"Certificazione digitale e PKI: le iniziative dell'Istituto di Informatica e Telematica"

Anna Vaccarelli

Sezione di Sicurezza dell'Informazione (SI!)
Chi siamo

- Anna Vaccarelli (responsabile)

  Luca Bechelli, Stefano Bistarelli, M. Claudia Buzzi, Fabio Dianda, Vincenzo Di Stefano, Davide Fais, Alessandro Falleni, Stefano Frassi, Filippo Giuntini, Fabio Martinelli, Andrea Marchetti, Savatore Minutoli, Paolo Mori, Marinella Petrocchi, Lorenzo Rossi, Maurizio Tesconi
- Per un totale di 17 persone tra ricercatori, tecnologi, software engineer, studenti di dottorato…

Principali temi di ricerca

- Data and communications security
- Formal analysis of security protocols.
- Biometric identification and authentication
- Multicast security protocols
- Xml and dataflow

Sommario

- **Firma digitale**
  - Elementi di crittografia
  - Tecnologia di firma digitale
- **Public Key Infrastructure**
  - Certificati Digitali
  - Certification Authorities
  - Le nostre PKI

Sicurezza dei dati in rete

- La rete è un mezzo intrinsecamente non sicuro
- I messaggi in rete possono essere intercettati e/o modificati
- Necessità di garantire:
  - riservatezza del contenuto
  - integrità del contenuto
  - autenticazione del mittente
  - non ripudio

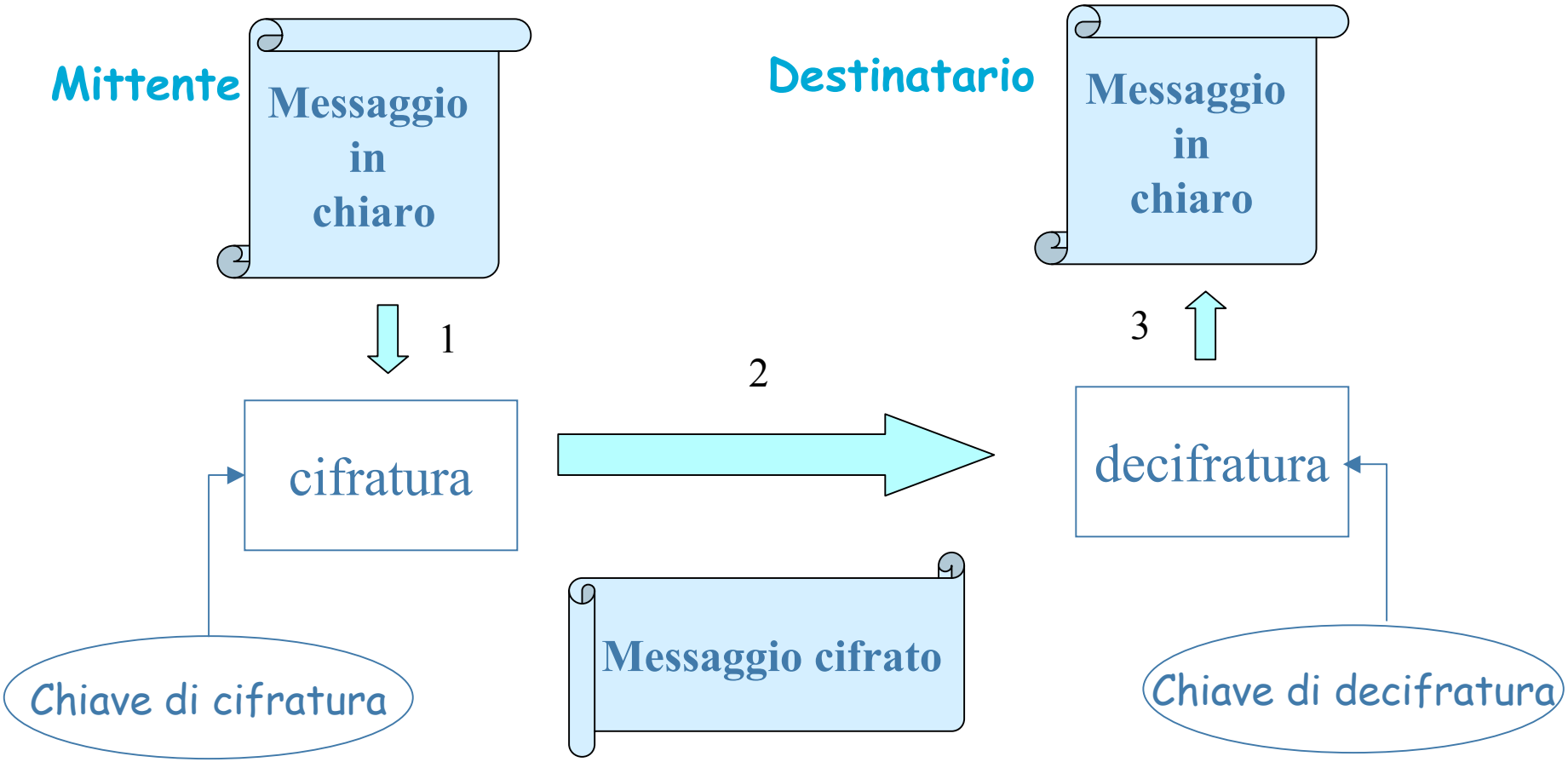
La crittografia (1)

- È una scienza antichissima
- Esistono "algoritmi" crittografici che risalgono all'epoca di Sparta
- Giulio Cesare: abile inventore di codici di crittografia
- In tempi recenti la crittografia è stata molto usata nello spionaggio tra USA e URSS
- A molti è nota come "protagonista" di film e libri di spionaggio.

