CriptoTema6.pdf

onafolch

Criptografia i Seguretat

3º Grado en Ingeniería de Datos

Escuela de Ingeniería
Universidad Autónoma de Barcelona

CRIPTOGRAFIA

PUBLIC KEY INFRAESTRUCTURE

1. INTRODUCCIÓ

Per vincular identitats amb les seves respectives claus públiques apareixen els certificats digitals i, amb ells, la infraestructura de clau pública (PKI). Permet transferir informació de manera segura, tot oferint serveis d'autenticació, integritat i confidencialitat.

La criptografia de clau pública es pot utilitzar tant per encriptar informació com per verificar l'autenticitat, però és molt lent respecte la criptografia de clau simètrica.

Quan es vol verificar l'autenticitat i la integritat, es signa el missatge amb una signatura digital. S'obté el hash del missatge i s'aplica la clau privada respectiva.

2. CERTIFICATS

Quan es vol encriptar una gran quantitat d'informació s'utilitza la clau simètrica. Per enviar la clau, aquesta s'encripta amb un criptosistema asimètric utilitzant la clau pública del receptor, i d'aquesta manera es garanteix la confidencialitat.

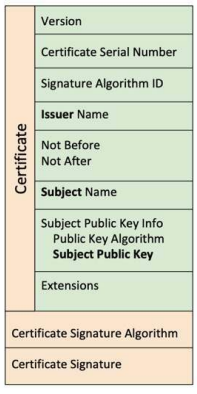
Però, com se jo que darrere de la clau pública del receptor que estic utilitzant és realment de qui jo em penso.

Podriem assumir que els usuaris obtenen les claus públiques d'un directori públic de confiança escrit (TPD Trusted Public Directory) restringit només per un manager el qual tothom hi confia. Però té certs problemes: pot convertir-se en un coll d'ampolla, la seguretat del TPD és crítica, i un atacant pot interceptar la clau pública consultada mentre està en trànsit des del TPD fins l'usuari que l'ha sol·licitat.

Per solucionar aquest problema utilitzem els **certificats** i les **autoritats de certificació** (CA).

Un certificat digital és una estructura de dades que conté informació sobre el propietari de les claus criptogràfiques, la clau pública i una signatura digital del certificat, que garanteix la integritat de les dades i el vincle entre la clau pública i el propietari.

Els camps bàsics d'un certificat X.509 són els següents:



Version: La versió del certificat (0, 1 o 2)
Serial Number: El número de sèrie del certificat, l'identificador únic proporcionat per la CA
Sign Algorithm: L'algoritme que utilitza el issuer (CA) per signar el certificat
Issuer Name: El nom de la CA que emet el certificat

Not Before/Not After: període de validesa del certificat

Subject Name: identifica el titular de la clau pública que està sent certificada
Subject Public Key Info: La clau pública associada al subject i l'algoritme de la clau pública
Extensions: Camp opcional que permet afegir nous camps. Es rebutja el certificat si troba alguna extensió crítica que no reconeix o que no es pot processar. Una extensió no-crítica es pot ignorar si no es reconeix.
Sign Algorithm: L'algoritme que utilitza el issuer (CA) per signar el certificat
Signature: La signatura del certificat

El nom està composat de diferents atributs, com Country (C), State or Province (SP), Locality (L), Organization (O), Organization Unit (OU) i Common name (CN).
Exemple: C=ES, L=Bellaterra, O=UAB, OU=DEIC, CN=Elizabeth Jennings

Ona Folch

3. PKI (Public Key Infraestructure)

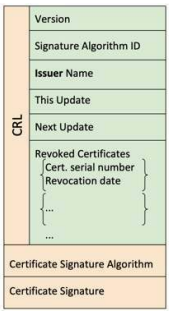
Una infraestructura de clau pública (PKI) són tots els components de programari i maquinari juntament amb usuaris, polítiques i procediments que permeten la creació i gestió de certificats digitals basats en la criptografia de clau pública.

L'objectiu principal de la PKI és la gestió eficient i fiable de claus criptogràfiques i certificats que es poden utilitzar amb finalitats d'autenticació, integritat, confidencialitat i no-repudi.

