Universitatea “Politehnică” din București

Facultatea de Electronică, Telecomunicații și Tehnologia Informației

**Student: Pătrașcu Cosmin-Mihnea**

**Disciplina: RCI**

**Master: SIVA, anul II**

|  |
| --- |
| Cuprins:  [1. Introducere 3](#_Toc378363920)  [1.1 Controlul legal al accesului 3](#_Toc378363921)  [1.2 Tipuri de clasificări 4](#_Toc378363922)  [1.3 Principiile protejării informaţiilor speciale 5](#_Toc378363923)  [1.4 Roluri şi responsabilităţi în procesul de clasificare a informaţiilor 6](#_Toc378363924)  [1.5 Tipuri de control al accesului în sistem 7](#_Toc378363925)  [1.6 Identificarea şi autentificare 8](#_Toc378363926)  [1.7 Autentificarea utilizatorilor 9](#_Toc378363927)  [1.8 Autentificarea documentelor 10](#_Toc378363928)  [2. Semnătura digitală/electronică 12](#_Toc378363929)  [3. Certificate 14](#_Toc378363930)  [4. Tehnologii de autentificare 16](#_Toc378363931)  [4.1. Token 16](#_Toc378363932)  [4.2. Carduri smart 17](#_Toc378363933)  [I. Concluzii 19](#_Toc378363934)  [II. Bibliografie 20](#_Toc378363935) Introducere O dată cu dezvoltarea internetului tot mai multe activităţi, cum ar fi socializarea, tranzacţiile bancare, plăţile la utilitaţi, shopping-ul, chiar şi arhivarea documentelor s-au mutat din mediul fizic în cel virtual.  Datorită faptului că, din ce în ce mai multe informaţii confidenţiale sunt stocate în mediul on-line, există tot mai multe persoane tentate să atace bazele de date cu scopul de a sustrage informaţii confidenţiale sau pur şi simplu sunt rău voitoare. O metodă de contracarare a acestor atacuri este clasificarea informaţiillor iar accesul la acestea să fie în funcţie de tipul utilizatorilor. O soluţie pentru verificarea tipului utilizatorului este prin autentificare. |

Clasificarea informaţiilor constă în etichetarea acestora în funcţie de importanţa lor. Etichetarea se realizează de la cel mai de jos nivel, unde se situează informaţiile deschise sau neclasificate, la cele confidenţiale, urcând spre informaţii secrete şi strict secrete. Informaţiile secrete sunt cele prin a căror compromitere sunt puse în pericol vieţile umane iar compromiterera celor strict secrete pune în pericol viaţa mai multor persoane.

# Controlul legal al accesului

Controlul legal al accesului îşi exercită forţa pe baza legilor existente (legea securităţii naţionale), prin care sunt stabilite două tipuri de structuri de control: *ierarhizate* şi *neierarhizate*. [1]

*Structura ierarhizată* încadrează informaţiile senzitive în patru categorii:

1. strict secrete: sunt într-o anumită măsură compartimentare, se numesc informaţii senzitive compartimentate şi presupun o atenţie deosebită la întrebuinţare
2. secrete
3. confidenţiale
4. neclasificate

Doar o categorie de informaţii este superioară informaţiilor secrete compartimantate, şi anume despre informaţiile din planul operativ integrat unic sau răspunsul naţional în caz de război.

În *structura neierarhizată*, sunt două categorii:

1. compartimentate: pot avea nume scurte, sugestive, care să scoată în relief anumite aspecte;
2. cu obiecţii sau ascunse vederii unor categorii de persoane: priveşte în special naţionalitatea potenţialilor cititori şi autori ai obiectelor.

În cazul procesului de clasificare a informaţiilor se parcurg trei etape:

* stabilirea nevoii de clasificare
* determinarea nivelului de clasificare
* determinarea duratei de clasificare

# Tipuri de clasificări

**La nivel naţional**, guvernul clasifică informaţiile în subiective şi obiective [1]:

*Informaţiile subiective* se mai numesc şi "*secrete adevărate*" sau *informaţii operaţionale*. Cât timp guvernul controlează şi protejează informaţiile pe baza cărora ia decizii, acele informaţii nu pot fi dezvăluite independent de către adversar.

Aceste informaţii au următoarele caracteristici:

* *dimensiune redusă* – secretul poate fi exprimat doar prin câteva cuvinte; din care cauză poate să fie uşor furat şi distribuit altora;
* *perceptibilitate universală* – nu este nevoie de pregătire specială pentru a înţelege secretul, oricine poate să-l fure;
* *supuse arbitrarului* – pentru a intra în posesia lor un adversar le poate fura, secretul nu poate fi descoperit independent;
* *conţinutul poate fi schimbat* – secretul poate fi modificat şi în ultima clipă;
* *sunt perisabile după scurt timp* – secretele au o viaţă scurtă, el poate fi ţinut doar pentru o perioadă scurtă de timp.

*Informaţiile obiective* sunt acelea care chiar dacă sunt descoperite, dezvoltate sau controlate de către guvern, pot fi deja cunoscute sau descoperite independent de o altă ţară. În această categorie intră informaţiile ştiinţifice sau secretele ştiinţifice.

