acest capitol vor avea probabil puterea de a convinge că această securitate este o problemă serioasă şi complexă, uneori implicând costuri destul de mari, şi căreia i s-a dat multă atenţie, cu scopul principal de a micşora riscurile de fraudă, obiectiv despre care se poate spune astăzi că a fost atins în bună măsură. Nu vom putea prezenta în această anexă toate noţiunile şi tehnologiile de securitate din domeniul serviciilor electronice. Vom face însă o rapidă trecere în revistă a unora din cele mai importante noţiuni teoretice, legate în special de criptografie, autentificare şi semnături digitale.

Metodele de securitate actuale, destul de complexe, bazate în principal pe criptografie şi autentificarea persoanelor, documentelor, aplicaţiilor şi sistemelor oferă o securitate a tranzacţiilor (tranzacţia este, într-un sens foarte general,

operaţia de apel şi execuţie a unui eServiciu) substanţial crescută. Desigur, nici o tehnologie de securizare nu poate fi 100% sigură, dar gradul de securitate atins este considerat satisfăcător sau chiar bun. Există şi posibilitatea de a asigura grade diferite de securitate (ca un compromis între cost şi performanţă) funcţie de natura serviciului – furnizarea unor informaţii generale (nu personale), de exemplu, nu necesită măsuri de securitate speciale, în vreme ce obţinerea unor beneficii sociale reclamă identificarea fără greşeală a beneficiarului.

1. Tehnici de securitate – criptare şi autentificare

Pentru a asigura securitatea unei tranzacţii ce reprezintă executarea unui eServiciu se folosesc trei procedee de bază – criptarea informaţiilor, autentificarea identităţii entităţilor care participă la tranzacţie, şi autentificarea documentelor.

Criptarea informaţiilor asigură că acestea nu pot fi citite decât de cel care deţine secretul decriptării (se asigură astfel confidenţialitatea informaţiilor).

Autentificarea identităţii urmăreşte să dovedească că o entitate participantă la tranzacţie (beneficiari, furnizori de eServicii, intermediari, aplicaţii din sisteme informatice) este într-adevăr entitatea care pretinde că este, şi nu cumva una falsă, cu intenţii frauduloase, care se prezintă drept una validă.

Autentificarea unui document asigură că documentul este autentic conform legilor, şi are valoare juridică, adică provine efectiv de la cine afirmă că l-a emis, nu este alterat (integritate), iar emitentul documentului nu poate nega ulterior că este expeditorul acelui document (nonrepudiere), şi se face prin semnătura digitală.

Criptarea/decriptarea informaţiilor se face prin algoritmi de criptare/decriptare al căror scop este transformarea la criptare a unei informaţii lizibile într-una care nu poate fi citită, iar la decriptare, transformarea celei criptate, înapoi în informaţia lizibilă iniţială. Se presupune că informaţia astfel criptată va circula pe drumul între participanţii la tranzacţie fără a exista riscul de a putea fi citită, în afară desigur de cei cărora le este destinată şi care deţin secretul decriptării.

Există două clase mari de algoritmi criptografici care se utilizează curent – algoritmi simetrici (sau cu o cheie secretă) şi algoritmi asimetrici (sau cu pereche de chei - secretă şi publică). Cheia unui algoritm criptografic este, în esenţă, un număr care spune algoritmului cum anume să facă criptarea sau decriptarea. Cine deţine

această cheie poate decripta orice informaţie care a fost criptată de algoritmul care a folosit acea cheie. Evident cheile trebuie ţinute secrete.

Autentificarea identităţii este procedeul principal prin care se stabileşte relaţia de încredere între două entităţi, care îşi dovedesc reciproc, una alteia, că sunt efectiv ceea ce par să fie, şi declară că sunt, înaintea autentificării. Autentificarea urmăreşte micşorarea riscului de a avea de-a face cu o identitate falsă, nelegală, şi care poate avea intenţii frauduloase.

