

PEM – STANDARDUL DE POȘTĂ ELECTRONICĂ CU FACILITĂȚI DE SECURITATE

Prof. univ. dr. ing. Ciprian Răcuciu
Drd. ing. Dragoș 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: poștă electronică, securitate, algoritmi criptografici, confidențialitate, integritatea legăturii.

1. INTRODUCERE

Cu siguranță serviciul de poștă electronică este una dintre cele mai folosite facilități de comunicație din prezent. Există însă mulți 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 aplicații folosite pe sistemele de calcul, ducând în același timp la dezvoltarea și răspândirea la nivel global a internetului.

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

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

În ceea ce privește însă securitatea, poșta electronică nu oferă condițiile 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 și pe cele de pe Sun, este folosit programul *Sendmail* pentru a recepționa și trimite poșta electronică. Versiunile mai vechi de *Sendmail* au unele deficiențe privind securitatea, permițând penetrarea în sistem, obținerea unor drepturi de acces și activarea unor programe sau scripturi în mod ilegal. O astfel de deficiență a fost folosită de către Viermele Internet.

Se consideră că poșta electronică este un mediu deschis, ceva similar cărților poștale, a căror confidențialitate este deosebit de precară. De exemplu, avocații și clienții lor folosesc zilnic poșta electronică, dar au realizat că mesajele schimbate prin rețea pot fi citite de către persoane străine. Și chiar dacă intuiesc vulnerabilitatea poștei electronice, comoditatea și credința că numărul mare de mesaje care circulă în Internet face improbabilă interceptarea corespondenței, conduc la folosirea fără precauție a e-mail-ului. Cei implicați trebuie să rețină că sentimentul de intimitate este fals. Datorită faptului că poșta electronică este memorată sub formă digitală, aceasta se pretează a fi supusă unei analize la scară foarte mare cu ajutorul unor programe speciale și, ca urmare, mijloacele de selectare a unei anumite corespondențe de interes sunt mult mai eficiente decât în poșta tradițională.

O soluție pentru asigurarea confidențialității mesajelor transmise prin Internet ar putea consta în utilizarea unui soft adecvat protecției criptografice a scrisorilor schimbate prin poșta electronică. Pentru asigurarea securității acestui serviciu, specialiștii recomandă standardul PEM (Privacy Enhanced Mail) și programul PGP (Pretty Good Privacy), dar deosebit de utilizat este și standardul MOSS (Microsoft Office Sharepoint Server), în multe privințe foarte asemănător cu PEM.

Scopul declanșării proiectului PEM (Privacy Enhanced Mail) l-a constituit necesitatea asigurării securității transmisiilor între utilizatorii poștei 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 POȘTĂ ELECTRONICĂ

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

- a) confidențialitatea (secretizarea) mesajelor;

- b) autentificarea originii mesajelor;
- c) integritatea legăturii în rețea;
- d) nerepudierea mesajelor prin dovada originii.

Aceste servicii, definite și în modelul de referință al securității, OSI, pot fi divizate în două grupe:

- toate mesajele prelucrate în PEM încorporează facilitățile de autentificare, integritate și nerepudiere;
- confidențialitatea este un serviciu opțional, la alegerea utilizatorului.

(a) *Confidențialitatea* protejează conținutul mesajelor împotriva citirii lor neautorizate, de către alte persoane decât receptorii specificați de emițător. Obiectivul acestei protecții îl constituie fie ascultarea și înregistrarea neautorizată a traficului de pe liniile de comunicații, fie posibilitatea accesului la cutiile de scrisori, care sunt de fapt niște fișiere disc; împotriva unor astfel de atacuri se preferă secretizarea (criptarea) mesajelor.

(b) *Autentificarea originii mesajelor* permite receptorului unui mesaj prin poșta electronică să determine în mod sigur identitatea emițătorului scrisorii. Este un serviciu de securitate foarte util astăzi, când în sistemele de poștă electronică este relativ ușor să forțezi emiterea unor scrisori în numele unor alți utilizatori. Acest lucru creează mari semne de întrebare asupra credibilității mesajelor primite prin poșta electronică.

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

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

3. INTEGRAREA PEM ÎN SISTEMELE DE POȘTĂ ELECTRONICĂ

Încă din proiectare s-a intenționat ca PEM să fie utilizat în conjuncție cu sistemele de poștă electronică existente la ora actuală în rețeaua Internet.