Informaţiile obiective au următoarele caracteristici:

* *sunt confuze* – de regulă, nu se bazează pe o formulă magică, pentru descrierea informaţiilor ştiinţifice sunt necesare rapoarte lungi, din această cauză ele nu se pot transmite uşor;
* *pot fi înţelese numai de oamenii de ştiinţă*;
* *nu sunt supuse arbitrarului* – şi alţii pot să afle răspunsul la o anumită întrebare ştiinţifică, dacă formulează întrebarea respectivă;
* *nu sunt supuse schimbării* – au caracter etern; un fenomen natural are o singură valoare;
* *pot avea o viaţă lungă ca secret* – alţii pot descoperi informaţiile în mod independent, dar o astfel de descoperire necesită mult timp, ceea ce va conduce la păstrarea secretului pentru o lungă perioadă de timp.

*Informaţiile tehnice – secrete obiective*

Această categorie nu se încadrează perfect într-una din cele anterioare. Informaţiile tehnice sunt de genul proiectelor şi execuţiilor tehnice (de exemplu ale unor noi arme), diferite de caracterul ştiinţific al proiectării.

Caracteristicile informaţiilor tehnice sunt asemănătoare celor ştiinţifice, dar există unele diferenţe. Faţă de informaţiile ştiinţifice, informaţiile tehnice nu sunt fenomene naturale, ci înseamnă o metodă, un proces, o tehnică sau un echipament angajate în crearea unui produs. Se poate afirma că informaţiile tehnice sunt utilizate pentru exploatarea informaţiilor ştiinţifice.

*Secrete comerciale*

Secretele comerciale includ informaţiile despre procesele de fabricaţie, reţetele unor produse, precum şi alte informaţii obiective care pot fi descoperite independent de către alţii. Multe secrete comerciale sunt asemănătoare informaţiilor ştiinţifice şi tehnice.

**La nivelul unei organizaţii**, informaţiile se încadrează în următoarele categorii [1]:

*Informaţii speciale* ***(S)*** – corespund informaţiilor strict secrete din clasificarea oferita de givern. Aceste informaţii necesită un control special, de unde le vine şi numele. În această categorie intră informaţiile şi materialele a căror dezvăluire ar duce la pierderea a 10% din profitul brut anual.

*Informaţii confidenţiale la nivel de unitate* **(C)**  – corespund informaţiilor secrete la nivel naţional. Această încadrare se atribuie informaţiilor şi materialelor a căror compromitere ar duce pa pierderea unui procent din profitul anual net.

*Informaţiile private* ***(P)***: cuprind informaţiile şi materialele a căror compromitere poate prejudicia statutul unei persoane din unitate sau al corporaţiei.

*Informaţii de uz intern* ***(R)***: prezintă restricţii în utilizare.

*Informaţii publice* ***(N)***, sau informaţii neclasificate.

La nivel guvernamental, orice informaţie neîncadrată într-una din categoriile speciale, sub incidenţa legii accesului liber la informaţiile publice, poate fi publicată de orice organ de presă scrisă, video sau audio, sub motivaţia că *"tot ceea ce nu este interzis este permis"*.

La nivelul organizaţiilor private, lucrurile stau invers, doar informaţiile care sunt specificate "pentru public" pot fi făcute publice, mergându-se pe principiul *"tot ceea ce nu este permis este interzis"*.

.

# Principiile protejării informaţiilor speciale

Pentru protejarea informaţiilor speciale se pot defini zece principii [1]:

*1. principiul delimitării autorizării*– repartizarea informaţiilor pe tipuri va consta într-o grupare ierarhică plus suma compartimentărilor în care se regăseşte informaţia. Autorizarea unei persoane presupune stabilirea sferei de exercitate a funcţiei şi ea constă din autorizarea pe criteriul ierarhic al persoanei plus suma autorizărilor compartimentărilor persoanelor din subordinea sa.

2. *principiul securităţii simple*– nici o persoană, dintr-o anumită subordonare, nu trebuie să vadă informaţia unei categorii care depăşeşte autorizarea sa.

3. *principiul stea* – nici o persoană nu va scrie ceva pe obiectele dintr-o categorie inferioară celei la care persoana are acces.

4. *primul principiu al integrităţii*– nici un program de calculator nu va accepta informaţii de la un program inferior lui, pe linia privilegiilor;

5. *al doilea principiu al integrităţii*– nici un program pentru calculator nu va scrie ceva într-un program superior lui, prin prisma privilegiilor;

6. *principiul etichetării* **–** fiecare purtător de informaţii va fi etichetat clar cu categoria informaţiilor conţinute, în format accesibil omului şi în format sesizabil de către echipamentele periferice;

7. *principiul clarificării* **–** nici o persoană sau procedură nu va schimba categoriile existente ale informaţiilor şi nici autorizările existente, conform unor proceduri în vigoare;

8. *principiul inaccesibilităţii*– nici o informaţie nu va fi lăsată la dispoziţia altor persoane sau procese, cu excepţia celor consemnate prin norme interne;

9. *principiul verificabilităţii*– pentru toate activităţile semnificative pe linia securităţii se vor crea înregistrări imposibil de şters, cu rolul facilitării verificării sistemului.

