**Certificate digitale în comerţul electronic**

1. **Semnătura digitală**
   1. **Definire şi informaţii**

O semnatura digitala reprezinta o informatie care il identifica pe expeditorul unui document. Semnatura digitala este creata prin criptarea continutului documentului, folosind cheia criptografica a expeditorului. Aceasta face ca semnatura sa fie unica atat pentru fisier cat si pentru detinatorul cheii. Orice modificari aduse documentului afecteaza semnatura, oferindu-se astfel atat integritate cat si autentificare. Semnaturile digitale utilizeaza criptarea asimetrica, in care se foloseste o cheie pentru a crea semnatura si o alta cheie, legata de prima, pentru a o verifica. Intr-un sistem de securitate a cheii publice, toti participantii au nevoie de propria cheie de semnare, sau cheie privata. Cheia publica este raspandita si identificata de catre certificatele digitale. Certificatele sunt emise de terti de incredere, cunoscuti sub numele de autoritati de certificare (AC), care isi asuma responsabilitatea pentru identificarea utilizatorilor si pentru acordarea cheilor. AC-urile sunt deseori administrate de companii care sunt in masura sa garanteze pentru dreptul de desfasurare a afacerii. In mod asemanator, companiile mari pot folosi AC-uri interne organizationale pentru a identifica personalul si functia fiecaruia, in scopul autentificarii tranzactiilor de comert electronic.

* 1. **Istoric**

În 1976, Whitfield Diffie și Martin Hellman au descris pentru prima dată noțiunea de schemă de semnătură digitală, cu toate ca ei presupuneau că există astfel de sisteme bazate pe funcții care sunt permutări-trapă, în sens unic. Curând după aceea, Ronald Rivest, Adi Shamir, și Len Adleman au inventat algoritmul RSA, care poate fi utilizat pentru a produce semnături digitale primitive (deși numai ca demonstrație –semnăturile RSA „simple” nu sunt sigure). Primul pachet de software comercializat pe scară largă care a oferit semnătură digitală a fost IBM Lotus Notes⁠ 1.0, lansat în 1989, care folosea algoritmul RSA.

Alte scheme de semnătură digitală au fost elaborate curând după RSA, cele mai vechi fiind semnăturile Lamport⁠, semnăturile Merkle (denumite și „arbori Merkle” sau mai simplu „arbori hash”), și semnătura Rabin⁠.

În 1984, Shafrira Goldwasser⁠, Silvio Micali⁠, și Ronald Rivest au devenit primii care au definit riguros cerințele de securitate pentru schemele de semnături digitale. Ei au descris o ierarhie de modele de atacuri asupra schemelor de semnătură, și au prezentat și schema de semnătură GMR, prima despre care se putea demonstra că previne chiar și un fals existențial împotriva unui mesaj de atac ales, care este în prezent definiția acceptată a securității schemelor de semnătură. Primul astfel de sistem, care nu este construit pe baza funcțiilor-trapă, ci mai degrabă pe o familie de funcții cu o cerință mult mai relaxată a acestor permutări cu sens unic, a fost prezentat de către Moni Naor⁠ și Moti Yung.

* 1. **Aplicații ale semnăturilor digitale**

Pe măsură ce organizațiile s-au îndepărtat de documentele pe hârtie cu semnături olografe sau cu ștampile de autenticitate, semnăturile digitale oferă un plus de asigurare a dovezii provenienței, identității și stării unui document electronic, precum și recunoașterea consimțământului informat și aprobarea sa de către semnatar. Government Printing Office (GPO) din Statele Unite publică versiunile electronice ale bugetului, ale legilor publice și private, precum și procesele legislative din Congres cu semnături digitale. Universități, între care Penn State, Universitatea din Chicago, și Stanford publică matricolele studenților cu semnătură digitală.Mai jos sunt câteva motive comune pentru care se recurge la semnătura digitală pentru comunicații:

