PEM – STANDARDUL DE POŞTĂ ELECTRONICĂ CU FACILITĂŢI DE SECURITATE

Prof. univ. dr. ing. Ciprian Răcuciu
Drd. ing. Dragoş Glăvan

Abstract:

In this thesis is presented Privacy-Enhanced Mail (PEM), an Internet standard that provides for secure exchange of electronic mail. PEM employs a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity. The message integrity aspects allow the user to ensure that a message hasn't been modified during transport from the sender. The sender authentication allows a user to verify that the PEM message that they have received is truly from the person who claims to have sent it. The confidentiality feature allows a message to be kept secret from people to whom the message was not addressed.

Cuvinte cheie: poştă electronică, securitate, algoritmi criptografici, confidențialitate, integritatea legăturii.

1. INTRODUCERE

Cu siguranţă serviciul de poştă electronică este una dintre cele mai folosite facilităţi de comunicaţie din prezent. Există însă mulţi utilizatori care încă nu au avut posibilitatea, interesul sau poate curajul să-i cunoască avantajele. Cert este că, în scurt timp, e-mail-ul va deveni un instrument indispensabil pentru oricine.

Sistemul de e-mail este una dintre cele mai importante aplicaţii folosite pe sistemele de calcul, ducând în acelaşi timp la dezvoltarea şi răspândirea la nivel global a internetului.

Printre principalele avantaje ale sistemului de poştă electronică, care au dus la răspândirea sa, sunt:

- fiabilitatea, garanţia că mesajele ajung la destinatar;
- timpul scurt, de ordinul secundelor sau a minutelor, între momentul în care un mesaj este expediat şi momentul în care ajunge la destinatar;
- securitatea, putându-se utiliza mecanisme de criptare a conţinutului mesajelor;
- flexibilitatea, permiţând trimiterea într-un mesaj electronic (de obicei ca ataşament) a oricărui tip de date: multimedia, documente, semnături electronice, facturi de plată, etc.

În ceea ce priveşte însă securitatea, poşta electronică nu oferă condiţiile ideale. Mesajele pot fi interceptate, în mod voit sau din eroare, de către persoane neautorizate sau de către administratorii sistemelor de calcul. În cele mai multe versiuni de sisteme, UNIX, derivate Berkeley, incluzând şi pe cele de pe Sun, este folosit programul *Sendmail* pentru a recepţiona şi trimite poşta electronică. Versiunile mai vechi de *Sendmail* au unele deficienţe privind securitatea, permiţând penetrarea în sistem, obţinerea unor drepturi de acces şi activarea unor programe sau scripturi în mod ilegal. O astfel de deficienţă a fost folosită de către Viermele Internet.

Se consideră că poşta electronică este un mediu deschis, ceva similar cărţilor poştale, a căror confidenţialitate este deosebit de precară. De exemplu, avocaţii şi clienţii lor folosesc zilnic poşta electronică, dar au realizat că mesajele schimbate prin reţea pot fi citite de către persoane străine. Şi chiar dacă intuiesc vulnerabilitatea poştei electronice, comoditatea şi credinţa că numărul mare de mesaje care circulă în Internet face improbabilă interceptarea corespondenţei, conduc la folosirea fără precauţie a e-mail-ului. Cei implicaţi trebuie să reţină că sentimentul de intimitate este fals. Datorită faptului că poşta electronică este memorată sub formă digitală, aceasta se pretează a fi supusă unei analize la scară foarte mare cu ajutorul unor programe speciale şi, ca urmare, mijloacele de selectare a unei anumite corespondenţe de interes sunt mult mai eficiente decât în poşta tradiţională.

O soluţie pentru asigurarea confidenţialităţii mesajelor transmise prin Internet ar putea consta în utilizarea unui soft adecvat protecţiei criptografice a scrisorilor schimbate prin poşta electronică. Pentru asigurarea securităţii acestui serviciu, specialiştii recomandă standardul PEM (Privacy Enhanced Mail) şi programul PGP (Pretty Good Privacy), dar deosebit de utilizat este şi standardul MOSS (Microsoft Office Sharepoint Server), în multe privinţe foarte asemănător cu PEM.

