Securitatea sistemelor informatice - PKI

Aldea Constantin Lucian

Universitatea Transilvania din Brașov

costel.aldea@unitbv.ro

April 14, 2016

Cuprins

Introducere

Sistemele complexe de afaceri, e-commerce și tranzacțiile de afaceri automatizate necesită măsuri de securitate robuste și riguroase.
Companiile care folosesc Internet-ul pentru a-și conduce afacerile au mai mult succes dacă satisfac nevoia de securitate și confidențialitate a clientelei.
Pentru securizarea informației se folosesc diferiți algoritmi de criptare.
Aceștia pot fi de două tipuri:

1. algoritmi simetrici
2. algoritmi asimetrici.

Introducere - Algoritmi de criptare simetrici

Algoritmii de criptare simetrici (criptografia tradițională) folosesc aceiași cheie atât pentru criptare cât și pentru decriptare. Pentru a putea folosi acești algoritmi atât receptorul cât și emițătorul ar trebui să cunoască cheia secretă. În acest caz trebuie găsită o metodă sigură de transmitere a cheii secrete.

Introducere - Algoritmi de criptare asimetrici

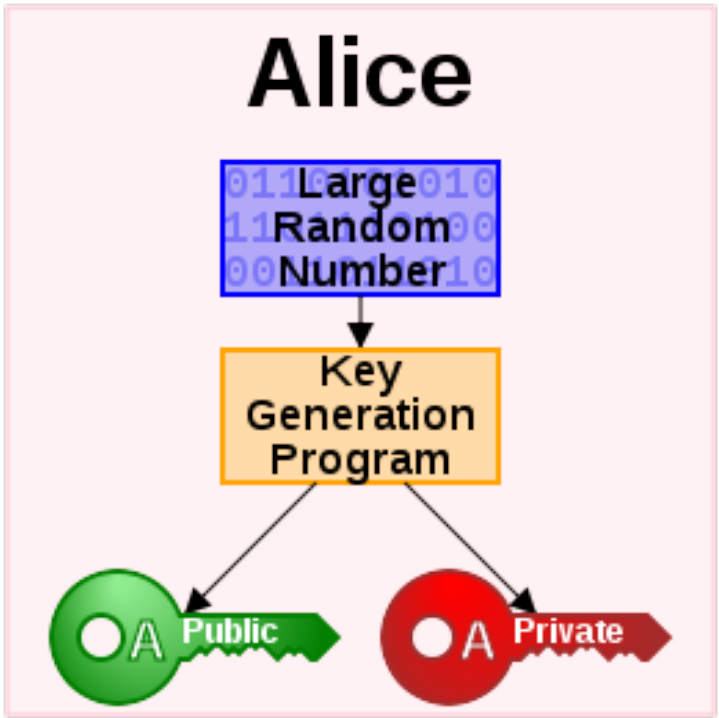
Criptografia asimetrică rezolvă acest neajuns (schimbarea chei secrete) al criptografiei simetrice. Algoritmii asimetrici folosesc pentru criptare/decriptare o pereche de chei: o cheie privată și una publică. Cheia privată nu poate fi obținută din cheia publică. Un mesaj criptat cu o cheie publică poate fi decriptat doar folosind cheia secretă asociată cheii publice respective.

Exemplu - transmiterea unui mesaj criptat cu o cheie publică

Pentru a înțelege modul de funcționare a criptării cu cheie publică vom lua un exemplu. Să presupunem că Alice vrea să îi trimită un mesaj confidențial lui Bob și vrea să primească tot un răspuns confidențial.

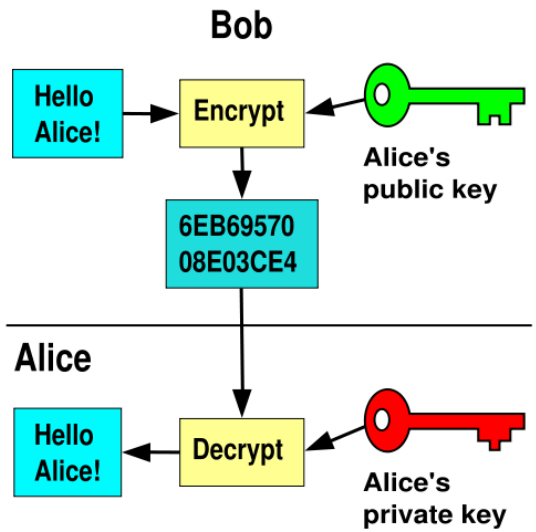
Generarea unei perechi de chei

- Alice și Bob își generează câte o pereche de chei.
- Alice și Bob își transmit cheia publică

