# Criptografie și Securitate

## - Prelegerea 23 -
## Semnături digitale

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

# Cuprins

1. Scheme de semnătură digitală

2. Infrastructură cu chei publice - PKI

# Scheme de semnatură digitală

- Schemele de semnătură digitală reprezintă echivalentul MAC-urilor în criptografia cu cheie publică, deși există câteva diferențe importante între ele;

# Scheme de semnatură digitală

- Schemele de semnătură digitală reprezintă echivalentul MAC-urilor în criptografia cu cheie publică, deși există câteva diferențe importante între ele;
- O schemă de semnătură digitală îi permite unui semnatar S care a stabilit o cheie publică *pk* să semneze un mesaj în așa fel încât oricine care cunoaște cheia *pk* poate verifica originea mesajului (ca fiind S) și integritatea lui;

# Scheme de semnatură digitală

- Schemele de semnătură digitală reprezintă echivalentul MAC-urilor în criptografia cu cheie publică, deși există câteva diferențe importante între ele;
- O schemă de semnătură digitală îi permite unui semnatar S care a stabilit o cheie publică *pk* să semneze un mesaj în așa fel încât oricine care cunoaște cheia *pk* poate verifica originea mesajului (ca fiind S) și integritatea lui;
- De pildă, o companie de software vrea să transmită patch-uri de software într-o manieră autentificată, așa încât orice client să poată recunoaște dacă un patch e autentic;

# Scheme de semnatură digitală

- Schemele de semnătură digitală reprezintă echivalentul MAC-urilor în criptografia cu cheie publică, deși există câteva diferențe importante între ele;
- O schemă de semnătură digitală îi permite unui semnatar S care a stabilit o cheie publică *pk* să semneze un mesaj în așa fel încât oricine care cunoaște cheia *pk* poate verifica originea mesajului (ca fiind S) și integritatea lui;
- De pildă, o companie de software vrea să transmită patch-uri de software într-o manieră autentificată, așa încât orice client să poată recunoaște dacă un patch e autentic;
- În schimb, o persoană malițioasă nu poate păcăli un client să accepte un patch care a nu a fost realizat de compania respectivă.

# Scheme de semnatură digitală

- Pentru aceasta, compania generează o cheie publică *pk* împreună cu o cheie secretă *sk* și distrubie cheia *pk* clienților săi, păstrând cheia secretă;

# Scheme de semnatură digitală

- Pentru aceasta, compania generează o cheie publică *pk* împreună cu o cheie secretă *sk* și distrubie cheia *pk* clienților săi, păstrând cheia secretă;
- Atunci când lansează un patch de sotware $m$, compania calculează o semnătură digitală $\sigma$ pentru $m$ folosind cheia *sk* și trimite fiecărui client perechea $(m, \sigma)$;

# Scheme de semnatură digitală

- Pentru aceasta, compania generează o cheie publică $pk$ împreună cu o cheie secretă $sk$ și distrubie cheia $pk$ clienților săi, păstrând cheia secretă;
- Atunci când lansează un patch de sotware $m$, compania calculează o semnătură digitală $\sigma$ pentru $m$ folosind cheia $sk$ și trimite fiecărui client perechea $(m, \sigma)$;
- Fiecare client stabilește autenticitatea lui $m$ verificând dacă $\sigma$ este o semnătură legitimă pentru $m$ cu privire la cheia publică $pk$;

# Scheme de semnatură digitală

- Pentru aceasta, compania generează o cheie publică $pk$ împreună cu o cheie secretă $sk$ și distrubie cheia $pk$ clienților săi, păstrând cheia secretă;
- Atunci când lansează un patch de sotware $m$, compania calculează o semnătură digitală $\sigma$ pentru $m$ folosind cheia $sk$ și trimite fiecărui client perechea $(m, \sigma)$;
- Fiecare client stabilește autenticitatea lui $m$ verificând dacă $\sigma$ este o semnătură legitimă pentru $m$ cu privire la cheia publică $pk$;
- Deci compania folosește aceeași cheie publică pentru toți clienții și calculează o singură semnătură pe care o trimite tuturor.