Scopul declanşării proiectului PEM (Privacy Enhanced Mail) l-a constituit necesitatea asigurării securităţii transmisiilor între utilizatorii poştei electronice din rețeaua Internet. Eforturile au început în 1985 în cadrul comisiei PSRG (Privacy and Security Research Group), sub auspiciile consiliului IAB (Internet Architecture Board). Rezultatele cercetării s-au concretizat în RFC-urile (Request for Coment) 1421-1424 care constituie propuneri de standarde pentru Internet. Aceste RFC-uri sunt produsul grupului de lucru PEM din interiorul IEFT (Internet Engineering and Task Force), care face parte din IAB (Internet Architecture Board).

2. SERVICII DE SECURITATE PENTRU POŞTA ELECTRONICĂ

Standardul PEM oferă o varietate de servicii de securitate pentru utilizatorii poştei electronice:

a) confidenţialitatea (secretizarea) mesajelor;
b) autentificarea originii mesajelor;
c) integritatea legăturii în reţea;
d) nerepudierea mesajelor prin dovada originii.

Aceste servicii, definite şi în modelul de referinţă al securităţii, OSI, pot fi divizate în două grupe:
- toate mesajele prelucrate în PEM încorporează facilităţile de autentificare, integritate şi nerepudiere;
- confidenţialitatea este un serviciu opţional, la alegerea utilizatorului.

(a)Confidenţialitatea protejează conţinutul mesajelor împotriva citirii lor neautorizate, de către alte persoane decât receptorii specificaţi de emiţător. Obiectivul acestei protecţii îl constituie fie ascultarea şi înregistrarea neautorizată a traficului de pe liniile de comunicaţii, fie posibilitatea accesului la cutiile de scrisori, care sunt de fapt nişte fişiere disc; împotriva unor astfel de atacuri se preferă secretizarea (criptarea) mesajelor.

(b)Autentificarea originii mesajelor permite receptorului unui mesaj prin poşta electronică să determine în mod sigur identitatea emiţătorului scrisorii. Este un serviciu de securitate foarte util astăzi, când în sistemele de poştă electronică este relativ uşor să forţezi emiterea unor scrisori în numele unor alţi utilizatori. Acest lucru creează mari semne de întrebare asupra credibilităţii mesajelor primite prin poşta electronică.

(c)Integritatea legăturii în reţea furnizează receptorului siguranţa că mesajul primit este identic cu mesajul emis la origine. Acest serviciu protejează împotriva unor atacuri care vizează modificarea mesajelor aflate în tranzit prin reţea. Deşi cele două servicii de autentificare şi de integritate au fost descrise separat, ele sunt furnizate de obicei în tandem.

(d)Împiedicarea nerecunoaşterii mesajului de către expeditor (nerepudierea mesajelor) garantează integritatea şi originea datelor din punctul de vedere expeditorului, nu al destinatarului. Se împiedică astfel ca expeditorul unui mesaj de poştă electronică să nege transmiterea scrisorii. De asemenea, se permite scrisorilor să fie transmise mai departe la alţi destinatari, care să poată verifica identitatea originii (nu numai a intermediarului) mesajului. La recepţie, se poate verifica că mesajul nu a fost alterat, inclusiv (ulterior) de către emiţătorul său autentic. O utilizare deosebită a acestui serviciu este pusă în evidenţă în activităţile comerciale, când trebuiesc transmise prin e-mail comenzi sigure, care să fie apoi confirmate şi a căror recepţie să poată fi dovedită.

3. INTEGRAREA PEM ÎN SISTEMELE DE POŞTĂ ELECTRONICĂ

Încă din proiectare s-a intenţionat ca PEM să fie utilizat în conjuncţie cu sistemele de poştă electronică existente la ora actuală în reţeaua Internet.

