REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Firma digitale e Certificati uno strumento a servizio dell'amministrazione digitale

Giuseppe Russo
Chief Technologist
Principal Engineer & Security Ambassador

Sun Microsystems, Inc.

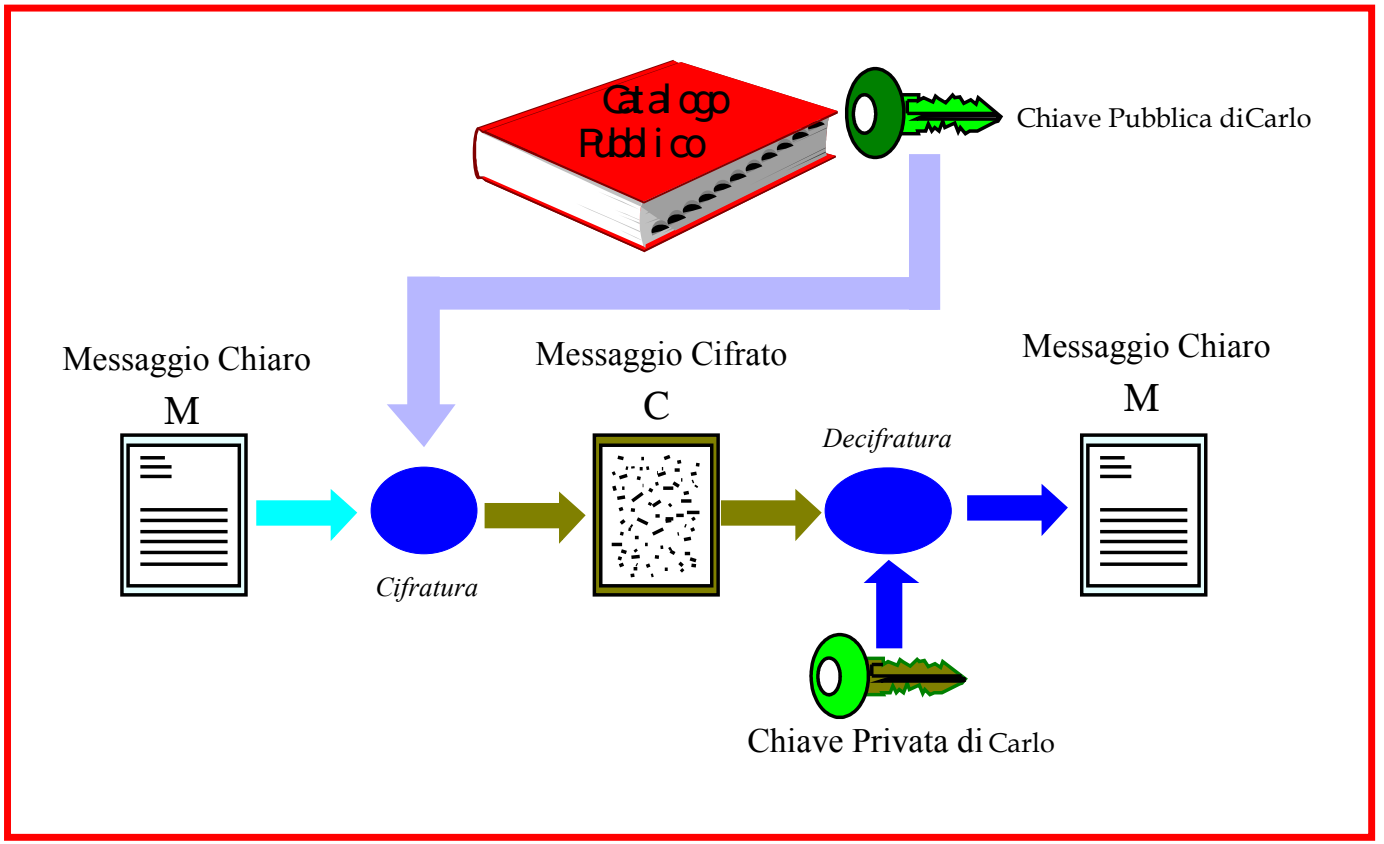
Agenda

- L'amministrazione digitale D.L. 82/2005
- La Firma Digitale
- Le Autorità di Certificazione
- Le Infrastruttura abilitanti all'uso di crittografia a chiave pubblica
- La Certification Authority di Regione Veneto
- Esempi di benefici per l'amministrazione digitale dalla autenticazione alla PEC

Il codice dell'Amministrazione digitale

- DL n.82 del 2005 e sua integrazione con il DL n.159 del 2006
  - L'informazione digitale
  - La formazione del documento (*documento informatico e firma digitale*)
  - Gestione e conservazione (protocollo e procedimento informatico)
  - Trasmissione tramite Posta Elettronica Certificata
  - Disponibilità dell'informazione digitale in termini di:
    - *accesso*
    - *fruibilità*