Există mai multe metode de autentificare a identităţii, dintre care vom prezenta pe scurt doar metodele mai frecvente, numite autentificarea prin nume şi parolă (user name, password), şi autentificarea prin certificate de autenticitate (authenticity certificates).

Cea mai simplă formă de autentificare a identităţii, utilizată curent în mai multe domenii, inclusiv în plăţile electronice prin carduri financiare (unde este necesar un grad sporit de securitate), este autentificarea identităţii unei entităţi printr-un nume şi o parolă. Numele şi parola sunt fie alese de entitate (de regulă beneficiarul), apoi verificate şi acceptate de cealălată entitate (de regulă furnizorul eServiciului), fie îi sunt alocate acelei entităţi direct de către eServiciu, după care sunt memorate de ambele entităţi pentru a fi folosite la fiecare tranzacţie în care sunt necesare.

Autentificarea identităţii entităţilor prin metoda certificatelor de autenticitate presupune existenţa unei entităţi speciale în care toate celelalte entităţi decid că au deplină încredere, numită Autoritatea de Certificare (CA, Certification Authority), şi care, cunoscând bine fiecare entitate din sistem, generează pentru fiecare entitate câte un certificat de autenticitate, unic şi specific, care identifică entitatea în mod complet şi unic, şi asumând-şi responsabilitatea garanţiei de identitate pe care o oferă. Astfel, dacă două entităţi doresc să stabilească o relaţie de încredere, în care fiecare să fie sigură de autenticitatea celeilalte, atunci îşi vor trimite reciproc certificatele de autenticitate, iar fiecare entitate va putea verifica autenticitatea celeilalte.

Certificatul de autenticitate al unei entităţi este o informaţie care conţine datele de identificare ale acelei entităţi (nume, cod, adresă, etc.) şi cheia publică proprie entităţii (care va servi în schimbul de date criptate între entităţi), iar această informaţie este la rândul ei criptată de către Autoritatea de Certificare cu cheia sa privată. Desigur cheia de criptare publică a Autorităţii de Certificare trebuie cunoscută de toate entităţile, iar fiecare entitate va trebui să dispună de propria ei

cheie. În acest protocol de autentificare se foloseşte de regulă criptografia asimetrică, cu pereche de chei – publică şi secretă.

Practic, fiecare entitate va trimite celeilalte certificatul propriu de autenticitate. Fiecare entitate, cunoscând cheia publică de criptare a Autorităţii de Certificare, va decripta certificatul de autenticitate al celeilalte entităţi, va constata că este autentic, şi va folosi cheia publică a entităţii aflată în certificat pentru a comunica confidenţial cu respectiva entitate.

În cazuri speciale verificarea autenticităţii unei identităţi se poate face verificând şi caracteristicile biometrice ale persoanei. Aceste caracteristici definesc o persoană fizică şi pot fi caracteristici biometrice fizice – ca de exemplu amprenta digitală, înregistrarea imaginii palmei, a feţei, a irisului sau retinei, şi caracteristici biometrice comportamentale – ca de exemplu vocea sau semnătura. Caracteristicile biometrice sunt captate digital (de exemplu scanate) şi memorate în cardul cu cip de identitate, de unde sunt apoi preluate de un terminal special care are capacitatea de a capta caracteristica biometrică a deţinătorului de card în momentul în care acesta face o tranzacţie, şi de a o compara apoi cu cea memorată în cip. De exemplu, o înregistrare scanată a amprentei degetului mare are circa 1000 de octeţi, iar terminalul special care face autentificarea dispune de o mică fereastră pe care se lipeşte degetul pentru a face scanarea, care e urmată apoi de comparare. O imagine de retină sau de iris are câteva zeci de octeţi, dar terminalul cu facilitatea de captare a respectivei imagini este mult mai complicat. Nu vom intra în detalii, am semnalat doar această metodă de autentificare pentru că este considerată cea mai sigură dintre toate metodele de autentificare a identităţii (fără a fi absolut sigură) (1)(2).

Probarea autenticităţii unui document electronic se face prin semnătura digitală ataşată documentului, aşa cum se prezintă pe scurt în capitolul 3.