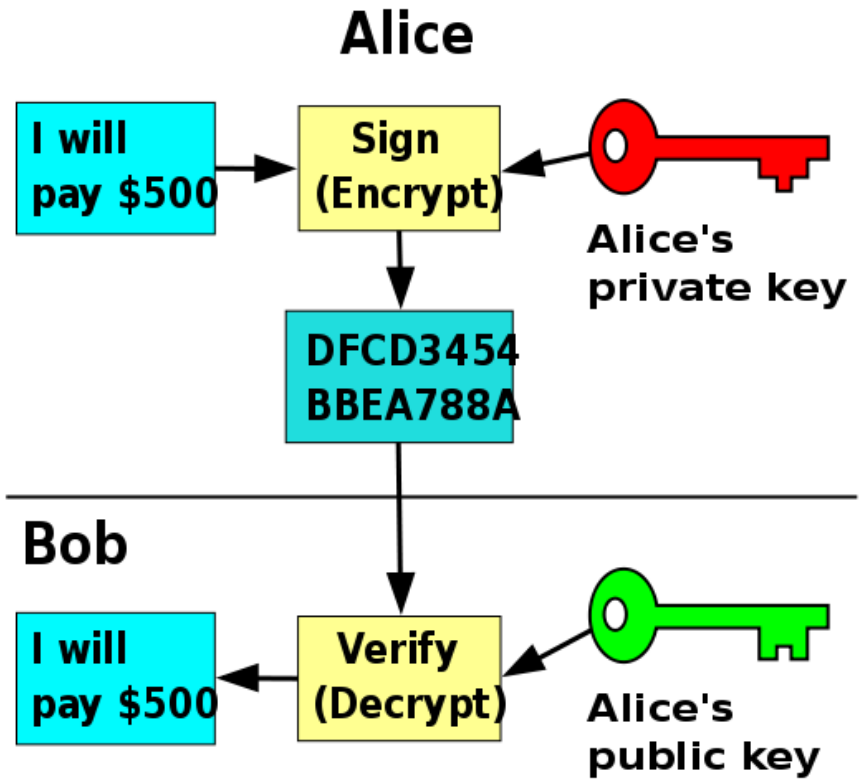


Transmiterea unui mesaj criptat

- Bob criptează mesajul folosind cheia publică a lui Alice
- Bob transmite mesajul lui Alice
- Alice decriptează mesajul folosind cheia sa privată



Semnătura digitală (1)



Semnătura digitală (2)

- Alice transmite un mesaj semnat digital
- Mesajului original i se va aplica o funcție de hash.
- Valoarea rezultată va fi criptată folosind cheia privată a lui Alice
- Mesajul este transmis lui Bob împreună cu valoarea hash criptată
- Bob verifică integritatea mesajului
- Pentru aceasta aplică mesajului aceiași funcție de hash pe care a folosit-o și Alice
- Decriptează valoarea de hash folosind cheia publică a lui Alice.
- Compară valoarea de hash transmisă cu cea obținută
- Dacă cele două coincid înseamnă că mesajul nu a fost alterat

Probleme ale criptografiei cu cheie publică - autentificarea cheii

- Autentificarea cheii reprezintă procesul de asigurare a faptului că cheia publică a persoanei A, care este la persoana B chiar aparține persoanei A și nu altei persoane.
- Cea mai simplă soluție : întâlnirea față în față a persoanelor pentru schimbarea cheilor publice.
  - Dezavantaj:nu se poate aplica în cazul sistemelor cu un număr mare de utilizatori, sau în cazul sistemelor în care nu toți utilizatorii se cunosc între ei.
- Soluția generală a acestei probleme: folosirea *certificatelor* emise de autorități speciale de certificare printr-o infrastructură de chei publice (PKI - Public Key Infrastructure).
- Autoritatea certificatoare acționează ca o terță persoană de încredere oferind certificate prin care ambele părți implicate în conversație sunt încredințate că discută cu cine trebuie.