Entitats:

- **CA (Certification Authority):** és una entitat que certifica o revoca l'enllaç entre la clau pública i l'usuari. Aquesta certificació es realitza mitjançant la signatura digital d'una estructura de dades (certificat) que conté tant la identitat com la clau pública corresponent. Una PKI pot tenir una o diverses CA.
- **RA (Registration Authority)**: és una autoritat que verifica l'enllaç entre l'usuari i la seva clau pública. Pot ser part de la CA (per reduir la càrrega de treball de la CA). Cada RA té el seu propi criteri per acceptar o no, com per exemple podria ser ensenyar el DNI. Per aplicacions que no són d'alta seguretat, la RA pot ser automàtica mitjançant una comprovació del propietari del correu.
- **Repositoris**: els repositoris són estructures de dades que contenen informació relacionada amb una PKI. Els principals són el repositori de certificats (on tindré els certificats) i la CRL (Certificate Revocation List). Els repositoris no cal que siguin de confiança (els certificats i les CRLs estan signades per la CA).

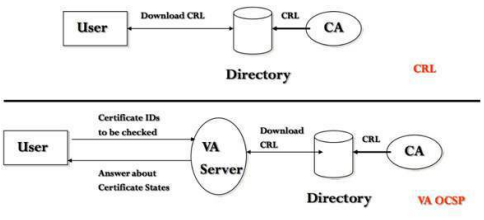
  Una CRL és una llista dels certificats digitals que no són vàlids abans de la seva data de caducitat. Els seus camps són la CA i el DN (Distinguished Name), l'hora de l'actualització, hora de la pròxima actualització, llista dels números de sèrie dels certificats revocats amb les dates i motius, i la signatura de la CA.

  Els Complete CRL tenen diverses avantatges, com per exemple que és complet i senzill. Però té alguns problemes d'escalabilitat (la CRL pot arribar a ser massa gran) i de temps (per culpa de la mida de la CRL).

  Els Delta CRL són una solució per quan els Complete CRL són massa grans. Enlloc de tenir només el Complete, s'emet un CRL Delta (només conté els certificats addicionals afegits durant un període de temps) amb una CRL BaseComplete (que conté el conjunt complet de certificats revocats fins un moment determinat). $CRL_{New} = BaseCompleteCRL_{old} + DeltaCRL$. Es pot tenir molts DeltaCRL del mateix BaseCRL (per exemple, s'emet el CRL complet un cop per setmana, i un nou DeltaCRL (que conté els DeltaCRL anteriors) que s'emet cada dia).
- **Validation Authority (VA)**: és el que verifica la validació del certificat. És opcional i pot reduir la càrrega de treball de la CA.

  Els protocols de validació són mecanismes que donen informació sobre l'estat del certificat (vàlid, revocat, etc) o informació relacionada amb la cadena de certificació necessària per validar el certificat. Els dos protocols principals de validació de certificats són: Protocol d'estat de certificat en línia (OCSP) i Protocol de validació de certificat simple (SCVP).

  Al tenir una CRL, l'usuari se l'ha descarrega i pot mirar tots els certificats revocats. Amb VA OCSP, sol·licita l'estat d'un certificat en concret.

Usuaris:

- **Subscriptor**: és el titular del certificar. Qui té la clau pública i privada juntament amb un certificat digital de la clau pública
- **Relying party**: usuari que pot validar les signatures digitals produïdes pels subscriptors. Els clients també poden xifrar la informació dels subscriptors.

Ona Folch

4. KEY LIFE CYCLE

Generació de la clau: Es genera un parell de claus privades i públiques. Aquesta generació pot ser realitzada per l'usuari o per una part de confiança (o ordinador) sempre que no es reveli la clau privada.

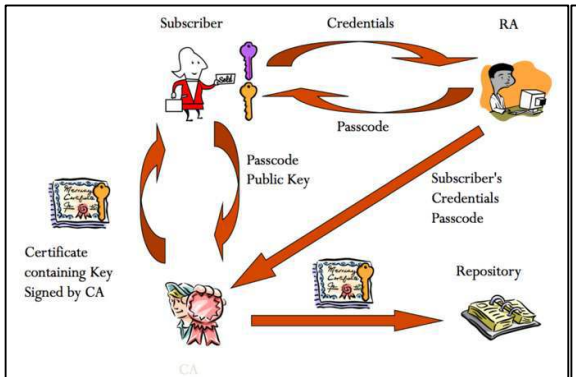
Registre: L'usuari registra la seva clau pública, la qual cosa significa que posseeix la clau privada corresponent. L'autoritat de registre (RA) és la que verifica aquest procés de registre. Normalment implica un Certificate Signing Request (CSR) o certification request.

Certificació: Una vegada s'ha generat el parell de claus i s'ha verificat la identitat de l'usuari, es crea el certificat digital, on la CA valida l'enllaç entre l'usuari i la clau pública verificada per la RA. Un certificat digital acredita aquest enllaç.