10. *principiul încrederii în software*– cât timp nici un calculator nu poate controla perfect respectarea principiilor anterioare, dar, totuşi, efectuează activităţi utile, încrederea în software va permite apariţia unor excepţii de la regulă, dacă este cazul.

Modurile de funcţionare prin care sistemele de prelucrare automată a datelor pot asigura protecţia informaţiilor speciale:

* *modul dedicat* – toate informaţiile prelucrate de sistem fac parte din aceeaşi categorie, iar persoanele sistemului posedă autorizaţie de acces la categoria respectivă;
* *modul sistem superior* – informaţiile prelucrate de sistem pot să aparţină unor categorii diferite, dar toate persoanele angajate în această operaţiune posedă autorizaţii care să le ofere accesul la nivelul cel mai ridicat al informaţiilor prelucrate;
* *modul controlat* – un sistem poate prelucra informaţii din categorii diverse şi persoanele să aibă autorizaţii diferite, iar sistemul se va baza pe restricţii fizice, prin care să se respecte toate principiile securităţii informaţiilor – operaţiune destul de dificilă.
* *modul securităţii stratificate* – sistemele prelucrează informaţii aparţinând diverselor categorii, iar personalul, de asemenea, dispune de autorizaţii diferite.

# Roluri şi responsabilităţi în procesul de clasificare a informaţiilor

Principalele roluri în procesul de clasificare le au proprietarul, utilizatorul sau custodele datelor clasificate.[1]

***Proprietarul informaţiilor*** poate fi administratorul sau directorul unei organizaţii. O astfel de persoană răspunde de averile informaţionale încredinţate. Spre deosebire de custode, proprietarul are responsabilitatea finală a protecţiei datelor şi răspunde în faţa legii în cazul neachitării de această obligaţie. Cu toate acestea, tendinţa actuală este de deplasare în afara unităţii, de externalizare, prin semnarea actelor de custodie.

Printre responsabilităţile unui proprietar se află:

* întreprinde demersuri pentru stabilirea nivelului de clasificare a informaţiilor, care înseamnă, de fapt, cerinţele organizaţiei de protejare a acestora;
* efectuează verificări periodice ale clasificărilor existente, în vederea adaptării la cerinţele organizaţiei;
* delegă responsabilitatea protejării datelor către un custode specializat şi autorizat.

***Custodele informaţiilor*** este cel care prestează un serviciu externalizat organizaţiei, delegându-i-se responsabilităţile pe linia protejării informaţiilor. Acest rol este îndeplinit de specialişti în tehnologii informaţionale. Dintre obligaţiile acestuia, amintim:

* efectuează copii de siguranţă periodice şi teste de rutină a validităţii datelor;
* efectuează restaurări de dare din copiile de siguranţă, când este cazul;
* întreţine datele înregistrate, în concordanţă cu politicile de clasificare a informaţiilor.

De multe ori, custodele trebuie să alcătuiască schema de clasificare a informaţiilor, preluând aceste împuterniciri de la proprietarul lor.

***Utilizatorul*** este considerat orice persoană, operator, angajat, persoană din afară, care foloseşte informaţiile. El este considerat consumator de date care are nevoie, zilnic, să acceseze informaţii pentru a-şi duce la îndeplinire obligaţiile de serviciu ce îi revin.

Obligaţiile utilizatorilor sunt:

* de a urma întocmai procedurile de funcţionare, definite prin politicile de securitate ale organizaţiei, şi să respecte normele publicate privind utilizarea informaţiilor;
* să acorde toată atenţia menţinerii informaţiilor în timpul activităţii prestate, după cum se stipulează în politicile de utilizare a informaţiilor emise de organizaţia proprietară. Ei trebuie să asigure protejarea împotriva accesului neautorizat la informaţiile clasificate;
* să folosească resursele informaţionale ale firmei numai în scopul urmărit de aceasta, nu şi în scop personal.

# Tipuri de control al accesului în sistem

Controlul accesului în sistem are rolul de a reducerea riscului la care sunt supuse sistemele şi pentru reducerea eventualelor pierderi. Controlul poate fi:

* *preventiv*are ca scop preîntâmpinarea apariţiei unor incidente în sistem.
* *detectiv*presupune descoperirea unor apariţii ciudate în sistem
* *corectiv*este folosit pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

Pentru a putea fi atinse obiectivele enumerate mai sus, controalele pot fi:

1. *administrative****:*** exercitate prin politici şi proceduri, instruire cu scop de conştientizare, verificări generale, verificări la locul de muncă, verificarea pe timpul concediilor şi o supraveghere exigentă.
2. *logice sau tehnice:*cuprinde restricţii la accesarea sistemului şi măsuri prin care se asigură protecţia informaţiilor. Din această categorie fac parte sistemele de criptare, cardurile de acces, listele de control al accesului şi protocoalele de transmisie.
3. *fizice****:*** reprezentate de gărzile de pază şi protecţie, securitatea clădirilor: sisteme de încuiere a uşilor, securizarea camerelor cu servere, protecţia cablurilor, separarea atribuţiilor de serviciu, şi nu în ultimul rând realizarea copiilor de siguranţă a fişierelor.