Infrastructuri cu chei publice (PKI - Public Key Infrastructure)

- PKI reprezintă o combinație între hardware și software, politici și proceduri, ce asigură securitatea necesară pentru a comunica în siguranță.
- Criptografia bazată pe chei publice suportă mecanisme de securitate precum confidențalitatea, integritatea, autentificarea și non-repudierea, însă pentru a implementa cu succes aceste mecanisme trebuie planificată cu atenție o infrastructură pentru a le administra. Peste o infrastructură cu chei publice (PKI) se construiesc alte aplicații de sistem și componente de securitate în rețea.
- Implementarea unei infrastructuri de chei publice aduce aceste mecanisme care asigură menținerea încrederii. Principalele funcții de securitate pentru realizarea cărora PKI oferă suport sunt confidențialitatea, integritatea, non-repudierea și autentificarea.
- Trebuie subliniat faptul că PKI nu servește o anumită funcționalitate, ci oferă o fundație pentru alte servicii de securizare. Principala funcție a PKI este permiterea distribuirii și folosirii cheilor publice și certificatelor cu securitate și integritate. Printre sistemele care cer de obicei mecanisme de securitate bazate pe PKI enumerăm email-ul, aplicațiile de e-commerce, home banking, etc. PKI permite autentificarea entităților.