Crittografia Asimmetrica

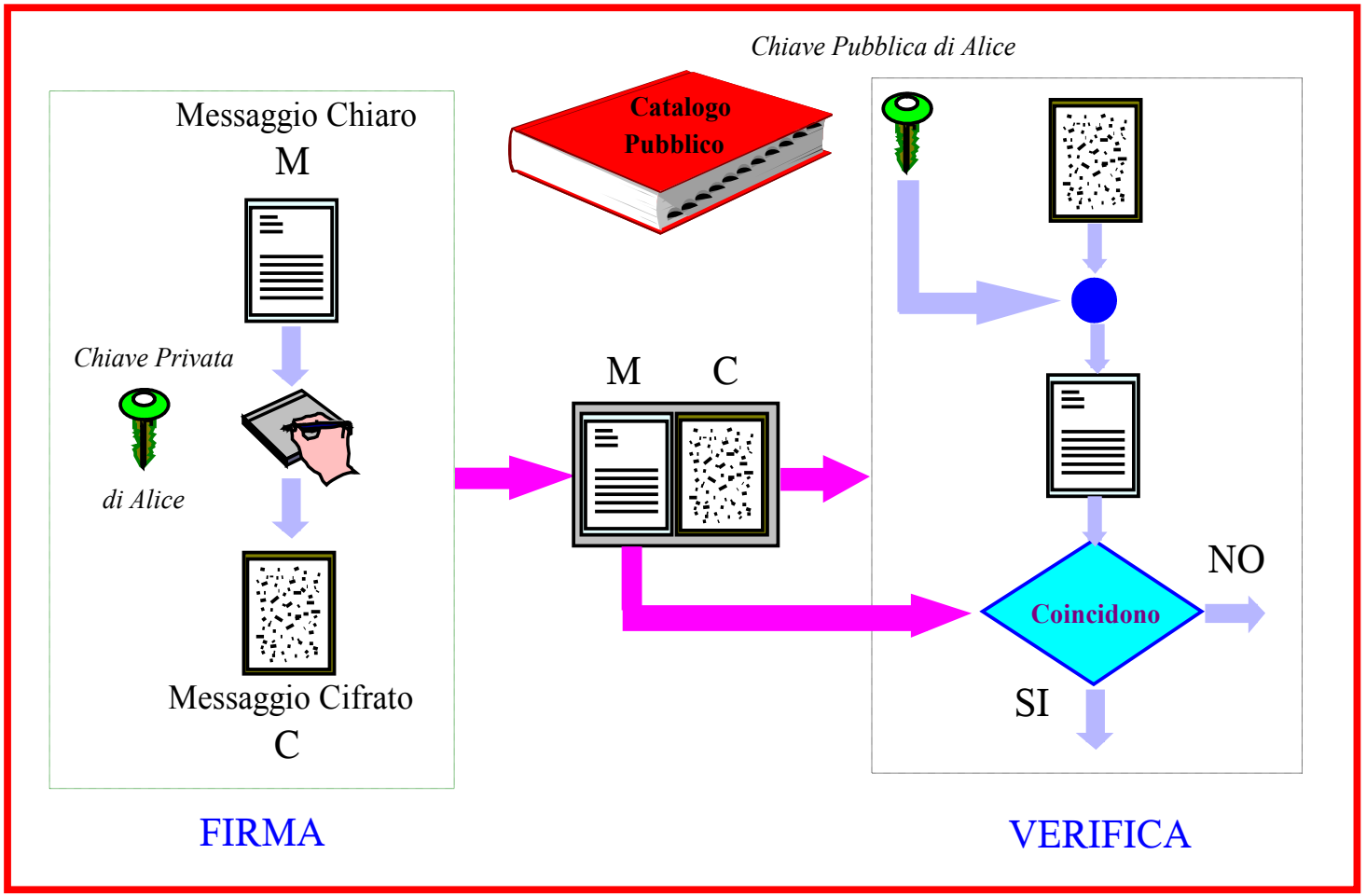


Consente di implementare il meccanismo di NON-RIPUDIO

Considerazioni

- Chiave Pubblica e Chiave privata sono interscambiabili
- Un messaggio cifrato con la *chiave pubblica* può essere letto solo da chi possiede la *chiave privata* (**certezza del destinatario**)
- *È come se il messaggio fosse stato messo in una scatola chiusa a chiave ed il destinatario è l'unico a possedere la chiave per aprire la scatola*
- Un messaggio cifrato con la *chiave privata* può essere letto da chiunque, ma può essere stato *scritto solo da chi possiede tale chiave privata* (**certezza del mittente**)

La firma digitale



- Firma Digitale con recupero del messaggio -

Funzioni Hash

- una funzione ***h( )*** che accetta un input di **lunghezza qualsiasi** e produce un output a **lunghezza fissa**
- le funzioni hash sono utilizzate per:
  - *per rilevare una modifica nei file*
  - *per verificare password*
  - *come seme di generazioni di eventi casuali*
  - *per ottimizzare le firme digitali*
  - *ecc.*

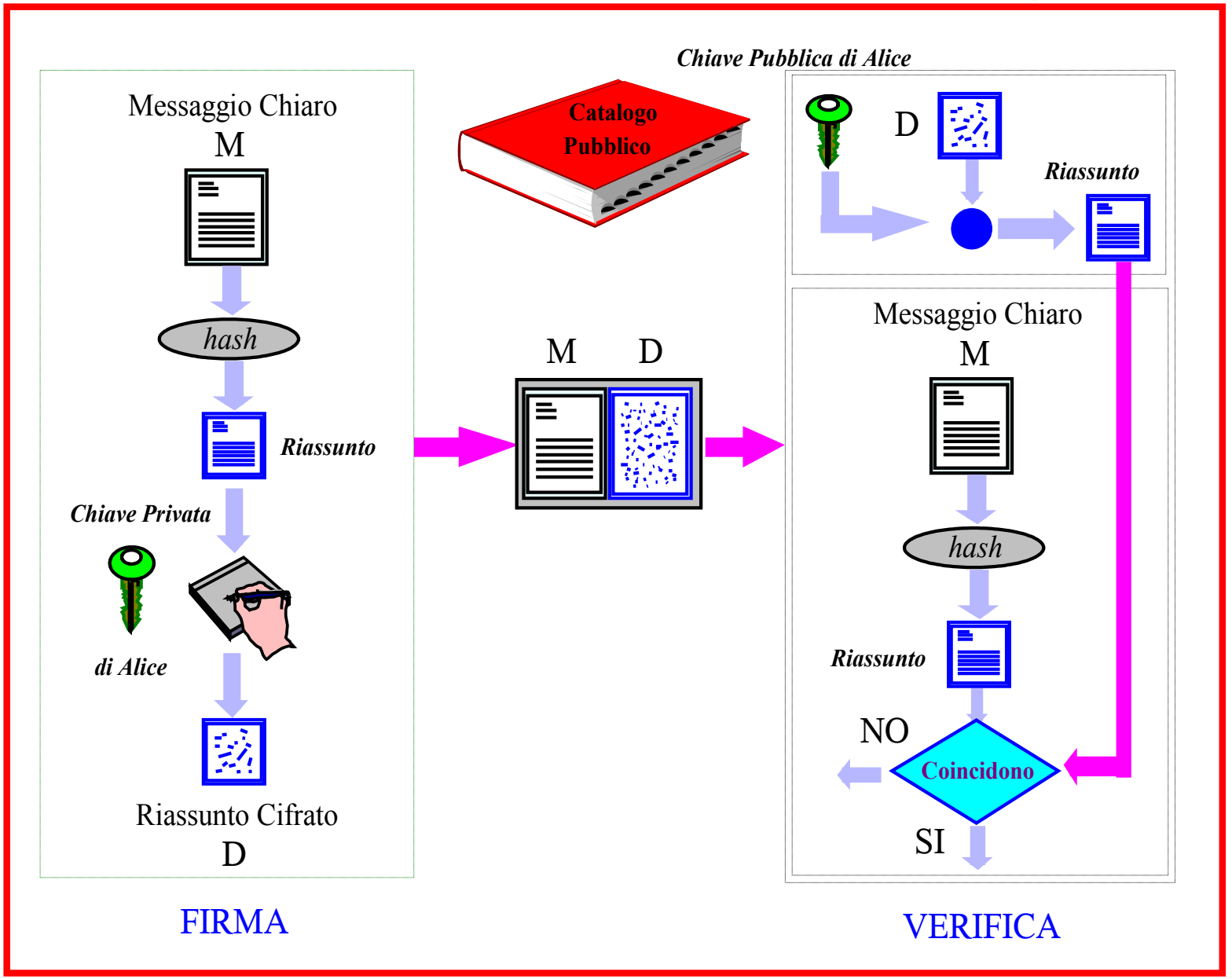
Funzioni Hash (2)

- quelle usate in crittografia devono essere ***one-way*** cioé:
  - se ***y*** é il valore di hash, é "***arduo***" trovare il valore ***m*** tale che ***h(m) = y***
  - dato un input **m** ed ***h(m)***, é "***arduo***" trovare un altro input m_1 tale che $h(m)=h(m_1)$
  -
- ***h( )*** deve essere *libera da collisioni* cioé:
  - deve essere "arduo" trovare ***m*** e m_1 tale che $h(m)=h(m_1)$

Funzioni Hash (3)

- le funzioni hash maggiormente utilizzate in crittografia sono:
  - **RIPEM-D** produce un output a 160 bit
  - Message Digest 5 (**MD5**), progettata da Rivest che produce un output a 128 bit
  - Secure Hash Algorithm (**SHA-1**) prodotto all'interno del progetto Capstone, produce un output a 160 bit
  - Secure Hash Algorithm (**SHA-256**) produce un output a 256 bit
  - Secure Hash Algorithm (**SHA-512**) produce un output a 512 bit

La firma digitale (2)