2. Elemente de criptografie

În acest capitol se face o foarte sumară prezentare a unor noţiuni de criptografie, suficiente totuşi pentru înţelegerea ideilor principale pe care se bazează securitatea tranzacţiilor (3).

Scopul principal al criptografiei este de a face documentele (informaţia în general, indiferent de forma de prezentare, inclusiv informaţia aflată sub formă binară, de şir de biţi) neinteligibile decât de către entităţile cărora le este adresată, pentru a asigura confidenţialitatea corespondenţei.

Criptarea se face cu un algoritm şi cu o cheie. Textul CARD, de exemplu, poate fi criptat în ECTF, dacă algoritmul de criptare constă în schimbarea fiecărei litere cu cea de a doua următoare în alfabet. În acest exemplu simplu algoritmul constă în deplasarea fiecărei litere a textului clar (lizibil) cu două poziţii mai jos în alfabet, iar cheia algoritmului este numărul doi, care spune cu câte poziţii se deplasează litera în alfabet. Algoritmul de decriptare foloseşte aceeaşi cheie şi se aplică în sens invers asupra textului criptat. Cheia spune algoritmului cum trebuie să facă criptarea sau decriptarea. Acelaşi algoritm aplicat asupra aceluiaşi text cu chei diferite va produce texte criptate diferit. Evident algoritmul şi cheia trebuie cunoscute de ambele părţi, iar ambele trebuie ţinute secret. (Se pare că acest algoritm de criptare a fost folosit pentru prima oară de Cezar în vremea războaielor din Galia pentru a comunica cu partizanii lui din Roma, cheia fiind trimisă separat de textul criptat).

Algoritmii criptografici care se folosesc în domeniu se împart în două categorii – algoritmi simetrici (sau cu o cheie secretă) şi algoritmi asimetrici (sau cu pereche de chei – cheie privată, sau secretă, şi cheie publică).

Alţi algoritmi utilizaţi frecvent sunt algoritmii cu funcţie de rezumat (hash), sau amprentă, care servesc în construirea semnăturilor digitale utilizate în procedurile de autentificare a documentelor, precum şi algoritmii care generează numere aleatoare.

Întrucât algoritmii trebuie cunoscuţi de prea multe părţi (beneficiari persoane fizice şi juridice, funcţionari publici, intermediari) ei nu mai sunt păstraţi secreţi, ci sunt publici şi standardizaţi, iar secretul se păstrează numai prin păstrarea secretă a cheilor.

Algoritmii simetrici folosesc o singură cheie, care trebuie cunoscută de toate părţile implicate, şi trebuie păstrată secretă. Cheia secretă e folosită atât la criptare cât şi la decriptare.

Algoritmii asimetrici folosesc două chei, o cheie secretă, sau privată, şi o cheie publică, formând o pereche în care cele două chei sunt legate între ele printr-o relaţie matematică specifică algoritmului. Această relaţie între chei este de o asemenea natură încât dacă se cunoaşte o cheie (cea publică) nu este practic fezabil (chiar cu calculatoare puternice), în prezent, să se obţină cealaltă cheie (cea secretă), deşi, teoretic vorbind, acest lucru este posibil. O informaţie criptată cu una din chei poate fi decriptată numai cu cealălaltă cheie.

Cheia privată e ţinută secretă de fiecare entitate expeditoare şi este folosită pentru a cripta mesajele pe care le expediază către celelalte entităţi receptoare din sistem. Entităţile receptoare pot decripta mesajul criptat dacă au cheia publică a entităţii expeditoare. Desigur entitatea expeditoare trebuie să distribuie cheia sa