# Avantaje semnături digitale față de MAC-uri

- MAC-urile și schemele de semnătură digitală sunt folosite pentru asigurarea integrității (autenticității) mesajelor cu următoarele **diferențe**:

# Avantaje semnături digitale față de MAC-uri

- MAC-urile și schemele de semnătură digitală sunt folosite pentru asigurarea integrității (autenticității) mesajelor cu următoarele **diferențe**:

- Schemele de semnatură digitală sunt *public verificabile*...

# Avantaje semnături digitale față de MAC-uri

- MAC-urile și schemele de semnătură digitală sunt folosite pentru asigurarea integrității (autenticității) mesajelor cu următoarele **diferențe**:
- Schemele de semnatură digitală sunt *public verificabile*...
- ...ceea ce înseamnă că semnăturile digitale sunt *transferabile* - o terță parte poate verifica legitimitatea unei semnături și poate face o copie pentru a convinge pe altcineva că aceea este o semnătură validă pentru $m$;

# Avantaje semnături digitale față de MAC-uri

- MAC-urile și schemele de semnătură digitală sunt folosite pentru asigurarea integrității (autenticității) mesajelor cu următoarele **diferențe**:
- Schemele de semnatură digitală sunt *public verificabile*...
- ...ceea ce înseamnă că semnăturile digitale sunt *transferabile* - o terță parte poate verifica legitimitatea unei semnături și poate face o copie pentru a convinge pe altcineva că aceea este o semnătură validă pentru $m$;
- Schemele de semnătură digitală au proprietatea de *non-repudiere* - un semnatar nu poate nega faptul că a semnat un mesaj;

# Avantaje semnături digitale față de MAC-uri

- MAC-urile și schemele de semnătură digitală sunt folosite pentru asigurarea integrității (autenticității) mesajelor cu următoarele **diferențe**:
- Schemele de semnatură digitală sunt *public verificabile*...
- ...ceea ce înseamnă că semnăturile digitale sunt *transferabile* - o terță parte poate verifica legitimitatea unei semnături și poate face o copie pentru a convinge pe altcineva că aceea este o semnătură validă pentru $m$;
- Schemele de semnătură digitală au proprietatea de *non-repudiere* - un semnatar nu poate nega faptul că a semnat un mesaj;
- MAC-urile au avantajul că sunt cam de 2-3 ori mai eficiente (mai rapide) decât schemele de semnătură digitală.

# Construcție scheme de semnătură digitală

- Se pot construi scheme de semnătură digitală pe baza problemei RSA (semnarea se face prin decriptare iar verificarea prin criptare) însă acestea sunt complet nesigure;

# Construcție scheme de semnătură digitală

- Se pot construi scheme de semnătură digitală pe baza problemei RSA (semnarea se face prin decriptare iar verificarea prin criptare) însă acestea sunt complet nesigure;
- Paradigma "hash-and-sign" este mai sigură: înainte de semnare, mesajul trece printr-o funcție hash; varianta aceasta se folosește pe larg în practică;

# Construcție scheme de semnătură digitală

- Se pot construi scheme de semnătură digitală pe baza problemei RSA (semnarea se face prin decriptare iar verificarea prin criptare) însă acestea sunt complet nesigure;
- Paradigma "hash-and-sign" este mai sigură: înainte de semnare, mesajul trece printr-o funcție hash; varianta aceasta se folosește pe larg în practică;
- Există scheme de semnătură *one-time* care sunt sigure atâta timp cât sunt folosite pentru semnarea unui singur mesaj;

