OpenCA - OS PKI

Bologna, 28/29 Ottobre 2000

21 ottobre 2000

1 1. Introduzione sulle PKI

1.1 Cosa Sono

Con il termine PKI si indica un' Infrastruttura a chiavi pubbliche (Public Keys Infrastructure) e sotto questa denominazione sono compresi tutti gli elementi necessari per la fornitura di servizi di certificazione: CA, RA, LDAP, OCSP, etc... La fornitura dei servizi di certificazione, come si può intuire, comprende un gran numero di componenti atti a garantire, da un lato, l'ente di certificazione e, dall'altro, l'utente.

I primi tipi di applicazione degli algoritmi crittografici basati sull'utilizzo di una coppia di chiavi (numeri primi) di cui una pubblica ed un'altra privata hanno evidenziato fin dal principio problemi legati all'identità dei possessori delle chiavi stesse. Problemi di questo tipo sono presenti in prodotti pionieristici quali PGP o GPG. Una delle soluzioni possibili è appunto l'adozione di un terzo soggetto, la cui autorita' viene riconosciuta da entrambi, che si incarichi di garantire sia Bob che Alice sulle rispettive identità.

1.2 A cosa servono

I CSP, ovverosia i fornitori di servizi di certificazione, hanno quindi il compito di garantire, da un lato, l'identità del possessorei del certificato e dall'altro la validità dello stesso. Mentre per fornire il servizio di certificazione vengono coinvolti alcuni componenti essenziali quali l'RA/RAServer e la CA, la garanzia di validita' del certificato implica l'utilizzo di strumenti aggiuntivi quali CRL, OCSP, SCVP, etc...

2 I certificati digitali

2.1 Il formato X.509v3

Il certificato digitale deve quindi contenere alcuni dati sull'identità dell'intestatario (solamente dati non sensibili - e, possibilmente, non soggetti a frequenti cambiamenti), la chiave pubblica (di cui la rispettiva chiave privata deve essere accessibile da parte del solo "proprietario") e delle estensioni atte a facilitare la

gestione degli stessi e dei servizi fruibili. Un esempio di certificato, in formato testo, e' riportato di seguito. Come possiamo notare e' composto da tre sezioni principali: la prima contenente dati del proprietario del certificato e della CA che lo ha emesso, la seconda contenente dati sulla chiave pubblica e la terza contenente le estensioni atte a definirne i campi di validita'.

```
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: CN=Certification Authority, O=OpenCA, C=IT
Validity Not Before: Jan 8 13:14:10 2000 GMT
Not After : Jan 7 13:14:10 2001 GMT
Subject: C=IT, O=OpenCA, OU=Project Manager, CN=Massimiliano Pala/Email=madwolf@comune.modena.it
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:c3:e0:1d:23:fd:d2:14:fc:13:5f:00:2a:de:55:
            7c:bf:b1:2e:74:1a:cd:86:71:07:80:6d:9d:5b:e3:
            1c:82:5d:c3:2b:6c:a2:94:6c:42:d4:90:49:b5:16:
            22:02:1f:5f:91:9b:11:67:67:41:7f:a9:1c:67:41:
            e3:7e:32:e0:8a:c9:3e:46:51:61:3d:f6:1a:b7:17:
            c5:43:18:6d:d3:03:80:5e:38:1a:cd:38:dd:57:b0:
            19:80:1c:61:47:19:3b:31:d4:ee:b2:5d:ff:cc:2e:
            ee:61:dd:eb:e0:9b:79:bb:07:34:c7:5f:41:80:e2:
            8d:97:94:5c:d3:ef:7e:79:c5
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    Netscape Cert Type:
        SSL Client, S/MIME X509v3
    Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
    Netscape Comment:
        OpenCA User Certificate
    X509v3 Subject Key Identifier:
        16:E0:37:01:3D:C2:F0:1F:EF:F3:DE:40:A1:32:95:1B:A6:A7:40:32
    X509v3 Authority Key Identifier:
        keyid:0B:4B:D3:C8:B1:F4:C6:CA:5C:CF:79:D1:AB:7C:BF:FC:91:48:C7:7B
        DirName:/CN=Certification Authority/O=OpenCA/C=IT
        serial:00
    X509v3 Subject Alternative Name:
        email:madwolf@comune.modena.it
    X509v3 Issuer Alternative Name:
        <EMPTY>
    Netscape CA Revocation Url:
        https://www.openca.org/cgi-bin/getcrl
    Netscape Revocation Url:
        https://www.openca.org/cgi-bin/getcrl
    Netscape Renewal Url:
        https://www.openca.org:4443/renewal
```