publică, care nu este secretă, către toate entităţile receptoare din sistem cu care doreşte să schimbe informaţii confidenţiale. În acest fel fiecare entitate dispune de o pereche de chei, din care pe cea privată o ţine secretă, iar pe cea publică o distribuie tuturor celorlalte entităţi. La rândul lor entităţile receptoare pot folosi cheia publică a entităţii expeditoare pentru a cripta mesaje pe care le trimit entităţii expeditoare şi care nu pot fi decriptate decât cu cheia privată – perechea celei publice, şi aflată numai la entitate expeditoare. În acest fel ambele chei, cea privată şi cea publică, servesc atât la criptare cât şi la decriptare. De remarcat acum că această modalitate de criptare-decriptare asimetrică poate servi şi la autentificarea identităţii entităţii expeditoare, deoarece numai aceasta deţine cheia privată, iar o decriptare corectă cu cheia sa publică poate servi ca dovadă de autenticitate a entităţii expeditoare, singura care deţine cheia privată cu care s-a făcut criptarea.

Algoritmii asimetrici prezintă o serie de avantaje faţă de algoritmii simetrici (se evită de exemplu procedura potenţial periculoasă de a distribui unica cheie secretă multelor entităţi participante), şi asigură şi un grad mai mare de siguranţă (dar implementarea lor e mai complicată şi costă mai mult).

În figura A1-1 se prezintă schematic procesul de criptare-decriptare şi algoritmii simetrici şi asimetrici.

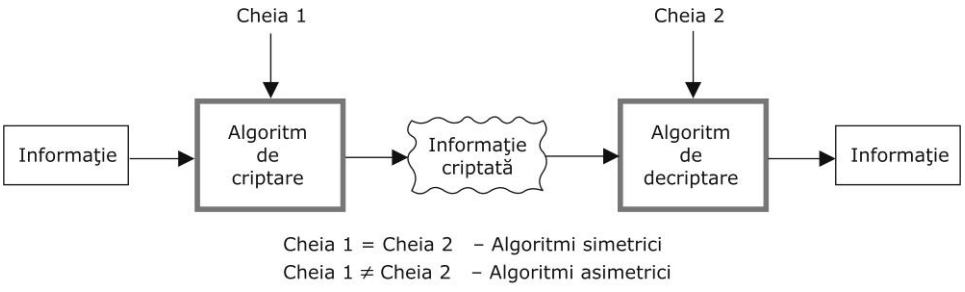

Figura A1-1. Algoritmi de criptare-decriptare

a) Algoritmi simetrici

Algoritmii simetrici cei mai folosiţi în domeniu sunt algoritmul DES (Data Encription Standard), şi varianta sa mai nouă 3DES (Triple DES). Algoritmul DES foloseşte o cheie secretă de 56 biţi iar algoritmul 3DES este o variantă a sa mult mai sigură, pentru că poate folosi până la 3 chei diferite de 56 biţi fiecare. Evident toate cele 3 chei trebuie distribuite tuturor participanţilor la sistem şi trebuie păstrate secrete (ceea ce constituie o problemă practică uneori dificilă).

Algoritmul DES a fost proiectat de compania americană IBM în 1972 şi a fost adoptat ca standard naţional american în 1977. În 1998 un text criptat cu DES a fost

´spart´ de un echipament special care a lucrat 4,5 zile continuu. Ca urmare algoritmul a fost înlocuit cu o variantă a sa, 3DES, de până la trei ori mai lentă, dar de câteva miliarde de ori mai sigură, întrucât lucrează cu trei chei de câte 56 biţi fiecare. Algoritmul 3DES se descrie simplu prin: $C = E_{K3}(D_{K2}(E_{K1}(L)))$, unde L e textul lizibil, C este textul criptat care rezultă, E este procedura de criptare obişnuită DES, D este procedura de decriptare DES, iar $K_{1,2,3}$ sunt trei chei de 56 biţi fiecare. Pentru a obţine textul criptat C se criptează mai întâi cu K_1 textul L, apoi rezultatul se decriptează cu K_2, iar acest rezultat se criptează din nou cu K_3. Decriptarea se face invers: $L=D_{K1}(E_{K2}(D_{K3}(C)))$. Pentru a mai reduce din volumul de memorie necesar pentru chei, se poate lucra numai cu două chei diferite (caz în care $K_3 = K_1$), sau chiar cu o singură cheie ($K_3 = K_2 = K_1$).