# Identificarea şi autentificare

Sistemul de securitate trebuie să discearnă care sunt persoanele autorizate, care sunt vizitatori şi care sunt categoriile neautorizate, acest lucru se realizează prin identificare şi autentificare.

***Autentificarea*** este definită ca procesul de verificare sigură a identităţii cuiva sau a ceva.

În cadrul autentificării deosebim trei cazuri:

1. *autentificarea a două sisteme de calcul*
2. *autentificarea identităţii unui utilizator către un sistem de calcul*
3. *autentificarea unui document*

*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.

Există mai multe modalităţi prin care un utilizator se poate autentifica în sistem. Acestea sunt autentificarea bazată pe parole, autentificarea bazată pe adresă şi autentificarea criptografică, [2]

*Autentificarea bazată pe parole*

Este cea mai simplă dintre metode şi presupune transmiterea în clar a parolei de acces.

Anumite sisteme de autentificare folosesc o parolă introdusă de utilizator pe post de cheie criptografică sau pentru generarea unor valori folosite ulterior în operaţii criptografice.

Această metodă de autentificare a apărut datorită dispozitivelor care nu ai putere de calcul proprie, deci nu pot efectua calcule criptografice de niciun fel.

*Autentificarea bazată pe adresă*

Autentificarea bazată pe adresă presupune că identitatea sursei se poate deduce din analiza adresei de reţea de la care provin pachetele. Ideea de bază este că fiecare computer memorează informaţii despre conturile altor sisteme care au acces la resursele sale.

*Autentificarea criptografică*

A apărut datorită creşterii puterii de calcul.

Această metodă de autentificare presupune existenţa unei chei de criptare, publică (asimetrică) sau secretă (simetrică) şi un algoritm de criptare/decriptare.

Ideea din spatele autentificării criptografice este că Alice îşi dovedeşte identitatea către Bob prin efectuarea unei operaţii criptografice asupra unei entităţi cunoscute de ambii participanţi sau oferită de Bob. Operaţia criptografică efectuată de Alice se bazează pe o cheie criptografică. Aceasta poate fi fie o cheie secretă sau o cheie privată dintr-un sistem cu chei asimetrice.

# Autentificarea utilizatorilor

Autentificarea se face diferenţiat, în funcţie de subiectul autentificării. Cele două capacităţi importante sunt memorarea unei chei criptografice de înaltă calitate şi efectuarea de operaţii criptografice. În acest caz, o cheie de înaltă calitate este o cantitate secretă aleasă dintr-un spaţiu foarte mare astfel încât o căutare exhaustivă să fie nefezabilă din punct de vedere computaţional. Un computer are ambele capacităţi, pe când un utilizator nu are nici una dintre ele.

Autentificarea utilizatorilor constă în verificarea de către un computer că identitatea este cea declarată. Cele trei tehnici principale sunt:

* *ceea ce utilizatorul ştie;*
* *ceea ce utilizatorul are;*
* *ceea ce utilizatorul este.*

*One-factor authentication*

Autentificarea printr-un singur factor constă în utilizarea unei singure tehnici din cele trei prezenate mai sus. Cea mai întâlnită, astfel de metodă utilizează *ceea ce utilizatorul ştie* cum ar fi un nume sau o parolă.

*Two-factor authentication (TFA)*

Autentificare prin doi factori a apărut datorită numărului tot mai mare de furturi de parole.

Cea mai comună metodă online de acest tip implică trimiterea unei chei temporare, utilizatorului (pe telefonul modil, adresa de e-mail, etc) care apoi va fi introdusă împreună cu numele şi parola utilizatorului. În viaţa de zi cu zi TFA este cel mai des întâlnită la extragerile de numerar, deoarece în acest proces sunt necesare cardul ATM şi un cod PIN. [10]

# Autentificarea documentelor

Pentru a asigura credibilitatea conţinutului multimedia şi pentru a le proteja împotriva furtului sau a distribuţiei ilegale s-au dezvolatat mai multe tehnici printre acestea numărându-se:

* *criptarea informaţiilor*

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. [4]

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. [4]

Criptarea se face cu un algoritm şi cu o cheie. 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.

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).

Dezavantajul acestei metode constă în faptul că, o dată decriptat, documentul poate fi modificat, retransmis fară a se putea urmări traseul lui sau să se verifice autenticitatea acestuia.

* *watermarking-ul*

Watermarkingul ascunde informaţii în fişierele multimedia fără a influenţa conţinutul acestora.

Watermark-ul digital a fost propus ca un mijloc de autentificare a documentelor, în special imaginilor. Scheme propuse: semnătura încorporată, watermark-ul fragil reinscriptibil, watermark-ul semifragil, watermark-ul robust, watermark-ul autoîncorporat. Toate aceste abordări constau fie prin inserarea în timpul înregistrării unui cod imperceptibil (watermark) a unei imaginii, sau în extragerea la momentul înregistrării unui cod (semnătură) din imagine şi reintroducerea lui în imagine sau în header-ul acesteia. Cu presupunerea că manipularea digitală va altera watermark-ul (sau semnătura), o imagine poate fi autentificată prin verificarea ca watermark-ul extras sa fie acelaşi cu cel inserat.[8]

Un sistem de watermarking este caracterizat prin transparenţă perceptuală, robusteţe şi securitatea oferită. Transparenţa percepătuală este trăsătura de a fi sau a nu fi detectat de ochiul/urechea umană. Robusteţea constă în rezistenţa watermarkului la procesări de semnal, distorsiuni neintenţionate şi atacuri, iar securitatea reprezintă faptul că, chiar dacă se cunoaşte exact algoritmul de ascundere şi de extragere a watermarului o parte neautorizată nu îl poate extrage.[5]

Spre deosebire de criptografie, prin intermediul acestuia, se poate verifica oricând autenticitatea documentului. În cazul în care se va realiza orice fel de modificare la nivelul documentul, aceasta va modifica şi conţinutul watermarkingului.