2.2 Terminologia di base

L'utilizzo di acronimi spesso inglesi rappresenta una costante in tutti i discorsi sulle PKI. Alcuni termini la cui comprensione risulta indispensabile sono:

- ***PKI (Public Key Infrastructure)***: questa è l'intera infrastruttura a chiavi pubbliche che viene implementata dal fornitore di servizi;
- ***CA (Certification Authority)***: computer dedicato alla gestione dei certificati (emissione, revoca, etc...);
- ***Policy***: Insieme delle regole seguite dal CSP che definiscono gli ambiti di utilizzo dei servizi e le pratiche seguite dal fornitore stesso;
- ***X509v3***: Standard per la definizione del formato di un certificato digitale. Evoluzione del formato X509 (ITU-T X.509 o CCITT X.509) - pubblicato come parte integrante delle raccomandazioni X.500 - che aggiunge la possibilità di definire delle estensioni per la gestione di informazioni legate alle policy, agli attributi, etc..;
- ***Directory Name (DN)***: Identificativo del soggetto del certificato. Questo campo del certificato definisce l'utente accreditato all' lutilizzo della coppia di chiavi (di cui quella pubblica è contenuta nel certificato);
- ***RSA***: Uno degli algoritmi di di cifratura asimmetrici piu' diffusi al mondo - da poco tempo diventato patent free;
- ***RAServer***: computer dedicato alla gestione centralizzata delle richieste di certificazione e gateway per le comunicazioni dalla e alla CA;
- ***Operatore RA***: personale addetto all'approvazione delle richieste di certificazione da parte dell'utente;
- ***Operatore CA***: personale addetto allapprovazione delle richieste di certificazione e allemissione dei certificati;
- ***CRL***: Lista dei certificati revocati la cui validita' risulta quindi essere in qualche modo compromessa. I certificati riportati sono da ritenere non piu' validi.
- ***Repository***: Archivio delle informazioni pubbliche come le CRL e i certificati;
- ***LDAP***: directory server spesso utilizzato come ottimo repository pubblico per i certificati;
- ***OCSP***: protocollo per la verifica dello stato dei certificati.

2.3 Applicazioni Attuali

Correntemente il numero ed il tipo di applicazioni effettive di queste tecnologie risultano essere molto limitate, sia per il fatto che mancano le applicazioni (non solo quelle che necessitano di altissimi livelli di sicurezza ma anche quelle la cui realizzazione dovrebbe risultare più semplice) che l'utente trovi utile, sia per il fatto che vi è probabilmente scetticismo spesso dettato da mancanza di conoscienze sull'argomento.

Il timore principale associato a questo tipo di tecnologia e' probabilmente legato al fatto che la sua sicurezza non e' dimostrabile in maniera assoluta (ma nemmeno la sua vulnerabilita'). In piu' bisogna considerare che esiste la possibilita' di automatizzare gli attacchi e quindi di portare questi ultimi per periodi idefinitamente lunghi.