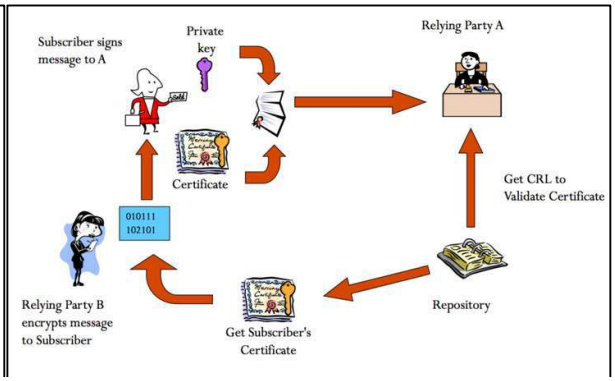
Revocació del certificat: En cas de comprometre la clau privada, l'usuari informa a la CA que s'ha trencat l'enllaç entre les claus públic-privades i la identitat de l'usuari. La CA revoca el certificat corresponent i l'inclou en una llista de revocació de certificació (CRL).

Renovació del certificat: Els certificats digitals inclouen una data de caducitat. La renovació del certificat s'ha de realitzar per obtenir una nova certificació amb una altra data de caducitat.

Com la PKI emet certificats



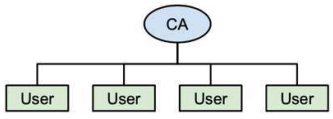
Com s'utilitzen els certificats



5. MODELS

Plain Model

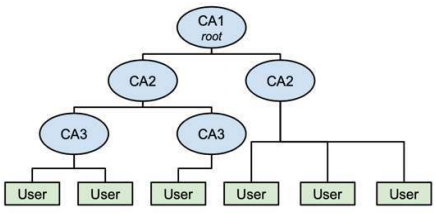
És el més simple, on només existeix una CA. Qualsevol usuari pot validar un certificat digital mitjançant el certificat CA auto-firmat, un certificat digital on l'emissor (issuer) i el CN (Common Name) del subjecte són iguals, i la clau pública inclosa és la mateixa que la utilitzada per validar el certificat.



Model jeràrquic

També coneguda com a jerarquia subordinada. Cada CA està certificada per una altra CA del nivell superior (certificats jeràrquics). En aquests certificats, tant l'emissor com el CN del subjecte són CA però diferents.

La CA de nivell superior es coneix com a CA arrel, i les altres CA són CA intermèdies o subordinades.

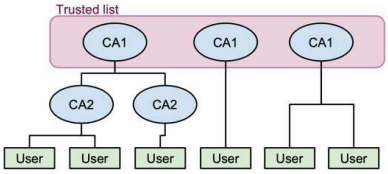


Aquest tipus d'estructura proporciona cadenes de certificats, garantint així un punt de confiança comú. L'única clau que queda sense certificar és la clau pública arrel, que s'ha de difondre àmpliament (per exemple, al butlletí oficial, etc.).

Ona Folch

Model jeràrquic amb llista de confiança

Assumir una única CA arrel per a totes les aplicacions i dominis PKI no és realista. En el model de llista de confiança PKI, cada aplicació conté una llista de vàries CAs arrel en què confia l'aplicació.

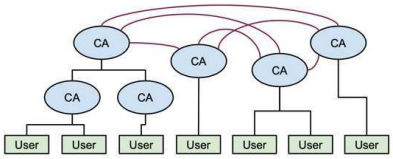


Cada arrel CA pot ser part d'un plain model o d'un model jeràrquic. Aquestes llistes haurien d'estar protegides contra modificacions externes (un exemple típic són els navegadors web, que contenen una llista de centenars de CAs arrel).

Certificació creuada

En un model de certificació creuada, cada CA arrel emet un certificat per a altres CA arrel. Tant l'emissor com el CN del subjecte són CA però són diferents i pertanyen a una jerarquia CA diferent.

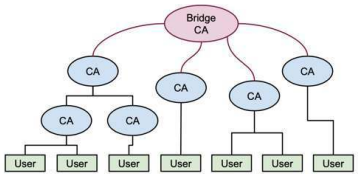
A les aplicacions que utilitzen un model de certificació creuada, l'usuari no pot afegir CA noves tret que aquesta nova CA estigui certificada per una altra ja reconeguda. Això també es coneix com a estructura de malla (o PKI de malla).



Bridge CA

El problema d'un model de certificació creuada és que el nombre de certificats creuats creix molt quan el nombre de CAs implicades creix de manera exponencial. Una Bridge CA inclou una CA externa que actuarà com a pont entre diferents CA.

