

Certificati di Attributi



a cura di: R.Gaeta, F.Zottola

Sicurezza dei dati in rete

- La rete è un mezzo non sicuro
- I messaggi in rete possono essere intercettati e/o modificati



Sicurezza dei dati in rete

Necessità di garantire:

- Riservatezza del contenuto
- Integrità del contenuto
- Autenticazione del mittente
- Non ripudio



Una scienza antichissima: La Crittografia

- **Cifratura:** Trasformazione di un testo in chiaro in un testo cifrato
- **Decifratura:** Trasformazione di un testo cifrato in un testo in chiaro
- Trasformazione basata in genere su:
 - **chiave**
 - **algoritmo** (procedimento ben definito e pubblico)



Una scienza antichissima: La Crittografia

La sicurezza si basa su:

- segretezza della chiave
- robustezza dell'algoritmo



Le tecniche di sicurezza basate su chiavi di crittografia

	Autenticazione	Privacy	Integrità	NonRipudio
User ID	■			
pwd	■			
Crittografia simmetrica (DES)	■	■	■	
Crittografia asimmetrica (RSA)	■	■	■	■

Algoritmi a chiavi asimmetriche

- **2 chiavi diverse:** cifratura e decifratura (RSA/DSA – 1024/2048 bit)
- Ogni corrispondente:
 - **Chiave privata:** segreto da custodire
 - **Chiave pubblica:** informazione da diffondere



Algoritmi a chiavi asimmetriche

Ogni chiave può essere usata indifferentemente per cifrare o decifrare

- **Vantaggi:** flessibilità (riservatezza, autenticità, integrità)
- **Svantaggi:** algoritmi “lenti”



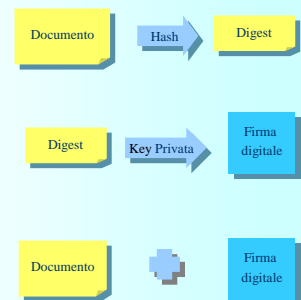
La firma digitale

È una procedura che si basa su complessi algoritmi di cifratura e attribuisce un valore giuridico ad un documento informatico



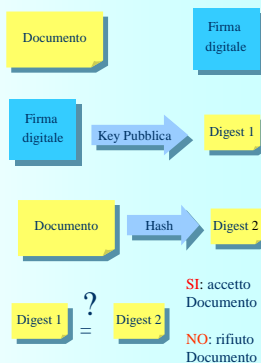
Generazione della firma

- Calcolare il **digest** del documento
- **Cifrare** il digest con la chiave privata del mittente (si ottiene la firma digitale)
- Aggiungere al documento originale la firma digitale ottenuta e inviare la coppia (**Messaggio, Firma**)



Verifica della firma

- **Separare** il messaggio dalla firma
- **Decifrare** la firma usando la chiave pubblica del mittente
- Applicare al documento la **funzione Hash** cioè calcolare il digest
- **Verificare** che i due risultati coincidano



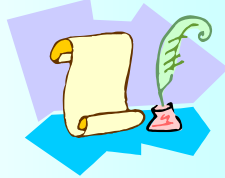
Garanzie della firma

- **Autenticità** del mittente
- **Integrità** del messaggio durante il percorso mittente/destinatario



Il Certificato Digitale

È utilizzato per identificare in maniera univoca oggetti reali, come utenti o computer



Il Certificato Digitale

Un documento d'identità:

- Associa l'identità di una persona (nome, cognome, data di nascita....) al suo aspetto fisico (foto)
- È emesso da un'autorità riconosciuta



Certificato di Chiave Pubblica

- È un documento elettronico
- Associa l'identità di una persona ad una chiave pubblica
- È emesso secondo standard internazionali (X.509 raccomandato dall'ITU-T (International Telecommunication Union – Settore Telecomunicazioni), da una CA riconosciuta
- È firmato digitalmente con chiave privata della CA



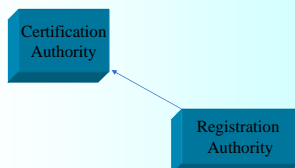
Certification Authority (CA)

Certifica il legame chiave pubblica/identità
cioè garantisce che la chiave pubblica
trascritta su un registro pubblico
ed abbinata a Mario sia
rilasciata proprio a Mario



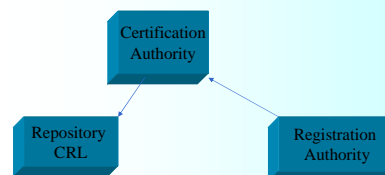
Registration Authority (RA)

- Ha la responsabilità di registrare e verificare alcune o tutte le informazioni riguardanti l'utente che richiede il certificato
 - È un'entità separata dalla CA
- La registrazione dell'utente da parte della RA avviene prima dell'emissione del PKC da parte della CA



Certificate Revocation List (CRL)

Un certificato può essere revocato prima della sua scadenza naturale su richiesta del soggetto o autonomamente dall'emittente. Tale certificato viene così inserito in una lista di certificati revocati o CRL



