O ANALIZĂ PKI - PROTECȚIE ABSOLUTĂ SAU DOAR O ALTĂ SCHEMĂ DE SECURITATE?

Cristian Marinescu

cristian.marinescu@omicron.at
Universitatea „Politehnica" Bucureşti

Nicolae Voicu

voinick@hotmail.com
Academia Technică Militară

Rezumat: Comunicația prin intermediul rețelelor de calculatoare a luat amploare în ultimul timp, dar fără a ține seamă de necesitatea tot mai mare de securitate a diverselor aplicații. Protocolul TCP/IP, ce stă la baza acestei revoluții, a facilitat dezvoltarea rapidă, dar ideea de securitate a avut, de cele mai multe ori, de suferit, fiind nu de puține ori în contradicție cu scopul declarat al comunicației libere. Tehnologii diverse şi-au făcut apariția cu promisiunea de a realiza o siguranță absolută, în încercarea de a acoperi acest gol de securitate.

Infrastructurile cu chei publice sunt o tehnologie relativ nouă, ce se bazează pe criptografia asimetrică şi oferă diverse servicii în încercarea de a rezolva diverse probleme de securitate. Scopul articolului de față este de a realiza un studiu sumar al PKI, dar, mai ales, de a analiza, într-un mod cât mai realist posibil, problemele cu care se confruntă această tehnologie. A vedea doar beneficiile aduse de PKI, care de altfel nu pot fi tăgăduite, nu îmbunătățeşte în nici un caz siguranța, subminând doar ideea de securitate şi de încrederea în aceasta tehnologie.

Cuvinte cheie: certificate, PKI, securitate.

1. Modelul PKI

O infrastructură cu chei publice (PKI) se bazează pe criptografia asimetrică şi reprezintă cadrul şi serviciile ce pun la dispoziția utilizatorului metode pentru a genera, distribui, controla, contoriza şi revoca certificate cu chei publice. O structură PKI se constituie, de obicei, din una sau mai multe autorități de certificare (CA), un container cu certificate, şi documentația ce include politica de certificare, baza fiind însă reprezentată de certificatul cu cheie publică. Într-un sens mai larg, se poate spune că PKI integrează certificatele digitale, criptografia cu cheie publică şi noțiunea de autoritate de certificare într-o arhitectură de securitate a rețelei.

Din punct de vedere funcțional, PKI oferă suport pentru semnare şi criptare digitală a datelor. Acestea pot fi folosite în cadrul diverselor servicii de securitate [1]:

- **identificarea** şi **autentificarea** sunt realizate cu ajutorul semnăturilor digitale; entitatea ce trebuie autentificată sau identificată va semna o provocare cu ajutorul cheii sale private. Verificatorul semnăturii poate fi sigur de *identitatea* celui cu care discută în baza a trei condiții presupuse a fi îndeplinite: 1. cheia privată este cunoscută doar proprietarului său; 2. există o singură cheie privată, care să corespundă cheii publice din certificatul digital; 3. certificatul face legătura nemijlocită între identitatea proprietarului şi cheia sa publică. Presupunând aceste condiții îndeplinite, verificarea semnăturii digitale va duce implicit la „cunoaşterea" partenerului de dialog [2];
- **integritatea datelor** este obținută tot prin intermediul semnăturilor digitale; verificarea cu succes a semnăturii (operație efectuată cu ajutorul cheii publice), duce la concluzia că datele nu au fost modificate ulterior procesului de semnare;
- **confidențialitatea** este realizată cu ajutorul procesului de criptare; folosirea cheii publice dintr-un certificat pentru stabilirea unui canal de comunicație criptat are ca rezultat faptul că doar entitatea menționată în certificat (cea care este şi deținătoarea cheii private) va fi capabilă să decripteze mesajele criptate;
- **nonrepudierea** datelor este asigurată prin intermediul semnăturilor digitale; presupunând că posesorul certificatului este singura entitate care cunoaşte cheia privată, verificarea semnăturii realizate asupra unor date va duce la certitudinea că posesorul certificatului este emitentul sau distribuitorul datelor sau a fost de acord cu semnarea lor în forma respectivă.