# Construcție scheme de semnătură digitală

- Se pot construi scheme de semnătură digitală pe baza problemei RSA (semnarea se face prin decriptare iar verificarea prin criptare) însă acestea sunt complet nesigure;
- Paradigma "hash-and-sign" este mai sigură: înainte de semnare, mesajul trece printr-o funcție hash; varianta aceasta se folosește pe larg în practică;
- Există scheme de semnătură *one-time* care sunt sigure atâta timp cât sunt folosite pentru semnarea unui singur mesaj;
- Un alt exemplu folosit în practică este Digital Signature Algorithm (DSA) bazat pe problema logaritmului discret (a devenit standard US în 1994) dar și ECDSA (varianta DSA bazată pe curbe eliptice devenită standard în 1998), ambele fiind incluse în DSS (Digital Signature Standard).

# Certificate și PKI

# Certificate și PKI

- O problemă a criptografiei cu cheie publică o reprezintă distribuirea cheilor publice;

# Certificate și PKI

- O problemă a criptografiei cu cheie publică o reprezintă distribuirea cheilor publice;
- Se rezolvă tot cu criptografia cu cheie publică: e suficient să distribuim o singură cheie publică în mod sigur...

# Certificate și PKI

- O problemă a criptografiei cu cheie publică o reprezintă distribuirea cheilor publice;
- Se rezolvă tot cu criptografia cu cheie publică: e suficient să distribuim o singură cheie publică în mod sigur...
- Ulterior ea poate fi folosită pentru a distribui sigur oricât de multe chei publice;

# Certificate și PKI

- O problemă a criptografiei cu cheie publică o reprezintă distribuirea cheilor publice;
- Se rezolvă tot cu criptografia cu cheie publică: e suficient să distribuim o singură cheie publică în mod sigur...
- Ulterior ea poate fi folosită pentru a distribui sigur oricât de multe chei publice;
- Ideea constă în folosirea unui *certificat digital* care este o semnătura care atașeaza unei entități o anume cheie publică;

# Certificate și PKI

- De exemplu, dacă Charlie are cheia generată $(pk_C, sk_C)$ iar Bob are cheia $(pk_B, sk_B)$, iar Charlie cunoaște $pk_B$ atunci el poate calcula semnătura de mai jos pe care i-o dă lui Bob:

$$\mathrm{cert}_{C \to B} = \mathrm{Sign}_{sk_C}(\text{"}\textit{Cheia lui Bob este } pk_B\text{"})$$

# Certificate și PKI

- De exemplu, dacă Charlie are cheia generată $(pk_C, sk_C)$ iar Bob are cheia $(pk_B, sk_B)$, iar Charlie cunoaște $pk_B$ atunci el poate calcula semnătura de mai jos pe care i-o dă lui Bob:

$$\mathrm{cert}_{C \to B} = \mathrm{Sign}_{sk_C}(\text{"}\textit{Cheia lui Bob este } pk_B\text{"})$$

- Această semnătură este un *certificat* emis de Charlie pentru Bob;

# Certificate și PKI

- De exemplu, dacă Charlie are cheia generată $(pk_C, sk_C)$ iar Bob are cheia $(pk_B, sk_B)$, iar Charlie cunoaște $pk_B$ atunci el poate calcula semnătura de mai jos pe care i-o dă lui Bob:

$$\mathrm{cert}_{C \to B} = \mathrm{Sign}_{sk_C}(\text{"}\textit{Cheia lui Bob este } pk_B\text{"})$$

- Această semnătură este un *certificat* emis de Charlie pentru Bob;

- Atunci când Bob vrea să comunice cu Alice, îi trimite întâi cheia publică $pk_B$ împreună cu certificatul $\mathrm{cert}_{C \to B}$ a cărui validitate în raport cu $pk_C$ Alice o verifică;

# Certificate și PKI

- Rămân câteva probleme: cum află Alice $pk_C$, cum poate fi Charlie sigur că $pk_B$ este cheia publică a lui Bob, cum decide Alice dacă să aibă încredere în Charlie;