* *codul de bare*

Codul de bare este o reprezentare de [date](http://ro.wikipedia.org/wiki/Dat%C4%83) codificată ([cifrată](http://ro.wikipedia.org/wiki/Cifru" \o "Cifru)), destinată a fi citită pe cale optică. Un cod de bare are aspectul unui șir de bare negre de diverse grosimi pe un fundal alb. În general fiecare cifră sau literă se reprezintă printr-o anumită combinație de 1 sau mai multe bare. Există mai multe formate (sisteme) de coduri de bare.[9]

Codurile de bare sunt citite și decodate cu ajutorul unor [scanere](http://ro.wikipedia.org/wiki/Scaner) speciale. Acestea măsoară reflexia luminii, interpretează codurile drept cifre și litere și trimit acestea unui [calculator](http://ro.wikipedia.org/wiki/Calculator) sau altui dispozitiv de gestionare a datelor. Scanerele actuale recunosc mai multe formate.

Setul de simboluri utilizate este în general restrâns (cuprinde de obicei literele, cifrele și câteva semne speciale), dar sistemele de alcătuire (formatele) codurilor de bare sunt foarte variate. Multe coduri de bare constau în bare verticale după diverse formate. Lungimea codului de bare depinde de cantitatea de date ce trebuie reprezentată.

Toate codurile de bare dispun de un caracter special de start/stop ce permite citirea atât de la stânga la dreapta, cât și de la dreapta la stânga. Prin convenție caracterul din stânga este considerat caracterul de start și caracterul din dreapta caracterul de stop.

* *semnătura digitală*

O semnătură digitală este un marcaj electronic de securitate care se poate adăuga fișierelor. Permite verificarea editorului fișierului și ajută la verificarea dacă fișierul s-a modificat sau nu de când a fost semnat digital.

* *certificate digitale*

Certificatul digital este o „carte de identitate” virtuala, care permite identificarea fara echivoc pe Internet prin crearea si utilizarea semnaturii electronice cu valoare legala. El garanteaza identitatea, autenticitatea, integritatea si nerepudierea documentelor in format electronic.

# Semnătura digitală/electronică

Legal, *semătura electronică* este definită ca reprezentarea, în formă electronică a unor date, care sunt atasate sau logic asociate cu alte date in forma electronica si care servesc ca metoda de identificare [art. 4 pct. 3 din [Legea 455/2001](http://codfiscal.net/legea-4552001-semnatura-electronica/)].

Termenul de *semnătură electronică* are interpretări mai largi, pornind de la semnături criptografice digitale până la o imagine scanată a unei semnături de mână. În ambele cazuri, se defineşte calea pentru utilizarea legală a semnăturilor digitale în comunicaţiile electronice.

Semnătura digitală oferă trei servicii de securitate de bază:

1. *autentificare* - desi documentele digitale pot sa includa informatii despre idetitatea celui care le-a emis, aceste informatii pot sa nu fie corecte. Semnatura digitala poate fi folosita pentru autentificarea sursei documentului. Atunci cand dreptul de proprietate asupra unei semnturi digitale apartine unei anumite persoane, semnatura digitala arata ca documentul a fost eliberat de catre acea persoana. Importanta acestui aspect apare in dovedirea autenticitatii documentelor digitale in context financiar-contabil. De exemplu actele contabile ale unei firme sunt trimise corect de catre firma de contabilitate catre administratorul firmei. Daca acesta va modifica aceste acte incercand sa schimbe informatiile financiare sau orice fel de informatii transmise ca fisier PDF/A semnat electronic, pentru a putea obtine un credit de la o banca, in momentul in care banca deschide acele documente, semnatura electronica va fi invalidata, deci firma de contabilitate nu va putea fi considerata responsabila de continutul documentului, persoana care a transmis documentul modificat nu va putea fi urmarita in justitie pentru fals si uz de fals, iar banca va fi asigurata ca nu cade in capcana acordarii unui credit pe baza unor documente false.
2. *integritate* - semnatura digitala aplicata unui document electronic reprezinta o garantie a integritatii documentului atunci cand este validata de o autoritate publica. Cheia aleatoare se creeaza pe baza unor criterii multiple care includ printre altele si detalii despre continutul documentului. Orice modificare a continutului unui document digital inseamna o chaie aleatoare noua diferita de cheia aleatoare folosita pentru aplicarea semnaturii digitale. In clipa in care se solicita validarea documentului cele doua chei aleatoare din imaginea de mai sus vor fi diferite, iar documentul se va putea considera ca avand continutul alterat.
3. *nerepudiere* - odata ce este emis un document digital semnat electronic, atata vreme cat semnatura electronica este valida pe documentul digital, autorul documentului nu isi poate declina raspunderea pentru continutul documentului cu semnatura electronica valida. In plus, nu poate nega faptul ca documentul a fost semnat personal, deoarece legislatia in vigoare prevede faptul ca detinatorul unei semnaturi digitale NU are dreptul sa instraineze/imprumute token-ul pe care exista certificatul digital calificat pe care il detine. Din acest punct de vedere, exemplul de mai sus in care firma de contabilitate transmite documentele financiare firmei pentru care le intocmeste, daca a comis greseli in intocmirea acestor acte, ramane responsabila pentru datele prezentate, cata vreme documentul digital transmis poarta o semnatura valida.

