6. SECURITATEA ACCESULUI IN INTERNET

In cadrul operatiunilor (tranzactiilor on line) ce se efectueaza in Internet se impun masuri de securitate deosebite, ce trebuie sa limiteze accesul la informatii, asigurând in principal caracterul privat al datelor, integritatea si imposibilitatea repudierii.

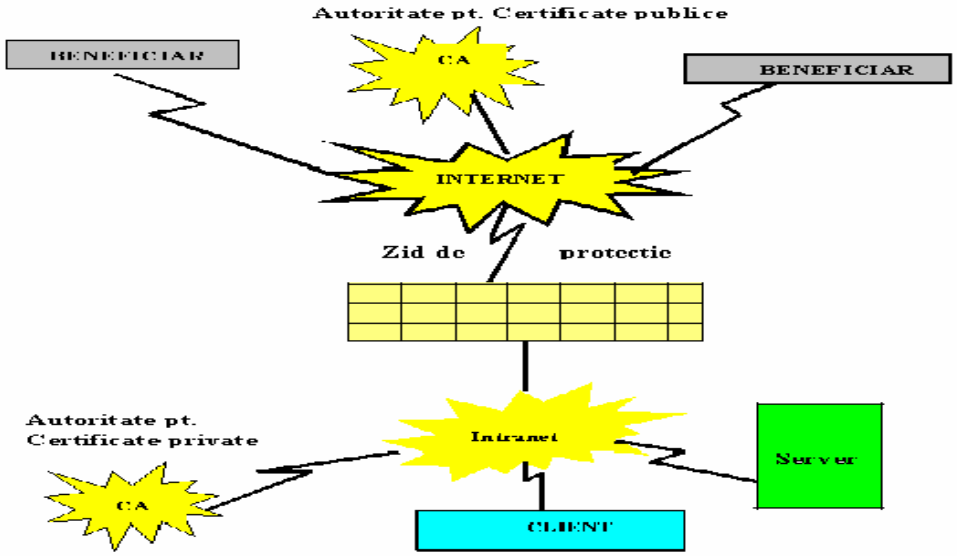

Fig. 3. Securitatea datelor in Internet

Accesul este controlat prin intermediul certificatelor digitale. Certificatul digital se obtine prin informarea unei autoritati de certificare CA privind datele personale. O data autentificat, se poate incepe sesiunea de lucru cu criptare si securitate (Fig. 3).

Sistemele firewall

Firewall (parafoc - zid de protectie) reprezinta o procedura de securitate care plaseaza un calculator special programat, intre reteaua locala (LAN) a unei organizatii si Internet. Calculatorul firewall impiedica accesul spargatorilor de coduri la reteaua interna (intranet).

Din pacate nu permite nici utilizatorilor retelei locale obtinerea accesului direct la Internet, permitând doar un acces indirect, controlat de programe numite *servere delegate.*

Sistemele firewall utilizeaza de cele mai multe ori una din urmatoarele doua metode :

- Filtrarea pachetelor
- Servicii proxy

Sistemele ***firewall cu filtrarea pachetelor de date*** examineaza fiecare pachet care "vrea" sa intre sau sa iasa in/din retea si-l compara cu o lista de criterii programata. Pachetele sunt blocate, daca nu sunt marcate specific ca "libere".

Sistemele ***firewall proxy*** actioneaza ca intermediari la cererile retelei, necesitând ca fiecare client sa fie astfel configurat incât sa ceara serviciile proxy sa se conecteze la un server inainte de a apela serviciile retelei.

In acest domeniu, programele **CyberGuard Firewall si CheckPoint Firewall,** ofera in prezent o teleadministrare sigura si eficienta a tranzactiilor si operatiunilor on line.

Semnaturi digitale

Semnaturile digitale asigura un nivel de integritate si imposibilitatea de repudiere pentru oricine este ingrijorat de folosirea datelor si accesul neautorizat la informatii in cadrul diferitelor servicii Internet.

Exista multi algoritmi de semnatura digitala in literatura de specialitate. Practic s-au impus trei dintre acestia :

- Standardul de semnatura digitala (DDS) a guvernului SUA
- Semnatura pe baza de hash
- Semnatura RSA creata prin utilizarea algoritmului clasic dezvoltat de Don Rivest

Fiecare dintre algoritmi are utilizare diferita si cerinte diferite.