# Certificate și PKI

- Rămân câteva probleme: cum află Alice $pk_C$, cum poate fi Charlie sigur că $pk_B$ este cheia publică a lui Bob, cum decide Alice dacă să aibă încredere în Charlie;
- Toate aceastea sunt specificate într-o *infrastructură cu chei publice* (PKI-public key infrastructure) care permite distribuirea la scară largă a cheilor publice;

# Certificate și PKI

- Rămân câteva probleme: cum află Alice $pk_C$, cum poate fi Charlie sigur că $pk_B$ este cheia publică a lui Bob, cum decide Alice dacă să aibă încredere în Charlie;
- Toate aceastea sunt specificate într-o *infrastructură cu chei publice* (PKI-public key infrastructure) care permite distribuirea la scară largă a cheilor publice;
- Există mai multe modele diferite de PKI, după cum vom vedea în continuare;

# PKI cu o singură autoritate de certificare

- Aici există o singură autoritate de certificare (CA) în care toată lumea are încredere și care emite certificate pentru toate cheile publice;

# PKI cu o singură autoritate de certificare

- Aici există o singură autoritate de certificare (CA) în care toată lumea are încredere și care emite certificate pentru toate cheile publice;
- CA este o companie, sau agenție guvernamentală sau un departament dintr-o organizație;

# PKI cu o singură autoritate de certificare

- Aici există o singură autoritate de certificare (CA) în care toată lumea are încredere și care emite certificate pentru toate cheile publice;
- CA este o companie, sau agenție guvernamentală sau un departament dintr-o organizație;
- Oricine apelează la serviciile CA trebuie să obțină o copie legitimă a cheii ei publice $pk_{CA}$;

# PKI cu o singură autoritate de certificare

- Aici există o singură autoritate de certificare (CA) în care toată lumea are încredere și care emite certificate pentru toate cheile publice;
- CA este o companie, sau agenție guvernamentală sau un departament dintr-o organizație;
- Oricine apelează la serviciile CA trebuie să obțină o copie legitimă a cheii ei publice $pk_{CA}$;
- Cheia $pk_{CA}$ se otine chiar prin mijloace fizice; deși inconvenient, acest pas este efectuat o singură dată;

# PKI cu mai multe autorități de certificare

- Modelul cu o singură CA nu este practic;

# PKI cu mai multe autorități de certificare

- Modelul cu o singură CA nu este practic;
- In modelul cu multiple CA, dacă Bob dorește să obțină un certificat pentru cheia lui publică, poate apela la oricare CA dorește, iar Alice, care primește un certificat sau mai multe, poate alege în care CA să aibă încredere;

# PKI cu mai multe autorități de certificare

- Modelul cu o singură CA nu este practic;
- In modelul cu multiple CA, dacă Bob dorește să obțină un certificat pentru cheia lui publică, poate apela la oricare CA dorește, iar Alice, care primește un certificat sau mai multe, poate alege în care CA să aibă încredere;
- De exemplu, browser-ele web vin preconfigurate cu un număr de chei publice ale unor CA stabilite ca toate fiind de încredere în mod egal (în configurația default a browser-ului);

# PKI cu mai multe autorități de certificare

- Modelul cu o singură CA nu este practic;
- In modelul cu multiple CA, dacă Bob dorește să obțină un certificat pentru cheia lui publică, poate apela la oricare CA dorește, iar Alice, care primește un certificat sau mai multe, poate alege în care CA să aibă încredere;
- De exemplu, browser-ele web vin preconfigurate cu un număr de chei publice ale unor CA stabilite ca toate fiind de încredere în mod egal (în configurația default a browser-ului);
- Utilizatorul poate modifica această configurație așa încât să accepte doar certificate de la CA-uri în care el are încredere;

# Delegare și lanțuri de certificate

- Charlie este un CA care emite certificate, inclusiv pentru Bob;

