PKI e gestione delle Identità degli accessi

Franco Tafini

Security Solution Leader
INTESA *An IBM Company*

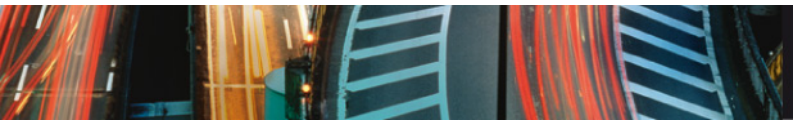
Roma 10 Giugno 2008

Firma Digitale e non solo ….

Come nella quotidianità, anche in campo informatico, il problema di conoscere l'identità della persona con la quale si sta interagendo è di importanza fondamentale.

Una decisiva spinta verso l'implementazione di nuovi sistemi di identificazione digitali è oggi data dalle comunicazioni inter-aziendali, da quelle bancarie e relativamente al nostro sistema paese con i portali e i servizi della PA accedibili con la CIE e la CNS.

Nel corso degli anni si sono così sviluppate molte soluzioni tecnologiche atte a a garantire l'identità di un utente, di un dipendente utilizzando vari dispositivi quali la firma digitale ,i certificati digitali, i security token, gli apparati biometrici.



Il ruolo di una CA: certificati self signed e pubblici

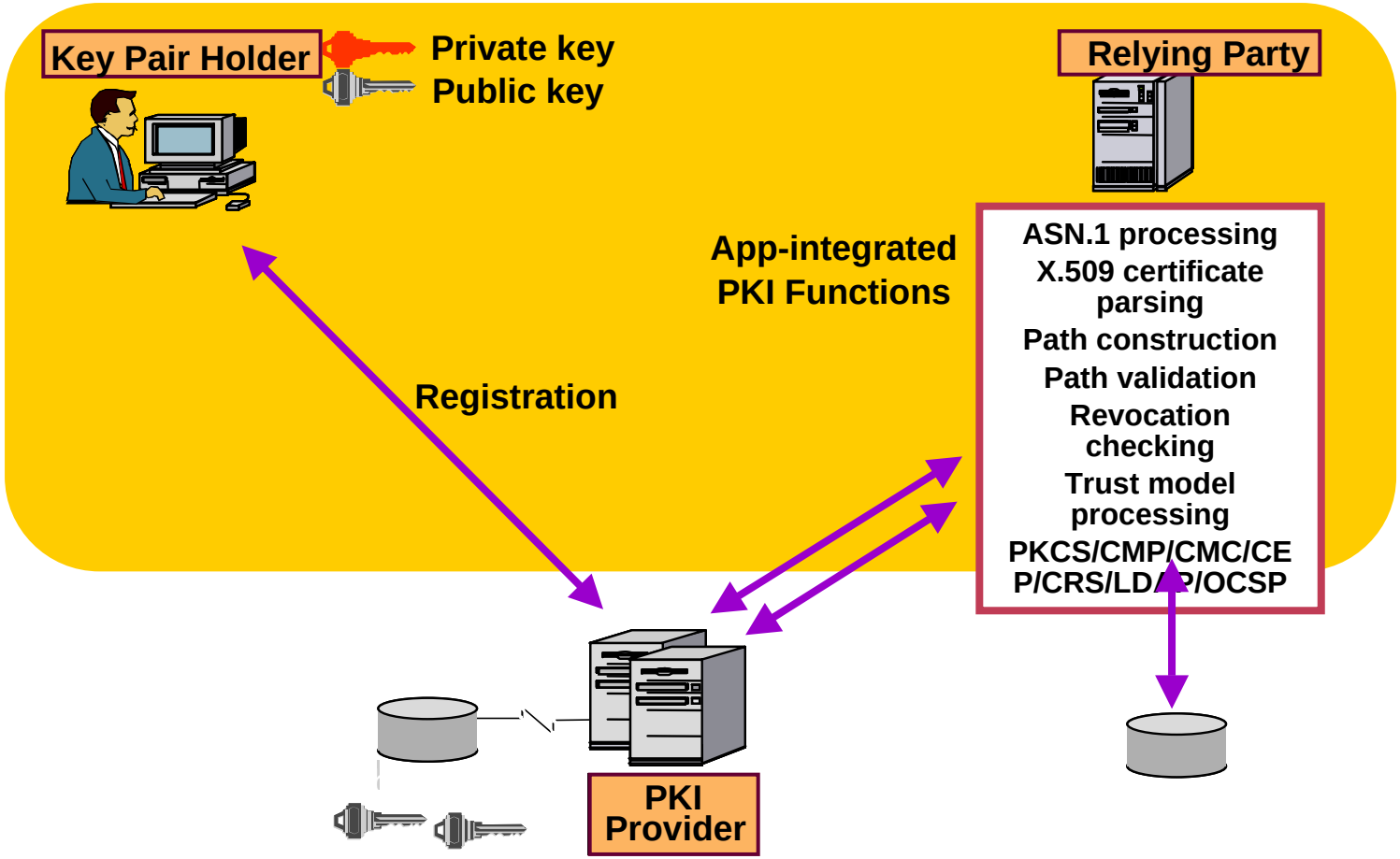
Certificati Self-Signed

- Queste CA non necessitano di nessun riconoscimento da parte di un'autorità superiore, non hanno ovviamente particolare credibilità.