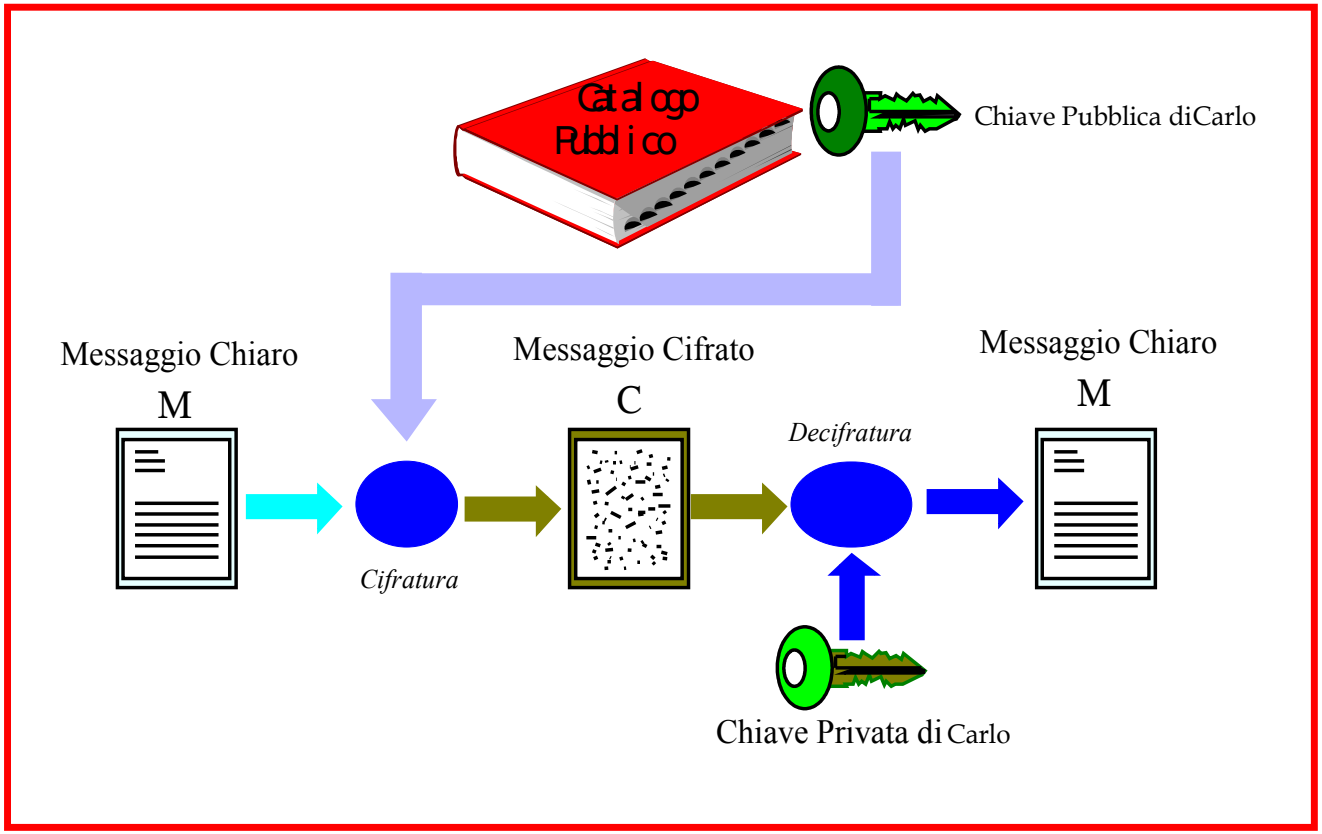


- Firma Digitale con Appendice -

La firma digitale garantisce...

- L'integrità delle Informazioni
- L'autenticità del mittente
- La non falsificabilità delle Firme
- Il non ripudio della transazione

Un possibile attacco alla PKC

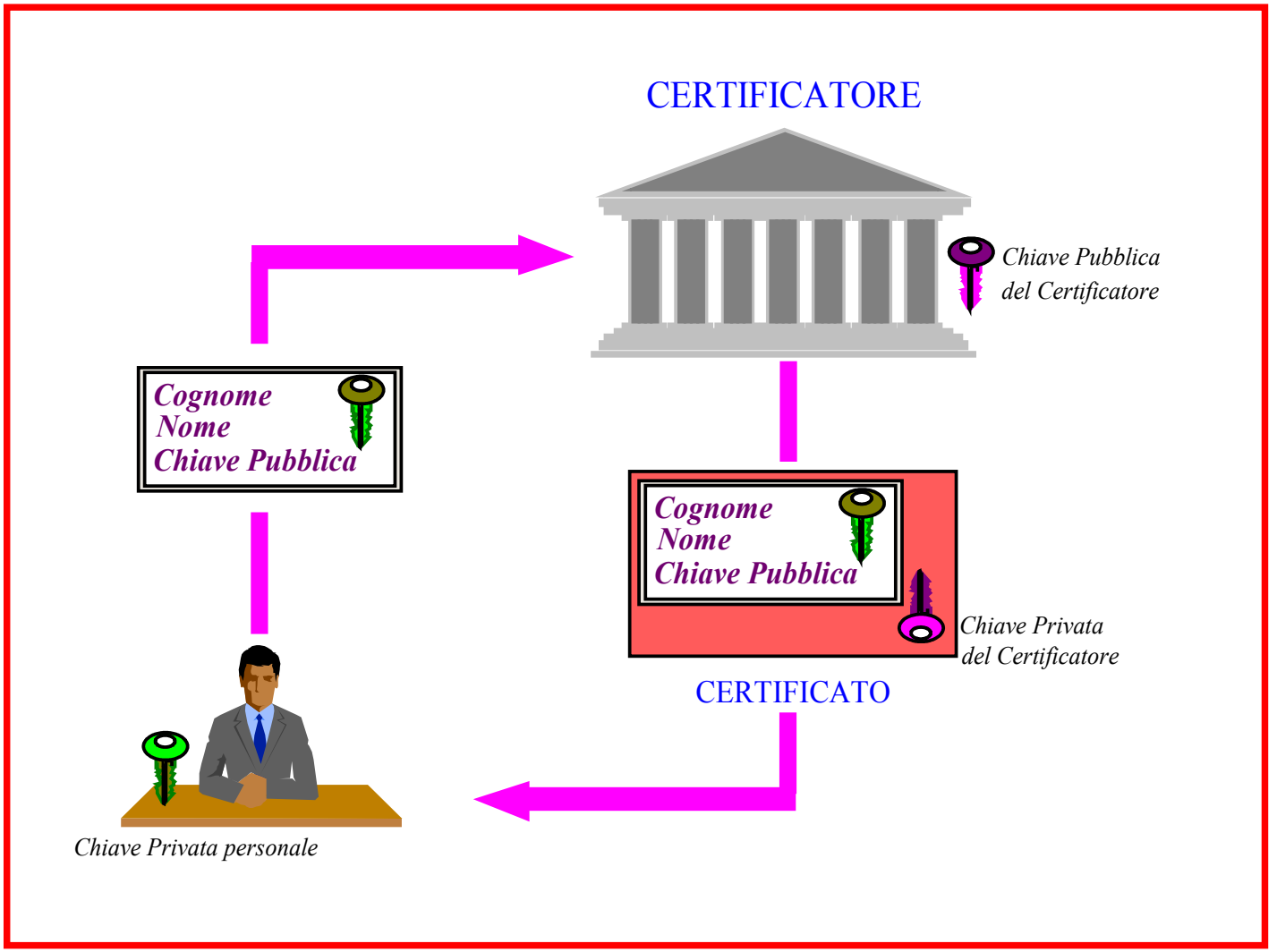


Se un impostore sostituisce, nel catalogo pubblico, la propria chiave pubblica al posto di quella di Carlo, riesce a leggere tutti i messaggi riservati indirizzati a Carlo

Autenticità della chiave pubblica

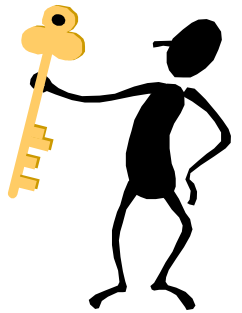
- affinchè uno schema crittografico asimmetrico funzioni correttamente occorre essere certi che la chiave pubblica dell'utente Giuseppe Russo, contenuta nel catalogo pubblico, sia veramente la sua
- tale garanzia di autenticità si ottiene coinvolgendo nel protocollo una ***terza parte fidata***