* **Autentificare:** Deși mesajele pot adesea să includă informații despre entitatea care trimite un mesaj, informațiile pot să nu fie corecte. Semnăturile digitale pot fi utilizate pentru a autentifica sursa mesajelor. Atunci când proprietatea asupra cheii secrete a semnăturii digitale este legată de un anumit utilizator, o semnătură validă arată că mesajul a fost trimis de către acel utilizator. Importanța încrederii mari în autenticitatea expeditorului este evidentă mai ales într-un context financiar. De exemplu, presupunem că filiala unei bănci trimite instrucțiuni către biroul central pentru a solicita o schimbare a balanței unui cont. Dacă oficiul central nu este convins că un astfel de mesaj este cu adevărat trimis de la surse autorizate, a răspunde favorabil unei asemenea cereri ar putea fi o greșeală gravă.
* **Integritatea:** În multe scenarii, expeditorul și destinatarul unui mesaj ar putea avea nevoie de încredere că mesajul nu a fost modificat în timpul transmisiei. Deși criptarea ascunde conținutul unui mesaj, un atacator ar putea schimba un mesaj criptat fără a-l și înțelege. (Unii algoritmi de criptare, cunoscuți sub numele de algoritmi nonmaleabili⁠, împiedică acest lucru, dar alții nu.) Cu toate acestea, dacă un mesaj este semnat digital, orice schimbare asupra mesajului îi anulează semnătura. În plus, nu există nicio modalitate eficientă de a modifica un mesaj și semnătura lui astfel încât să rezulte un mesaj nou cu o semnătură validă, pentru că acest lucru este considerat a fi de imposibil din punct de vedere computațional din cauza nivelului de securitate al celor mai multe funcții hash criptografice.
* **Non-repudierea⁠:** Non-repudierea, sau, mai precis, non-repudierea originii, este un aspect important al semnăturii digitale. Prin această proprietate, o entitate care a semnat unele informații nu mai poate, la un moment ulterior, să nege faptul că a semnat-o. Similar, accesul doar la cheia publică nu permite falsificarea unei semnături valide de către un terț.
* Aceste proprietăți de autentificare, non-repudiere etc. sunt valabile în condițiile în care cheia secretă de nu a fost revocată înainte de utilizarea ei. Revocarea publică a unei perechi de chei este o abilitate necesară, altfel scurgerile de chei secrete pe alte canale vor duce la implicarea perpetuă a pretinsului proprietar al perechii de chei. Verificarea stării de revocare impune o verificare „on-line”; de exemplu, verificarea unei liste de certificate revocate⁠ sau prin intermediul Online Certificate Status Protocol⁠. Foarte aproximativ, acest lucru este analog cu un furnizor care primește carduri de credit, care verifică în primul rând on-line la emitentul cardului pentru a afla dacă un anumit card a fost declarat pierdut sau furat. Desigur, cu perechile de chei furate, furtul este adesea descoperit numai după ce cheia secretă este utilizată, de exemplu, pentru a semna un certificat fals în scopuri de spionaj.

1. **Certificatul digital**
   1. **Definire si informatii**

Un certificat digital este o carte de identitate electronică (un element software) care conţine informaţiile de identificare ale posesorului şi este folosit pentru afaceri sau tranzacţii pe www. Este emis de o autoritate de certificare (CA). Conţine numele deţinătorului, un număr serial (unic), data de expirare, o copie a cheii publice a deţinătorului şi semnătura electronică a autorităţii de certificare pentru a se putea verifica autenticitatea certificatului. Unele certificate digitale se conformează unui standard (ex: X.509). Certificatele digitale pot fi stocate în regiştri iar utilizatorii autentificaţi pot accesa cheile publice ale altor utilizatori si este utilizat pentru autentificarea online

Certificatul digital este utilizat pentru o gamă variată de tranzacţii electronice ce include e-mail, comerţul electronic, transferul electronic de fonduri. În mod obişnuit, comerţul electronic impune şi utilizarea unui certificat pentru securizarea serverului. Certificatul digital reprezintă un instrument în stabilirea unui canal securizat pentru comunicarea informaţiilor confidenţiale.

Orice persoană care doreşte să obţină un certificat digital se adresează mai întâi unei autorităţi de certificare autorizată. Orice autoritate de certificare solicită utilizatorului informaţii minime privind identitatea acestuia, înainte de a-i elibera acest certificat. După furnizarea acestor informaţii şi verificarea lor, autoritatea de certificare respectivă aprobă sau respinge, după caz, cererea formulata de către acea persoană.

Certificatul digital se utilizează atunci când când se primesc mesaje semnate digital, putând verifica certificatul digital al semnatarului pentru a afla daca acesta nu e falsificat.   
În momentul în care se trimit mesaje, acestea se pot semna şi se poate alătura certificatul digital pentru a asigura destinatarul că acel mesaj a fost trimis chiar de dvs. Pot fi alaturate mai multe certificate digitale, care formează un lanţ de certificare, în care un certificat digital asigură autenticitatea certificatului anterior. La cel mai înalt nivel al ierarhiei se află o autoritate de certificare credibilă fără a avea un certificat digital emis de altă autoritate. Cheia publică a autorităţii de certificare de la cel mai înalt nivel trebuie să fie recunoscută în mod independent (publicată pe scară largă). De asemenea, certificate digitale se pot folosi şi pentru a accesa un site web securizat în calitate de membru al acestuia.

Certificatul digital foloseşte tehnici de criptare cu cheie publică utilizând o pereche de chei, legate între ele, o cheie publică şi o cheie privată. În procedeul criptării cu cheie publică, cheia publică este disponibilă pentru oricine vrea să comunice cu posesorul acelei perechi de chei. Cheia publică poate fi utilizată pentru a verifica un mesaj semnat cu cheie privată sau pentru a cripta un mesaj ce poate fi decriptat folosind doar cheia privată. Securitatea mesajelor criptate se bazează pe securitatea cheii private, ce trebuie protejată împotriva utilizării neautorizate.