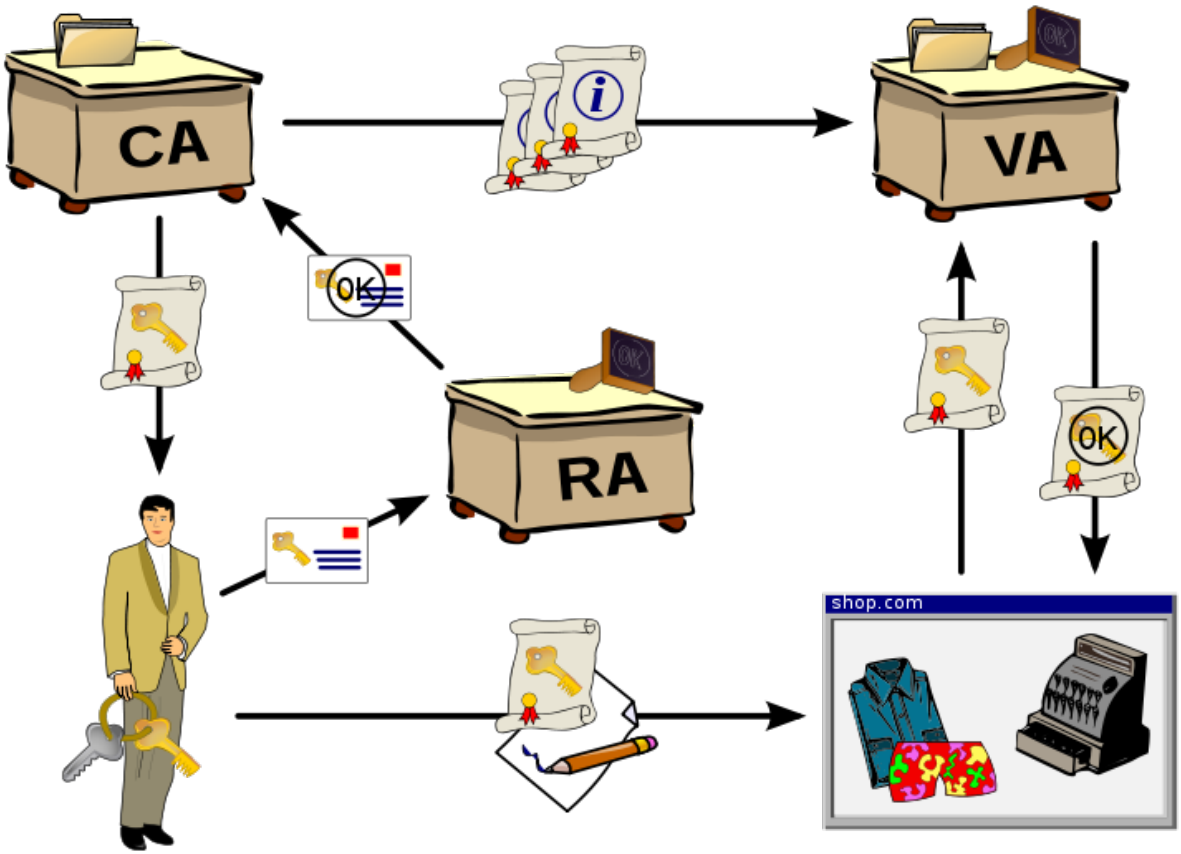
Structura și componentele PKI

- Generarea, distribuirea și managementul cheilor publice și a certificatelor asociate sunt realizate de obicei de către Autorități Certificatoare (CA - Certification Authorities) și Autorități de Înregistrare (RA Registration Authorities).
- Pentru stocarea certificatelor emise se folosesc servicii director (directory services).
- Prin CA se stabilește o ierarhie de încredere.
- CA, RA și serviciile director permit implementarea certificatelor digitale care pot fi folosite pentru a identifica diferite autorități.
- Scopul PKI este să ofere suport pentru schimbul sigur de informații, credențiale în diferite medii care de obicei nu sunt sigure precum Internet-ul.

Mod de funcționare (1)

- In Internet, entitățile necunoscându-se nu au suficientă încredere pentru a face afaceri, a incheia contracte sau alte tipuri de tranzacții. Implementarea PKI folosind CA oferă această incredere.
- Entitățile participante, care nu se cunosc stabilesc o relație de incredere cu CA. CA efectuează la un anumit nivel o autentificare a entităților, conform regulilor de funcționare stabilite și apoi eliberează câte un certificat digital pentru fiecare entitate.
- Aceste certificate sunt semnate de CA, deci asigură identitatea entităților.
- Indivizii care nu se cunosc personal pot folosi acum certificatele pentru a stabili o relație de încredere între ei, deoarece ei au încredere in CA, ca a autentificat corespunzator cealalta entitate, iar semnatura CA atesta acest lucru.
- Un avantaj major al PKI este stabilirea unei ierarhii de incredere intr-un mediu eterogen.

Mod de funcționare (2)



Certificarea incrucișată

Este posibil ca o entitate certificată de un CA să aibă nevoie de autentificarea unei entități certificate de un alt CA. Dacă se permite certificarea incrucișată, adică un CA să certifice un alt CA, atunci in acest caz cele doua entități ar avea incredere una in alta deoarece CA in care entitatea are incredere contrasemneaza certificatul eliberat de celalalt CA, deci entitatea respecta si regulile CA-ului in care are incredere. Acest tip de certificare ofera scalabilitate și flexibilitate PKI.

Principalele obiective de securitate care pot fi implementate

Confidențialitatea - menținerea caracterului privat al informației (secretizarea informației)
Integritatea - dovada că respectiva informație nu a fost modificată (asigurarea impotriva manipulării frauduloase a informației). Certificatele cheilor publice și semnăturile digitale trebuie să aibe integritate. Integritatea poate fi oferită in PKI prin folosirea criptografiei simetrice sau asimetrice. De obicei se folosește criptografia asimetrică în conjuncție cu un algoritm de hash.
Autentificarea - dovada identității celui ce transmite mesajul (verificarea identității unui individ sau a unei aplicații). Se verifică certificatele și CA.
Non-repudierea - siguranța că cel care generează mesajul nu poate să îl denigreze mai târziu (asigurarea paternității mesajului). Acest lucru se realizează prin semnătura digitală.

Componentele logice

PKI este un framework de persoane, politici, procese, protocoale, hardware, software folosite pentru a genera, administra, stoca, desfășura și a revoca certicatele cheilor publice.
Principalele componente logice:

- Entitățile finale sau abonații
- Autoritățile certificatoare (CA)
- Regulile de funcționare CA
- Certificatele cheilor publice
- Extensiile certificatelor
- Autoritatile de inregistrare
- Depozitele de certificate

Componentele logice PKI - Entitățile finale sau abonații

Entitățile finale sunt persoanele sau calculatoarele care au nevoie de un certificat digital pentru a se identifica din diferite motive. Această entitate trebuie să aibă capacitatea de a-și genera o pereche de chei, una publică și una privată. De obicei CA generează aceste chei.