De remarcat că dacă un număr binar are o lungime de n biţi atunci numărul zecimal care îi corespunde are aproximativ n/3,3 cifre zecimale, deci o cheie binară de 512 biţi este un număr zecimal cu 155 de cifre zecimale, adică ceva de forma 10^{155} (a se compara cu numărul total de atomi din univers, estimat la 10^{77}), iar descoperirea prin încercări a unei astfel de chei necesită o enormă putere de calcul, indisponibilă în prezent.

Alţi algoritmi simetrici sunt AES (adoptat recent de guvernul american pentru a înlocui DES; foloseşte chei de până la 256 biţi), IDEA (cu cheie de 128 biţi), CAST–128, RC6 şi Twofish.

b) Algoritmi asimetrici

Cei mai folosiţi algoritmi asimetrici, cu pereche de chei secretă-publică, sunt algoritmii RSA şi ECC. Cheile, secretă şi publică, sunt de lungime egală, iar cu cât o cheie e mai lungă cu atât e mai greu de decriptat, în mod fraudulos, un şir de biţi criptat cu acea cheie.

Algoritmul RSA (numit după numele inventatorilor Rivest, Shamir, Adleman) foloseşte chei secrete şi publice de 1024 de biţi fiecare şi, pentru o securitate deosebită, chiar chei de 2048 de biţi.

Algoritmul ECC (Elliptic Curve Cryptosystem) pare a fi succesorul lui RSA prin faptul că este de circa 10 ori mai rapid, este mult mai sigur, şi foloseşte chei mai scurte, de 160 de biţi.

Alţi algoritmi asimetrici sunt algoritmii Diffie-Hellman, Elgamal, Fortezza şi DSA (Digital Signature Algorithm) (1).

c) Algoritmi rezumat sau amprentă (Hash Algorithms)

Algoritmii rezumat (Hash Algorithms) sunt proceduri (fără cheie) care se aplică unui text (informaţie) de orice lungime, pentru a produce la ieşire un rezumat (digest) al textului, de lungime fixă, care reprezintă textul, fiind un fel de ´amprentă´ (thumbprint, fingerprint) a acestuia. Algoritmul este de tipul mulţi-către-unul (many-to-one) ceea ce înseamnă că pot exista mai multe texte care conduc la acelaşi rezumat. Rezumatul, sau amprenta, are proprietăţile că orice modificare în textul iniţial produce un alt rezumat, şi, dat fiind un rezumat, este imposibilă reconstituirea textului iniţial care l-a generat, şi este practic imposibilă (computaţional nefezabil) găsirea unui alt text, diferit de cel iniţial, care să producă acelaşi rezumat. Evident acest rezumat va putea fi folosit pentru a depista schimbări în textul iniţial. Algoritmii rezumat produc de regulă rezumate de 128 biţi sau 160 de biţi, rezumate care sunt folosite în semnăturile digitale din procedeele de autentificare. Rezumatul serveşte la a proba că textul este integru, adică nu a fost alterat.

Cei mai răspândiţi algoritmi rezumat sunt MD5 şi SHA-1. MD5 (Message Digest, version 5) produce un rezumat de 128 biţi pentru un text (informaţie binară) la intrare de orice lungime. SHA-1 (Secure Hash Algorithm, version 1) produce un rezumat de 160 de biţi, şi pare a urma să-l înlocuiască pe MD5 pentru că este considerat mai sigur.

d) Algoritmi care generează numere aleatoare

Numerele aleatoare sunt necesare în procedurile de securitate deoarece pot fi folosite în calitate de chei (de regulă de unică folosinţă) pentru diverşi algoritmi de criptare/decriptare (de exemplu în telecomunicaţii – protocoalele SSL şi TLS), precum şi în alte situaţii.