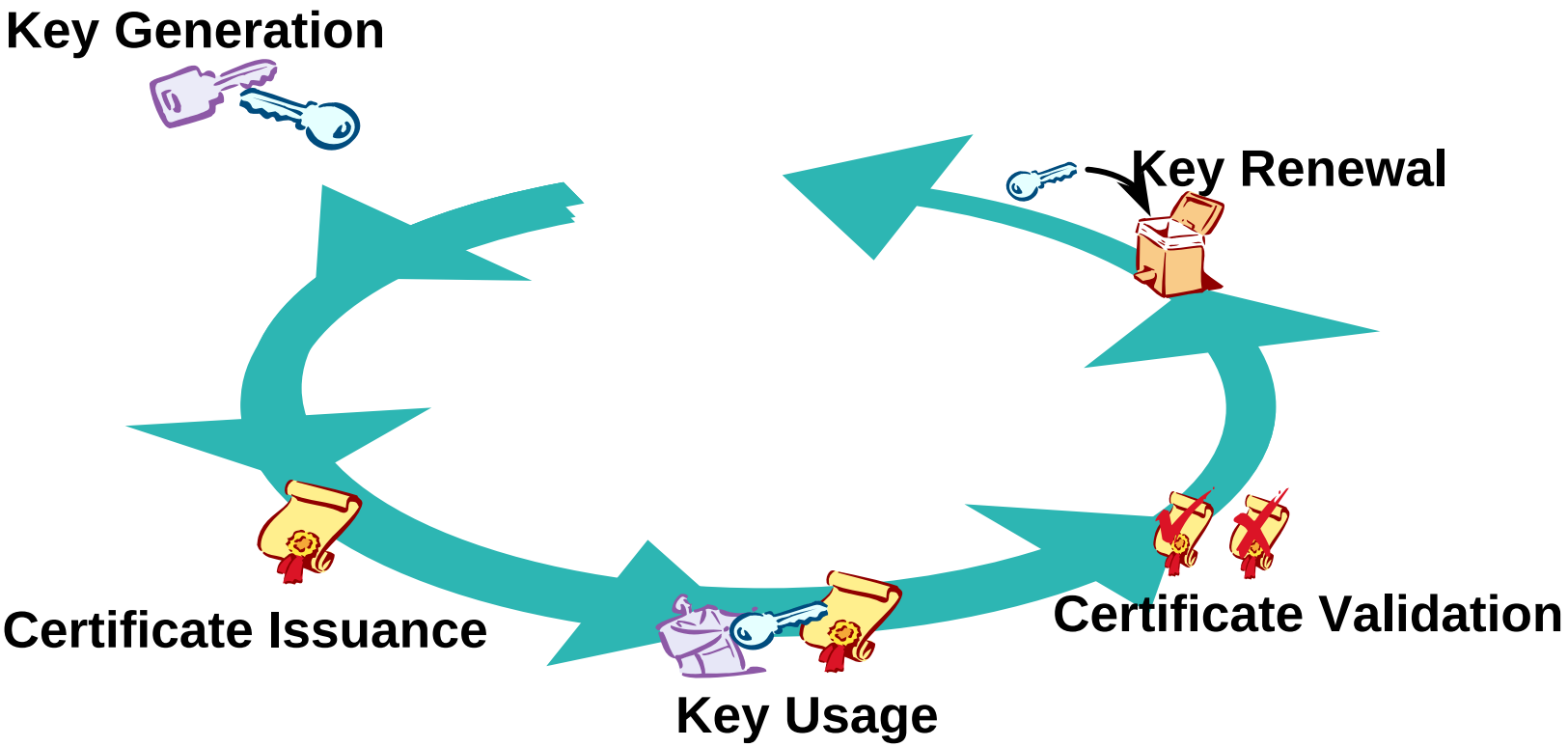
Public Certificate Authorities

- In questo caso I certificati vengono emessi con l'obiettivo che vengano immediatamente riconosciuti da tutti gli utilizzatori e terze parti coinvolte nei processi che li richiedono.
- E' pertanto indispensabile che anche il certificato root della CA con il quale tali certificati vengono firmati deve essere facilmente riconoscibile.
- Se tali certificati non sono "trusted" una serie di warning viene presentata all'utilizzatore degli stessi.