El model és similar a un model jeràrquic, però el Bridge CA no es defineix com un punt central de confiança, només és un punt d'interconnexió.



6. AUTENTICACIÓ DEL CERTIFICAT

Alice vol tenir el certificat del Bob, i el Bob li envia, però això no és suficient per verificar l'autenticitat del Bob, perquè podria ser que un atacant (Eve) m'envies el certificat del Bob fent-se passar per ell.

El primer repte és demostrar que el Bob té la clau privada que correspon a la clau pública del certificat. Per aquesta raó, envia a Alice el certificat, i el certificat encriptat amb la seva clau privada, però això tampoc és suficient, perquè podria ser que Eve crees un certificat amb la seva clau privada i la identitat del Bob.

El segon repte és que el certificat estigui firmat per algú amb reputació. Una CA amb reputació no signarà res sense pensar, i Alice no acceptarà cap certificat signat per algú sense reputació.

Quan Alice rebi un certificat, primer de tot mirarà si el subject és el correcte i seguidament comprova que sigui vàlid (comprovar la firma), i que estigui firmat per una CA de confiança. Quan rebi el certificat, farà el hash de les dades del certificat, i utilitzarà la clau pública de la CA per desencriptar la signatura (que és el hash del certificat encriptat per la clau privada de la CA), i si els dos valors de hash són iguals, significa que està parlant amb el Bob.

Ona Folch

7. MODEL DISTRIBUÏT

Cada usuari actua com a CA i les claus públiques poden ser signades per diversos usuaris/CA. Aquest model es coneix com a xarxa de confiança. La idea és que els amics dels meus amics són els meus amics. Es basa en els paradigmes de les xarxes d'un món petit.

Cada clau pública té un camp, el valor de confiança de la clau, per indicar fins a quin punt confiem en el propietari per certificar les claus públiques.

Valors de confiança d'una clau:

- **Untrusted**: No se sap res del judici del propietari en la signatura de claus. Les claus tenen inicialment aquest nivell de confiança.
- **None**: Se sap que el propietari signa altres claus incorrectament.
- **Marginal**: El propietari entén les implicacions de la signatura de claus i valida les claus correctament abans de signar-les.
- **Full**: El propietari té una comprensió excel·lent de la signatura de claus i la seva signatura en una clau seria tan bona com la teva.

Una clau K és vàlida si:

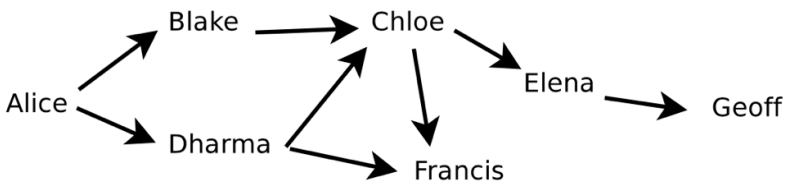
1. Està signada amb suficients claus vàlides, és a dir: L'has signat personalment i s'ha signat amb 1 clau fully trusted o ha estat signada per 3 claus de confiança marginal.
2. El camí de les claus signades que porten des de K fins a la vostra pròpia clau és de 5 passos o menys.

Es pot ajustar la longitud del camí, el nombre de claus de confiança marginal requerides i el nombre de claus de total confiança necessàries. Els números indicats anteriorment són els valors predeterminats utilitzats per GnuPG.

El nivell de confiança de les claus és assignat per l'usuari, i el nivell de validesa el calcula GnuGP en funció dels valors de confiança de claus vàlides. Si tenim full validity, la clau és valida, i si tenim marginal validity, hi ha un camí de confiança però no prou fort per ser considerat vàlid (no compleix totes les condicions de validesa).

Només es té en compte la confiança de les claus totalment vàlides (full validity) per calcular la validesa, i les claus signades per mi sempre són totalment vàlides (independentment del seu nivell de confiança).

Exemple: una fletxa significa que A ha firmat una clau de B. La clau és vàlida si la signat 1 full key o 2 marginal keys, i la longitud màxima és 3.



Case	Trust		validity	
	Marginal	**Full**	**Marginal**	**full**
1		Dharma		Blake, Chloe, Dharma, Francis
2	Blake, Dharma		Francis	Blake, Chloe, Dharma
3	Chloe, Dharma		Chloe, Francis	Blake, Dharma
4	Blake, Chloe, Dharma		Elena	Blake, Chloe, Dharma, Francis
5		Blake, Chloe, Elena		Blake, Chloe, Dharma, Elena, Francis

Ona Folch