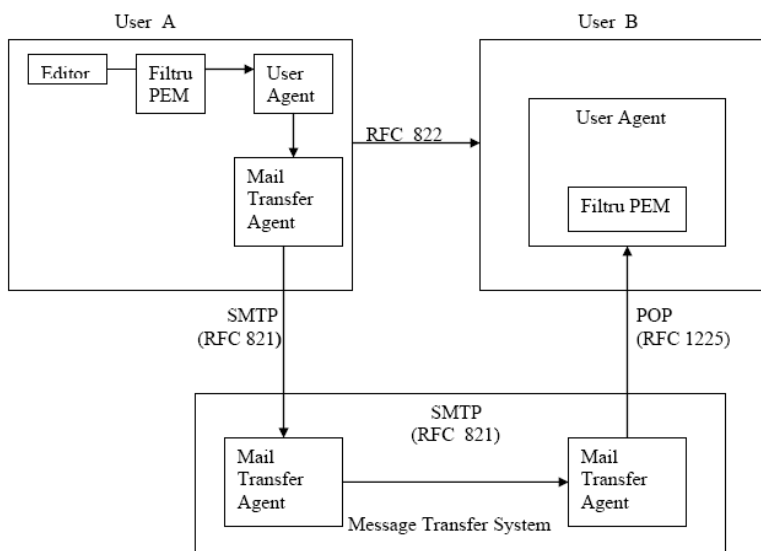


Figura 1 - Integrarea PEM în sistemele de poștă actuale

4. ALGORITMI CRIPTOGRAFICI UTILIZAȚI ÎN PEM

Pentru a se putea folosi serviciile de securitate oferite de PEM, acesta folosește o varietate de algoritmi criptografici, aceștia fiind necesari pentru cifrarea mesajelor, pentru distribuția cheilor criptografice utilizate la cifrare și descifrare, pentru verificarea integrității mesajelor și pentru autentificarea emițătorului și receptorului unui mesaj informațional.

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

- 1) Cu includerea funcțiilor de securitate în User Agent (UA); avantajul acestei variante constă în obținerea unei interfețe mai bune cu utilizatorul.
- 2) Fără modificarea User Agent-ului, prin realizarea unui filtru de securizare a mesajelor în exteriorul UA. Avantajele acestei variante sunt: posibilitatea folosirii filtrului în conjuncție cu o gamă largă de programe de tip UA existente și excluderea problemelor de integrare.

În cazul sistemelor criptografice simetrice (cu cheie secretă) se folosește aceeași cheie atât la cifrarea cât și la descifrarea mesajelor. Cheia secretă este folosită atât de către emițător cât și de către receptor. PEM folosește sisteme simetrice pentru a asigura secretizarea conținutului scrisorilor. În sistemele criptografice asimetrice (cu chei publice), în procesele de cifrare și de descifrare, se folosește o pereche de chei distincte (dar matematic legate una de alta). Una dintre aceste chei este menținută secretă și este cunoscută doar de către proprietarul ei. În același 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 și de distribuție sigură a cheilor de cifrare.

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

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

a) *Criptarea datelor.*

Dacă se dorește serviciul de confidențialitate 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 octeți) sunt:

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

b) *Integritatea mesajelor.*

Dacă se doresc serviciile de securitate, de integritate și de autentificare a expeditorului, atunci reprezentarea ASCII, a mesajului conținut, 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 definiți trei algoritmi în acest scop:

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

c) *Criptarea cheilor.*

După ce au fost generate, cheile de criptare și MIC-urile sunt trimise la receptor, ca parte a mesajului PEM. Pentru criptarea cheilor se utilizează un algoritm aparte. La momentul actual sunt definiți 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 distribuția cheilor, datorită ușurinței gestionării lor în comunitățile de utilizatori numeroase și foarte larg distribuite. Abordarea sistemelor cu chei publice în standardul PEM se face utilizând conceptul de certificat, așa 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 niște atribute de utilizator. Atributele pot fi, de exemplu, informații de identificare (nume, adresă) sau informații de autorizare (dreptul de a folosi o resursă). În structura certificatului sunt următoarele câmpuri:

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

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

5. PRELUCRAREA UNEI SCRISORI PEM

De regulă, autorul unui mesaj de poștă electronică securizată este un utilizator obișnuit, nu un specialist în criptografie și, de aceea, se dorește 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 poștă 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 – conține informația care furnizează serviciile de sporire a securității. Corpul acestui mesaj este numit “mesajul interior”;
- mesajul interior – mesajul pe care dorește 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, transmițând în condiții sigure mesajul la destinație.