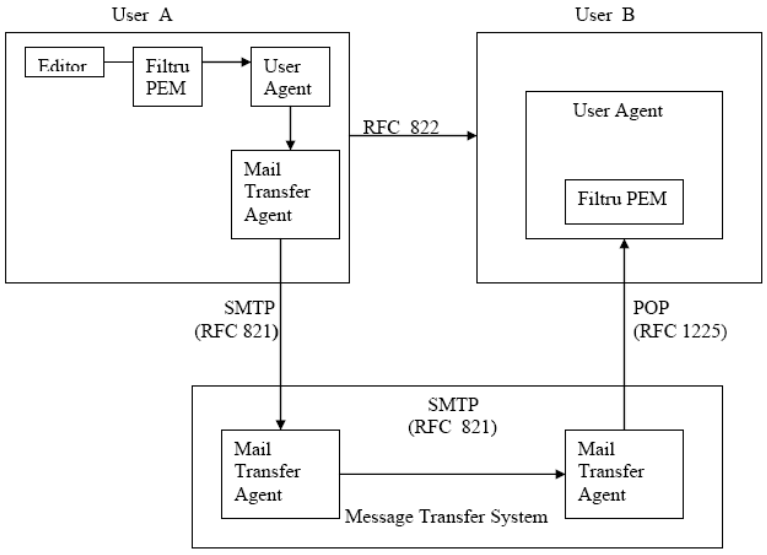

Figura 1 - Integrarea PEM în sistemele de poştă actuale

Implementarea serviciilor de securitate în conformitate cu standardul PEM se face peste infrastructura de poştă electronică existentă. Există două variante de integrare (figura 1):

1) Cu includerea funcţiilor de securitate în User Agent (UA); avantajul acestei variante constă in obţinerea unei interfeţe mai bune cu utilizatorul.
2) Fară modificarea User Agent-ului, prin realizarea unui filtru de securizare a mesajelor în exteriorul UA. Avantajele acestei variante sunt: posibilitatea folosirii filtrului în conjuncţie cu o gama largă de programe de tip UA existente şi excluderea problemelor de integrare.

4. ALGORITMI CRIPTOGRAFICI UTILIZAŢI ÎN PEM

Pentru a se putea folosi serviciile de securitate oferite de PEM, acesta foloseşte o varietate de algoritmi criptografici, aceştia fiind necesari pentru cifrarea mesajelor, pentru distribuţia cheilor criptografice utilizate la cifrare şi descifrare, pentru verificarea integrităţii mesajelor şi pentru autentificarea emiţătorului şi receptorului unui mesaj informaţional.

În cazul sistemelor criptografice simetrice (cu cheie secretă) se foloseşte aceeaşi cheie atât la cifrarea cât şi la descifrarea mesajelor. Cheia secretă este folosită atât de către emiţător cât şi de către receptor. PEM foloseşte sisteme simetrice pentru a asigura secretizarea conţinutului scrisorilor. În sistemele criptografice asimetrice (cu chei publice), în procesele de cifrare şi de descifrare, se foloseşte o pereche de chei distincte (dar matematic legate una de alta). Una dintre aceste chei este menţinută secretă şi este cunoscută doar de către proprietarul ei. În acelaşi timp, cealaltă cheie (perechea ei) este făcută publică, motiv pentru care a apărut denumirea de criptografie cu cheie publică. Sistemele criptografice cu chei publice sunt folosite de PEM în procesul de semnătură digitală şi de distribuţie sigură a cheilor de cifrare.

Standardele PEM nu specifică în mod concret algoritmii criptografici care să fie folosiţi pentru asigurarea serviciilor de securitate. Un standard distinct (RFC 1423) identifică o listă de algoritmi care pot fi utilizaţi în PEM, listă care poate fi îmbogăţită odată cu definirea altor algoritmi noi.

Algoritmii criptografici, în contextul PEM-ului, sunt folosiţi în trei scopuri:

a) *Criptarea datelor*.

Dacă se doreşte serviciul de confidenţialitate a datelor, atunci reprezentarea ASCII a mesajului este trecută printr-un algoritm de criptare a datelor. Acesta poate fi: DES (în varianta CBC) sau IDEA (în variantele CBC sau CFB). Parametrii acestui algoritm (fiecare de 8 octeţi) sunt:

- cheia de criptare a datelor (DEK – Data-Encryption Key);
- vectorul de iniţializare (IV – Initialization Vector).

b) *Integritatea mesajelor*.