La Certification Authority



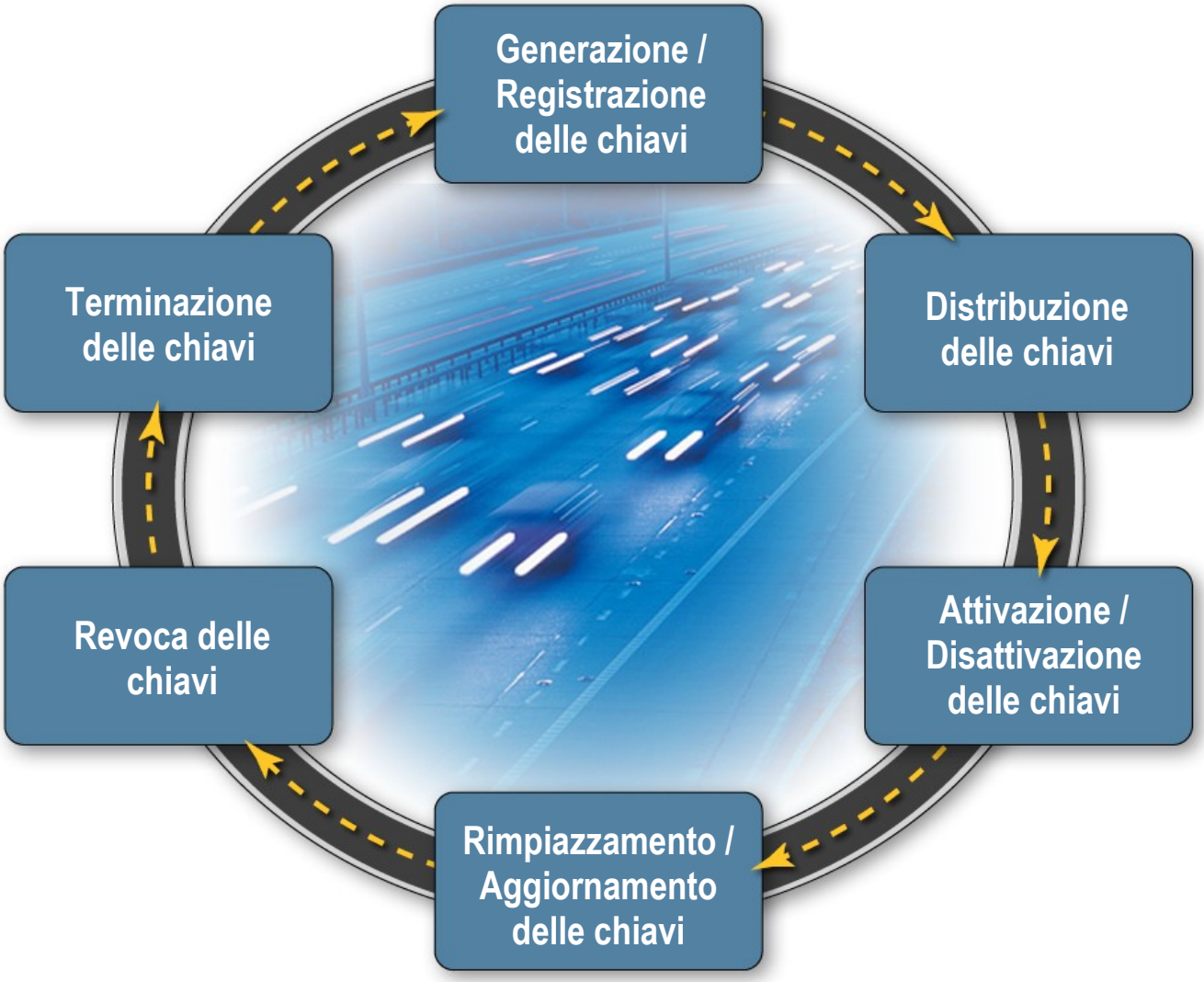
Il certificato digitale

- garantisce l'associazione fra una chiave pubblica ed un identificativo
- definito dallo standard X509v3
- generalmente contiene:
  - Nome del proprietario (**Owner**) e sua chiave pubblica
  - Nome e signature della CA che lo ha emesso (**Issuer**)
  - Periodo di validità, numero di serie e algoritmo di firma
  - La firma digitale della CA



Un esempio di certificato digitale

Il ciclo di vita di chiavi e certificati



I certificati e Certificatori nella PA Digitale

- Due tipologie di Certificati
  - Certificato Qualificato
    - *Insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.*
  - Certificato non Qualificato

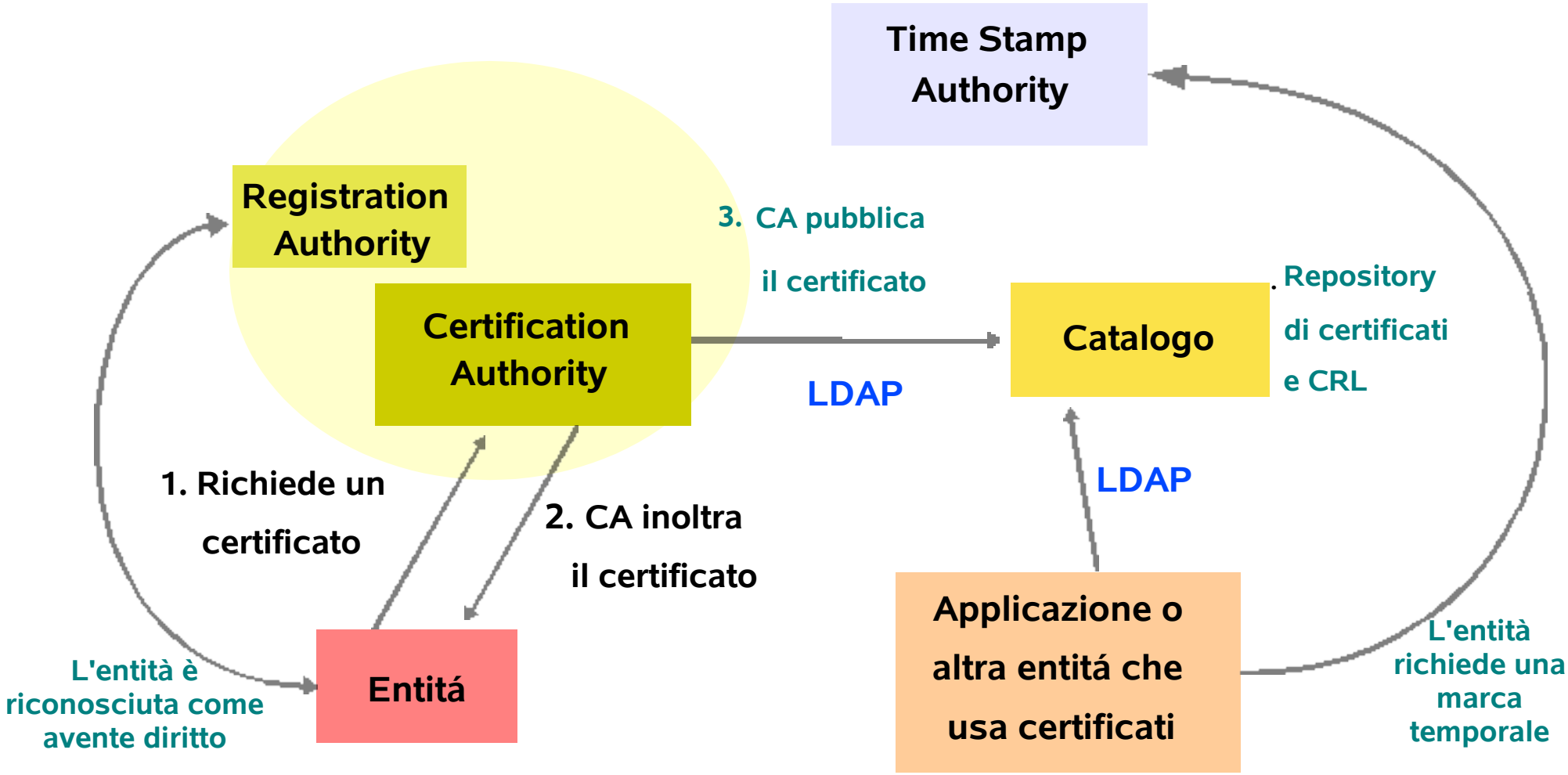
I certificati e Certificatori nella PA Digitale