O scrisoare este formată din două zone: antetul mesajului și conținutul mesajului.

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

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

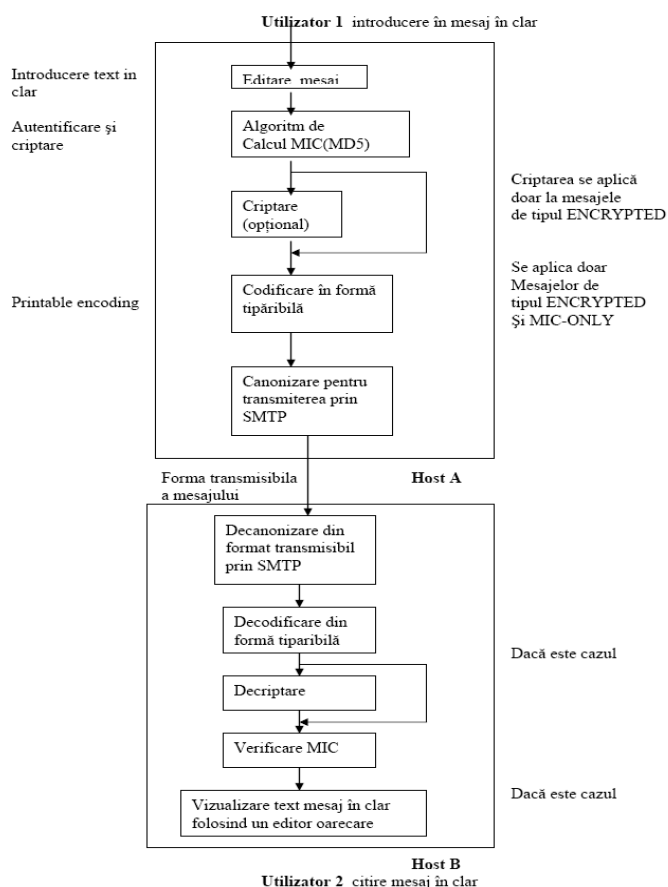


Figura 2 Prelucrarea unei scrisori PEM

Conținutul mesajului PEM este încadrat la început și la sfârșit de două mesaje separatoare.

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

1) MIC-CLEAR – este un tip de mesaj care folosește un algoritm criptografic pentru verificarea integrității și autenticității mesajului (MIC); nu se folosește cifrarea pentru secretizarea mesajului;

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

3) ENCRYPTED – este un tip de mesaj care adaugă serviciul de confidențialitate la cele de integritate și autentificare. Se folosește și codificarea de la MIC-ONLY deoarece, altfel, ieșirea binară a procesului de cifrare ar face ca mesajul să nu fie capabil să tranziteze acele sisteme de poștă 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.

Părțile 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 rețelei. 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 poșta neprotejată. O altă posibilitate poate fi, de exemplu, ASN.1;

- calculul valorii de integritate a mesajului (MIC – Message Integrity Code). Singura cerință impusă de standard, în acest caz, este ca PEM să folosească un algoritm de calcul MIC foarte puternic, bazat pe o funcție de dispersie one-way, greu inversabilă. Acest lucru reprezintă o consecință a nevoii de a se evita situația în care: un mesaj creat de utilizatorul A este adresat atât lui B cât și lui C, însă atunci când ajunge la B, el este modificat de acesta și trimis mai departe la utilizatorul C, fără ca acesta să-și dea seama că a primit un mesaj fals. Valoarea MIC este calculată pentru versiunea canonică a mesajului, pentru a putea fi verificată de rețele 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 și autentifica emițătorul, precum și pentru nerepudierea mesajului prin dovedirea originii, MIC trebuie protejat în așa fel încât să fie specific emițătorului autentic. Pentru aceasta, MIC este semnat printr-un cifru cu chei publice (RSA), folosind cheia privată a emițătorului scrisorii. Această semnătură poate fi verificată de către orice utilizator cu ajutorul cheii publice a emițătorului. Câmpul MIC-Info conține valoarea MIC semnată. Pentru ca recepția să se poată stabili în mod sigur, realizarea legăturii dintre MIC și emițătorul mesajului, antetul PEM conține un câmp care permite identificarea originii mesajului. Acest câmp conține certificatul de cheie publică al emițătorului mesajului care va fi folosit de receptor pentru verificarea integrității valorii MIC. În mesajul PEM pot exista mai multe câmpuri *Issuer-Certificate* care conțin alte certificate din ierarhia de emiteri a lor, necesare pentru validarea valorii MIC. Pentru mai multă siguranță, față de atacatori profesioniști, în cazul în care mesajul este cifrat pentru confidențialitate, se va cifra cu aceeași cheie și același algoritm simetric și valoarea MIC semnată, din câmpul MIC-Info;