Dacă se doresc serviciile de securitate, de integritate şi de autentificare a expeditorului, atunci reprezentarea ASCII, a mesajului conţinut, este prelucrată printr-un algoritm de dispersie (hash) denumit Message Digest (MD). Algoritmul va realiza un rezumat (digest) al mesajului, numit MIC (Message Integrity Check). În standardul PEM sunt definiţi trei algoritmi în acest scop:

- RSA-MD5 (RFC 1321);
- RSA-MD2 (RFC 1319);
- MAC (Message Authentification Code) – calculat folosind varianta CBC a DES.

c) *Criptarea cheilor*.

După ce au fost generate, cheile de criptare şi MIC-urile sunt trimise la receptor, ca parte a mesajului PEM. Pentru criptarea cheilor se utilizează un algoritm aparte. La momentul actual sunt definiţi trei algoritmi în acest scop:

- DES-ECB (varianta Electronic CodeBook a algoritmului DES);
- DES-EDE (varianta Encrypt-Decrypt-Encrypt sau Triple Encryption a algoritmului DES);
- RSA (algoritmul de criptare cu chei publice RSA).

În cadrul standardelor PEM se încurajează folosirea sistemelor cu chei publice în distribuţia cheilor, datorită uşurinţei gestionării lor în comunităţile de utilizatori numeroase şi foarte larg distribuite. Abordarea sistemelor cu chei publice în standardul PEM se face utilizând conceptul de certificat, aşa cum a fost el definit în recomandările CCITT X.509. Un certificat de cheie publică reprezintă o structură de date folosită pentru a se putea asocia în mod sigur o cheie publică la nişte atribute de utilizator. Atributele pot fi, de exemplu, informaţii de identificare (nume, adresă) sau informaţii de autorizare (dreptul de a folosi o resursă). În structura certificatului sunt următoarele câmpuri:

- Versiunea – permite să se facă distincţie între versiuni succesive ale formatelor de certificat;
- Numărul serial – identifică în mod unic certificatul dintre cele emise de aceeaşi entitate;
- Algoritmul de semnătură – identifică algoritmul folosit pentru calcularea semnăturii digitale la acel certificat;
- Emitent – conţine numele distinct al entităţii (autorităţii) care a creat certificatul şi garantează pentru legătura corectă *cheie publică – subiect*; de fapt, este numele autorului certificatului;
- Subiect – conţine numele distinct al entităţii care reprezintă subiectul certificării şi proprietarul cheii publice cuprinse în certificat;
- Valabilitate – cuprinde intervalul de timp (data de început şi cea de sfârşit) în care certificatul este valabil;
- Cheie publică subiect – conţine un identificator al algoritmului folosit precum şi parametrii ceruţi de algoritm, care constituie cheia publică a subiectului – proprietar al certificatului;
- Semnătura – conţine semnătura digitală a certificatului şi este adăugată celorlalte câmpuri ale acestuia. De exemplu, funcţia de dispersie poate fi MD5, iar algoritmul cu chei publice, RSA. Semnătura se aplică de către autoritatea *Emitentă,* folosind cheia sa privată şi poate fi verificată oriunde, folosind cheia publică a *Emitentului*.

După cum se vede, problema obţinerii cheii publice a unui utilizator *Subiect* constă în validarea semnăturii digitale a certificatului acestuia, care se face cu cheia publică a *Emitentului*. Obţinerea cheii publice a *Emitentului* este o problemă similară cu cea de validare a certificatului acestuia. Ca urmare, procesul de validare a certificatelor este recursiv şi se bazează pe un graf de certificare.

5. PRELUCRAREA UNEI SCRISORI PEM

De regulă, autorul unui mesaj de poştă electronică securizată este un utilizator obişnuit, nu un specialist în criptografie şi, de aceea, se doreşte minimizarea implicării sale în tehnologia de securizare a mesajului.