- Due tipologie di Certificatori
  - Rilascia Certificati Qualificati
  - Rilascia Certificati non Qualificati
- 19 Certificatori Qualificati per la PA:
  - *http://www.cnipa.gov.it/site/it-IT/Attività/Certificatori_accreditati/Elenco_certificatori_di_firma_digitale/*

Public Key Infrastructure

Una PKI è una infrastruttura che fornisce un insieme di servizi di sicurezza che consentono di usare e gestire la crittografia a chiave pubblica, i certificati, le chiavi, e la politica di sicurezza ad essa associata

PKI: Componenti Fondamentali

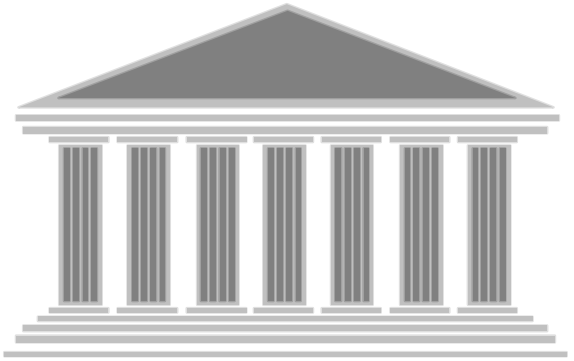


PKI: Certification Authority

- La CA ha il compito di creare ed inoltrare i certificati nel proprio dominio di sicurezza
- La CA compone il certificato, lo firma con la sua chiave privata, inoltra al cliente e lo pubblica su un repository pubblico
- La CA gestisce e pubblica la lista dei certificati la cui validitá o autenticitá é venuta meno: la **Certification Revocation List (*CRL*)**

PKI: Certification Authority (2)

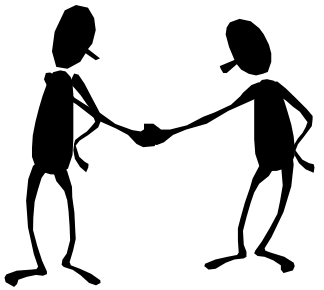
- La **CA** ha il compito di definire la politica dei certificati relativa alla:
  - *Emissione*
  - *Revoca*
  - *Rinnovo*
  - *Modello di Trust*



- può inoltrare diverse classi di certificati.

CA e Modello di Trust

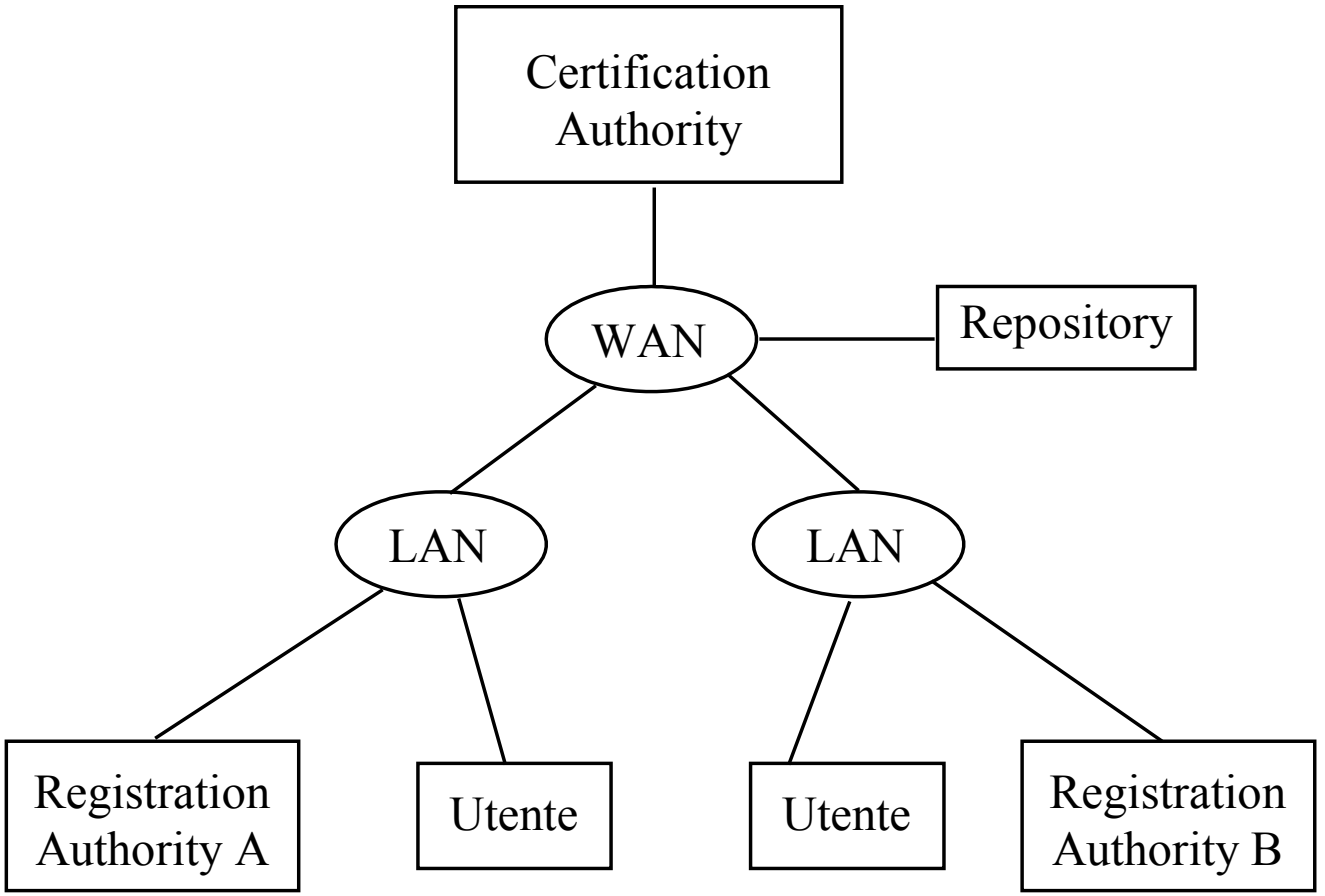
- **Gerarchico**
  - basato su gerarchie di CA strutturate ad albero
  - consente di implementare politiche flessibili e scalabili
- **Diretto**
  - utilizzabile in ambienti amichevoli
  - caratterizzato da bassa scalabilità



PKI: Registration Authority

- La RA garantisce l'autenticitá della associazione (*identificativo dell'entitá, chiave pubblica dell'entitá*)
- genera i report relativi ai certificati revocati all'interno del proprio sottodominio di sicurezza
- esegue funzioni di gestione

PKI: Registration Authority (2)

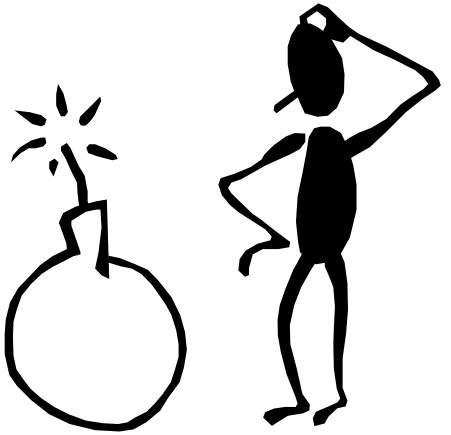


PKI: Repository e directory

- La CA conserva tutte le informazioni relative ai certificati che essa ha generato. Allo scopo utilizza due tipi di repository:
  - uno per se stessa per conservare copie dei certificati, delle chiavi e delle informazioni relative a certificati scaduti (*Master*)
  - uno per tutta la comunità PKI (*Slave*)
- Per accedervi la CA utilizza il Lightweight Directory Access Protocol (**LDAP**).