Certificato di Chiave Pubblica

Version: v2
 Serial Number: 1234
 Signature: 1.2.840.113549.1.1.5
 Subject: CN=Mario Rossi, O=xy, C=IT
 Issuer: CN=Sia S.p.a., O=xy, C=IT
 Validity Period: 1.1.2006 - 1.1.2007
 Subject Public Key Info: 9f0A34...
 Extensions: ...
 CA digital signature

Public Key Infrastructure (PKI)

E' l'insieme di hardware, software, persone, politiche e procedure necessarie per creare, gestire, memorizzare, distribuire e revocare PKC

Public Key Infrastructure: componenti

- Certification Authority
- Registration Authority
- Sistema distribuito di directory
 - contiene i certificati di chiave pubblica e la lista dei certificati revocati
- Database
 - contiene un backup delle chiavi
 - accessibile solo dalla CA
- Generatore di chiavi
 - crea coppie di chiavi pubbliche e/o private
- Name server
 - responsabile del trattamento dello spazio dei nomi

Il Processo Identificativo

La procedura di verifica dell'identità del mittente

Ma al di là della sua identità.....
il firmatario possiede davvero
i privilegi, le funzioni, le abilitazioni
 necessarie affinché il suo messaggio si possa ritenere valido a tutti gli effetti?

Non è sufficiente...

...sapere chi ha firmato un documento, ma è importante essere certi che egli era autorizzato a farlo, quindi...

...al Processo Identificativo segue sempre il Processo Autorizzativo



Un progetto per la costruzione di un'opera edile deve essere firmato da un ingegnere



Un ordine di carcerazione può essere emesso solo da un giudice

Identificazione vs Autorizzazione

- Il processo **identificativo** si basa sull'identità del soggetto
- Il processo **autorizzativo** si basa invece sugli **attributi** del soggetto: *ruolo, mansioni, rango, privilegi, abilitazioni, etc...*



Il Processo Autorizzativo Tradizionale



Si basa sul vecchio concetto di "anagrafica utenti" (database locale contenente **informazioni** sugli utenti)

Le informazioni nel database sono facilmente **modificabili** e ciò comporta un serio problema....



Il Processo Autorizzativo Tradizionale

- I documenti firmati digitalmente potrebbero essere esaminati dal destinatario non immediatamente alla loro ricezione ma dopo diverse settimane o mesi, quando gli attributi del mittente-firmatario potrebbero anche essere cambiati
- Se il database è gestito dal destinatario non può essere considerato affidabile "erga omnes"



Il Processo Autorizzativo Tradizionale



Perché i normali certificati non bastano?

È possibile includere nel PKC informazioni relative agli attributi del titolare

- Il **Distinguished Name (DN)** del titolare può includere una serie di **campi opzionali** (*title, description, directoryAttributes, etc...*)
- Le **estensioni** (una fonte inesauribile di ulteriori possibilità)



Ma...

...Due forti ragioni

per **non includere informazioni autorizzative** nel certificato di chiave pubblica:



- La CA **non è l'ente più adatto** per attestare gli attributi degli utenti e ne esistono già appositi che lo fanno a livello istituzionale
- Gli attributi di un utente **variano frequentemente nel corso del tempo**... Fissare gli attributi in un PKC comporta la necessità di revocare il certificato al variare di quest'ultimi

Una soluzione migliore: il Certificato di Attributi



- simile al certificato di chiave pubblica
 - contiene il distinguished name del titolare
 - non contiene la sua chiave pubblica ma uno o più attributi che specificano gruppo di appartenenza, ruoli, funzioni, etc...
- firmato digitalmente da una terza parte, **l'Autorità degli Attributi**

Attribute Authority (AA)

Non è propriamente una "Trusted Third Party" in quanto non necessariamente è "third" né "trusted"

- Non svolge il suo compito in virtù del fatto di essere affidabile ma perché ha l'autorità di assegnare e modificare gli attributi
- Solo un ente che abbia una conoscenza "intima" degli attributi degli utenti può svolgere il ruolo di AA



Attribute Authority

Per i dipendenti di un'azienda, la AA non può essere che l'azienda stessa



Per i clienti di un servizio, la AA non può essere che il servizio stesso

Per gli appartenenti ad un ordine professionale, la AA non può essere che l'ordine professionale stesso



Requisiti di una AA

La AA è un sistema molto simile alla CA

- Si appoggia ad un database relazionale
- È dotato di un'interfaccia web
- Usa un dispositivo crittografico hardware
- Interagisce con un directory server



Certificato di Attributi: sintassi

```
AttributeCertificate ::= SEQUENCE
{
    acinfo      AttributeCertificateInfo,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE
{
    version      AttCertVersion,
    holder       Holder,
    issuer       AttCertIssuer,
    signature    AlgorithmIdentifier,
    serialNumber CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes   SEQUENCE OF Attribute,
    issuerUniqueID UniqueIdentifier OPTIONAL,
    extensions   Extensions OPTIONAL
}
```



Certificato di Attributi: esempio

Version: v2
 Owner: c=IT, O=Policlinico, CN=Rossi Mario
 Issuer: c=IT, O=Policlinico, CN=Ufficio Ruoli
 Signature: 1.2.840.113549.1.1.5
 Serial Number: 1234
 Validity: 1.1.2004 - 1.1.2005
 Attributes: title=Radiologo
 IssuerUniqueID: 22431
 Extensions: ...