Componentele logice PKI - Autoritățile certificatoare (CA)

CA este o autoritate recunoscută de mai mulți utilizatori care generează și asignează chei publice și private și certificate pentru cheile publice.
CA certifică identitatea unei entități. Certificarea se face pe baza indepliniri unui set de reguli de catre entitate.
Daca entitatea este considerata sigura se emite un certificat digital care este semnat de CA.
Cheile publice ale tuturor entitatilor certificate de CA trebuie să fie distribuite tuturor entitatilor care au încredere în acel CA. CA rădăcină trebuie să distribuie propriile chei publice semnate de el însuși.
Principalele funcții efectuate de un CA sunt:

- Generarea certificatelor
- Revocarea certificatelor

Componentele logice PKI - Regulile de funcționare CA

Acestea reprezintă regulile de care se ține cont la eliberarea certificatelor, practicile procedurale și operaționale ale PKI.
Acestea trebuie să detalieze toate procesele din cadrul ciclului de viață al unui certificat incluzând generarea lui, eliberarea, administrarea, stocarea, desf'u așurarea și revocarea lui.
Obiectivul acestor reguli este să ofere încredere în PKI, astfel încât utilizatorii să aibă suficientă încredere astfel încât să participe.

Componentele logice PKI - Certificatele cheilor publice - certificatele digitale

CA generează, administrează, stocehaza si revoca certificate.
Un certificat atesta legătura dintre o cheie publică și identitatea unei anumite entități.
El conține suficiente informații pentru ca o alta entitate să poate verifica identitatea deținã torului certificatului.
Principalele componente ale unui certificat digital sunt:

- cheia publică
- informația ce leagă cheia publică de deținã torul ei
- informația de validitate a certificatului
- semnătura digitală

Certificatele digitale VeriSign

VeriSign a introdus conceptul de clase de certificate digitale:

- **clasa I**: certificate pentru indivizi 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-mailului.
- **clasa a II-a**: certificate pentru organizații, pentru care se verifică identitatea
- **clasa a III-a**: certificate pentru servere și semnare de software, pentru care verificarea și validarea identității și autorizăr ii este intocmită de Autoritatea Certificatoare.
- **clasa a IV-a**: pentru tranzacțiile online dintre companii
- **clasa a V-a**: pentru organizații private sau securitate guvernamentală

Aceste certificate au un anumit format.

Componentele logice PKI - Extensiile certificatelor

Pe lângă informațiile de bază un certificat mai poate conține și alte informații, în functie de nevoile organizațiilor. Acestea însă pot afecta interoperabilitatea certificatelor în diverse aplicații.

Componentele logice PKI - Autoritățile de înregistrare

Acestea sunt componente opționale ale PKI. Acestea de obicei preiau o parte din responsabilitățile CA, devenind o interfață între entitate și CA. Principala responsabilitate a RA este verificarea identității entității și eligibilității entității pentru obținerea unui asemenea certificat.

Componentele logice PKI - Depozitele de certificate

Această componentă este opțională. Ea permite stocarea certificatelor.
Această componentă poate fi o soluție eficientă pentru sistemele închise precum un intranet. De asemenea poate exista un depozit al certificatelor revocate.
Aceste depozite sunt controlate de CA sau RA. Distribuirea certificatelor în acest caz este simplă, CA trebuie doar să actualizeze depozitul și să dea acces la depozit pentru citire.
LDAP este un exemplu bun de protocol care poate fi folosit drept depozit de certificate.

Funcțiile PKI

Principalele funcții ale PKI sunt următoarele:

- Criptografia bazată pe chei publice - include generarea, distribuirea, administrarea și controlul cheilor de criptare
- Eliberarea certificatelor - leagă o cheie publică de un individ, organizație sau altă entitate
- Validarea certificatelor - verifică să existe o relație de încredere și dacă un certificat mai este valid pentru anumite operații
- Revocarea certificatelor - anulează un certificat emis anterior și publică această anulare în depozitul certificatelor revocate

Exemplu de implementare PKI

În acest exemplu atât Alice cât și Bob folosesc certificate digitale semnate de aceiași CA.

Precondiții:

1. Alice și Bob și-au generat fiecare câte o cheie publică și una privată. Tratam acest caz, desi este posibil ca CA să genereze aceste chei și apoi să le distribuie.
2. In cazul in care Alice și Bob și-au generat singuri cheile, transmit cheile publice, numele și alte informații descriptive unei Autoritati de Inregistrare (RA)
3. RA validează credențialele și transmite cererile de creare de certificate catre CA
4. CA generează cate un certificat pentru cheia publică a lui Alice si pentru cea a lui Bob, care conțin cheile lor publice formatate și alte informații, după care le semnează folosind propriile chei private.
5. Rezultatul acestor operații este ca Alice și Bob au fiecare câte o cheie publică și una privată și un certificat pentru cheia publică.
6. Alice și Bob generează o cheie secretă simetrică.