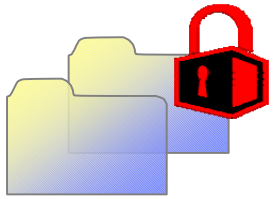
Le PKI di prima generazione sono una risposta parziale



Per gestire l’intero ciclo di vita dei certificati



Esaminiamo le funzioni della PKI del CG-SPC



La PKI del Centro Gestione è progettata per garantire:

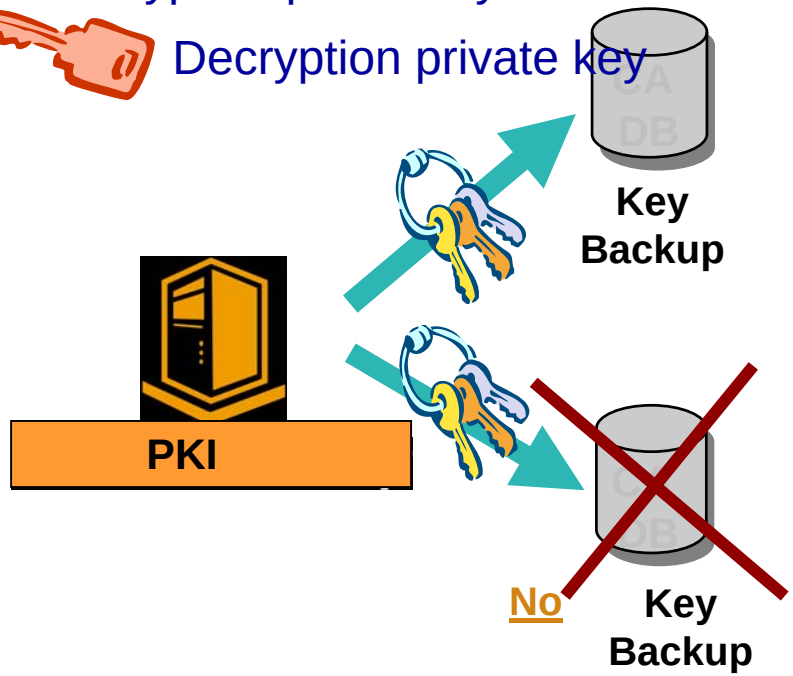
- Realizzazione di reti virtuali private sicure (certificati IPSec)
- Autenticazione e confidenzialità nelle le transazioni client-server (certificati SSL)
- Autenticazione all'accesso di risorse informatiche afferenti al SPC (certificati di autenticazione)
- Confidenzialità nel trattamento di documenti informatici e/o di messaggi di posta elettronica (certificati per la cifratura)
- Autenticazione del codice eseguibile (certificati object signing)

CG-SPC presenta funzioni complesse

Encryption key pair:

Encryption public key

Decryption private key



Digital Signature key pair

- Gestione gerarchica delle CA
  - Cross Certification
  - Peer-to-Peer
- Distribuzione di Trusted Certificate List
- Key backup, history and recovery
- Alta scalabilità sul numero di utenti
- Ruoli e deleghe nei processi amministrativi della CA
- Audit e reporting
- Aderenza agli standard (X.509. PKIX-CMP, PKCS#7/10, SCEP),
- Interoperabilità con Smart Card, LDAP, OCSP responders

Registration Authority

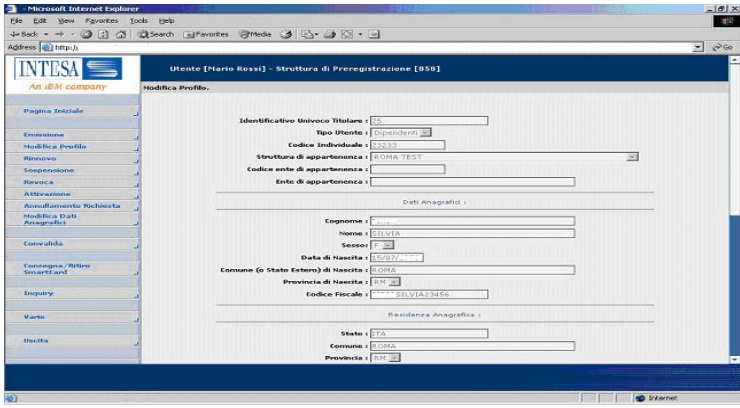
Entità che ha il compito e la responsabilità di identificare i soggetti esterni che devono interagire con la CA.