Identità del titolare

Autorità che ha rilasciato e firmato il certificato

Identificatore dell'algoritmo di firma

Informazioni aggiuntive

Mario Rossi è un radiologo del Policlinico e questa funzione gli è stata attribuita dall'Ufficio Ruoli

Durata di attributi

La durata degli attributi è classificata in relazione al periodo di validità del PKC di riferimento:

- attributi *"a vita"*, la cui validità segue il titolare per tutta la sua vita, salvo revoche in casi eccezionali
- attributi *"a lunga durata"*, la cui validità supera quella del PKC di riferimento
- attributi *"di breve durata"*, la cui validità è inferiore a quella del PKC di riferimento



Revoca di attributi

Un AC può essere revocato prima della sua scadenza naturale:

- su richiesta del titolare
- autonomamente dall'emittente
- implicitamente, con brevi periodi di validità
- come i PKC, usando Attribute Certificate Revocation List (ACRL)
 - emesse periodicamente dall'emittente dell'AC
 - contengono i numeri seriali dei certificati revocati



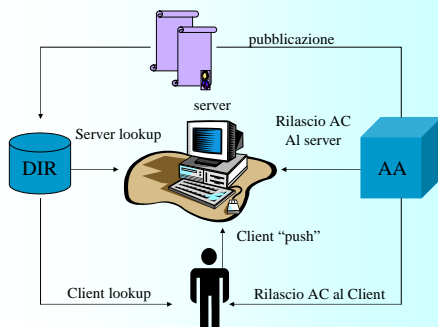
Modelli di distribuzione di AC

- Modello *"Pull"*
 - il server recupera da una directory l'AC del client
- Modello *"Push"*
 - il client presenta il suo AC al server
 - più efficiente
 - non c'è bisogno di una richiesta aggiuntiva da parte del server per recuperare l'AC dalla repository



La scelta di uno dei due modelli dipende dalle esigenze del sistema

Modelli di distribuzione di AC



Privilege Management Infrastructure (PMI)

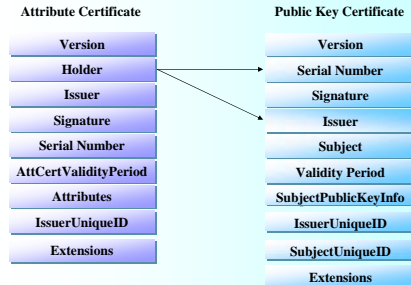
- Infrastruttura per l'uso e la gestione dei certificati di attributo
- Definita nel 2001, nella quarta edizione dello standard X.509
- Fornisce i servizi di autorizzazione dopo che è avvenuta l'autenticazione fornita dalla PKI



Privilege Management Infrastructure: componenti

- **Source of Authority**
 - decide quali privilegi sono necessari per accedere alle risorse e li assegna agli utenti
- **Attribute Authority**
 - assegna i privilegi su delega della SOA
- **Privilege holder**
 - possessore dei privilegi
- **Repository**
 - contiene AC, ACRL e privilege policy

Legame tra AC e PKC



PKC vs AC: esempio

- **PKC** → **carta d'identità**
 - identifica il possessore
 - dura per molto tempo
 - non dovrebbe essere banale da ottenere
- **AC** → **carta di credito**
 - rilasciata da un'autorità diversa
 - di durata minore
 - ottenerla tipicamente richiede di presentare una carta d'identità

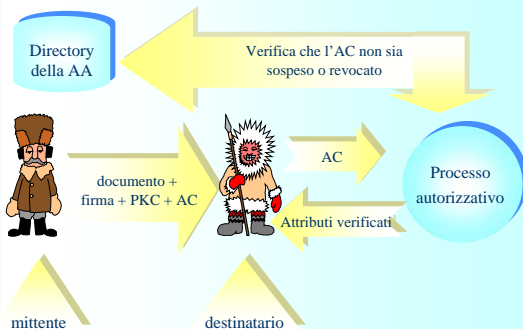


Cifratura di AC

- Se un AC contiene informazioni importanti, come un'applicazione username/password, allora può essere necessario cifrare gli attributi in esso contenuti
 - gli attributi sono cifrati prima che l'AC venga firmato
 - viene usata la struttura EnvelopedData specificata nell'RFC 2630 (Cryptographic Message Syntax)



Processo Autorizzativo basato sugli AC



Conclusioni



Come abbiamo visto, la certificazione di attributi rappresenta una tecnologia innovativa a supporto del processo autorizzativo. Si tratta di una tecnologia ancora relativamente giovane ed immatura dal punto di vista del mercato, ma tuttavia assai elegante e promettente. Gli standard di riferimento hanno già fissato gli aspetti principali, ma permangono delle "aperture" che fanno da ostacolo all'interoperabilità. Col tempo, comunque, questi problemi saranno risolti ed è prevedibile che la tecnologia degli AC si diffonderà sempre di più.