La crittografia (2)

- 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)
- La sicurezza si basa su:
  - segretezza della chiave
  - robustezza dell'algoritmo

Cifratura e decifratura



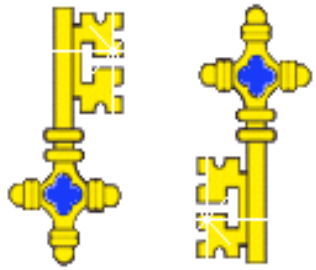
Algoritmi a chiavi simmetriche

- Stessa chiave per cifratura e decifratura (DES – 64 / 128 bit)
- Segretezza della chiave
- *Vantaggi*:

  Algoritmi "veloci" per cifrare e decifrare
- *Svantaggi*:

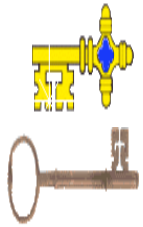
  Preliminare scambio della chiave segreta

  Per una comunita' di ***n*** utenti sono necessarie ~ n^2 chiavi



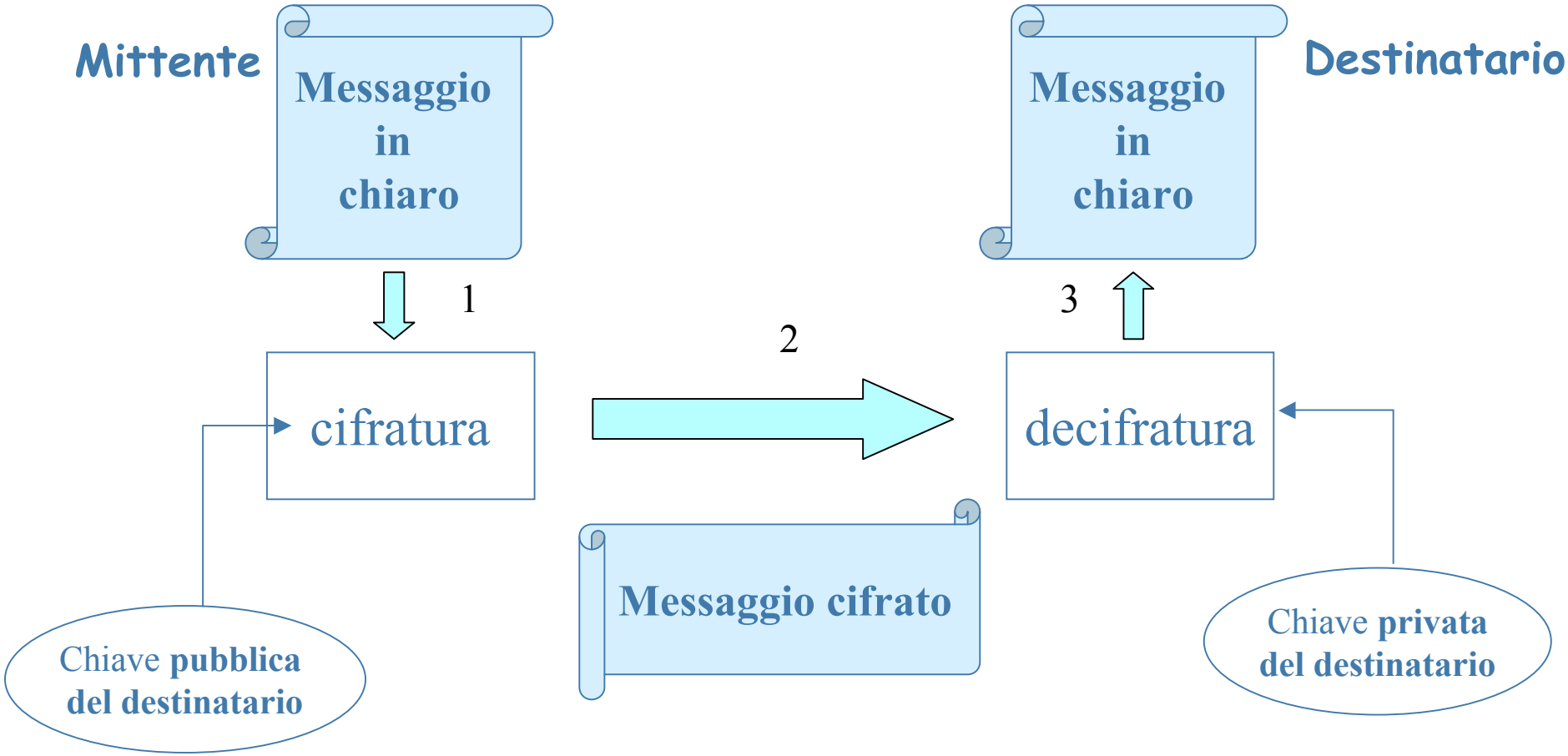
Algoritmi a chiavi asimmetriche

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

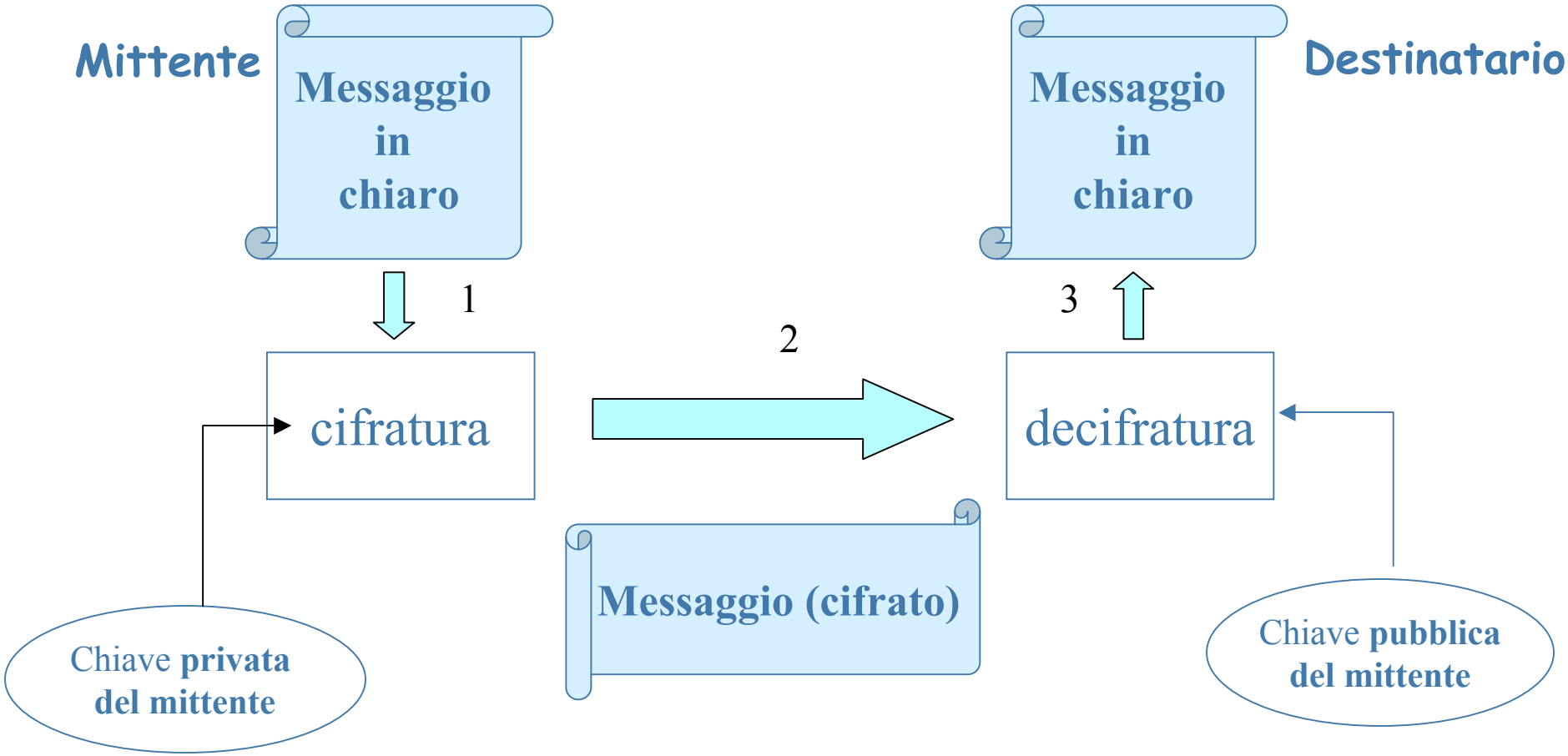


- Ogni chiave può essere usata indifferentemente per cifrare o decifrare
- *Vantaggi*: flessibilità (riservatezza, autenticità, integrità)
- *Svantaggi*: algoritmi "lenti"