Possono essere previsti ruoli e autorizzazioni differenziate

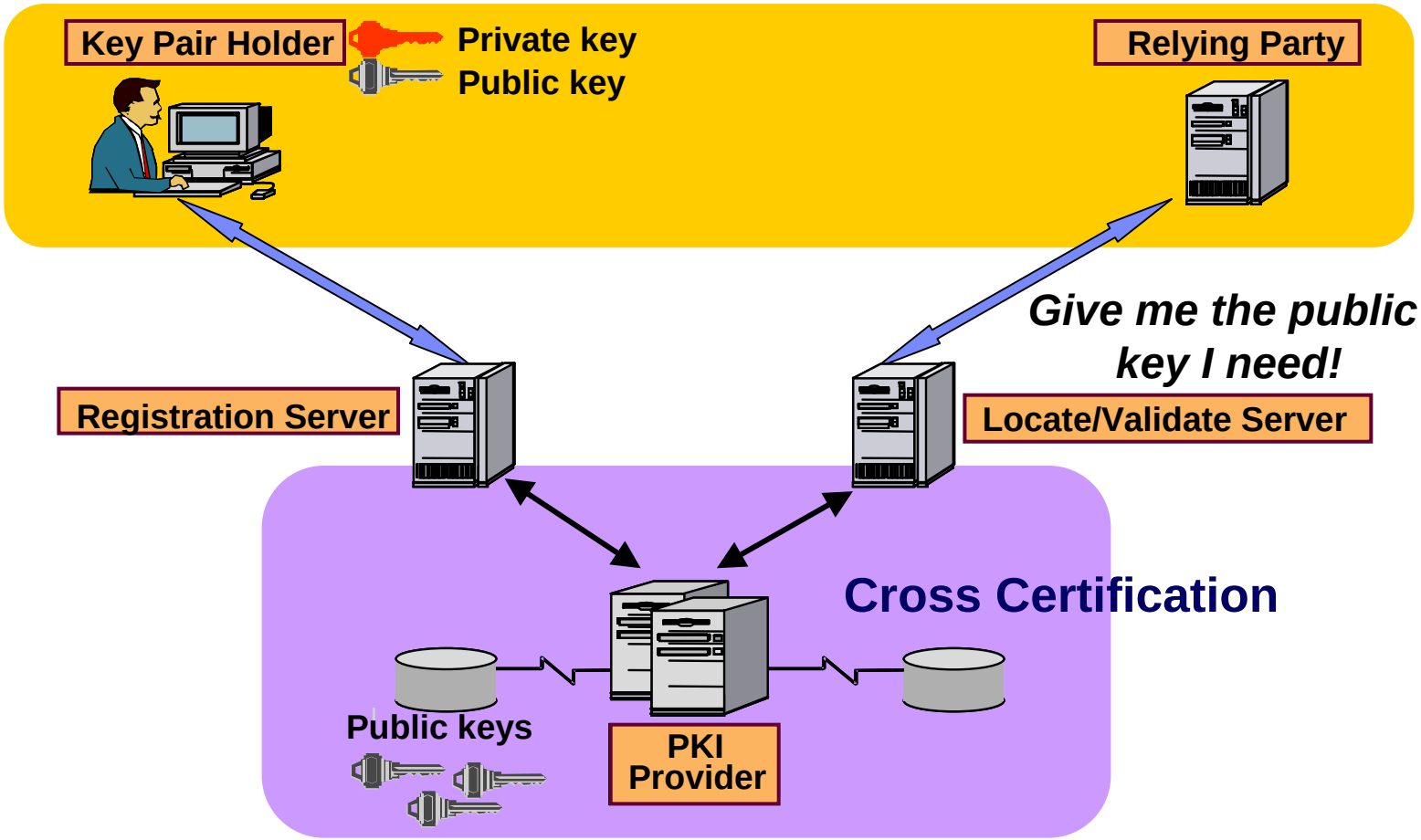
Può avere una struttura a più livelli (servizio centrale, local RA)

Richieste che possono essere gestite da una RA:

- Prima emissione o rinnovo di un certificato
- Revoca, sospensione o riattivazione dei propri certificati
- Convalida delle richieste
- Modifica profilo utente
- Inquiry



Si arriva così alle PKI della seconda generazione



CA Gerarchiche – Cross Certificate

- Procedure di audit sono state previste per assicurare che i processi organizzativi e di gestione delle CA gerarchicamente dipendenti da quella del Centro Gestione siano sufficienti se comparate a quelle messe in atto dal CNIPA.
- Al fine di stabilire e mantenere nel tempo un rapporto di fiducia (trust) tra le CA devono essere previste delle procedure di sicurezza e gestione delle attività PKI che dovranno essere oggetto di periodiche verifiche.
- Insufficienti controlli e/o mancato rispetto di tale procedure finirebbe con il limitare/indebolire il livello di sicurezza complessivo dell'intero progetto.
- Per tale motivo nel caso di CA gerachicamente dipendenti da quella CNIPA sono previsti controlli annuali di conformità sulle Certificate Policy, Certificate Practice Statement e sui controlli e le procedure implementate per il Key Management.