Un mesaj PEM este format din header-e (antete), urmate de un corp. Un mesaj de poştă electronică este format, de fapt, din trei mesaje imbricate:

- mesajul exterior – mesajul ce este prezentat MTA-ului local. Corpul acestui mesaj este constituit dintr-un "mesaj cu securitate sporită";
- mesajul cu securitate sporită – conţine informaţia care furnizează serviciile de sporire a securităţii. Corpul acestui mesaj este numit "mesajul interior";
- mesajul interior – mesajul pe care doreşte să îl trimită expeditorul în forma sa de dinainte ca serviciile de securitate să fie apelate; el va fi disponibil în mailbox-ul destinatarului după ce aceste servicii de securitate au fost implementate, transmiţând în condiţii sigure mesajul la destinaţie.

O scrisoare este formată din două zone: antetul mesajului şi conţinutul mesajului.

Datele conţinute în antet vor trece de obicei nemodificate prin prelucrările PEM. Poate face excepţie câmpul *Subiect-scrisoare* care, dacă este senzitiv, poate fi omis sau înlocuit cu o informaţie benignă ("Encrypted Message"). Indiferent de situaţie, este necesar ca identificatorul receptorului să rămână *în clar*, deoarece pe baza lui se realizează controlul procesului de criptare.

În poşta electronică clasică, antetul este separat de conţinut printr-o linie liberă. În cazul folosirii PEM, în cadrul conţinutului mesajului sunt mai multe câmpuri care constituie antetul-PEM şi care sunt despărţite prin separatori proprii. Aceste informaţii din antetul-PEM sunt folosite de receptor pentru a valida integritatea şi autenticitatea mesajului primit şi pentru a descifra mesajul. După acest antet-PEM, înainte de mesajul propriu-zis, este inserată o linie liberă.

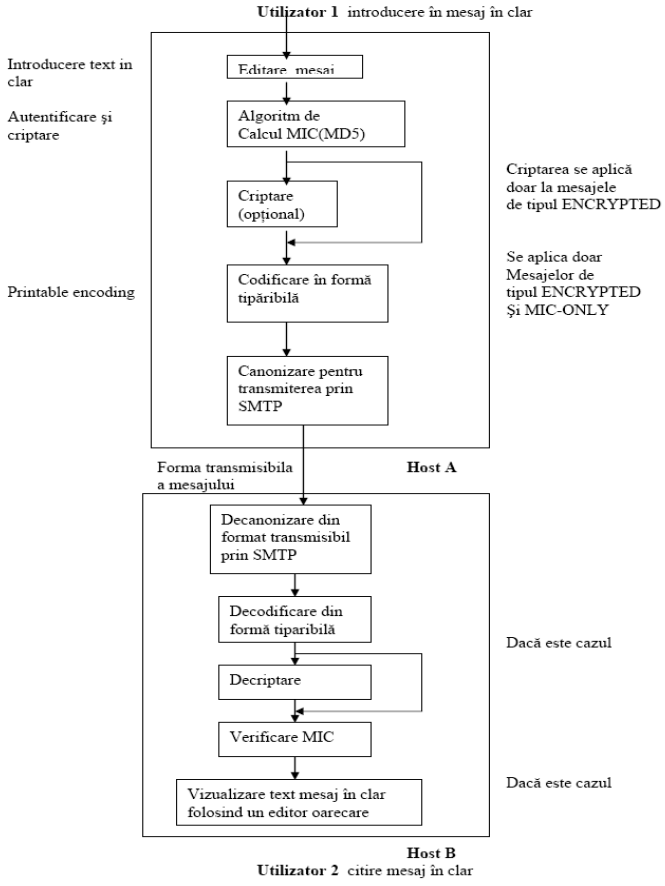

Figura 2 Prelucrarea unei scrisori PEM

Conţinutul mesajului PEM este încadrat la început şi la sfârşit de două mesaje separatoare.