Într-un certificat digital, perechea de chei este evidenţiată de numele utilizatorului şi alte informaţii de identificare. Certificatul digital funcţionează ca un mijloc electronic credibil ce poate fi verificat de site. Aceasta permite certificatelor digitale să înlocuiască modalitatea furnizării unei parole pentru a accesa informaţii confidenţiale sau de a restricţiona accesul utilizatorilor ocazionali.

Un certificat digital este semnat de către autoritatea de certificare care emite acel certificat. Cea mai înalta autoritate din cele din lanţul de încredere a certificatului trebuie sa fie o autoritate independentă, cunoscută şi credibilă pentru beneficiar.

Datele cuprinse în certificatul digital sunt: prenumele persoanei, numele persoanei , adresa de e-mail, societatea în care lucrează, funcţia persoanei , User Windows Domain( cont utilizator domeniu), ţara în care îşi desfăşoară activitatea.

De asemenea certificatul conţine date privind autoritatea de certificare emitenta (Organization, Organization Unit), versiunea, extensiile certificatului, numărul serial, algoritmul de semnare, perioada de valabilitate, cheia publică, punctul de distribuţie al certificatelor revocate).

Adresa de e-mail solicitată reprezintă adresa de e-mail căreia i se va ataşa certificatul digital, de pe care se vor putea trimite mesaje semnate sau criptate. Adresa de e-mail trebuie să reprezinte un cont de e-mail existent, valid, tip organizaţie. Nu se pot asocia certificate digitale unor adrese de e-mail de pe internet (yahoo, hotmail, etc.)

* 1. **Campuri comune**

Acestea sunt unele dintre cele mai frecvente câmpuri din certificate. Cele mai multe certificate conțin un număr de câmpuri care nu sunt enumerate aici. Rețineți că, în ceea ce privește reprezentarea X.509 a unui certificat, un certificat nu este „plat”, ci conține aceste câmpuri imbricate în diferite structuri din certificat.

* **Număr de serie:** utilizat pentru a identifica în mod unic certificatul în cadrul sistemelor unei CA. În special, acesta este utilizat pentru a urmări informațiile de revocare.
* **Subiect:** entitatea căreia îi aparține un certificat: o mașină, un individ sau o organizație.
* **Emitent:** entitatea care a verificat informațiile și a semnat certificatul.
* **Nu înainte:** cea mai timpurie dată și dată la care certificatul este valabil. De obicei setat la câteva ore sau zile înainte de momentul emiterii certificatului, pentru a evita problemele de înclinare a ceasului.
* **Nu după:** ora și data în care certificatul nu mai este valabil.
* **Utilizare cheie:** utilizările criptografice valide ale cheii publice a certificatului. Valorile comune includ validarea semnăturii digitale, cifrarea cheilor și semnarea certificatului.
* **Utilizare cheie extinsă:** Aplicațiile în care poate fi utilizat certificatul. Valorile comune includ autentificarea serverului TLS, protecția prin e-mail și semnarea codului.
* **Cheie publică:** o cheie publică aparținând subiectului certificatului.
* **Algoritm de semnătură:** algoritmul utilizat pentru semnarea certificatului de cheie publică.
* **Semnătură:** O semnătură a organismului de certificat de către cheia privată a emitentului.
  1. **Autorităţi de certificare**

În modelul de încredere X.509, o autoritate de certificare (AC) este responsabilă pentru semnarea certificatelor. Aceste certificate acționează ca o introducere între două părți, ceea ce înseamnă că o AC acționează ca o terță parte de încredere. O AC procesează solicitările de la persoane sau organizații care solicită certificate (numiți abonați), verifică informațiile și poate semna un certificat de entitate finală pe baza informațiilor respective. Pentru a îndeplini acest rol în mod eficient, o AC trebuie să aibă unul sau mai multe certificate rădăcină sau certificate intermediare de încredere și cheile private corespunzătoare. AC-urile pot obține această încredere largă prin includerea certificatelor rădăcină în software-ul popular sau prin obținerea unei semnături încrucișate de la o altă autoritate de delegare a AC Alte AC sunt de încredere într-o comunitate relativ mică, cum ar fi o companie, și sunt distribuite prin alte mecanisme, cum ar fi politica de grup Windows.

Autoritățile de certificare sunt, de asemenea, responsabile de menținerea informațiilor de revocare actualizate despre certificatele pe care le-au emis, indicând dacă certificatele sunt încă valabile. Acestea furnizează aceste informații prin Protocolul de stare a certificatelor online (OCSP) și / sau Listele de revocare a certificatelor (CRL). Unele dintre autoritățile de certificare mai mari de pe piață includ IdenTrust, DigiCert și Sectigo.

1. **Bibliografie:**
2. Cursul 6
3. <https://ro.wikipedia.org/wiki/Semn%C4%83tur%C4%83_digital%C4%83>
4. <https://en.wikipedia.org/wiki/Public_key_certificate>
5. <https://graduo.ro/referate/calculatoare/certificat-digital-115258>
6. <https://biblioteca.regielive.ro/referate/calculatoare/autentificarea-prin-semnatura-digitala-inteligenta-artificiala-2471.html>