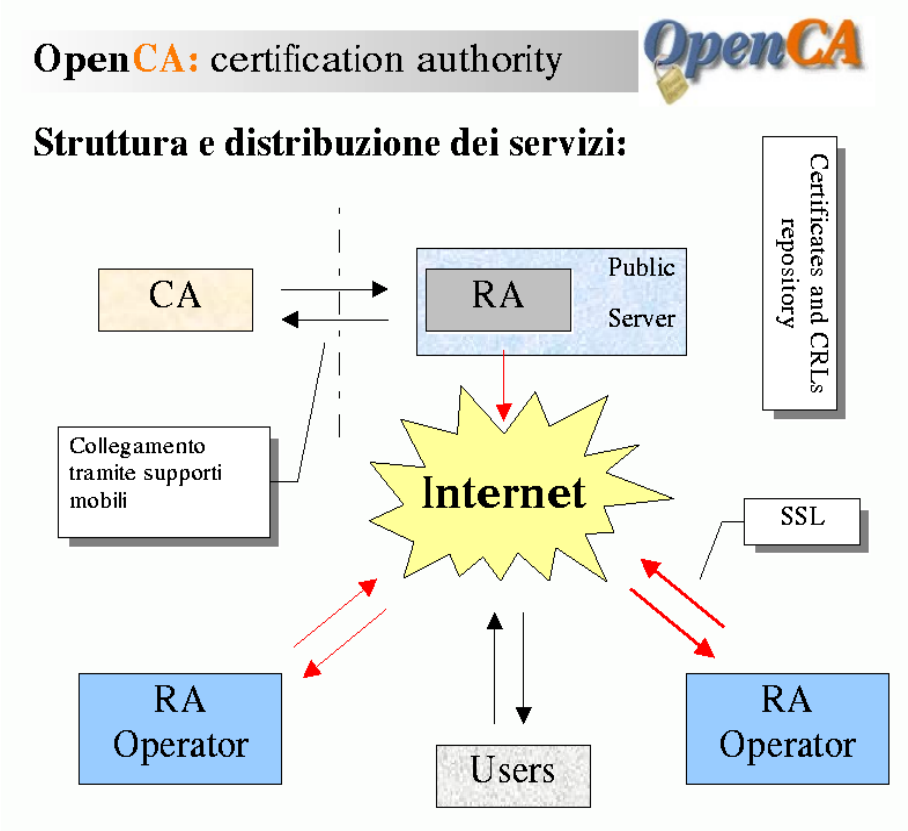
Allo stato attuale delle cose ci si sta concentrando forse più del dovuto sulla realizzazione di strutture di certificazione "perfette", senza pensare agli aspetti applicativi che potrebbero comprendere casistiche molto più estese delle sole transazioni sicure via Internet. Importante e' anche sottolineare il fatto che i due aspetti di Certificazione ed Applicativo vengono spesso ed erroneamente confusi. Mentre per il primo aspetto gli enti eletti per vocazione potrebbero essere gli stessi Comuni, la fornitura di servizi e/o applicativi puo' tranquillamente essere sviluppata da terze parti (spostando di fatto il guadagno sulla fornitura di servizi piuttosto che sul singolo certificato favorendone sicuramente lo sviluppo).

3 Il progetto OpenCA

Il progetto OpenCA o "Open Certification Authority" si innesta in un panorama che vede i costi di avviamento e di gestione di un'ente di certificazione spesso spropositati ed inaffrontabili per i possibili interessati, favorendo in questo modo, l'accentramento nelle mani di pochi e potenti colossi di un servizio basato su tecnologie a bassissimo costo. Il progetto OpenCA si pone come obbiettivo principale quello di fornire una soluzione di PKI basata su software Open Source quanto più possibile completa ed affidabile. Parte del software utilizzato viene sviluppato indipendentemente come OpenSSL o mod_ssl e parte è sviluppato direttamente dalla comunità legata al progetto. Attualmente il progetto sembra aver incontrato molto interesse sulla rete ed in Italia in particolare. Molto interesse sembra anche esserci da parte sia dell'est europeo, sia da paesi orientali quali Giappone e Cina.

3.1 Attuale struttura di OpenCA

In figura (Fig. 1) si può notare come il progetto sia stato pensato tenendo in mente, come modello di riferimento, l'RFC 2510 proposto dall'IETF.



Attualmente la maggior parte del software è sviluppato in PERL, Javascript e C, utilizzando come interfaccia di base Apache (web server) fruibile attraverso un browser quale Netscape. La scelta di utilizzare un'interfaccia basata su HTML è nata dall'esigenza di fornire un'implementazione quanto più possibile semplice, intuitiva e portabile tenendo conto del fatto che, a regime, l'utilizzo del sistema di certificazione avverà probabilmente da parte di persone tecnicamente non preparate (comprendendo con questo sia il/i responsabile/i della CA che gli operatori abilitati alla validazione delle richieste) e che l'utilizzo di Netscape non dovrebbe rappresentare un ostacolo essendo probabilmente un programma gia' largamente utilizzato all'interno di molte organizzazioni.