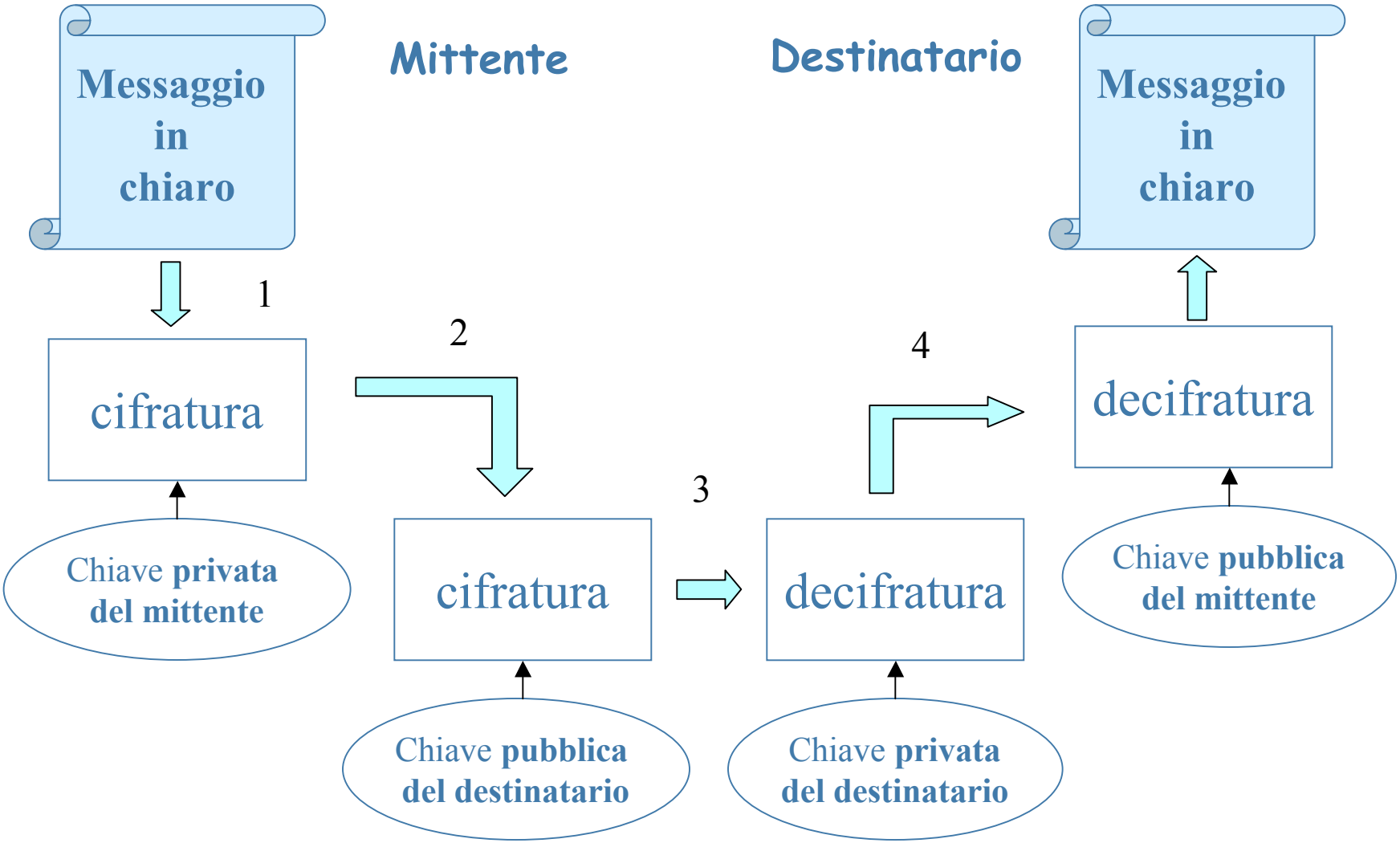
Riservatezza di un messaggio



Autenticità e integrità



Autenticità e riservatezza



La firma digitale ….

È una procedura informatica basata sugli

algoritmi di crittografia

a chiavi asimmetriche

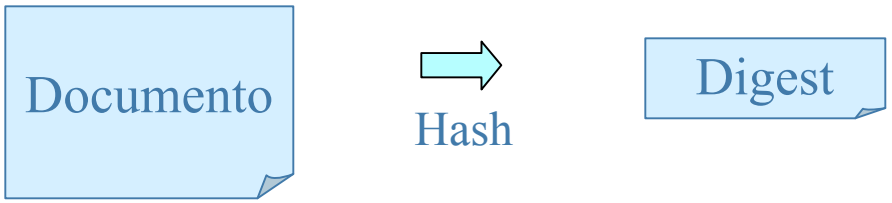
Funzioni di Hash

- Permettono di generare un'impronta digitale che identifica univocamente il messaggio di partenza
  - input: dimensione arbritaria -> output: lunghezza fissa (DIGEST)
  - funzioni non invertibili
  - "collision free"

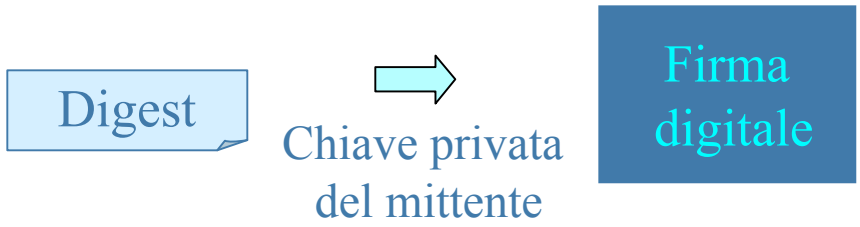
- Fini raggiunbili:
  - integrità dei messaggi
  - apposizione di firma digitale a file di grandi dimensioni