Algoritmii care generează numerele aleatoare folosite în sistemele criptografice utilizate în asigurarea securităţii sunt algoritmi pseudo-aleatori, realizaţi printr-un program care generează un şir de biţi (16 - 48 de biţi, de regulă, dar pot fi de practic orice lungime dorită) ce reprezintă numărul aleator. Există mulţi astfel de algoritmi şi fiecare sistem foloseşte de regulă proprii lui algoritmi. Standardul american ANSI X9.17, de exemplu, reglementează metodologia de generare a numerelor aleatoare şi pseudo-aleatoare.

3. Semnături digitale. Certificate de autenticitate şi sisteme de chei publice

Semnătura digitală a unei entităţi expeditoare, ataşată unui document (şir de biţi, numit şi mesaj) trimis unei entităţi receptoare, este un scurt bloc de date (şir de biţi) expediat împreună cu documentul, care dovedeşte că documentul este autentic, adică provine într-adevăr de la entitatea expeditoare, este nealterat (integru), iar expeditorul nu poate contesta, ulterior expedierii, că a trimis efectiv documentul (nonrepudiere). Există mai multe scheme de utilizare a semnăturilor digitale. Dintre acestea vom prezenta pe scurt o schemă care foloseşte criptografia asimetrică şi este folosită frecvent în domeniul plăţilor electronice, în cazul cardurilor inteligente, precum şi în comerţul electronic şi în afacerile electronice. În acest caz entităţile din sistem posedă fiecare câte o pereche de chei – una secretă, şi una publică. Fiecare entitate cunoaşte de asemenea cheile publice ale entităţilor cu care doreşte să schimbe informaţii sigure.

Semnătura digitală se compune dintr-un rezumat, sau amprentă, de exemplu de 160 biţi, al documentului, obţinut ca urmare a aplicării unei funcţii rezumat (de exemplu SHA-1), rezumat care este apoi criptat cu cheia secretă a expeditorului, şi trimis receptorului împreună cu documentul (care poate fi şi el criptat, sau nu) şi cu cheia publică. Receptorul decriptează semnătura digitală cu cheia publică a expeditorului, calculează el însuşi (folosind desigur acelaşi algoritm SHA-1) rezumatul documentului primit, şi-l compară cu rezumatul primit de la expeditor. Dacă cele două rezumate sunt egale aceasta înseamnă că: a) documentul este autentic, adică a fost într-adevăr expediat de expeditor pentru că numai el are cheia secretă cu care a fost criptat rezumatul; b) documentul e integru (nu a fost alterat pe parcursul transmiterii) pentru că rezumatul calculat de receptor coincide cu rezumatul venit de la expeditor; c) expeditorul nu poate nega că a trimis documentul deoarece numai el dispunea de cheia cu care a fost criptată semnătura primită de receptor. În figura A1-2 se prezintă schema de principiu a semnării digitale şi a verificării semnăturii digitale.