# Delegare și lanțuri de certificate

- Charlie este un CA care emite certificate, inclusiv pentru Bob;
- Dacă $pk_B$ este o cheie publică pentru semnătură, atunci Bob poate emite certificate pentru alte persoane; un certificat pentru Alice are forma

$$\mathrm{cert}_{B \to A} = \mathrm{Sign}_{sk_B}(\text{"}\textit{Cheia lui Alice este } pk_A\text{"})$$

# Delegare și lanțuri de certificate

- Charlie este un CA care emite certificate, inclusiv pentru Bob;
- Dacă $pk_B$ este o cheie publică pentru semnătură, atunci Bob poate emite certificate pentru alte persoane; un certificat pentru Alice are forma

$$\mathrm{cert}_{B\to A} = \mathrm{Sign}_{sk_B}(\text{"}\textit{Cheia lui Alice este } pk_A\text{"})$$

- Atunci când comunică cu Dan, Alice îi trimite

$$pk_A, \mathrm{cert}_{B\to A}, pk_B, \mathrm{cert}_{C\to B}$$

# Delegare și lanțuri de certificate

- Charlie este un CA care emite certificate, inclusiv pentru Bob;
- Dacă $pk_B$ este o cheie publică pentru semnătură, atunci Bob poate emite certificate pentru alte persoane; un certificat pentru Alice are forma

$$\mathrm{cert}_{B\to A} = \mathrm{Sign}_{sk_B}(\text{"}\textit{Cheia lui Alice este } pk_A\text{"})$$

- Atunci când comunică cu Dan, Alice îi trimite

$$pk_A, \mathrm{cert}_{B\to A}, pk_B, \mathrm{cert}_{C\to B}$$

- De fapt, $\mathrm{cert}_{C\to B}$ conține, în afară de $pk_B$ și afirmația "Bob este de încredere pentru a emite certificate"; astfel, Charlie îl deleagă pe Bob să emită certificate;

# Delegare și lanțuri de certificate

- Charlie este un CA care emite certificate, inclusiv pentru Bob;
- Dacă $pk_B$ este o cheie publică pentru semnătură, atunci Bob poate emite certificate pentru alte persoane; un certificat pentru Alice are forma

$$\mathrm{cert}_{B\to A} = \mathrm{Sign}_{sk_B}(\text{"}\textit{Cheia lui Alice este } pk_A\text{"})$$

- Atunci când comunică cu Dan, Alice îi trimite

$$pk_A, \mathrm{cert}_{B\to A}, pk_B, \mathrm{cert}_{C\to B}$$

- De fapt, $\mathrm{cert}_{C\to B}$ conține, în afară de $pk_B$ și afirmația "Bob este de încredere pentru a emite certificate"; astfel, Charlie îl deleagă pe Bob să emită certificate;
- Totul se poate organiza ca o ierarhie unde există un CA "rădăcină" pe primul nivel și $n$ CA-uri pe al doilea nivel.

# Modelul "web of trust"

- Aici oricine poate emite certificate pentru orice altcineva și fiecare utilizator decide cât de multă încredere poate acorda certificatelor emise de alți utilizatori;

# Modelul "web of trust"

- Aici oricine poate emite certificate pentru orice altcineva și fiecare utilizator decide cât de multă încredere poate acorda certificatelor emise de alți utilizatori;
- De exemplu, dacă Alice are cheile publice $pk_1, pk_2, pk_3$ corespunzătoare lui $C_1, C_2, C_3$...