- cifrarea reprezintă al treilea pas (opțional) 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 emițător o cheie de cifrare care va fi folosită pentru protecția unui singur mesaj. Algoritmul solicită în plus, față de cheie, o valoare aleatoare de 8 octeți de inițializare, 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 deține cheia privată pereche, va putea descifra în clar cheia de mesaj; apoi, cu aceasta va face descifrarea mesajului confidențial. În cazul în care sunt mai mulți 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 pentru 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 și prin numărul serial al certificatului său, conform recomandărilor X.509;

- codificarea în vederea transmisiei are rolul de a converti mesajele de tip MIC ONLY și ENCRYPTED PEM în șiruri 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 poștă din rețeaua Internet.

La recepție, algoritmul PEM presupune să se parcurgă mai întâi mesajul, apoi se analizează antetul PEM pentru a identifica tipul mesajului și versiunea PEM. În funcție de aceste informații se parcurg mai mulți pași de prelucrare: decodificarea, descifrarea și verificarea integrității mesajului.

6. PEM versus PGP

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

În mod intenționat, PGP se bazează pe algoritmi de criptare existenți, care au fost analizați anterior în detaliu. Sistemul folosește amprente de timp, iar în procesul de criptare se aplică și algoritmul de compresie al cunoscutului program ZIP (creat de Ziv și Lempel, 1977). Pentru asigurarea unei securități adecvate, utilizatorul poate alege lungimea cheii de criptare (mai exact, pentru algoritmul RSA): uzuală (384 biți = 480, poate fi spartă de "cei cu bugete mari"), comercială (512 biți = 640 - poate fi spartă de "organizații care se ocupă de securitatea statului"), militară (1024 biți = 1280 - "nici un pământean nu o poate sparge"). În abordarea inițială, o cheie de 2048 biți = 2560 era considerată "extraterestră" (care să nu poată fi spartă de nimeni), dar azi se discută și despre chei de 4096 de biți, și este foarte probabil ca resursele de calcul ale viitorului să poată "descifra" și cifruri cu asemenea chei.

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

și a mesajului propriu-zis, șir care ulterior este criptat, folosind algoritmul DES. Mesajul criptat este apoi codificat, utilizând o codificare în baza 64, și transmis destinatarului. Ca și 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 folosește algoritmul DES, ceea ce este considerat "suspect" de către specialiști, ținând cont de lungimea mică a cheii DES (56 de biți). 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 și confidențială, acordată și validată după reguli riguroase de certificare; această cheie va fi folosită în paralel cu cheia publică. Politica autorităților 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 și 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 opțională. 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 și în plus, a fost distribuit gratuit, pe când PEM, s-a dezvoltat în etape, folosind mai multe standarde Internet pentru diverse componente și o structură organizatională rigidă, pe cele trei niveluri, cu tipuri diferite de autorități de certificare și completată cu reglementări oficiale de certificare. Implementările PEM au apărut mai târziu decât cele ale PGP și s-au dovedit ceva mai puțin inspirate, din punct de vedere calitativ, cantitativ și al disponibilității pe diverse platforme. De aceea, PGP a devenit un pachet tipic pentru Internet, mult mai larg folosit decât PEM.

Pentru utilizatorii obișnuiți 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 restricții pe intranet sau Internet, iar mesajele criptate cu această cheie de către un emițător vor putea fi decriptate numai utilizând cheia privată, care este deținută exclusiv de către destinatar. Astfel, nici măcar expeditorul nu ar putea realiza decriptarea mesajului trimis.

7. CONCLUZII

Sistemul de poștă electronică este în acest moment o aplicație necesară pentru utilizatorii de calculatoare și alte dispozitive ce permit accesul la e-mail, iar protocoalele implementate pentru manipularea mesajelor electronice oferă utilizatorilor siguranța că acestea ajung la destinație în timp util.

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

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

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.