Serviciile enumerate anterior necesită câteva clarificări. În primul rând, trebuie remarcată diferența dintre autentificare şi identificare. Practic, dacă certificatul a fost generat de o CA, atunci se presupune că, la generarea acestuia, CA - ul s-a asigurat într-un anume fel de identitatea celui ce va beneficia de certificat (că, de exemplu, numele menționat în certificat corespunde persoanei căreia i-a fost generat certificatul). În cazul în care certificatul nu a fost generat de o autoritate de certificare, ci a fost generat şi semnat, de exemplu, chiar de persoana care îl utilizează, nu se poate spune decât că interlocutorul a fost identificat ca posesor al cheii private, corespunzătoare cheii publice din certificat. În ceea ce priveşte nonrepudierea, trebuie menționată şi diferența dintre originea unui document şi simpla semnare a acestuia, originea neputând fi

confirmată doar în baza unei semnături. În general, semnătura digitală asupra unui document poate avea diverse înțelesuri, în funcție și de conținutul semnat. Totodată, trebuie remarcat faptul că PKI nu oferă în mod implicit servicii de audit, de autorizare, sau de analiză a privilegiilor. Serviciile menționate pot fi, însă, adăugate la cele existente, luând în calcul un oarecare efort suplimentar [3].

Autoritatea de certificare este entitatea implicată în generarea, verificarea, distribuirea și revocarea certificatelor. Într-un sens mai larg, se poate afirma că ea reprezintă inima sistemului PKI, fiind considerată o "Trusted Third Party" (TTP) în care toți utilizatorii pot avea încredere. Acest fapt este și unul din motivele de dispută, nu puțini fiind cei care au pus în discuție întregul sistem din această cauză. În realitate, se întâlnesc două tipuri de autorități de certificare:

- CA rădăcină, care își semnează singure propriile certificate,
- cele subordonate, ce vor apela la alte autorități de certificare pentru a le semna certificatele.

Există însă și o categorie de aplicații care acceptă certificate generate și semnate direct de utilizator, dar, de obicei, acestea sunt supuse unor restricții de utilizare. La generarea certificatului, verificările pot fi făcute direct de CA sau de un reprezentant al acestuia, autoritatea de înregistrare (RA), mandatată special în acest scop. După calitatea procesului de verificare a identității, certificatele se împart în patru clase:

- clasa I: certificate ce leagă, de obicei, o pereche de chei de o adresă de e-mail: pentru generarea acestora nu este verificată identitatea utilizatorului, certificatele din această clasă fiind utilizate privat pentru securizarea sau semnarea e-mail-ului;
- clasa a II-a: certificate ce includ ceva mai multe informații despre utilizator, dar care nu presupun în mod neapărat verificări din partea autorității de certificare;
- clasa a III-a: certificate pentru a căror generare CA va efectua o verificare a identității utilizatorului sau entității descrise de acesta;
- clasa a IV-a: certificate generate de guverne sau organizații ce necesită un grad ridicat de verificări asupra identității utilizatorului.

În general, se pot folosi două metode pentru generarea perechii de chei:

- utilizatorul își generează singur perechea de chei, urmând ca apoi să transmită cheia publică autorității de certificare, aceasta din urmă trebuind să genereze și să semneze certificatul;
- CA generează atât certificatul, cât și perechea de chei necesară: datorită faptului că încalcă principiul păstrării cheii secrete, această metodă este destul de controversată; unele implementări evită utilizarea ei tocmai din această cauză, utilizatorul trebuind să aibă o încredere sporită în autoritatea de certificare, și anume că aceasta nu va abuza de faptul că este practic a doua entitate ce cunoaște cheia privată; în plus, există pericolul unei intruziuni, ceea ce ar pune la dispoziția atacatorului posibilitatea de a afla cheile private ale certificatelor generate.

Autoritatea de certificare trebuie să publice un manifest de certificare, ce descrie pe scurt politicile și metodele folosite în generarea, revocarea și managementul cheilor. Manifestul specifică și cât de des este actualizată lista certificatelor revocate (CRL), listă ce conține certificatele declarate invalide, înaintea expirării termenului de valabilitate. Astfel, CRL reprezintă o metodă de a „retrage" certificatele din circulație, înainte ca termenul de valabilitate să expire. Problema CRL poate fi cuplată cu cea de distribuție de certificate. Se disting, astfel, două abordări în distribuția certificatelor:

- publicarea certificatelor în directoare, asemănătoare cu o carte electronică de telefon: aceasta are avantajul că, atunci când un certificat nu mai este valid, el poate fi șters sau însemnat ca atare în director (ștergerea introduce în plus problema verificărilor ulterioare invalidării); această metodă are, însă, și marele dezavantaj că presupune tot timpul un acces online la directorul cu certificate, ceea ce nu este întotdeauna posibil (o problemă o reprezintă chiar atacurile de tipul "Denial of Service", care ar împiedica accesul la director, inducând concluzia falsă că, din moment ce un certificat nu poate fi accesat, el nu mai este valid);
- trimiterea certificatelor tuturor entităților care au nevoie de ele sau publicarea lor pe site-uri unde toată lumea le poate accesa de câte ori este necesar: această metodă introduce nevoia de a menține o listă de revocare a certificatelor; în acest caz, folosirea unui certificat necesită verificarea CRL pentru a constata dacă certificatul în cauză a fost revocat înaintea datei de expirare.

Se pot imagina și soluții mixte, care, deși utilizează un director electronic pentru certificate, utilizează o CRL pentru invalidarea acestora.

Verificarea stării (valid/invalid) unui certificat reprezintă o problemă pentru aplicațiile care folosesc PKI. Folosirea CRL a fost preluată după metodele de verificare a credit-card-urilor din anii '70. Credit-

card-urile care erau compromise erau adăugate într-o „listă-neagră", iar cei care verificau un credit-card trebuiau să caute în această listă pentru a se asigura că nu este revocat. Când aceste liste au devenit din ce în ce mai mari procesul de distribuție și verificare a devenit tot mai dificil. Aceleași probleme se întâlnesc și în folosirea CRL. O alternativă o reprezintă folosirea Online Certificate Status Protocol (OCSP) de fiecare dată când se dorește cunoașterea stării unui certificat [10]. Folosind acest protocol, aplicațiile nu trebuie să consulte o listă mare (și uneori neactualizată) de certificate (CRL), ci doar să trimită o cerere către un serviciu OCSP pentru starea certificatului în cauză. OCSP are dezavantajul că presupune un acces online la serviciul OCSP.

În general, există o serie de beneficii ce rezultă din adaptarea unor aplicații la modelul PKI: întregul sistem prezintă o portabilitate ridicată, utilizatorul având acces sigur din diverse locații la informațiile sale; utilizatorii sistemului vor beneficia de comunicații sigure și secrete cu ajutorul capacităților de criptare; sistemul permite atât separarea operației de identificare și autentificare de operația de autorizare, cât și faptul că actele în forma lor clasică (pe suport de hârtie) pot fi înlocuite cu documente în format electronic. Toate acestea vor avea ca rezultat o anumită automatizare a proceselor de prelucrare și, implicit, o schimbare a atitudinii utilizatorilor față de sistem.

Procesul de adaptare a unor aplicații existente și de integrare a acestora într-o infrastructură cu chei publice nu reprezintă o operație banală [6]. Aceasta presupune că aplicațiile sau mediul în care rulează ele să poată: să manipuleze cheile și certificatele în mod sigur; să accepte și să proceseze certificatele valide; să fie capabile să obțină date relevante pentru certificate și pentru revocarea acestora. Trebuie subliniată diferența dintre o infrastructură cu chei publice și o aplicație care este doar capabilă să folosească serviciile de securitate puse la dispoziție de aceasta.

2. Certificate cu cheie publică. Certificate X.509

Certificatele reprezintă o unealtă în criptografia cu chei publice, dar nu constituie o soluție în sine. Fără o infrastructură care să fie capabilă să gestioneze, genereze, verifice și invalideze certificate, acestea nu reprezintă decât o nouă structură de date. Una dintre problemele de bază în criptografia cu chei publice este determinarea identității entității care posedă o cheie privată. Pentru a rezolva această problemă, a fost introdus conceptul de certificat cu cheie publică sau, mai simplu, certificat. El reprezintă elementul de bază al unei infrastructuri cu chei publice. De altfel, el nu introduce un concept nou, reluând idei deja întâlnite sub diverse forme la cartea de credit și la cartea de vizită. Structura certificatului include, pe lângă cheia publică, și informații despre posesorul acesteia, putându-se afirma că un certificat nu reprezintă decât o legătură între identitatea unei entități și cheia sa publică.