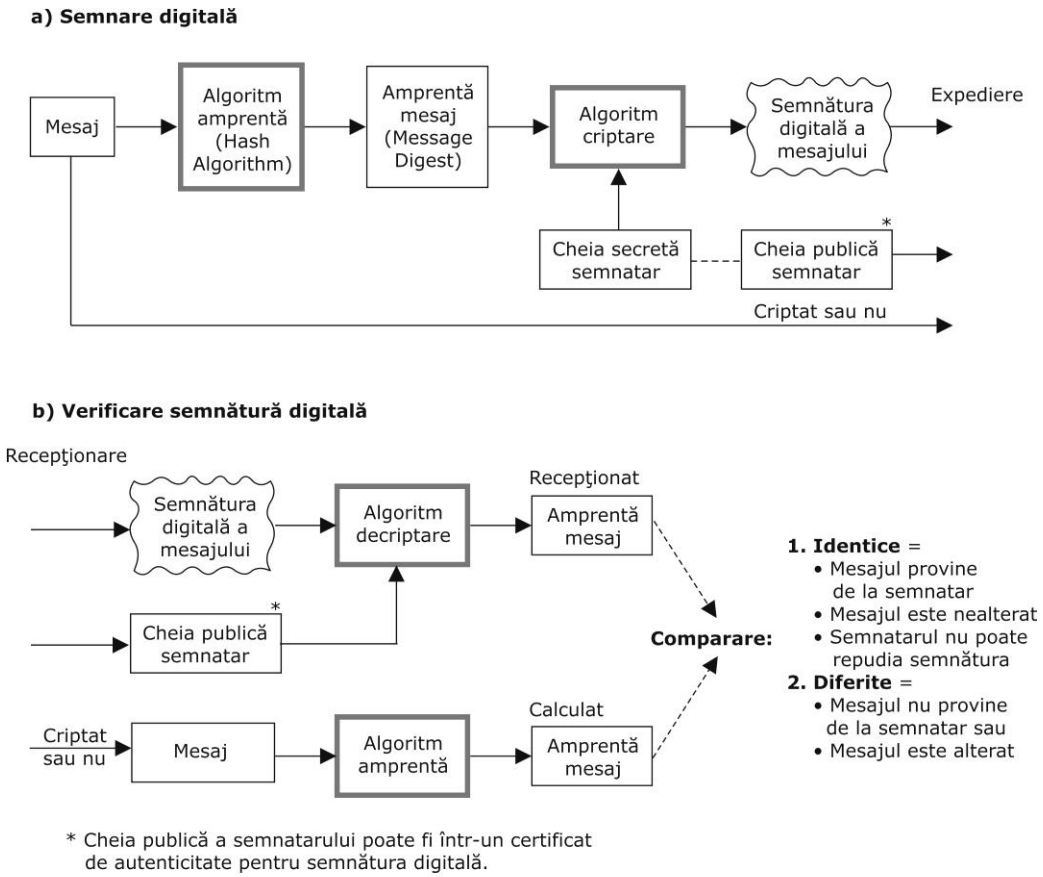

Figura A1-2. Semnătura digitală

Întrucât funcţia de amprentare nu este biunivocă, se poate găsi, teoretic vorbind, un alt document care să producă aceiaşi amprentă, dar această căutare este practic nefezabilă, chiar folosind calculatoare foarte puternice – dacă semnătura are 160 de biţi înseamnă că există circa 10^{48} amprente diferite pe cel puţin tot atâtea documente. Semnătura digitală trebuie asociată neaparat cu documentul semnat întrucât nu are sens decât împreună cu acesta.

Un dezavantaj al acestei metode de semnare a documentelor este faptul că fiecare entitate participantă în sistem trebuie să dispună de cheile publice ale tuturor celorlalte entităţi. Acest dezavantaj este eliminat prin schemele de autentificare care folosesc certificate de autenticitate emise de o Autoritate de Certificare (AC). În acest caz există de asemeni mai multe scheme de autentificare.

O Autoritate de Certificare, AC (CA, Certification Authority), este o entitate specială şi centrală, în care toate celelalte entităţi decid că au completă încredere. AC

verifică mai întâi fiecare entitate, după care îi eliberează (asumându-şi responsabilitatea) un certificat de autenticitate, pe care această entitate îl va folosi în schimbul de informaţii cu celelalte entităţi pentru a-şi dovedi autenticitatea, certificatul fiind făcut public.

Certificatul de autenticitate este un bloc de date (şir de biţi) criptat care cuprinde cel puţin două părţi: datele de identitate ale entităţii certificate (nume, cod, adresă, etc.) şi cheia publică a entităţii. Am putea scrie, simbolic, certificatul C_{AC} generat de AC pentru entitatea E, ca fiind $C_{AC}=S_{K\text{-}AC}$ (ID_E, K_E), unde ID şi K sunt identitatea şi cheia publică ale lui E, S este semnătura lui AC, iar K-AC este cheia secretă a lui AC, cu care criptează certificatul. Certificatul de autenticitate, care e criptat cu cheia secretă a Autorităţii de Certificare, mai conţine, printre altele, numărul certificatului, identitatea şi semnătura digitală a AC care a dat certificatul, precum şi perioada de valabilitate a certificatului. Semnătura digitală a AC, aflată într-un certificat, mai poate conţine şi o marcă de timp (time stamp) care probează că certificatul a fost emis în perioada de valabilitate a certificatului. Certificatele acordate sunt apoi făcute publice pe Internet. Certificatul de autenticitate a unei identităţi este, în esenţă, o legătură între acea identitate şi cheia sa publică (fie că această cheie este una de identitate, fie că este una folosită pentru semnătura digitală, când se mai numeşte şi cheie de nonrepudiere, acestea două putând fi diferite).