PKI - Sistema Pubblico di connettività

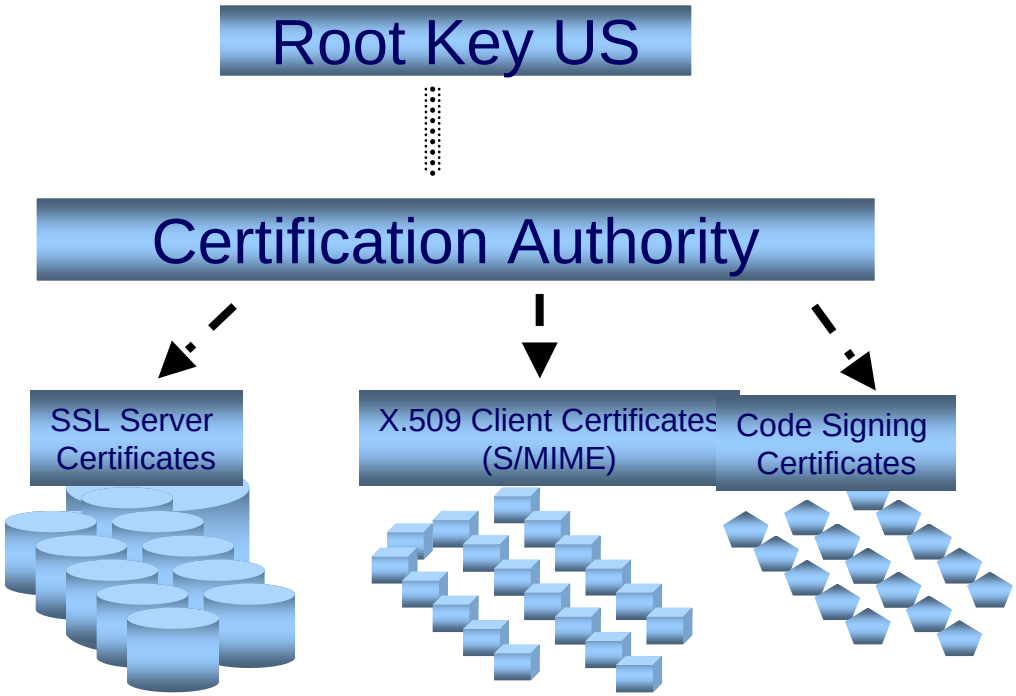
Nell'ambito del progetto è richiesta, in particolare, la realizzazione di una Public Key Infrastructure (PKI) per l'emissione e la gestione di certificati digitali.

Fra i componenti di cooperazione applicativa è richiesta una PKI in grado di emettere:

- Certificati di certificazione delle AC
- Certificati per la firma XML dei messaggi (busta e-gov),
- Certificati di autenticazione dei sistemi/applicazioni SSL/TLS 1.0
- Certificati per la Posta Elettronica Certificata (PEC)
- Certificati per il servizio di OCSP Responder
- Certificati di crittografia, utilizzati per la cifratura di dati e/o documenti e/o messaggi scambiati in SPCoop

Quando un certificato non è riconosciuto dai Browser

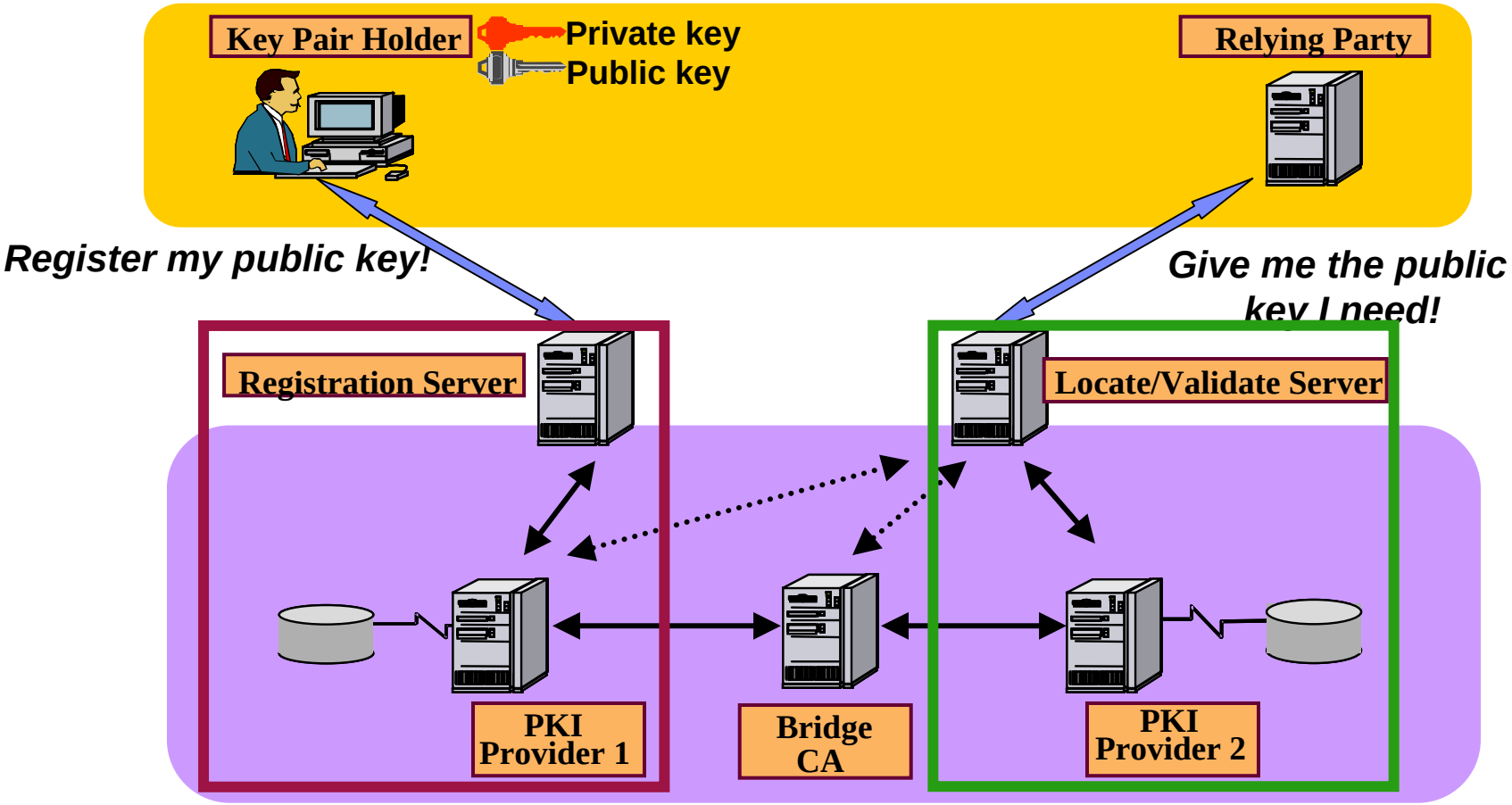
Anche per il sistema SPC si è ricorso a CA gerarchiche