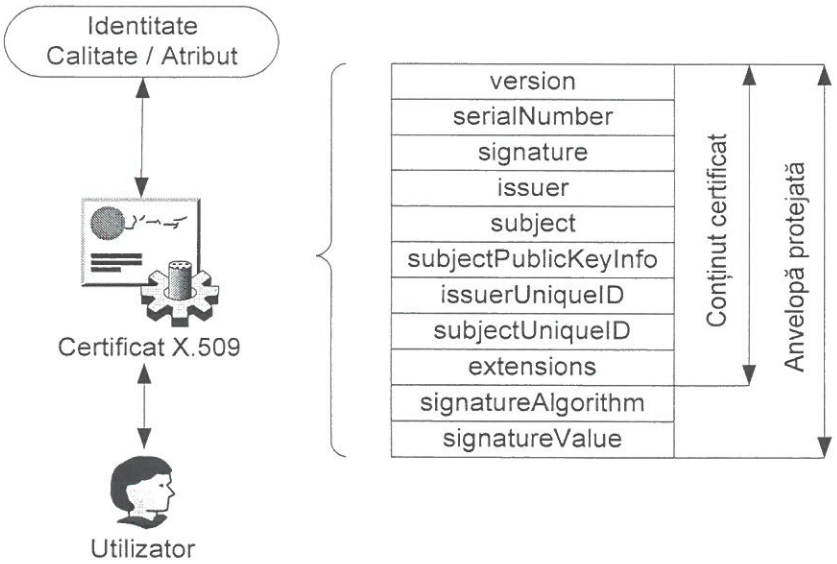

Figura 1 Conținutul certificatului X.509

Certificatul ideal combină proprietăți ale cărții de credit și ale cărții de vizită, cu diferența că încearcă, totodată, să rezolve problemele apărute în utilizarea acestora. Un certificat ideal întrunește următoarele proprietăți:

1. este un obiect pur digital, care poate fi procesat automat și distribuit prin intermediul unei rețele de calculatoare;

2. identifică posesorul său prin nume, eventual prin firma unde lucrează, şi conţine informaţia necesară contactării acestuia (adresa, adresa de poştă electronică etc.);
3. este uşor de determinat când a fost emis certificatul;
4. a fost generat de o autoritate neutră, în care se poate avea încredere, aşa numita "trusted third party";
5. include un identificator unic astfel încât să poată fi identificat şi deosebit de orice alt certificat emis de aceeaşi autoritate;
6. este uşor de stabilit dacă certificatul reprezintă un fals sau nu;
7. se poate determina dacă datele certificatului au fost modificate sau falsificate;
8. este uşor de verificat dacă certificatul este valabil, a expirat sau a fost revocat de către autoritatea emitentă;
9. se poate stabili modul şi contextul în care utilizatorul are dreptul de a utiliza certificatul.

După cum am menţionat, certificatul reprezintă un pas în soluţionarea anumitor probleme de securitate, însă, prezintă şi anumite dezavantaje. La o analiză mai atentă se poate observa faptul că se introduc o serie de alte probleme care, în unele cazuri, pot duce până la compromiterea ideii de securitate. Dintre acestea menţionăm:

- alegerea/acceptarea CA (certificatul necesită o autoritatea de certificare emitentă, în care utilizatorul să aibă încredere);
- acceptarea altor autorităţi emitente, atunci când utilizatorul primeşte un certificat generat de o autoritate necunoscută şi lanţul de certificate este greu/imposibil de verificat;
- compromiterea autorităţii de certificare duce la compromiterea tuturor certificatelor emise de aceasta şi, implicit, la compromiterea întregii scheme PKI.