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (1)

FIGURE 1 illustrates Alice using a digital signature to send data to Bob (steps 1-5).

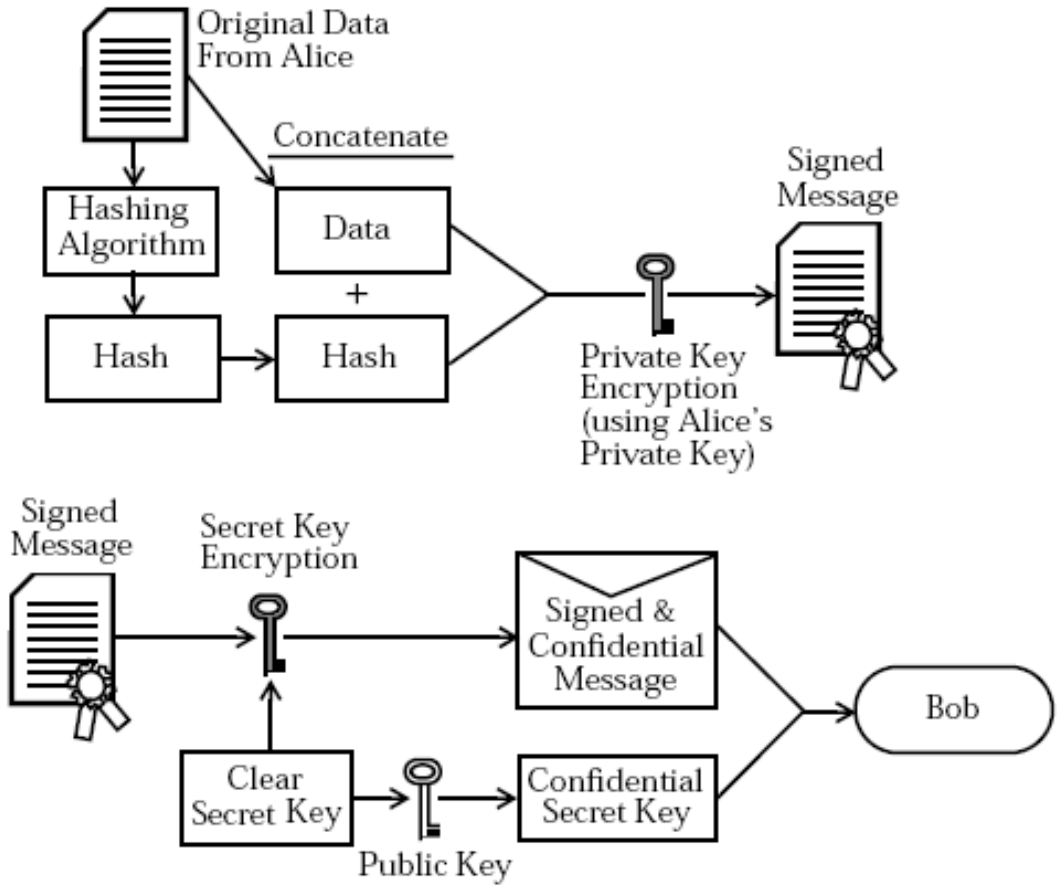


FIGURE 1 Overview of Using a Digital Signature

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (2)

Să presupunem că Alice vrea să trimită un mesaj confidențial, lui Bob. De asemenea doreste sa se asigure integritatea mesajului, adica continutul sa nu fie alterat. In continuare pasii de la 1 la 5 reprezinta trimiterea mesajului de catre Alice astfel incat sa fie confidential si sa continutul sa ramana integru. Pasii de la 6 la 10 descriu decriptarea mesajului de catre Bob.