Problemi di Gestione di una CA

- necessitá di gestire almeno due coppie di chiavi per utente (*una per firmare una per cifrare*)
- l'utente dimentica la password o passwfrase per accedere al suo repository delle chiavi
- l'utente smarrisce la smart card contenete le chiavi ed il certificato
- l'utente lascia l'organizzazione
- ecc.



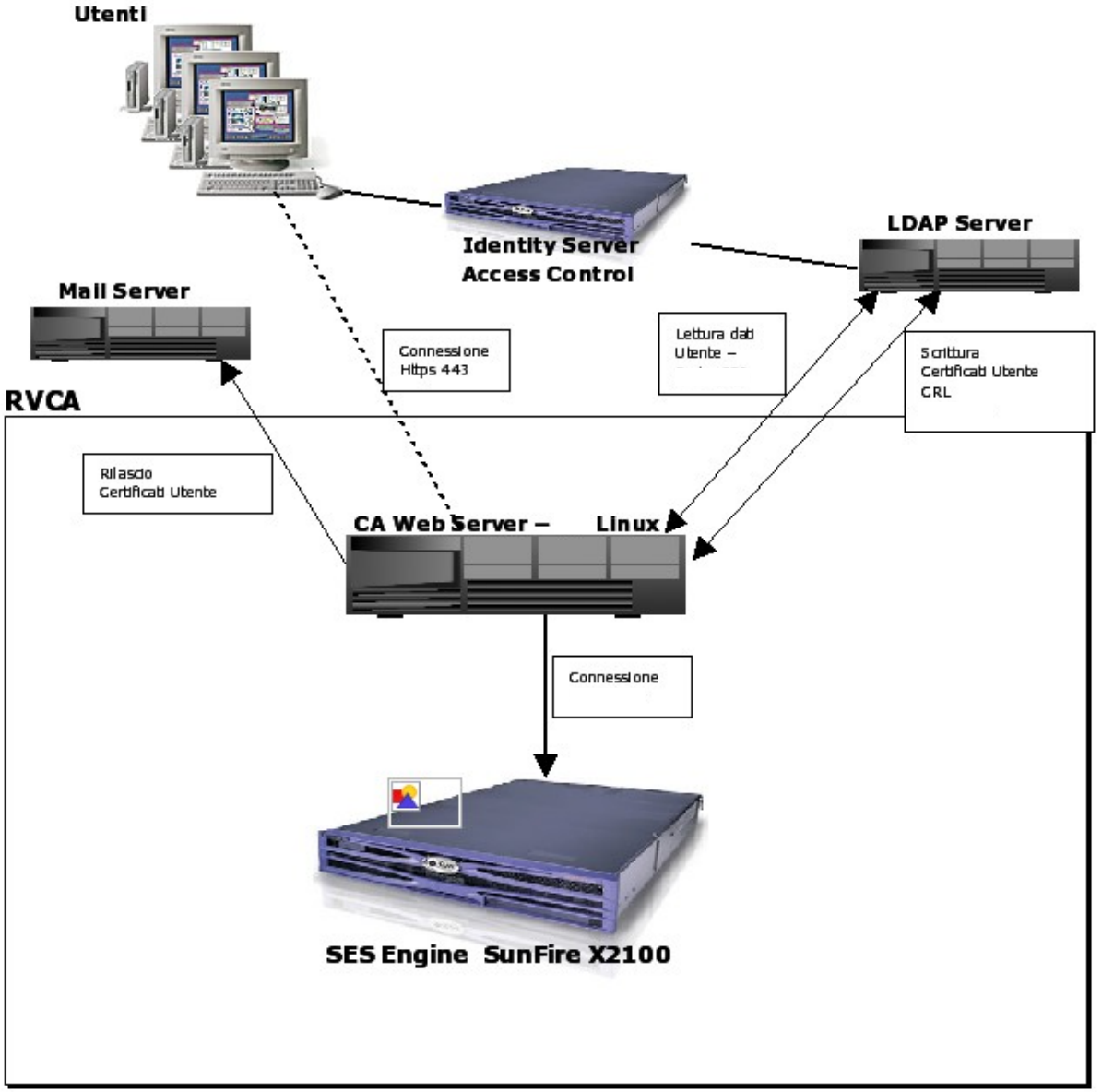
Funzionalità di Gestione di una CA

- generazione dei certificati
- revoca dei certificati
- creazione e gestione delle CRL (è il più oneroso)
- creazione e gestione delle relazioni di trust con altre CA

Esigenze di scalabilità di una CA

- Una delle esigenze fondamentali di una CA é quella di poter scalare in relazione all'aumentato numero di certificati, chiavi e CRL gestiti
- la scalabilitá va affrontata da due angolazioni:
  - capacitá di performarce computazionali proprie del prodotto, e della piattaforma, su cui il prodotto gira
  - in termini di gestibilitá, di facilitá d'uso e di contenimento dei costi