La Certification Authority operativa di secondo livello provvederà ad emettere certificati (SSL Server, S/MIME, Code Signing) secondo le proprie procedure.

Una root CA di livello gerarchico superiore è utilizzata per “trustare” la Certification Authority operativa.

Le PKI dell'ultima generazione



Il controllo della Validità dei Certificati Digitali

Esame delle prestazioni e delle caratteristiche di affidabilità dei sistemi per la convalida dei certificati digitali e presentazione di un sistema distribuito di validazione attualmente in uso presso il DoD (Dipartimento della Difesa US) in grado di servire fino a centinaia di milioni di utenti con costi di esercizio ridotti del 60% rispetto ai sistemi tradizionali

Un fattore determinante per il successo di questi programmi , occorre non dimenticarlo, è costituito dal modo con il quale gli utenti saranno in grado di apprezzare le prestazioni dell'infrastruttura.

Se le loro applicazioni saranno lente, se saranno costretti ad attendere mentre il sistema esegue i controlli di sicurezza o, peggio, se il sistema diventa indisponibile a causa di un elevato contemporaneo accesso di utenti (per non parlare di un attacco informatico e/o di un guasto del servizio) gli utenti potrebbero essere indotti a rifiutare l'uso delle applicazioni proposte.

Validazione e autenticazione identità e credenziali

- Su larga scala
- Geograficamente dispersi
- Persone appartenenti a organizzazione diverse
- In situazioni ambientali talvolta difficili, assenza di comunicazioni
- Con tempi di risposta immediati
- Con infrastruttura scalabile e adattabile alla crescita senza dover cambiare nulla

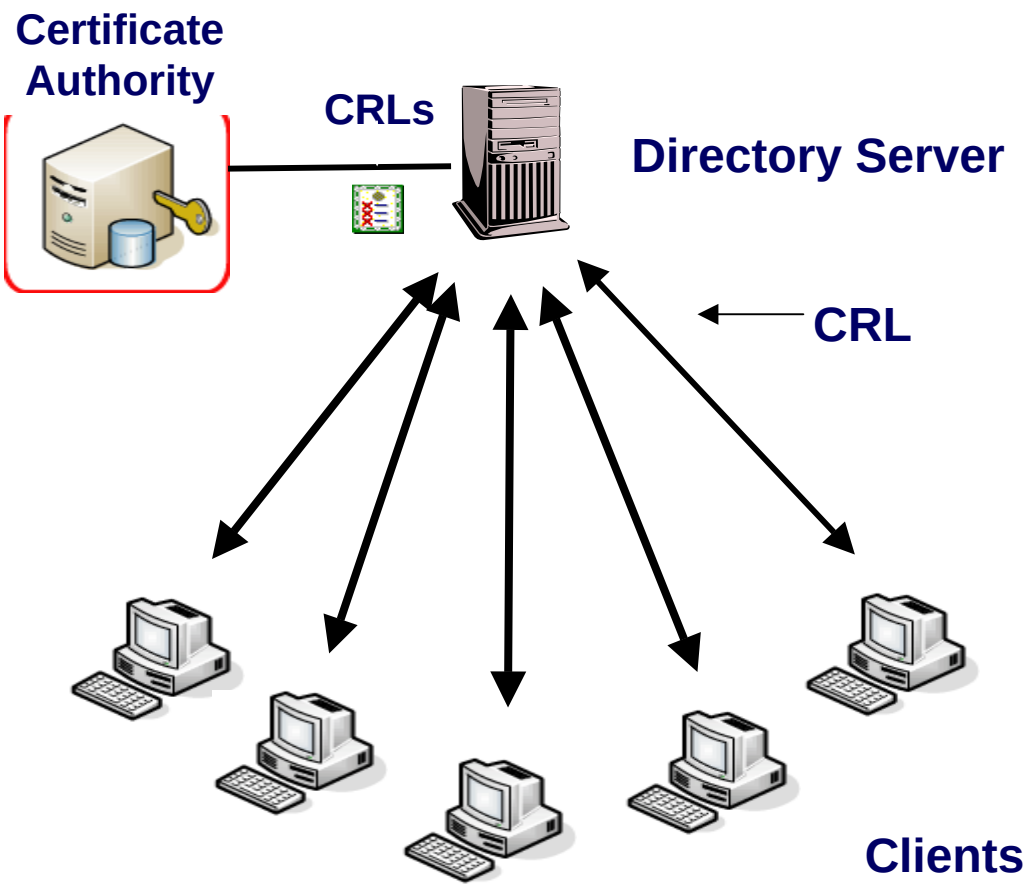
Scelta del sistema di validazione

Certificate Revocation Lists (CRLs)