Algoritmii cu funcţie de rezumat (hash), sau amprentă, servesc în construirea semnăturilor digitale utilizate în procedurile de autentificare a documentelor.

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.[4]

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 1048 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.

# Certificate

Dezavantajul semnăturii digitale este eliminat prin schemele de autentificare care folosesc certificate de autenticitate emise de o Autoritate de Certificare (AC).

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.[1]

Conform standardului X.509v3 definit în RFC 2459 un certificat digital conţine următoarele elemente:

1. *Certificate Version* - indică versiunea formatului unui certificat;
2. *Serial Number* - un număr unic asignat de către autoritatea de certificare, utilizat pentru urmărirea certificatelor;
3. *Signature* - identifică algoritmul de criptare şi funcţiile de tip message digest suportate de CA;
4. *Issuer name* - numele emitentului (al CA);
5. *Period of Validity* - datele între care certificatul este valid. Această perioadă nu exclude ca certificatul să fie revocat;
6. *Subject* - numele proprietarului certificatului;
7. *Subject's Public Key Info* - cheia publică şi algoritmul asociat cu câmpul Subject;
8. *Issuer Unique ID* - un câmp opţional utilizat pentru a identifica emitentul certificatului sau autoritatea de certificare. Utilizarea acestui câmp nu este recomandată în RFC 2459;
9. *Extensions* - câmp opţional utilizat pentru extensii proprietare. Acest câmp nu este definit dar cuprinde articole precum: alte denumiri ale subiectului, informaţii pentru utilizarea cheilor şi punctele de distribuţie a listelor de revocare a certificatelor (Certificare Revocation List - CRL);
10. *Encrypted* - acest câmp conţine semnătura în sine, identificatorul algoritmului, hash-ul securizat al celorlalte câmpuri din certificat şi semnătură digitală a hash-ului.

Certificatele necesită mijloace de gestionare a creării acestora, distribuirea lor, stocarea centralizată, revocarea, backup-ul cheilor şi actualizarea acestora. Acest sistem de management este cunoscut sub numele de *infrastructura de chei publice* ( *Public Key Infrastructure -* PKI). [1]

O infrastructură de chei publice este o arhitectură de securitate creată pentru a facilita instalarea tehnologiei de chei publice. Între componentele unui PKI se pot număra un depozit de certificate (de obicei un serviciu director compatibil LDAP), certificatele digitale, listele de revocare a certificatelor (CRL), software-ul pentru aceste aplicaţii, precum şi aspectul uman al acestor proceduri.

O PKI cuprinde câteva servicii de bază de securitate între care se numără autentificarea utilizatorilor, confidenţialitatea şi integritatea, ajutând de asemenea la implementarea nerepudierii.

O autoritate de certificare este o componentă a infrastructurii generale de chei publice şi este o componentă critică pentru o implementare la scară a acestei infrastructuri. Funcţia principală a unei autorităţi de certificare este aceea de a certifica faptul că perechea cheie publică / cheie privată aparţine într-adevăr unui individ anume.

# Tehnologii de autentificare

Pentru a creşte siguranţa datelor, se foloseşte tot mai des autentificarea prin mai mulţi factori, cea mai des întâlnită este prin doi facturi. Aceasta utilizează două din cele trei trei modalităţi din autentificare (ce ştiu, ce am, ce sunt). În general se foloseşte "ce ştiu" cu "ce am".

"Ce ştiu" este reprezentat de parolă sau nume de utilizator, iar "ce am" aanumite dispozitive de autentificare, printre acestea: token-ul, cardul smart.

Există din ce în ce mai multe firme specializate în securitatea informaţiilor care şi-au dezvoltat propriile tehnologii de securitate utilizând unul sau mai multe din dispozitivele enunţate precedent.

# Token

Token-ul este un dispozitiv de mici dimensiuni care generează şi afişează un şir de caractere aleator pentru a permite utilizatorilor să accesese în siguranţă anumite informaţii.

Este utilizat pentru a demonstra identitatea electronică a cuiva sau pentru a avea acces la ceva. Toke-uri pot stoca chei criptografice cum ar fi semnătura digitală sau date biometrice. Unele modele pot dispune de ambalaj rezistent în timp ce altele pot avea o mică tastatură pentru a permite introducerea unui cod PIN sau doar un simplu buton de start pentru a genera noul cod şi un ecran pentru afişarea acestuia.