Il layer crittografico - il software che fornisce le funzionalità di crittografia di base - è basato su OpenSSL a cui abbiamo contribuito per quanto riguarda il miglioramento dell'utility di gestione dei certificati. Ultimamente e' stato aggiunto un altro aspetto interessante di OpenSSL ovvero il supporto (ENGINE) per operazioni di crittografia effettuate direttamente su hardware dedicato ed in particolar modo su lettori di Smart Card.

3.2 Modello di sviluppo

Il modello di sviluppo scelto è stato fin dalla prima realizzazione basato sul "sistema" Open Source per alcuni motivi, tra i quali possiamo citare i seguenti:

- l'idea è nata da persone che credono profondamente nello sviluppo collaborativo e soprattutto nell'idea che un'applicativo di tale importanza dovesse essere disponibile per il più ampio numero di utenti possibile;
- per come si stava/sta configurando il mercato legato alla fornitura di sistemi di certificazione la maggior parte degli attori naturali (piccoli e medi comuni) per la certificazione non potevano/possono permettersi i costi proposti dalle grandi aziende se non per soluzioni vincolanti e per sperimentazioni temporalmente limitate;
- il principio della sicurezza basata su soluzioni proprietarie "Security throught Obscurity" si è già dimostrato perdente in partenza (una buona lettura sull'argomento è sicuramente l'ultimo libro di Bruce Shneier - Secrets and Lies) mentre l'adozione di un modello OS sembra essere uno strumento valido nella risoluzioni di progetti importanti legati alla sicurezza;

La licenza di utilizzo del software sviluppato dal progetto OpenCA e' del tipo FreeBSD ed e' allineata con quella del software di base utilizzato (OpenSSL, Apache, etc...).

3.3 Problemi legati alla gestione di CA

La gestione di un servizio di certificazione pone molti problemi che, contrariamente a quanto si potrebbe pensare, sono principalmente di carattere organizzativo e non tecnologico. Se si tiene presente questo aspetto risulta chiaro come di fondamentale importanza sia la definizione delle POLICY adottate dall'ente certificatore e che la loro definizione deve assumere alta priorità nella fase di setup della CA (aspetto spesso trascurato e sottovalutato).

Maggiori riferimenti sull'argomento possono essere recuperati consultando il sito del progetto europeo GUIDeS (*). Il documento presenta una trattazione dei maggiori problemi e dei principali aspetti di cui si deve tener presente durante la fase di setup della CA. Per questo motivo rappresenta una valida guida negli aspetti decisionali iniziali, con particolare riferimento ai problemi legati alle Pubbliche Amministrazioni.

3.4 Conclusioni

Il progetto OpenCA, si identifica come un'alternativa nel panorama dei software di certificazione che basa la sua "forza" sullo sviluppo OS ed l'utilizzo di standard IETF. Se volete contribuire al progetto, maggiori informazioni sono dispeonibili all'indirizzo http://www.openca.org

Riferimenti bibliografici

[1] OpenCA Project - Open Source PKI Infrastructure [http://www.openca.org]

[2] Open Source PKI Book (Simos Xenitellis) [http://ospkibook.sourceforge.net/]

[3] Guidelines, Methodologies and Standards to setup a CA of Digital Signature (GUIDeS) [http://www.regione.emilia-romagna.it/guides]

[4] Bruce Shneier - "Secrets & Lies" In a networked world [http://www.counterpane.com]

[5] IETF pkix workgroup resources [http://www.ietf.org/html.charters/pkix-charter.html]

[6] Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510) [http://www.ietf.org/rfc/rfc2510.txt]

[7] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) [http://www.ietf.org/rfc/rfc2560.txt]

[8] References Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459) [http://www.ietf.org/rfc/rfc2459]

[9] Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP) [http://www.ietf.org/internet-drafts/draft-ietf-pkix-time-stamp-10.txt]