# Modelul "web of trust"

- Aici oricine poate emite certificate pentru orice altcineva și fiecare utilizator decide cât de multă încredere poate acorda certificatelor emise de alți utilizatori;
- De exemplu, dacă Alice are cheile publice $pk_1, pk_2, pk_3$ corespunzătoare lui $C_1, C_2, C_3$...
- ...iar Bob, care vrea să comunice cu Alice, are certificatele $\mathrm{cert}_{C_1 \to B}$, $\mathrm{cert}_{C_3 \to B}$ și $\mathrm{cert}_{C_4 \to B}$ pe care i le trimite lui Alice;

# Modelul "web of trust"

- Aici oricine poate emite certificate pentru orice altcineva și fiecare utilizator decide cât de multă încredere poate acorda certificatelor emise de alți utilizatori;
- De exemplu, dacă Alice are cheile publice $pk_1, pk_2, pk_3$ corespunzătoare lui $C_1, C_2, C_3$...
- ...iar Bob, care vrea să comunice cu Alice, are certificatele $\mathrm{cert}_{C_1 \to B}$, $\mathrm{cert}_{C_3 \to B}$ și $\mathrm{cert}_{C_4 \to B}$ pe care i le trimite lui Alice;
- Alice nu are $pk_4$ și nu poate verifica $\mathrm{cert}_{C_4 \to B}$; deci ca să accepte $pk_B$, Alice trebuie să decidă cât de multă încredere are în $C_1$ și $C_3$;

# Modelul "web of trust"

- Aici oricine poate emite certificate pentru orice altcineva și fiecare utilizator decide cât de multă încredere poate acorda certificatelor emise de alți utilizatori;
- De exemplu, dacă Alice are cheile publice $pk_1, pk_2, pk_3$ corespunzătoare lui $C_1, C_2, C_3$...
- ...iar Bob, care vrea să comunice cu Alice, are certificatele $\mathrm{cert}_{C_1 \to B}$, $\mathrm{cert}_{C_3 \to B}$ și $\mathrm{cert}_{C_4 \to B}$ pe care i le trimite lui Alice;
- Alice nu are $pk_4$ și nu poate verifica $\mathrm{cert}_{C_4 \to B}$; deci ca să accepte $pk_B$, Alice trebuie să decidă cât de multă încredere are în $C_1$ și $C_3$;
- Modelul e atractiv pentru că nu necesită încredere într-o autoritate centrală;

# Invalidarea certificatelor

- Atunci când un angajat părăsește o companie sau își pierde cheia secretă, certificatul lui trebuie invalidat;

# Invalidarea certificatelor

- Atunci când un angajat părăsește o companie sau își pierde cheia secretă, certificatul lui trebuie invalidat;
- Există mai multe metode de invalidare între care:

# Invalidarea certificatelor

- Atunci când un angajat părăsește o companie sau își pierde cheia secretă, certificatul lui trebuie invalidat;
- Există mai multe metode de invalidare între care:
- **Expirarea.** Se poate include data de expirare ca parte a unui certificat, care trebuie verificată împreună cu validitatea semnăturii;

# Invalidarea certificatelor

- Atunci când un angajat părăsește o companie sau își pierde cheia secretă, certificatul lui trebuie invalidat;
- Există mai multe metode de invalidare între care:
- **Expirarea.** Se poate include data de expirare ca parte a unui certificat, care trebuie verificată împreună cu validitatea semnăturii;
- **Revocarea.** CA-ul poate, în mod explicit, revoca un certificat de îndată ce acesta nu mai poate fi folosit;

# Invalidarea certificatelor

- Atunci când un angajat părăsește o companie sau își pierde cheia secretă, certificatul lui trebuie invalidat;
- Există mai multe metode de invalidare între care:
- **Expirarea.** Se poate include data de expirare ca parte a unui certificat, care trebuie verificată împreună cu validitatea semnăturii;
- **Revocarea.** CA-ul poate, în mod explicit, revoca un certificat de îndată ce acesta nu mai poate fi folosit;
- Aceasta se poate realiza prin includerea unui număr serial în certificat; la sfârșitul unei zile CA generează o listă de certificate revocate (care conține numerele seriale) pe care o distribuie sau publică.

# Important de reținut!

- Semnături electronice
- Certificate digitale