Online Certificate Status Protocol (OCSP)

- Traditional OCSP
- Distributed OCSP

CRLs



Advantages
• Easy to manage for small numbers
• Works with all issued certificates
• Industry standard
Disadvantages
• Large bandwidth to the clients
• Does not scale
▪ Not suitable for mobile devices
▪ New applications using OCSP

= equires trust
physical and data security)

Sistemi OCSP

Il protocollo OCSP risolve il problema delle dimensioni della CRL poiché:

- Invia solo l'informazione sullo stato del certificato in questione (non l'intera lista)
- Consente una gestione centralizzata dello stato del certificato

Tuttavia l'OCSP comporta un aumento enorme del traffico dei dati.

Il risultato è il degrado delle prestazioni del sistema ed in particolare dei risponditori

- Quanti risponditori OCSP impiegare ?
- Dove mettere i risponditori ?
- Come può un utente sapere che può fidarsi della risposta che riceve da un risponditore ?

La certificazione della firma di un risponditore deve essere verificata

- Chi fornisce la convalida del certificato di firma del risponditore ?

Sistema OCSP Tradizionale

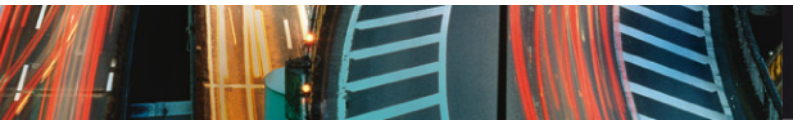
E’ necessario prevedere un’architettura distribuita che consenta la convalida dei certificati mediante l’impiego di risponditori ubicati vicini agli utenti.

I costi e la complessità dell’architettura distribuita limitano la soluzione.

Ciascun server OCSP deve essere messo in una postazione sicura e gestito da operatori fidati e la sua gestione diventa molto costosa.

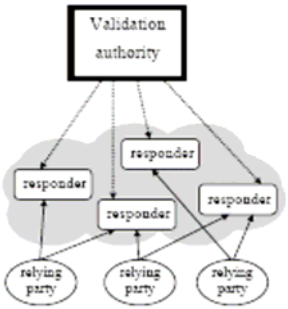
Ne consegue che:

1. Il numero dei risponditori sarà limitato
2. I risponditori dovranno essere messi in posti sicuri ad accesso controllato
3. Si spende molto per proteggerli



OCSP ad architettura distribuita

Il principio fondamentale su cui si basa un sistema sicuro di certificazione distribuita è la separazione dei dati di sicurezza sensibili e delle operazioni di sicurezza dal procedimento di consegna dei certificati di validità alle applicazioni degli utenti.



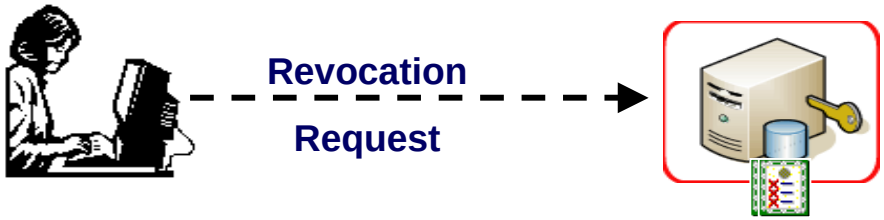
L'autorità di convalida (VA) ritiene i dati sensibili