Certificatul X.509 utilizat şi în cadrul PKI reprezintă o aproximare destul de bună a certificatului ideal, prezentat anterior. Figura 1 prezintă în detaliu câmpurile componente ale unui certificat X.509 [5]. Câmpul *version* indică versiunea certificatului, aceasta fiind, totodată, şi un indicator al sintaxei utilizate. Numărul de serie identifică în mod unic certificatele emise de o anumită autoritate de certificare. Câmpurile următoare indică algoritmul utilizat pentru semnătura digitală, emitentul certificatului, cât şi perioada de valabilitate a acestuia. Câmpul *subject* conţine numele posesorului certificatului (în fapt, al posesorului perechii de chei). Acesta poate fi un utilizator, o altă autoritate de certificare sau orice entitate bine definită. Câmpul *subjectPublicKeyInfo* conţine cheia publică, cât şi identificatorul algoritmului cu care poate fi utilizată aceasta (RSA, DSA, D-H etc.). În funcţie de algoritmul specificat, urmează o serie de parametri opţionali sau obligatorii, care sunt necesari alături de cheia publică în operaţiile de criptare şi de verificare din cadrul algoritmului. Câmpurile *issuerUniqueID* şi *subjectUniqueID* au fost introduse o dată cu versiunea 2, dar nu şi-au atins scopul de a identifica în mod corespunzător posesorul şi emitentul certificatului. De aceea, versiunea 3 recomandă ca diversele implementări să poată citi aceste câmpuri şi să respingă certificatele ce conţin aceste câmpuri. Câmpul opţional *extensions* conţine toate extensiile prezente şi viitoare ce pot fi adăugate ulterior certificatelor. Formatul ASN.1 al unui certificat X.509 este specificat în Figura 2.

Un certificat X.509 poate fi practic considerat ca fiind alcătuit din trei componente încapsulate. Componenta exterioară este reprezentată de anvelopa semnăturii digitale, asigurând propriu-zis integritatea datelor ce alcătuiesc conţinutul certificatului. În interiorul acesteia, se regăseşte certificatul de bază şi extensiile acestuia.

Este relativ uşor de observat că, în utilizarea zilnică a sistemelor PKI, utilizatorul va întâlni şi autorităţi emitente pe care nu le cunoaşte. Se pune astfel întrebarea, pe ce criterii va alege utilizatorul să aibă încredere într-o autoritate necunoscută. Mecanismele PKI introduc noţiunea de cale de certificare, prin care, o autoritate de certificare semnează certificatul altor autorităţi de certificare. Se creează astfel premisele ca utilizatorul care are încredere în autoritatea de certificare A, va avea posibilitatea să acorde încredere şi autorităţii de certificare B, atâta timp cât prima va garanta identitatea celei de-a doua, prin semnătura sa digitală. Trebuie totuşi remarcat faptul că soluţia propusă este greoaie. Dacă lanţul de certificare este lung, procesul de verificare este relativ greoi, presupunând o mulţime de operaţii de verificare a fiecărei verigi componente.

Certificat X.509 în format ASN.1

```
TBSCertificate ::= SEQUENCE {
version                 [0] EXPLICIT Version DEFAULT v1,
serialNumber            CertificateSerialNumber,
signature               AlgorithmIdentifier,
issuer                  Name,
validity                Validity,
subject                 Name,
subjectPublicKeyInfo    SubjectPublicKeyInfo,
issuerUniqueID          [1] IMPLICIT UniqueIdentifier OPTIONAL,
subjectUniqueID         [2] IMPLICIT UniqueIdentifier OPTIONAL,
extensions              [3] EXPLICIT Extensions OPTIONAL
}
```

Figura 2 Formatul ASN.1 al unui certificat X.509

Vom face, în continuare, câteva referiri la asemănările şi diferenţele dintre certificatele ideale şi cele X.509. Certificatele X.509 aproximează, în general, destul de bine certificatele ideale, existând însă şi mici diferenţe, datorate, în special, necesităţii de adaptare la lumea reală. Se poate observa că primele 6 proprietăţi ale unui certificat ideal sunt îndeplinite şi de un certificat X.509. Semnătura autorităţii de certificare asigură integritatea conţinutului certificatului (proprietatea a 7-a). Pentru a stabili dacă un certificat este valabil sau nu, utilizatorul trebuie să verifice dacă acesta se află în termenul de valabilitate, dacă conţinutul său nu a fost modificat şi semnătura digitală a autorităţii emitente este autentică, dacă acesta se află pe lista certificatelor revocate sau nu. CRL este publicată de către autoritatea emitentă, aceasta având datoria de a menţine lista la zi. Lista de revocare nu reprezintă o soluţie ideală, dar este o modalitate de a oferi informaţii despre certificatele compromise sau revocate anterior termenului de expirare. Dacă este inclusă în certificat şi informaţie despre modul şi contextul în care posesorul acestuia are dreptul să-l utilizeze, se poate spune că toate proprietăţile unui certificat ideal pot fi transferate şi asupra certificatelor X.509.