Generazione della firma

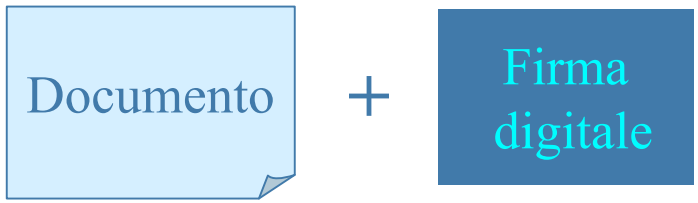
- **Calcolare il DIGEST del documento**



- **CIFRARE il digest con la chiave privata del mittente (si ottiene così la firma digitale)**

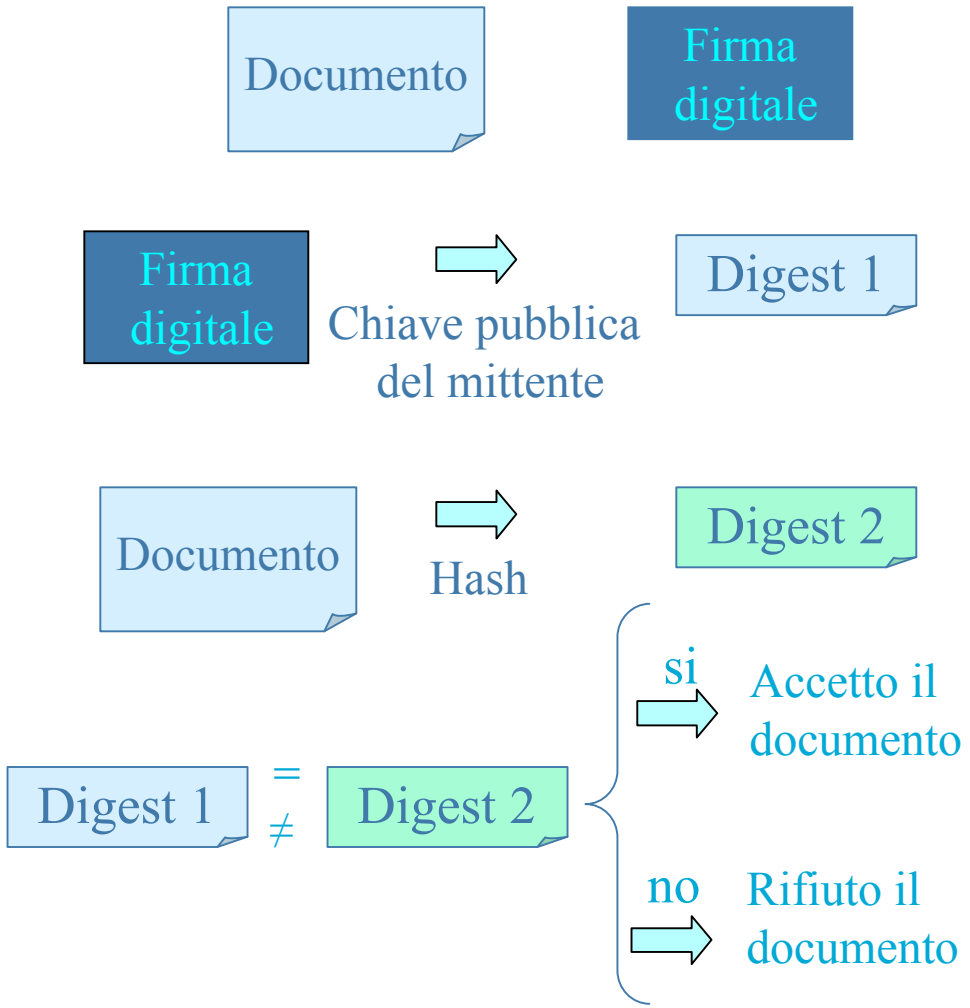


- **Aggiungere al documento originale la firma digitale ottenuta al passo precedente e inviare la coppia (Messaggio, Firma)**



Verifica della firma

- **Separare** il messaggio dalla firma
- **Decifrare la firma** usando la chiave pubblica del mittente
- **Applicare al documento la funzione di Hash** cioè calcolare il digest
- **Verificare** che i due risultati coincidano
  - si: accetto il documento
  - no: rifiuto il documento poiché è stato manomesso



La firma digitale

- Generata dal mittente utilizzando la sua chiave privata
  - autenticità
- Verificata dal destinatario
  - confronto tra il digest ricevuto e quello da lui generato
  - integrità ed autenticità
- Se è necessaria la riservatezza:cifratura con
  - chiave pubblica del destinatario
  - chiave simmetrica stabilita tramite scambio di messaggi riservati

Garanzie

- **Autenticità** del mittente

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

La "Certification Authority"

- Chi garantisce che la chiave pubblica trascritta su un registro pubblico ed abbinata a Bob sia stata rilasciata proprio a Bob?
- E' necessaria una terza parte fidata: il "soggetto certificatore" o "**Certification Authority CA**"
  - La **Certification Authority** certifica il legame chiave pubblica / identità

Il certificato digitale (1)

- Un documento di identità:

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

Il certificato digitale (2)

- Un certificato digitale:
  - è un **documento elettronico**
  - associa l'identità di una **persona** ad una **chiave pubblica**
  - emesso, secondo standard internazionali **(X.509 raccomandato dall'ITU-T (International Telecommunication Union - settore Telecomunicazioni)**, da una *CA* riconosciuta
  - firmato digitalmente con **chiave privata della *CA***

Compiti di una CA (1)

- **identificare con certezza la persona** che fa richiesta della certificazione della chiave pubblica
- rilasciare e rendere pubblico il **certificato**
- garantire l'accesso telematico al **registro delle chiavi pubbliche**
- informare i richiedenti sulla **procedura di certificazione** e sulle tecniche per accedervi
- dichiarare la propria **politica di sicurezza**

Compiti di una CA (2)

- attenersi alle **norme sul trattamento di dati personali**
- (non rendersi depositario delle chiavi private)
- procedere alla **revoca o alla sospensione** dei certificati in caso di richiesta dell'interessato o essendo a conoscenza di abusi o falsificazioni, ecc.