RVCA: la PKI di Regione Veneto

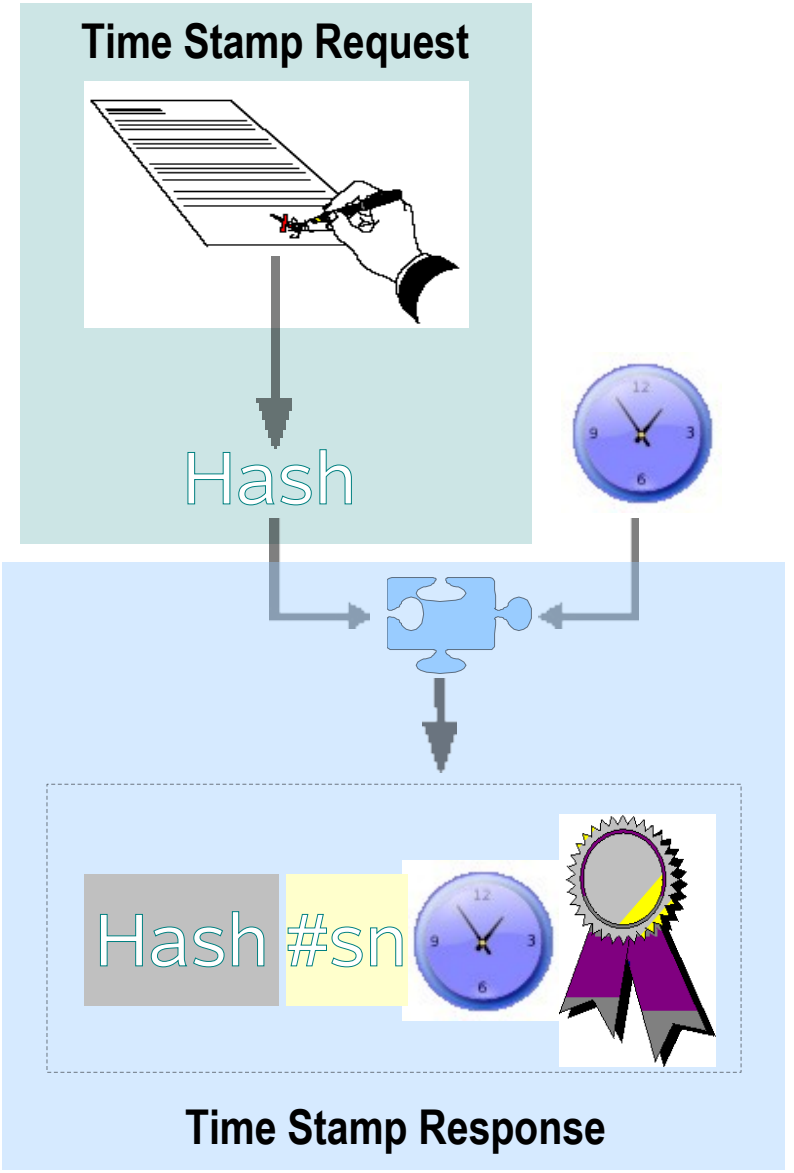


Time Stamp Authority

- I Certificati riportano informazioni temporali
- Occorre essere certi che le chiavi in essi contenute siano state utilizzate durante il periodo di validità
- Le firme apposte dopo il periodo di validità non devono ritenersi valide
- La time stamp authority garantisce che una certa operazione (ad es. apposizione di firma) è avvenuta in un istante di tempo certo

Time Stamp Authority

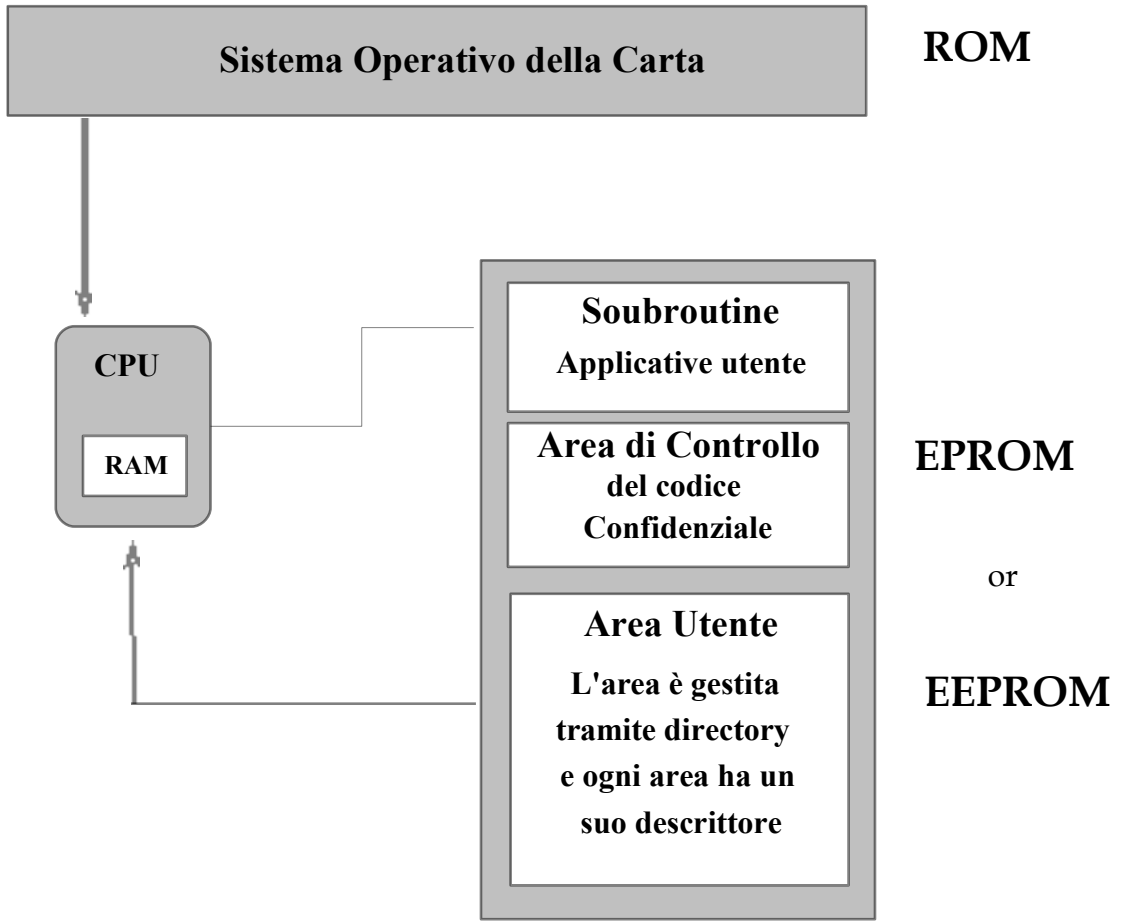
- Il codice AD la definisce all'articolo 1.1/bb):
  - *validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.*
- Decreta l'istante ufficiale nel quale è avvenuta l'operazione di firma
- RFC 3161



Dispositivo di Firma

- un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto la chiave privata e generare al suo interno le firme digitali
- Uno degli strumenti che è possibile utilizzare come dispositivo di firma è la smart card crittografica.

Schema interno di una Smart card



Smart Card Crittografiche

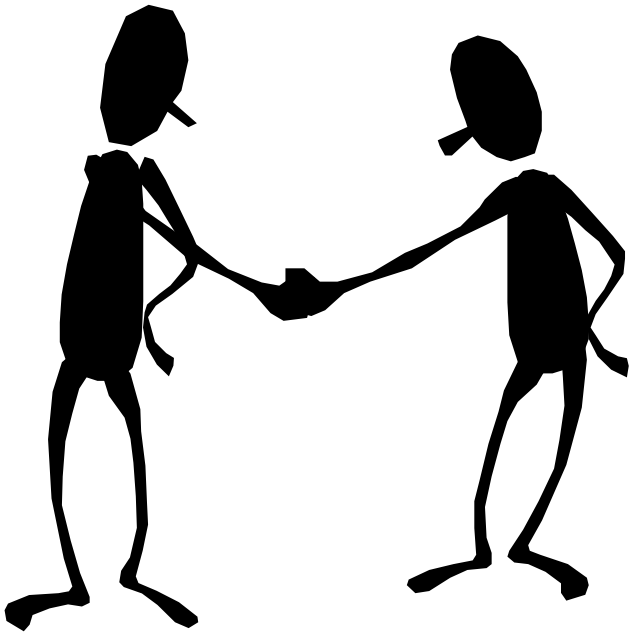
- Smart card dotate di **processore crittografico**
- Nel campo della firma digitale svolge principalmente le funzioni di:
  - *generazione e memorizzazione al suo interno della chiave privata di firma*
  - *apposizione della firma digitale a documenti informatici*
- La smart card si collega con il computer mediante un apposito lettore ed il relativo software di interfaccia (ISO7816)

Benefici di Crittografia, Certificati e PKI

- Consentono la cifratura dei messaggi per garantire la riservatezza
- Consentono la Firma digitale dei messaggi
- Rendono più sicure le logon utente
- Consentono la strong authentication del client, del server e/o di entrambi
- Consentono lo scambio di posta elettronica sicura (PEC)