3. O analiză a problemelor PKI

La o primă privire, s-ar putea afirma faptul că PKI reprezintă soluţia perfectă pentru majoritatea problemelor de securitate. Este însă important de remarcat că şi PKI, la fel ca şi alte tehnologii, prezintă o serie de dezavantaje şi puncte vulnerabile. Din păcate, acestea sunt de cele mai multe ori trecute sub tăcere, datorită faptului că această tehnologie a fost propulsată, în principal, de firme interesate în vânzarea propriilor produse. Piaţa ce se deschide pentru vânzarea de certificate cu cheie publică reprezintă o sursă importantă de venit, firmele încercând să-şi adjudece supremaţia prin impunerea în acest segment a propriilor variante PKI, care, de cele mai multe ori, nu sunt compatibile între ele. Procesul ulterior de standardizare a urmat o cale greoaie, şi nu a făcut decât să complice lucrurile [6].

Înainte de a trece la o analiză detaliată a diverselor probleme, trebuie menţionat faptul că securitatea poate fi comparată cu un lanţ, veriga cea mai slabă a acestuia dictând securitatea întregului sistem. Cu alte cuvinte, sistemul este la fel de sigur în ansamblul său ca şi cea mai nesigură componentă a sa. De aceea, este foarte importantă analiza detaliată a punctelor vulnerabile ale unui sistem.

De-a lungul timpului, au apărut o serie de dispute pe marginea întrebării dacă PKI oferă o securitate suficientă sau reprezintă doar o altă tehnologie având propriile sale probleme. Vom încerca, în continuare, să elucidăm răspunsul la aceasta întrebare, analizând diversele critici şi aducând argumente pro şi contra.

3.1. În cine avem încredere şi de ce?

Problema apare din definiţia imprecisă a nivelului de încredere. Se pleacă de la premisa că o autoritate de certificare este considerată, în mod automat, TTP şi că trebuie avut încredere în aceasta. Apar, în mod firesc, întrebările: cine a acordat CA dreptul să emită certificate? Este CA o autoritate nu numai în generarea certificatului, ci şi în ceea ce conţine certificatul sau, cu alte cuvinte, cât de temeinic a fost verificată informaţia (în special, identitatea) despre entitatea căreia i-a fost generat certificatul? Se poate argumenta că, la fel ca şi în multe alte protocoale existente la ora actuală în criptografie (în special la cele bazate pe criptografie asimetrică), nici PKI nu face excepţie de la aceste reguli, unul din elementele de bază fiind tocmai necesitatea de a considera autoritatea de certificare un TTP. Trebuie subliniat şi faptul că, în lumea

reală, majoritatea tehnicilor de securitate funcționează în baza existenței unui TTP. Dacă se acceptă acest risc în general, el poate fi la fel de bine acceptat şi în cazul PKI. Problema poate fi rezolvată lăsând la latitudinea utilizatorului să aleagă dacă are sau nu încredere într-o CA, dar, şi în acest caz, apar unele dezavantaje. Trebuie remarcat însă faptul că utilizatorul mediu nu are cunoştințele necesare în domeniul securității, de cele mai multe ori nefiindu-i clare implicațiile alegerilor sale. De aceea, posibilitatea de a-l lăsa să aleagă ori de câte ori este necesar, în special în cazurile limită, nu reprezintă o soluție.

3.2. Identificarea nu reprezintă implicit o autorizare

Este foarte răspândită confuzia ce se face între identificare şi autorizare, chiar şi în rândul specialiştilor în domeniu. Pornind de la următorul lanț logic: un certificat de identitate specifică numele posesorului perechii de chei, iar verificarea semnăturii indică cunoaşterea entității cu care comunicăm, deci autorizarea a fost reuşită, duce la confuzia mai sus amintită. Evitarea confuziei dintre cele două noțiuni are ca rezultat evitarea unor riscuri [7]. Procesul de autorizare este, de cele mai multe ori, asociat cu aplicațiile care folosesc PKI. Plecând de la identitatea obținută din certificat, se verifică dacă acestei identități îi este permisă o anumită acțiune (semnarea unui document, accesul la o resursă etc.)