Toate token-urile conţin o informaţie secretă pentru a dovedi identitatea utilizatorului. Pot fi patru modalităţi de utilizare a informaţiei [11]:

1. *token cu parolă statică*: dispozitivul conţine o parolă care este ascunsă utilizatorului, dar care este transmisă la fiecare autentificare. Acest tip este vulnerabil la atacuri de tip repetare;
2. *token cu parolă sincronizată dinamic*: este folosit un cronometru pentru a se roti prin mai multe combinaţii produse de un algoritm criptografic. Token-ul şi server-ul de autentificare trebuie să aibe ceasurile sincronizate;
3. *token cu parolă asincronă*: o parolă "în timp" este generată fără a utiliza ceasul printr-un algoritm de criptare;
4. *token cu răspuns la mesaj*: utilizând criptarea cu cheie publică, este posibil să dovedească posesia unei chei private fără a o dezvălui. Server-ul trimite un mesaj al cărui răspuns îl cunoaşte deoarece are o copie a cheii private; token-ul demonstrează că are aceeaşi cheie privată prin trimiterea aceluiaşi răspuns.

Cele mai simple tipuri de token-uri pot să nu fie conecate în niciun fel la calculator în timp ce altele se pot conecta prin USB, sau Bluetooth. Cele independente conţin un ecran fizic pe care este afişat un număr, acest număr va fi introdus de utilizator pentru a se autentifica. cele dependente transferă o secvenţă de chei clientului local sau celui mai apropiat punct de acces.

Cei de la *certSign*(companie membră a gruplui UTI, este furnizor acreditat de servicii de certificare) recumandă token-urile iKey 2032, şi Cryptoflex E-Gate.[14]

* **iKey 2032**
* Token USB cu autentificare pe bază de 2 factori pentru a oferi maximul de securitate.
* Perzintă un procesor 8-biţi, 32K de memorie, conectivitate USB 1.1/2.0 şi oferă un transfer 1.5Mbiţi/secundă.
* Funcţiile criptografice utilizate sunt: generare de perechi de chei asimetrice (RSA), generare de chei simetrice (DES, 3DES), gestiunea şi stocarea securizată hardware a cheii, semnătură electronică.
* Performaţele criptogarfice sunt: operaţii cu chei RSA de 1024-biţi şi 2048-biţi, generarea cheii se face în mai puţin de 90 de secunde cu tot cu verificarea cheii, semnătura electronică se realizează în ami puţin 1 secundă.
* Algoritmii cripografici utilizaţi: criptare cu cheie asimetrică RSA 1024-biţi, RSA 2048-biţi, algoritmi cu cheie simetrică DES, 3DES, semnătură electronică RSA 1024-biţi, RSA 2048, algoritm Hash Digest SHA-1.
* **Cryptoflex E-Gate**
* Poate fi folosit fie sub formă de smartcard, caz în care este nevoie şi de cititor, fie sub formă de token, fără a mai fi nevoie de cititor.
* Are o memorie de 32K, procesor criptografic şi foloseşte tehnologie de tip smartcard fără cititor USB v1.1
* Funcţiile criptografice utilizate: generare de chei RSA (lungimea cheilor 512, 768, 1024 şi 2048 biţi), semnătură electronică RSA, algoritm SHA-1, criptare simetrică DES sau 3DES, DES şi 3DES MAC, generare de chei DES (lungimea cheilor 56, 112 biţi), DES şi 3DES Chain Block Cipher (lungimea cheilor 56 şi 112 biţi).

# Carduri smart

Cardurile smart au aceeşi dimeniune cu un card de credit şi pot fi utilizate atât drept carduri de proximitate cât şi pentru accesul în reţea.

Pot fi carduri smart cu contact, fără contact şi hibride.

1. *Carduri smart cu contact*: au o zonă de contact pătrată de aproximativ 1 cm care conţine mai multe plăcuţe de contact placate cu aur. Aceste plăcuţe realizează conectivitate electrică în momentul în care sunt introduse în cititor, conectivitatea este utilizată pentru realizarea comunicaţiei dintre card şi gazdă sau telefon mobil.[12]
2. *Carduri smart fără contact* (carduri de proximitate): spre deosebire de cel cu contact, acesta poate fi citit fără să fie introdus într-un dispozitiv de citire, fiind suficientă ţinerea lui câteva secunde lângă acesta. Cardurile de proximitate pot fi citite de la aproximativ 5 cm, astfel că utilizatorul poate avea aces la o locaţie prin punerea portofolului, în care se află cardul, în dreptul cititorului. Acest tip de card poate conţine un echilibru de flux electronic folosit în sistemele de plăţi fără contact (cardul RATB).[13]
3. *Carduri hibride*: carduri cu interfaţă dublă, au implementată atat interfaţa de contact cât şi cea fără, pe un singur card cu elemente de stocare şi procesare comune.[12]

Cei de la *certSign* recomandă smart cardul **SafeNet 330**. Acest tip de smartcard dispune de protecţie software şi hardware împotriva atacurilor criptografice „differential power” şi „timing attacks”. Dispune de memorie EEPROM de 32K pentru stocarea sigură a cheilor, parolelor, certificatelor şi a datelor, în general şi de un procesor DES pentru criptare simetrică. Funcţii criptografice folosite sunt: generare de chei DSA (1024-biţi), generare de chei RSA (1024-biţi şi 2048-biţi ), algoritm RSA pentru semnare electronică, algoritm DSA pentru semnare electronică, algoritm RSA pentru schimbarea cheilor (key exchange), Diffie-Hellman key exchange, algoritm SHA-1, algoritm DES/3DES pentru criptare/decriptare.[14]

# Concluzii

Pentru a asigura securitatea informaţiilor este necesară o clasificare a acestora iar accesul se facă în funcţie de tipul beneficiarilor.