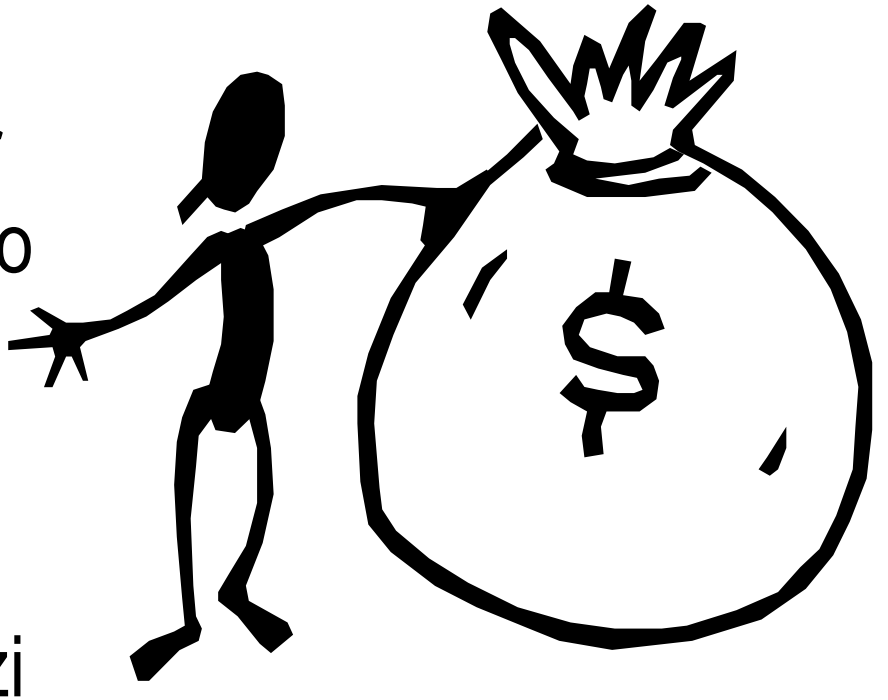
Server Authentication

- Il cittadino si connette al sito https://www.PA.gov.it
- Il server presenta un certificato firmato da una CA iscritta all'albo dei Certificatori
- Il cittadino è confidente che il sito a cui si è connesso è veramente quello che stava cercando



Client Authentication

- Il Cittadino si connette alla server https://www.PA.gov.it
- Il Cittadino presenta al server di autenticazione un certificato firmato da una CA riconosciuta
- La PA digitale consente al Cittadino di usufruire di servizi a valore aggiunto



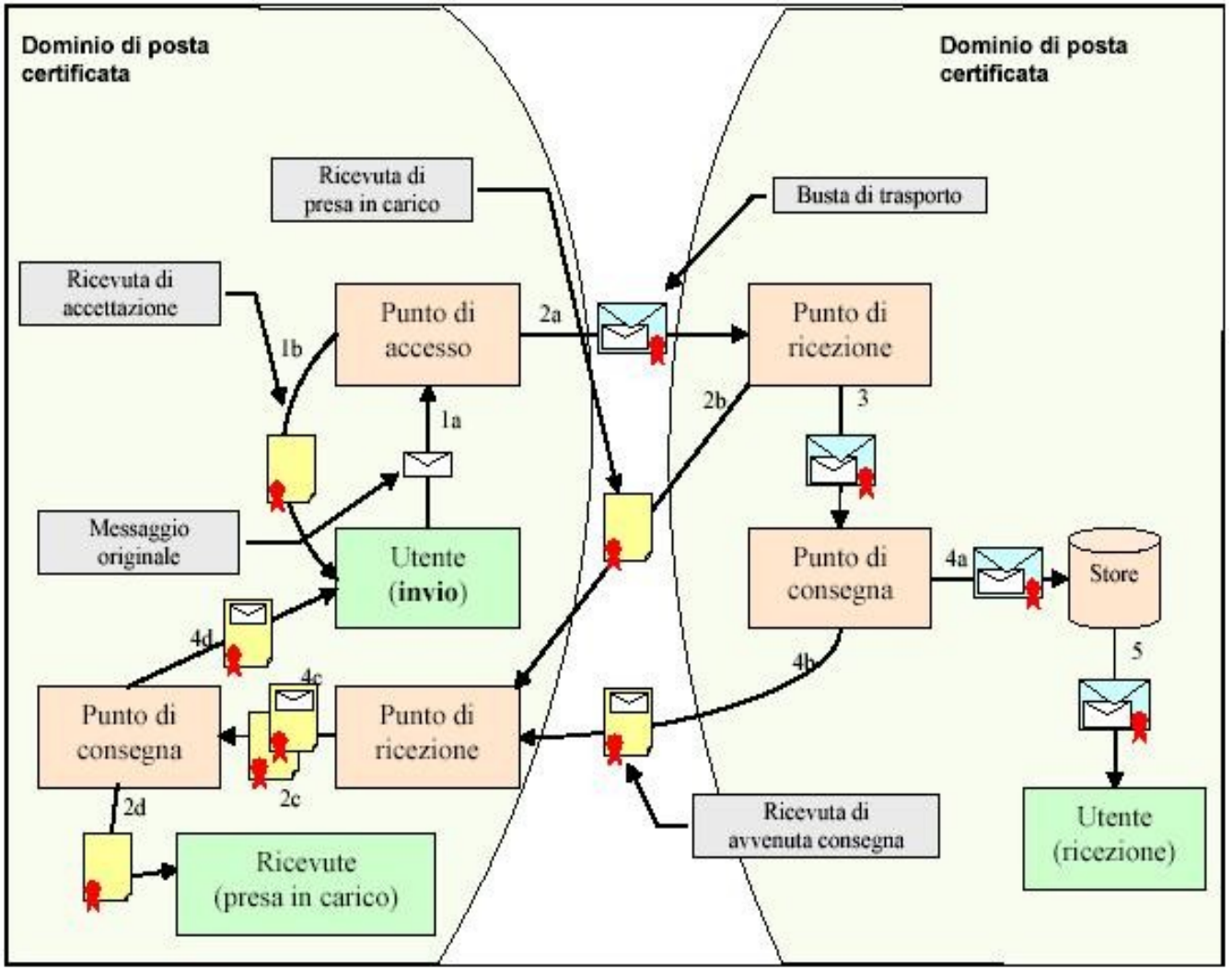
Posta Elettronica Certificata

- Definito nel DPR n.68 del 11 febbraio 2005
- insieme di componenti hardware e software che rendono il tradizionale servizio di posta elettronica (S/MIME) giuridicamente equivalente al servizio di posta tradizionale (raccomandata A/R).
- Strumento privilegiato di trasmissione documenti all'interno del Protocollo Informatico

PEC: chi la usa

- Le **Amministrazioni pubbliche** per la trasmissione dei documenti al loro interno e alle altre Amministrazioni o per l'invio delle comunicazioni ai cittadini ed alle imprese
- Le **imprese** per lo scambio di documenti con le Amministrazioni pubbliche e per le comunicazioni con le altre imprese e con i clienti
- I **cittadini** per scambiare comunicazioni elettroniche con valore legale con Amministrazioni pubbliche o imprese.

Schema logico della PEC



Fonte: Cnipa.gov.it

Firma Digitale e Amministrazione Digitale

- Servizi Camerali
- Mandato Informatico
- Conservazione Ottica
- Libro Matricola AA.CC.
- Protocollo Informatico
- Procedure Telematiche di Acquisto
- Processo Telematico
- Gestione delle Richieste e pareri CNIPA
- Sistemi di Workflow
- Avvisi di E-Governmet
- Gestione Documentale
- Carta Nazionale dei Servizi
- Carta di Identità Elettronica

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Grazie

Giuseppe Russo

Chief Technologist

Principal Engineer & Security Ambassador

Sun Microsystems, Inc.