În standardele PEM se definesc patru tipuri de mesaje PEM care permit realizarea a diferite combinaţii de servicii de securitate:

1) MIC-CLEAR – este un tip de mesaj care foloseşte un algoritm criptografic pentru verificarea integrităţii şi autenticităţii mesajului (MIC); nu se foloseşte cifrarea pentru secretizarea mesajului;

2) MIC-ONLY – este un tip de mesaj care oferă aceleaşi servicii de securitate ca MIC-CLEAR, dar la care se adaugă o codificare opţională, care asigură trecerea mesajului prin diferite calculatoare gateway fără a se modifica, lucru care i-ar afecta procesul de verificare a integrităţii;

3) ENCRYPTED – este un tip de mesaj care adaugă serviciul de confidenţialitate la cele de integritate şi autentificare. Se foloseşte şi codificarea de la MIC-ONLY deoarece, altfel, ieşirea binară a procesului de cifrare ar face ca mesajul să nu fie capabil să tranziteze acele sisteme de poştă electronică care nu permit transferarea de date binare, ci doar text;

4) CERTIFICATE REVOCATION (mesaj de revocare a autorizării) – care îi comunică unui UA că o autoritate de acordare a autorizărilor (certificatelor) a revocat una sau mai multe dintre aceste autorizări.

Părţile componente ale PEM:

• aducerea la forma canonică, numită canonizare, realizează transformarea mesajului din reprezentarea sa nativă, specifică calculatorului pe care s-a introdus scrisoarea, într-o formă standard, specifică reţelei. Tipul de canonizare folosit este specificat în câmpul *Content Domain* din antetul-PEM. De exemplu, aplicarea RFC 822 înseamnă utilizarea canonizării specifice protocolului SMTP pentru poşta neprotejată. O altă posibilitate poate fi, de exemplu, ASN.1;

• calculul valorii de integritate a mesajului (MIC – Message Integrity Code). Singura cerinţă impusă de standard, în aceast caz, este ca PEM să folosească un algoritm de calcul MIC foarte puternic, bazat pe o funcţie de dispersie one-way, greu inversabilă. Acest lucru reprezintă o consecinţă a nevoii de a se evita situaţia în care: un mesaj creat de utilizatorul A este adresat atât lui B cât şi lui C, însă atunci când ajunge la B, el este modificat de acesta şi trimis mai departe la utilizatorul C, fără ca acesta să-şi dea seama că a primit un mesaj fals. Valoarea MIC este calculată pentru versiunea canonizată a mesajului, pentru a putea fi verificată de reţele eterogene din punctul de vedere al resurselor de calcul. Algoritmul folosit pentru calculul MIC este specificat în antetul PEM, în câmpul MIC-Info. Pentru a se asigura şi autentifica emiţătorul, precum şi pentru nerepudierea mesajului prin dovedirea originii, MIC trebuie protejat în aşa fel încât să fie specific emiţătorului autentic. Pentru aceasta, MIC este semnat printr-un cifru cu chei publice (RSA), folosind cheia privată a emiţătorului scrisorii. Această semnătură poate fi verificată de către orice utilizator cu ajutorul cheii publice a emiţătorului. Câmpul MIC-Info conţine valoarea MIC semnată. Pentu ca recepţia să se poată stabili în mod sigur, realizarea legăturii dintre MIC şi emiţătorul mesajului, antetul PEM conţine un câmp care permite identificarea originii mesajului. Acest câmp conţine certificatul de cheie publică al emiţătorului mesajului care va fi folosit de receptor pentru verificarea integrităţii valorii MIC. În mesajul PEM pot exista mai multe câmpuri *Issuer-Certificate* care conţin alte certificate din ierarhia de emitere a lor, necesare pentru validarea valorii MIC. Pentru mai multă siguranţă, faţă de atacatori profesionişti, în cazul în care mesajul este cifrat pentru confidenţialitate, se va cifra cu aceeaşi cheie şi acelaşi algoritm simetric şi valoarea MIC semnată, din câmpul MIC-Info;