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (3)

1. Alice scrie mesajul, il formateaza conform protocolului cu care a fost de acord ea si Bob, dupa care aplica o functie de hashing mesajului. Functia hash furnizeaza o valoare unica pentru mesaj, care mai tarziu va fi folosita de Bob pentru a testa integritatea si validitatea mesajului.
2. Alice concateneaza mesajul si valoarea furnizata de hash si apoi semneaza acestea cu cheia ei privata. Aceasta semnatura confera mesajului integritate si Bob va stii ca mesajul este de la Alice deoarece doar ea are cheia privata. De remarcat faptul ca daca alta persoana are cheia public a lui Alice, va putea accesa mesajul deoarece acesta nu a fost si criptat pentru a asigura si confidentialitatea lui.
3. Deoarece Alice si Bob doresc pastrarea confidentialitatii mesajului, Alice cripteaza mesajul si hash-ul cu cheia ei secreta. Criptarea se putea face si altfel, de exemplu se cripta mesajul folosind cheia publica a lui Bob. In acest exemplu se foloseste o cheie secreta deoarece este mai eficienta aceasta criptare decat cea cu cheie publica.

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (4)

4. Alice trimite cheia secreta simetrica lui Bob, pentru ca acesta sa poata decripta mesajul. Alice cripteaza aceasta cheie folosind cheia publica a lui Bob. Presupunem ca Alice a obtinut in prealabil cheia publica a lui Bob. Acest mesaj va putea fi descifrat doar folosind cheia privata a lui Bob, deci doar Bob va putea decripta mesajul.
5. Alice trimite mesajul original si valoarea rezultata in urma aplicarii functiei hash criptate cu cheia secreta a lui Alice. Aceasta este transmisa lui Bob criptata cu cheia publica a acestuia.

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (5)

FIGURE 2 illustrates Bob decrypting the data and comparing hashes (steps 6-10).

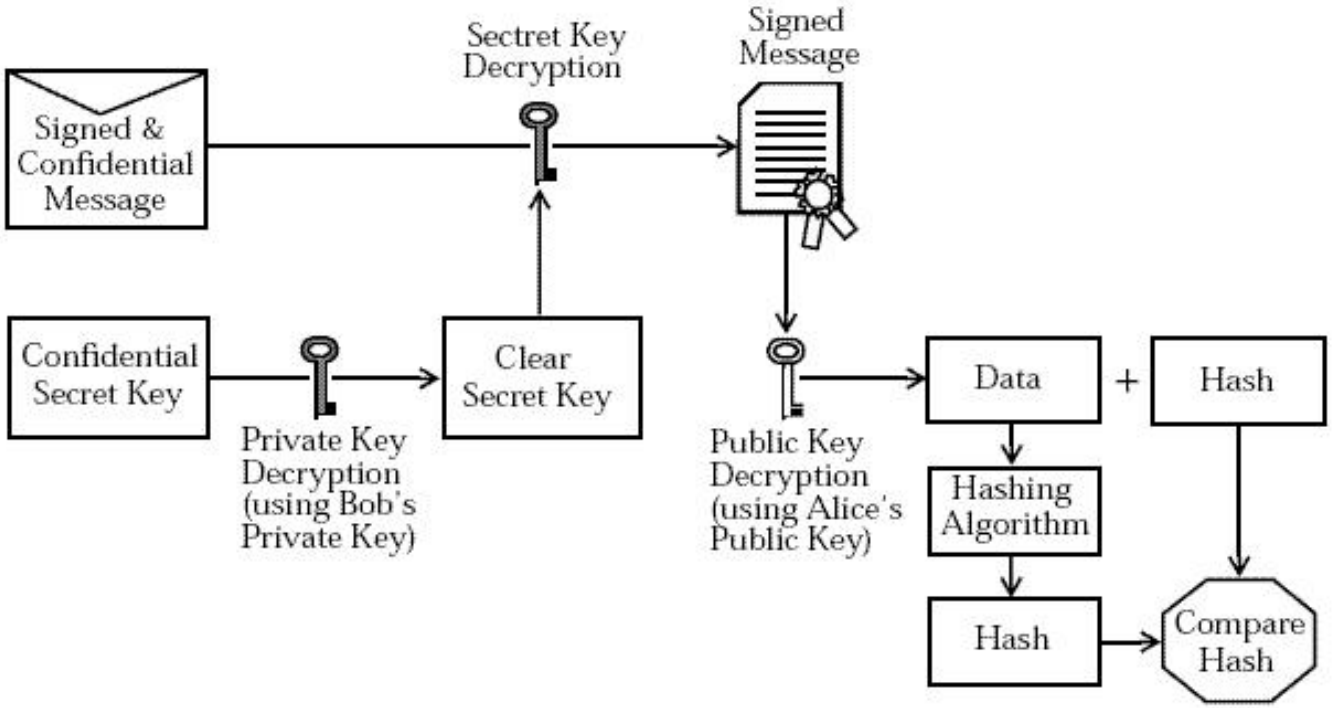


FIGURE 2 Overview of the Decryption and Hash Comparison Process

Exemplu de implementare PKI - transmiterea unui mesaj criptat și semnat digital (6)