La nivel guvernamental, informaţiile se clasifică în informaţii obiective, subiective, tehnice şi secrete comerciale, în timp ce la nivelul unei organizaţii acestea se încadrează în categoriile: speciale, confidenţiale la nivel de unitate, private, de uz intern şi publice.

La nivel guvernamental, orice informaţie neîncadrată într-una din categoriile speciale, sub incidenţa legii accesului liber la informaţiile publice, poate fi publicată de orice organ de presă scrisă, video sau audio, sub motivaţia că *"tot ceea ce nu este interzis este permis"*.

La nivelul organizaţiilor private, lucrurile stau invers, doar informaţiile care sunt specificate "pentru public" pot fi făcute publice, mergându-se pe principiul *"tot ceea ce nu este permis este interzis"*.

Beneficiarii pot fi de trei tipuri: proprietarul informaţiei, custodele şi utilizatorul.*Proprietarul informaţiilor* poate fi administratorul sau directorul unei organizaţii. O astfel de persoană răspunde de averile informaţionale încredinţate. Spre deosebire de custode, proprietarul are responsabilitatea finală a protecţiei datelor şi răspunde în faţa legii în cazul neachitării de această obligaţi. *Custodele informaţiilor* este cel care prestează un serviciu externalizat organizaţiei, delegându-i-se responsabilităţile pe linia protejării informaţiilor. Acest rol este îndeplinit de specialişti în tehnologii informaţionale. *Utilizatorul* este considerat orice persoană, operator, angajat, persoană din afară, care foloseşte informaţiile.

Pentru ca un sistem să poată verifica tipul beneficiarilor şi autenticitatea şi integritatea informaţiilor este necesară o utilizarea unei metode de autenficare şi identificare.

*Autentificarea* este definită ca procesul de verificare sigură a identităţii cuiva sau a ceva.

În cadrul autentificării deosebim trei cazuri:

1. *autentificarea a două sisteme de calcul*
2. *autentificarea identităţii unui utilizator către un sistem de calcul*
3. *autentificarea unui document*

Autentificarea documentelor se face prin intermediul criptografiei, watermarking-ului, coduruilor de date, semnăturii digitale şi certificatelor digitale.

Criptografia este ştiinţa creării şi menţinerii mesajelor secrete, în sensul imposibilităţii citirii lor de către neautorizaţi şi este de două tipuri: cu chei secrete (simetrice) sau cu chei publice (asimetrice).

Watermarking-ul constă în introducerea unui cod imperceptibil în fişierul cu informaţii astfel încât orice modificare ulterioară a informaţiei să fie sesizată datorită modificării watermark-ului.

Legal, *semătura electronică* este definită ca reprezentarea, în formă electronică a unor date, care sunt atasate sau logic asociate cu alte date in forma electronica si care servesc ca metoda de identificare [art. 4 pct. 3 din [Legea 455/2001](http://codfiscal.net/legea-4552001-semnatura-electronica/)].

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 ziua de azi, autentificarea şi identificarea utilizatorilor, se realizează prin intremediul unor dispozitive portabile, cele mai întâlnite fiind token-urile şi smart card-urile. Acestea conţin informaţii secrete cu care pot dovedi identitatea utilizatorului.

# Bibliografie

[1] Securitatea sistemelor informatice, Popa Sorin Eugen

[2] Studiu asupra nivelului de siguranţă oferit de protocoalele de autentificare, ing. Valer Bocan

[3] All About Bar Code, Datalogic

[4] Guvernarea electronică. O introducere, 2007, dr.ing. Dan Vasilache

[5] Securitatea conţinutului multimedia, prof.dr.ing. Nicolae Vizireanu, ş.l.dr.ing. Radu Preda

[6] Securitatea reţelelor de calculatoare, prof.dr.ing. Simona Halunga

[7] Reţele de calculatoare, 2008, Radu-Lucian Lupşa

[8] Detection of Copy-Move Forgery in Digital Images, Jessica Fridrich, David Soukal, and Jan Lukáš

­[9] <http://ro.wikipedia.org/wiki/Cod_de_bare>

[10] <http://www.intego.com/mac-security-blog/what-is-multi-factor-authentication-and-how-will-it-change-in-the-future/>

[11] <http://en.wikipedia.org/wiki/Security_token>

[12] <http://en.wikipedia.org/wiki/Smart_card>

[13] <http://en.wikipedia.org/wiki/Proximity_card>

[14]<http://www.certsign.ro/certsign/produse/siguranta-documentelor/dispozitive-criptografice>