• cifrarea reprezintă al treilea pas (opţional) în prelucrarea PEM a mesajului. În acest caz apare în antetul PEM, în câmpul *Proc-Type*, valoarea *ENCRYPTED*. Pentru a se aplica algoritmul de cifrare, se generează la emiţător o cheie de cifrare care va fi folosită pentru protecţia unui singur mesaj. Algoritmul solicită în plus, faţă de cheie, o valoare aleatoare de 8 octeţi de iniţializare, numită *Initialization Vector*. Această valoare este inclusă ca parametru în câmpul *DEK-Info* din antetul PEM. Mesajul este cifrat o singură dată, indiferent de numărul de destinatari cărora le este adresată. Un fapt foarte important de menționat îl constituie transmiterea sigură a cheii de cifrare a mesajului la destinatari. Acest lucru se realizează folosind cheia publică a destinatarului, cu ajutorul căreia se cifrează cheia mesajului, proces numit anvelopare. Numai destinatarul autentic care deţine cheia privată pereche, va putea descifra în clar cheia de mesaj; apoi, cu aceasta va face descifrarea mesajului confidenţial. În cazul în care sunt mai muţi destinatari, cheia unică de mesaj va fi cifrată cu fiecare cheie a fiecărui destinatar, toate acestea fiind păstrate în câmpuri *Key-Info* din antetul PEM. Aici se precizează algoritmul folosit pntru cifrarea cu cheie publică. Fiecare câmp *Key-Info* este precedat de un câmp *Recipient-ID-Asymmetric*, care identifică destinatarul sub forma numelui distinct al emitentului certificatului său şi prin numărul serial al certificatului său, conform recomandărilor X.509;

• codificarea în vederea transmisiei are rolul de a converti mesajele de tip MIC ONLY şi ENCRYPTED PEM în şiruri de caractere care pot fi transmise în sistemele de transport al mesajelor. Codificarea se face pe cuvinte de 6 sau 7 simboluri ASCII, ceea ce asigură o compatibilitate cu protocolul SMTP, recunoscut de toate sistemele de poştă din rețeaua Internet.

La recepţie, algoritmul PEM presupune să se parcurgă mai întâi mesajul, apoi se analizează antetul PEM pentru a identifica tipul mesajului şi versiunea PEM. În funcţie de aceste informaţii se parcurg mai mulţi paşi de prelucrare: decodificarea, descifrarea și verificarea integrităţii mesajului.

6. PEM versus PGP

Cele mai utilizate sisteme de e-mail "sigur" sunt PGP şi PEM.

În mod intenţionat, PGP se bazează pe algoritmi de criptare existenţi, care au fost analizaţi anterior în detaliu. Sistemul foloseşte amprente de timp, iar în procesul de criptare se aplică şi algoritmul de compresie al cunoscutului program ZIP (creat de Ziv şi Lempel, 1977). Pentru asigurarea unei securităţi adecvate, utilizatorul poate alege lungimea cheii de criptare (mai exact, pentru algoritmul RSA): uzuală (384 biţi = 48O, poate fi spartă de "cei cu bugete mari"), comercială (512 biţi = 64O - poate fi spartă de "organizaţii care se ocupă de securitatea statului"), militară (1024 biţi = 128O - "nici un pământean nu o poate sparge"). În abordarea iniţială, o cheie de 2048 biţi = 256O era considerată "extraterestră" (care să nu poată fi spartă de nimeni), dar azi se discută şi despre chei de 4096 de biţi, şi este foarte probabil ca resursele de calcul ale viitorului să poată "descifra" şi cifruri cu asemenea chei.

Mesajele trimise folosind PEM sunt mai întâi convertite într-o forma canonică, apoi este calculat un cod de dispersie al mesajului folosind MD2 sau MD5. După aceasta, se realizează concatenarea codului de dispersie

şi a mesajului propriu-zis, şir care ulterior este criptat, folosind algoritmul DES. Mesajul criptat este apoi codificat, utilizând o codificare în baza 64, şi transmis destinatarului. Ca şi PGP, fiecare mesaj este criptat cu o cheie unică, inclusă în mesaj. Cheia poate fi protejată cu RSA, sau DES.