6. Bob ia mesajul criptat cu cheia sa publica si il decripteaza folosind cheia privata. Astfel recupereaza cheia secreta cu care Alice a criptat celalalt mesaj.
7. Bob decripteaza mesajul de Alice si obtine mesajul clar si hash-ul semnate de Alice.
8. Bob decripteaza mesajul semnat si hash-ul mesajului folosind cheia publica a lui Alice. Reamintim ca un mesaj criptat cu o cheie poate fi decriptat doar cu perechea ei.
9. Pentru a se asigura ca mesajul nu a fost modificat, Bob ia mesajul original si ii aplica exact aceiasi functie de hash pe care a folosit-o Alice.
10. In final Bob compara hash-ul produs cu hash-ul recuperat din mesaul original primit de la Alice. Daca cele doua valori coincid inseamna ca s-a asigurat integritatea

Concluzii (1)

Folosirea unei infrastructuri cu chei publice prezintă o serie de avantaje printre care amintim:

- Securizarea mesageriei electronice
  Cea mai mare parte a interacțiunilor derulate prin Internet se realizează prin intermediul mesageriei electronice. Această activitate presupune însă acceptarea unui grad ridicat de risc, prin expunerea unor informații confidențiale și prin posibilitatea substituirii autorului unui mesaj sau chiar alterarea voită a conținutului mesajului.
- Sistem de administrare a documentelor și semnătură digitală
  O parte importantă a aplicaţilor software se referă la procesarea ţ arhivarea documentelor în format electronic. Deși aceste sisteme contribuie la diminuarea dificultăților în prelucrarea și arhivarea unui volum mare de documente, ele nu rezolvă complet trecerea de la documente în format tradițional la documente electronice. Ceea ce lipsește este posibilitatea de a semna aceste documente electronice și de a asigura în acest fel nonrepudierea acestora.

Concluzii (2)

- Securizarea aplicațiilor Intranet și Extranet
  Din ce în ce mai multe companii și organizații tind să-și transfere procesele de interacțiune către aplicații care rulează în mediul Internet. Indiferent dacă acestea se referă la relația cu proprii angajați și procesele interne ale organizației (aplicații Intranet), sau sprijină interacțiunea cu partenerii și clienții (aplicații Extranet), aceste aplicații își demonstrează din plin eficiența prin reducerea masivă a costurilor și îmbunătățirea eficienței. Pe măsură însă ce aceste informații sunt transferate către sistemele și aplicațiile Intranet/Extranet, riscul de securitate informațională crește semnificativ, în primul rând datorită faptului că Internetul reprezintă prin natura sa un mediu public.
- Criptarea datelor și a documentelor
  Securitatea datelor nu se referă numai la momentul în care acestea sunt utilizate într-un proces informațional, ci și la stocarea lor. Păstrarea confidențialității și integrității acestora îmbracă numeroase aspecte, care se referă atât la autentificarea accesului cât și la criptarea lor astfel încât să nu poată fi utilizate în cazul unui acces neautorizat.

Concluzii (3)

- Autentificare la nivelul sistemului de operare și al aplicațiilor
  Autentificarea prin nume și parolă este soluția cea mai vulnerabilă și în plus, obligă utilizatorul la memorarea unei astfel de combinații pentru fiecare aplicație folosită. Folosirea certificatului digital stocat pe smartcard contribuie nu numai la creșterea gradului de siguranță dar și la o utilizare mai facilă, prin folosirea unui mijloc unic de autentificare pentru toate aplicațiile folosite.

Bibliografie

1. http://en.wikipedia.org/wiki/Public_key_cryptography
2. http://en.wikipedia.org/wiki/Key_authentication
3. http://en.wikipedia.org/wiki/Public_key_infrastructure
4. http://www.sun.com/blueprints/0801/publickey.pdf
5. http://en.wikipedia.org/wiki/Public_key_certificate
6. Securitatea datelor și criptografie, Aldea Constantin Lucian, 2007

Întrebări