3.3. Cine utilizează şi cine are acces la cheia privată?

Problema păstrării cheii private într-un loc sigur, reprezintă în mod cert una dintre problemele cele mai mari în criptografia cu cheie publică. Această problemă nu este specifică doar tehnologiei PKI, în general, toate sistemele ce utilizează chei secrete sau private prezentând acest punct slab. Toată construcția se bazează pe presupunerea că posesorul cheii private este şi singurul care are acces la aceasta, sau că, altfel spus, orice program care trebuie să folosească cheia sa privată o va face doar cu acordul acestuia. Deci, o dată ce semnătura a fost creată şi există, posesorul cheii este responsabil de ceea ce a semnat, neavând dreptul să repudieze ceea ce a semnat. Din păcate, aceasta poate fi o problemă, majoritatea implementărilor PKI, preluând această idee, au forțat chiar şi legi în anumite țări (USA), unde posesorul cheii este considerat responsabil pentru tot ce a fost semnat cu cheia sa privată. Aceste legi încalcă, practic, metodele de lucru întâlnite la card-urile de credit, unde responsabiliatea revine companiei emitente (VISA, MASTERCARD etc.) de a demonstra că clientul a fost cel care a comandat produsul, şi nu invers. Aceasta face foarte dificilă retractarea unei semnături chiar şi in cazul în care aceasta ar trebui permisă (furtul cheii private).

De aceea, se recomandă păstrarea cheilor private pe smartcard-uri, şi nu local, pe discul calculatorului personal. În cazul în care nu este posibil acest lucru, se recomandă păstrarea cheilor private în fişiere criptate, accesibile cu PIN sau parolă, iar calculatorul să nu fie expus încercărilor de penetrare din exterior (protecție firewall etc.).

3.4. Pot fi falsificate certificatele?

Din păcate, răspunsul la această întrebare este afirmativ. PKI permite utilizarea unor certificate rădăcină, care sunt semnate de aceeaşi entitate care le-a şi generat. Este suficientă introducerea unui astfel de certificat în lista certificatelor rădăcină, apoi folosindu-l pe acesta drept certificat al autorității de certificare, pot fi generate certificate false fără nici o problemă. De aceea, pentru a preîntâmpina această vulnerabilitate, se recomandă impunerea unei metode diferite – *out of band* – de verificare a acestor certificate, diferită de cea aplicată la certificatele normale [8]. Din păcate, în funcție de soluția avută în vedere, un client PKI normal, va fi pus în situația de a nu putea verifica aceste certificate, având de ales între a-l accepta fără verificare sau a-l refuza.

3.5. Cât de precisă este identificarea unei entități?

Certificatele asociază, în general, o cheie publică cu un nume, dar, de obicei, nu se precizează că, în anumite cazuri, această identitate nu este suficientă, atâta timp cât acesta nu este un identificator unic. În aceste cazuri, este de dorit introducerea unor informații suplimentare, care să identifice în mod unic persoana sau entitatea în cauză (data de naştere, CNP, adresă etc.). În acest context, se revine din nou la prima problemă prezentată şi anume care este autoritatea CA de a verifica această informație şi de a asigura autenticitatea acesteia, şi, nu în ultimul rând, care este răspunderea CA în cazul unei erori.

3.6. Cât de sigur este calculatorul ce efectuează verificarea?

Procesul de verificare a unui certificat poate fi, în general, sabotat, dacă atacatorul câştigă acces la calculatorul ce va efectua această operaţie. Deşi verificarea se bazează doar pe date publice (verificarea se efectuează întotdeauna cu ajutorul cheii publice), dacă se reuşeşte măsluirea acestui proces se poate impune acceptarea unui certificat fals, ceea ce poate avea rezultate dezastruoase pentru securitatea sistemului.

Această problemă, deşi din punct de vedere teoretic reprezintă un punct vulnerabil, nu este relevantă datorită faptului că necesită, în general, un efort mult prea mare pentru a compromite calculatorul verificator, câştigul obţinut fiind mult prea mic (mai repede se încearcă furtul cheii private decât măsluirea procesului de verificare a unui certificat cu cheie publică). În general, în comerţul electronic, se va încerca compromiterea serverului, şi nu a clientului unde are loc această verificare. Totuşi, nu se pot şi nu e bine să se facă aprecieri asupra securităţii calculatorului ce efectuează verificarea unui certificat, fiind rezonabil a se lua în considerare şi această posibilitate.