În procesul de criptare, se foloseşte algoritmul DES, ceea ce este considerat "suspect" de către specialişti, ţinând cont de lungimea mică a cheii DES (56 de biţi). Cheile folosite de PEM sunt certificate de o autoritate de certificare, fiind valabile pentru o anumită perioadă de timp. Practic, fiecare utilizator va folosi o asemenea cheie privată, specifică şi confidenţială, acordată şi validată după reguli riguroase de certificare; această cheie va fi folosită în paralel cu cheia publică. Politica autorităţilor de certificare este destul de complexă, existând o organizare ierarhică, cu trei niveluri. Astfel, administrarea cheilor este structurată după principii mai complexe decât în cazul PGP. Evident, există şi un mecanism de revocare a cheilor, în cazul compromiterii lor, ceea ce face ca trimiterea unui mesaj să fie în mod necesar precedată de verificarea automată a celei mai recente liste de revocări.

În PEM, autentificarea este obligatorie, pe când în PGP este opţională. Paradoxal este însă faptul că PGP, care nu este un standard oficial, are "cultura" Internet-ului, corespunzând principiilor nescrise care au dus la expansiunea acestuia, comparativ cu standardul oficial PEM. Aplicația lui Zimmerman s-a dovedit a fi o soluție foarte performantă şi în plus, a fost distribuit gratuit, pe când PEM, s-a dezvoltat în etape, folosind mai multe standarde Internet pentru diverse componente şi o structură organizațională rigidă, pe cele trei niveluri, cu tipuri diferite de autorităţi de certificare şi completată cu reglementări oficiale de certificare. Implementările PEM au apărut mai târziu decât cele ale PGP şi s-au dovedit ceva mai putin inspirate, din punct de vedere calitativ, cantitativ şi al disponibilității pe diverse platforme. De aceea, PGP a devenit un pachet tipic pentru Internet, mult mai larg folosit decât PEM.

Pentru utilizatorii obişnuiţi ai Internet-ului, cei mai convenabili algoritmi de criptare sunt cei cu cheie publică fiindcă folosirea lor nu implică schimbul preliminar de chei pe canale de transmisie protejate, ca în cazul algoritmilor cu cheie secretă. Cheia publică poate fi distribuită fără restricţii pe intranet sau Internet, iar mesajele criptate cu această cheie de către un emiţător vor putea fi decriptate numai utilizând cheia privată, care este deţinută exclusiv de către destinatar. Astfel, nici măcar expeditorul nu ar putea realiza decriptarea mesajului trimis.

7. CONCLUZII

Sistemul de poştă electronică este în acest moment o aplicaţie necesară pentru utilizatorii de calculatoare şi alte dispozitive ce permit accesul la e-mail, iar protocoalele implementate pentru manipularea mesajelor electronice oferă utilizatorilor siguranţa că acestea ajung la destinaţie în timp util.

PEM - Privacy Enhanced Mail (poştă cu confidențialitate sporită) este un standard oficial care oferă o varietate de servicii de securitate pentru utilizatorii poştei electronice, respectiv asigurarea secretului şi autentificarea sistemelor de mail bazate pe standardul uzual.

Multe instituţii nu se împacă cu ideea că prin Internet doi utilizatori pot schimba mesaje fără să poată fi "supravegheaţi". Cu toate acestea motto-ul lui Zimmerman nu s-a schimbat: "dacă dreptul la confidenţialitate este în afara legii, atunci doar cei aflaţi în afara legii vor beneficia de confidenţialitate".

BIBLIOGRAFIE:

1. **Guidelines on Electronic Mail. Guidelines Mail Security - Recommendations of the National Institute of Standards and Technology -** Miles Tracy, Wayne Jansen, and Scott Bisker – National Institute of Standards and Technology, NIST Special Publication 800-45 version 2, February 2007.
2. **RFC 821 - SIMPLE MAIL TRANSFER PROTOCOL -** Jonathan B. Postel - Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California 90291, August 1982.
3. **RFC 1081 - Post Office Protocol Version 3** - Network Working Group, M. Rose, November 1988.