Come ottenere un Certificato Digitale (1)

- L'utente genera sul proprio PC una **coppia di chiavi**
  - offrono il servizio **i più comuni browser** (Netscape, Explorer) oppure **la CA stessa** tramite apposito software
  - la chiave privata è memorizzata localmente **in un file nascosto (o floppy disk)**
  - maggiore sicurezza: la coppia di chiavi può essere generata tramite **SmartCard o Token** collegati ad un PC - la chiave privata resta sempre memorizzata sulla **SmartCard/Token** (protetta da **PIN**)
- L'utente invia alla CA una **richiesta di certificato**, unitamente alla chiave pubblica generata

Come ottenere un Certificato Digitale (2)

- La CA provvede ad autenticare il richiedente, di solito richiedendo di recarsi di persona ad uno sportello di LRA (**Local Registration Authority**) collegato con la CA

- **Verificata l'identità, la CA emette il certificato**, lo invia al richiedente tramite posta elettronica ed inserisce la chiave certificata nel registro delle chiavi pubbliche

- Procedure di richiesta e gestione dei certificati sono gestite da **Infrastrutture a Chiave Pubblica (PKI - Public Key Infrastructure)**

La Public Key Infrastructure (PKI) (1)

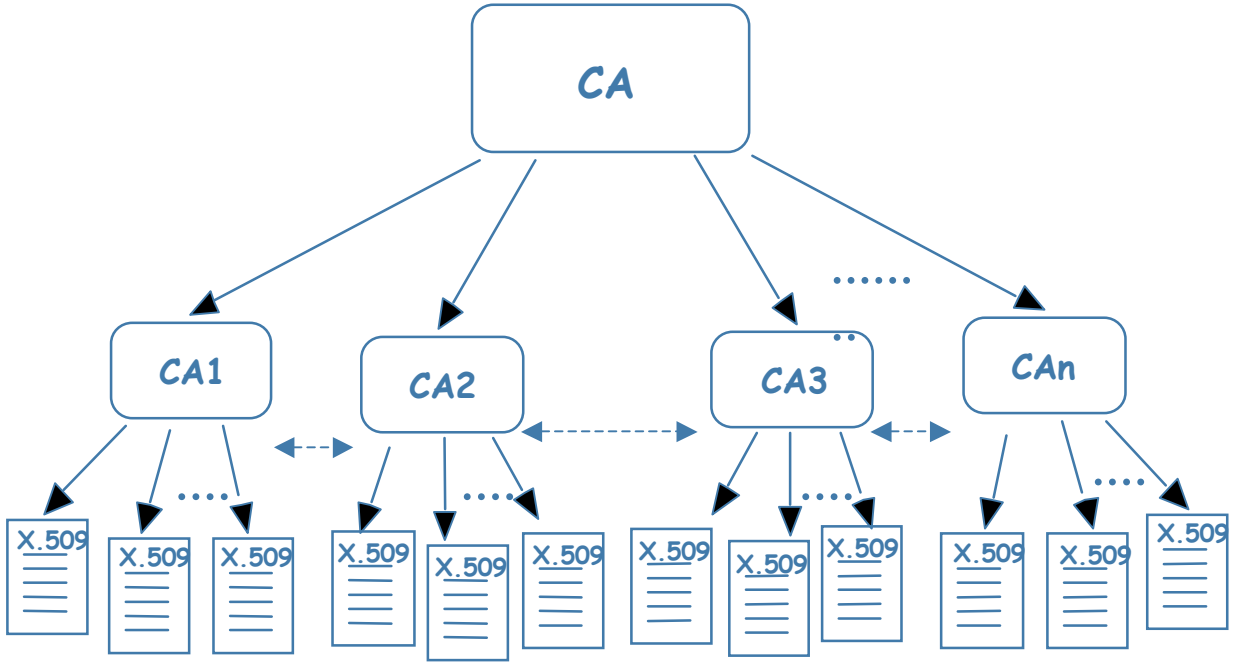
- La struttura minima di una PKI è costituita da una **CA e una Local Registration Authority (LRA)**
- LRA è uno "sportello" con un operatore (LRAO) che effettua il riconoscimento personale del richiedente. A seguito del riconoscimento effettuato da LRAO, la **CA emette il certificato**.
- Ogni CA può avere **più di un LRA**

La Public Key Infrastructure (PKI) (2)