Effettua tutte le operazioni di sicurezza

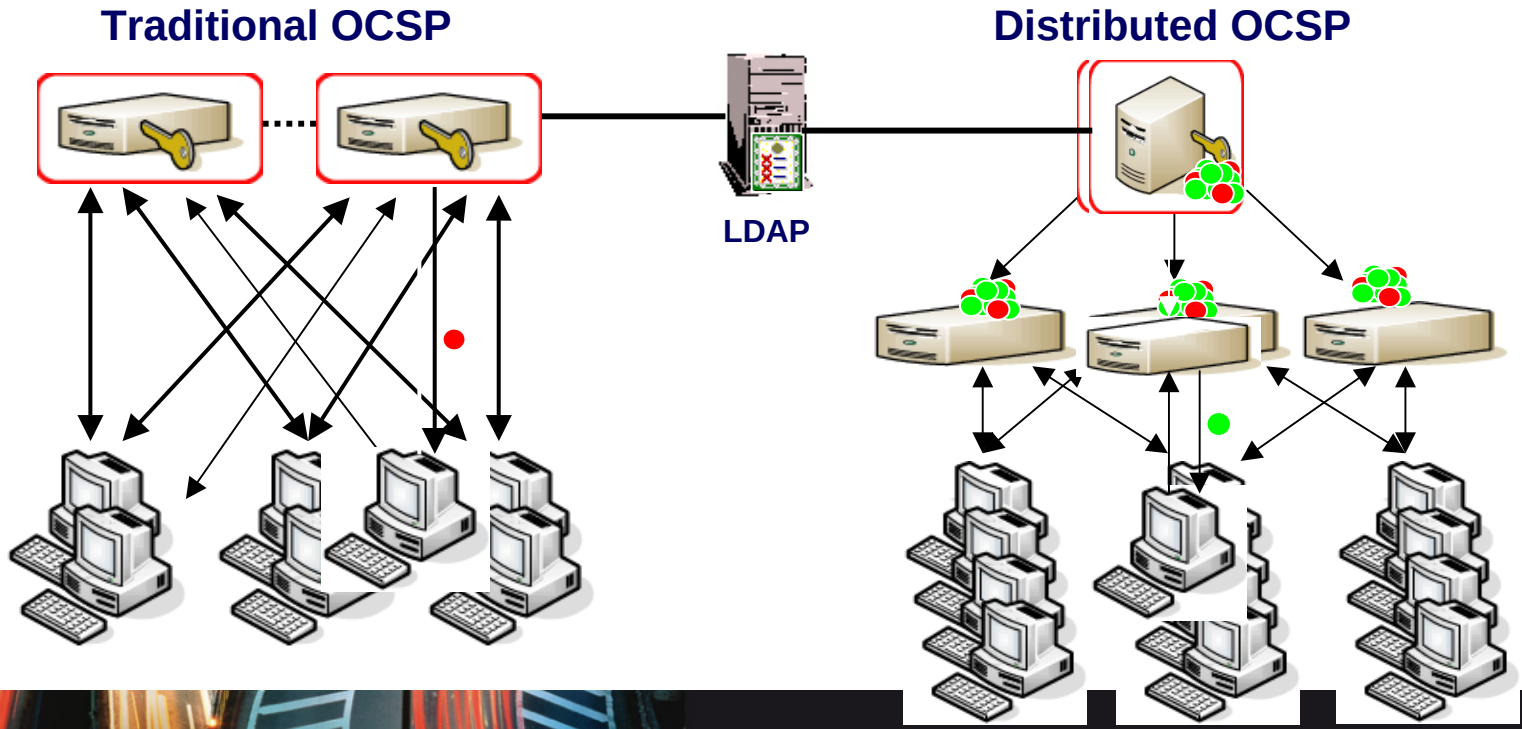
Si mantiene una singola VA con conseguente alleggerimento delle operazioni di sicurezza. Periodicamente la VA pre-elabora le prove di certificazione individuali, la periodicità di pubblicazione è determinata dalle singole politiche di sicurezza.

L'integrità di queste prove è protetto con firma digitale come avviene nel sistema OCSP tradizionale. I risponditori non costituiscono un problema per la sicurezza e possono essere sistemati vicino alle applicazioni degli utenti anche in ambienti non sicuri.

OCSP Validation



= requires trust
(physical and data security)



Vantaggi del sistema OCSP ad architettura distribuita

I vantaggi del sistema sono numerosi e comprendono:

Scalabilità effettiva: affidabilità, sicurezza, costi ridotti rispetto a sistemi tradizionali

Affidabilità elevata: gli utenti finali si collegano ad un risponditore locale

Prestazioni elevate: grazie alla ridotta la distanza tra utente ed il risponditore

Disponibilità elevata: gli attacchi multipli volti ad impedire il servizio sono virtualmente eliminati dall'impego di molteplici risponditori distribuiti geograficamente

Vantaggi del sistema OCSP ad architettura distribuita

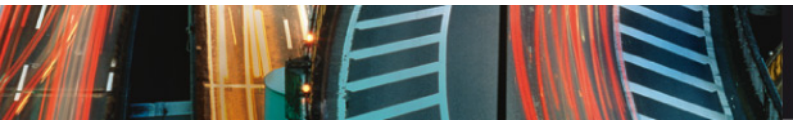
I vantaggi del sistema sono numerosi e comprendono:

Costo efficacia: I risponditori non richiedono comunicazioni, collocazioni o modalità operative sicure (piattaforme web server standard), I risponditori non contengono alcun dato sensibile ai fini della sicurezza possono essere dislocati anche in ambienti dove la minaccia di attacco è reale

Sicurezza elevata: rispetto ai sistemi OCSP tradizionali

Le richieste di validità dei certificati vanno solo ai risponditori e non alla VA.

Poiche la VA non ha comunicazioni con l'esterno la minaccia di un attacco è ridotta al minimo



IBM

G

Franco.tafini@intesa.it

INTESA
An IBM company