Certificatele de autenticitate internaționale sunt reglementate de standardul ISO/ITU X.509. Autorităţi de Certificare mai cunoscute, cu acoperire globală, sunt de exemplu companiile VeriSign şi Thawte în SUA, şi Globalsign în Belgia. În România există din 2004 compania e-Sign (www.e-sign.ro) care emite (în parteneriat cu VeriSign, care e autoritatea rădăcină) semnături digitale (şi certificate de server) conform legii române a semnăturii electronice. Dacă o AC este autorizată legal să emită certificate atunci aceste certificate au valabilitate juridică.

Dacă două entităţi din sistem doresc să comunice într-un mod sigur atunci vor cere fiecare în parte câte un certificat de autenticitate de la AC, pe care apoi şi-l vor trimite una alteia. Cum toate entităţile cunosc cheia publică a AC, vor decripta certificatul de autenticitate şi vor obţine astfel identitatea autentică şi cheia publică a celeilalte entităţi, cu care vor putea apoi comunica sigur, criptându-şi informaţiile pe care le expediază cu cheia publică a receptorului.

Acest sistem de autentificare, care presupune că există o Autoritate de Certificare iar fiecare entitate din sistem dispune de una, sau mai multe, perechi de chei (secretă, publică) proprii, precum şi de cheia publică a AC, se numeşte un

Sistem (sau o Infrastructură) de Chei Publice (PKI, Public Key Infrastructure; aceasta conţine şi alte elemente, cum ar fi Depozitul public de certificate, Lista certificatelor revocate, etc., dar nu mai intrăm în detalii). Într-un astfel de sistem este posibilă existenţa unei ierarhii de Autorităţi de Certificare, în care o AC principală, numită rădăcină (Root Certification Authority), certifică mai multe AC de nivel mai jos, care, la rândul lor, certifică mai multe AC de nivel şi mai jos, etc. La ultimul nivel de jos se află AC care vând efectiv certificatele de autenticitate. Cumpărătorul unui astfel de certificat va verifica autenticitatea AC care i-a generat certificatul mergând în sus pe ierarhia de AC, până la AC rădăcină, în care trebuie să aibă încrederea ultimă. O variantă de Sistem de Chei Publice este implementată pentru telefoane mobile (WPKI, Wireless PKI), servind în cazul în care certificatele de autenticitate de identitate şi de semnătură digitală se află în mobil (în cipul de SIM).

Note şi bibliografie

1. Payment Technologies for E-Commerce, Weidong Kou, Editor, Springer Verlag, 2003. Cartea cuprinde câteva capitole interesante şi utile de criptografie şi biometrică.

2. Caracteristicile biometrice se folosesc în special în cazul identificării şi controlului accesului (acces fizic – prin uşi, porţi, puncte de trecere, şi acces logic – la calculatoare şi reţele, inclusiv Internet). Într-o lucrare recentă (Februarie 2004) a guvernului american se găseşte o prezentare a problemelor de biometrică, cu referire şi la cardurile cu cip de identitate şi control acces. Puteţi vedea raportul public US General Services Administration, Government Smart Card Handbook, February 2004, la adresa www.smartcardalliance.org/pdf/industry_info/ smatcardhandbook.pdf.

3. A se vedea de exemplu ´Introduction to Cryptography: Principles and Applications´, Hans Delfs, Helmut Knebl, Springer, 2002. Este o prezentare a elementelor de criptografie utilizate în general în tehnologia calculatoarelor şi telecomunicaţiilor şi utile în special în domeniul securităţii.