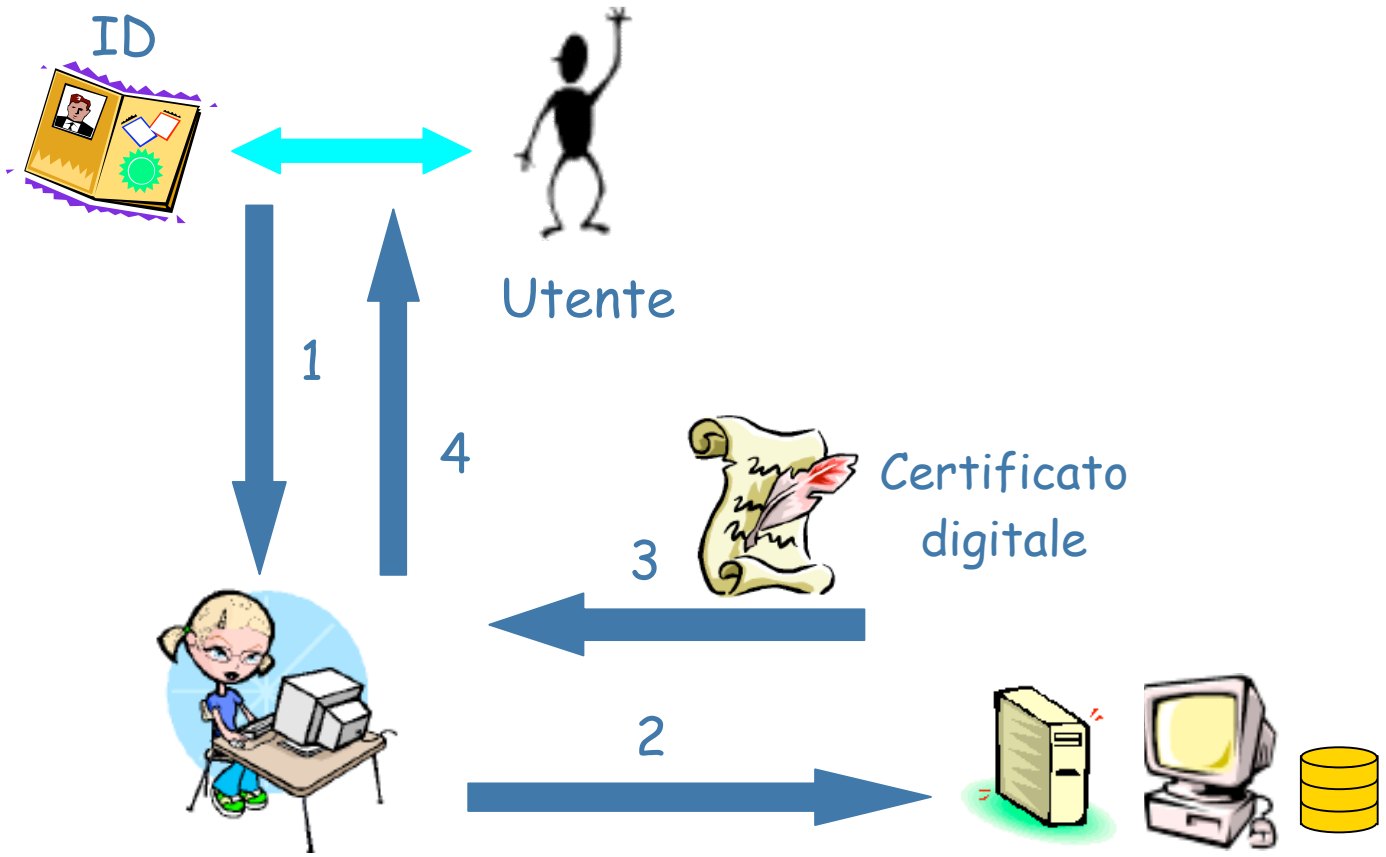
- Le CA possono certificarsi a vicenda, in modo da stabilire una "**catena di fiducia**".

- Molto spesso la struttura della catena di fiducia è ad **albero**, in cui la CA principale (**Root CA**) certifica le chiavi di CA subordinate. A loro volta esse possono certificarne altre (fino a certificare la chiave pubblica del singolo utente).