3.7. Ce rol joacă utilizatorul în luarea unei decizii pertinente?

Se pune întrebarea dacă utilizatorul este privit ca un participant la întregul proces şi dacă acesta a fost cuprins în faza de proiectare a sistemului. Majoritatea soluţiilor nu oferă posibilitatea de a consulta utilizatorul ori de câte ori apare o situaţie ce necesită luarea unei decizii. Implicarea utilizatorului în procesul decizional prezintă, în general, şi dezavantaje:

- utilizatorul care nu are cunoştinţe în domeniul securităţii, nu va fi în stare să ia o decizie pertinentă; în plus, de cele mai multe ori este de dorit, totuşi, o soluţie transparentă, care să nu implice pe parcurs o nouă decizie (un nou dialog de parcurs) din partea utilizatorului;
- majoritatea soluţiilor software existente nu încurajează această abordare, tocmai din dorinţa de a feri utilizatorul de astfel de decizii, în plus respingerea certificatului duce clar la abandonarea operaţiei în curs.

3.8. Este necesar PKI pentru a realiza comerţ electronic?

Răspunsul la această întrebare este negativ, deoarece nu este neapărat necesară o structură PKI pentru a realiza comerţ electronic. Acesta reuşise să se impună încă de pe vremea când încă nu existau certificate cu cheie publică. Este însă adevărat că PKI oferă propriu-zis o structură care poate facilita comerţul electronic. Modelul de autentificare este invers faţă de cel utilizat în mod clasic, în care utilizatorul este autentificat de către server. În această variantă, serverul de produse este entitatea care este autentificată de către client. Certificatul serverului nu face decât să lege numele DNS utilizat, de numele companiei sau al firmei care îşi oferă produsele spre vânzare pe Internet. Acest tip de certificat este, însă, destul de controversat, deoarece o autoritate de certificare nu este nici o autoritate DNS, şi nici un registru de comerţ care să poată verifica datele unei firme. De aici, se revine la prima problemă şi anume, care este autoritatea CA de a verifica această informaţie şi de a asigura autenticitatea acesteia?

După cum se poate observa din argumentele aduse anterior, vulnerabilităţile prezentate pot să scadă în mod considerabil securitatea unui sistem PKI. Este cert că şi o structură PKI poate fi compromisă, vina nefiind a criptografiei cu chei asimetrice (algoritmii asimetrici de genul RSA, DSA, încercaţi de-a lungul timpului pot fi consideraţi siguri până la o eventuală compromitere a acestora), ci mai ales datorită overhead-ului impus de lucrul cu certificate şi a negării existenţei acestor vulnerabilităţi.

Se impune, de asemenea, concluzia că nu numai tehnologia prezintă probleme, ci şi diversele implementări provenite de la producătorii de software, cel mai adesea interesaţi în realizarea unui profit, şi nu atât în realizarea unei soluţii sigure standardizate. Totodată, trebuie subliniat şi faptul că PKI rămâne totuşi la ora actuală, cel puţin din punct de vedere teoretic, una din tehnologiile cele mai importante în implementarea securităţii la scară largă [9].

Bibliografie

1. **ADAMS, C., S. LLOYD**: Understanding PKI: Concepts, Standards and Deployment Considerations, Addison–Wesley, 2003.
2. **SMITH, R. E.**: Authentication – From Passwords to Public Keys, Addison–Wesley, 2002.
3. **MENEZES, A., P. VAN OORSCHOT, S. VANSTONE**: Handbook of Applied Cryptography, CRC Press, 1996.
4. * * *: The DoD Public Key Infrastructure And Public Key–Enabling – Frequently Asked Questions, 2004, *http://iase.disa.mil/pki/faq-pki-pke-may-2004.doc*
5. * * *: PKCS #6: Extended–Certificate Syntax Standard", RSA Laboratories Technical Note, 1993, *http://www.rsasecurity.com/rsalabs/node.asp?id=2128*
6. **ELLISON, C., B. SCHNEIER**: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", *http://www.schneier.com/paper-pki.pdf*
7. **GUTMANN, P.**: X.509 Style Guide, *http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt*
8. **STALLINGS, W.**: Cryptography and Network Security – Principles and Practices", Prentice Hall, 2003.
9. **SCHNEIER, B.**: Applied Cryptography – Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1996.
10. **MYERS, M. et. al.**: Online Certificate Status Protocol – OCSP, RFC2560, June 1999.