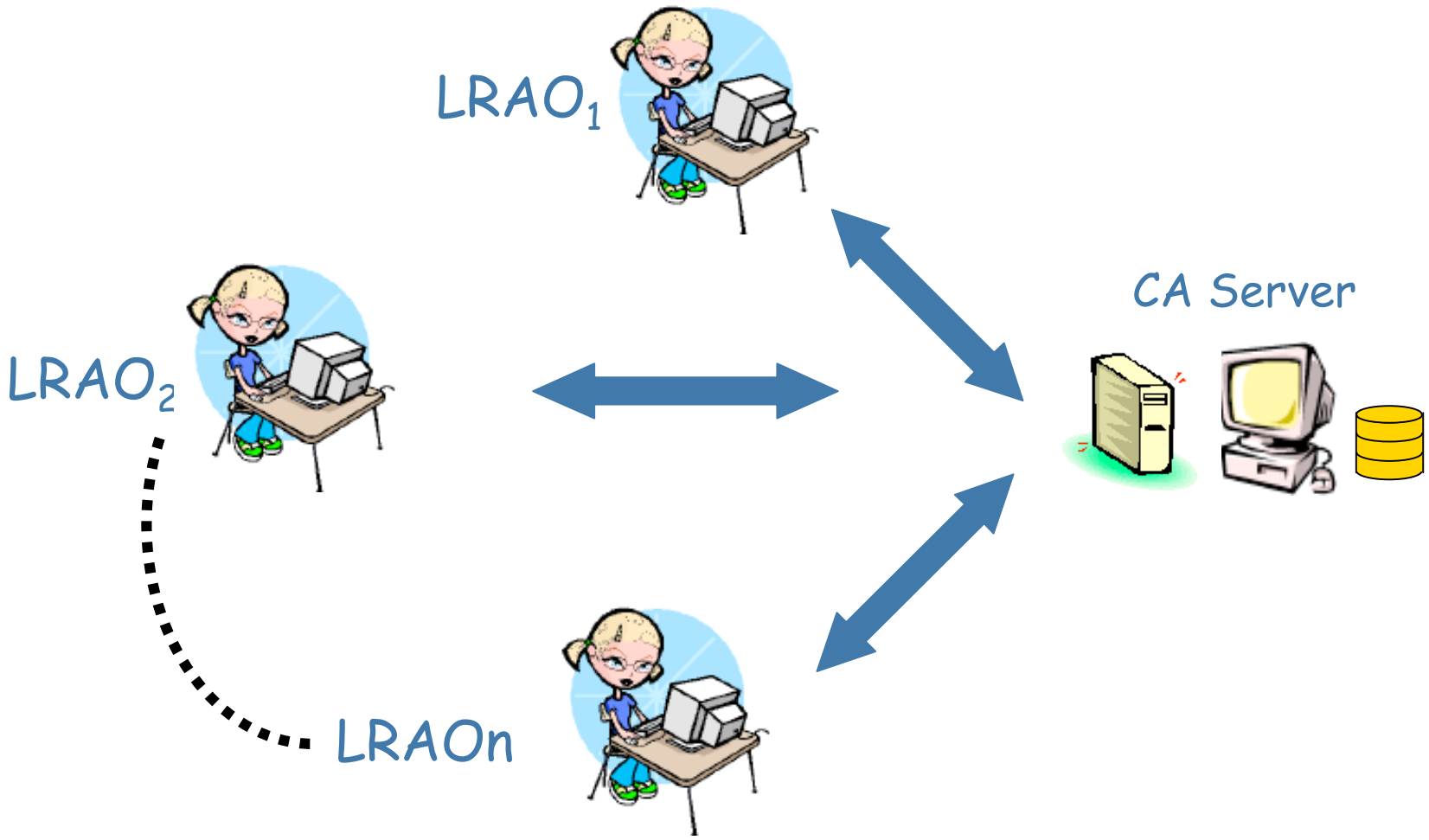
Schema gerarchico di PKI



Schema di base di una PKI



Schema di PKI con più LRA



Le nostre PKI

- Due PKI basate su OPEN CA
- Una CA destinata ad un utenza scientifica (http://pkp-ca.iit.cnr.it)
- Una CA destinata ai provider del Registro ".it" (http://pki-ra.iit.cnr.it)

Open Source

- La PKI-RA si basa esclusivamente su Software OpenSource

- Motivazioni:
  - Flessibilità
  - Supporto

I nostri certificati

- Sono conformi alla direttiva quadro europea
- Si possono collocare tra i certificati "qualificati" rispetto alla direttiva europea
- Richiediamo il riconoscimento personale

I certificati di attributo

- Sono "compagni" di un certificato X.509
- Contengono informazioni sul ruolo ed i conseguenti privilegi con cui il titolare di un certificato X.509 si presenta
- Il titolare di un certificato digitale X.509 può possedere più di un certificato di attributo

Gli strumenti di firma digitale SignIT

- SignIT è un client di firma *stand alone* progettato e realizzato dallo IIT, basato su Open Source Software
- Supporta di differenti modelli di smartcard e token, compresi alcuni tra i prodotti utilizzati dalle Autorità di Certificazione iscritte all'Elenco Pubblico dei Certificatori AIPA-CNIPA
- Verifica di documenti firmati da utenti delle nostre PKI, da Autorità di Certificazione "AIPA-CNIPA" e da Certification Authority commerciali riconosciute a livello internazione (es: Verisign)

SignIT: funzionalità

- Conforme alla Circolare AIPA CR/24-99 "Regole sull'Interoperabilità tra i Certificatori"
- Conforme alle direttive sulla interoperabilità dei sistemi di verifica emanate da Assocertificatori
- Conforme ai requisiti relativi ai dispositivi crittografici per la Carta di Identità Elettronica.

SignIT: funzionalità

- Firma di documenti:
  - Firme singole
  - Firme multiple indipendenti
  - Firme multiple contestuali
- Verifica di documenti firmati:
  - Verifica crittografica
  - Controllo della validità temporale del certificato
  - Verifica che il certificato sia emesso da una CA considerata affidabile
  - Verifica dello stato del certificato (CRL)

Grazie per l'attenzione.
Ci sono domande?