

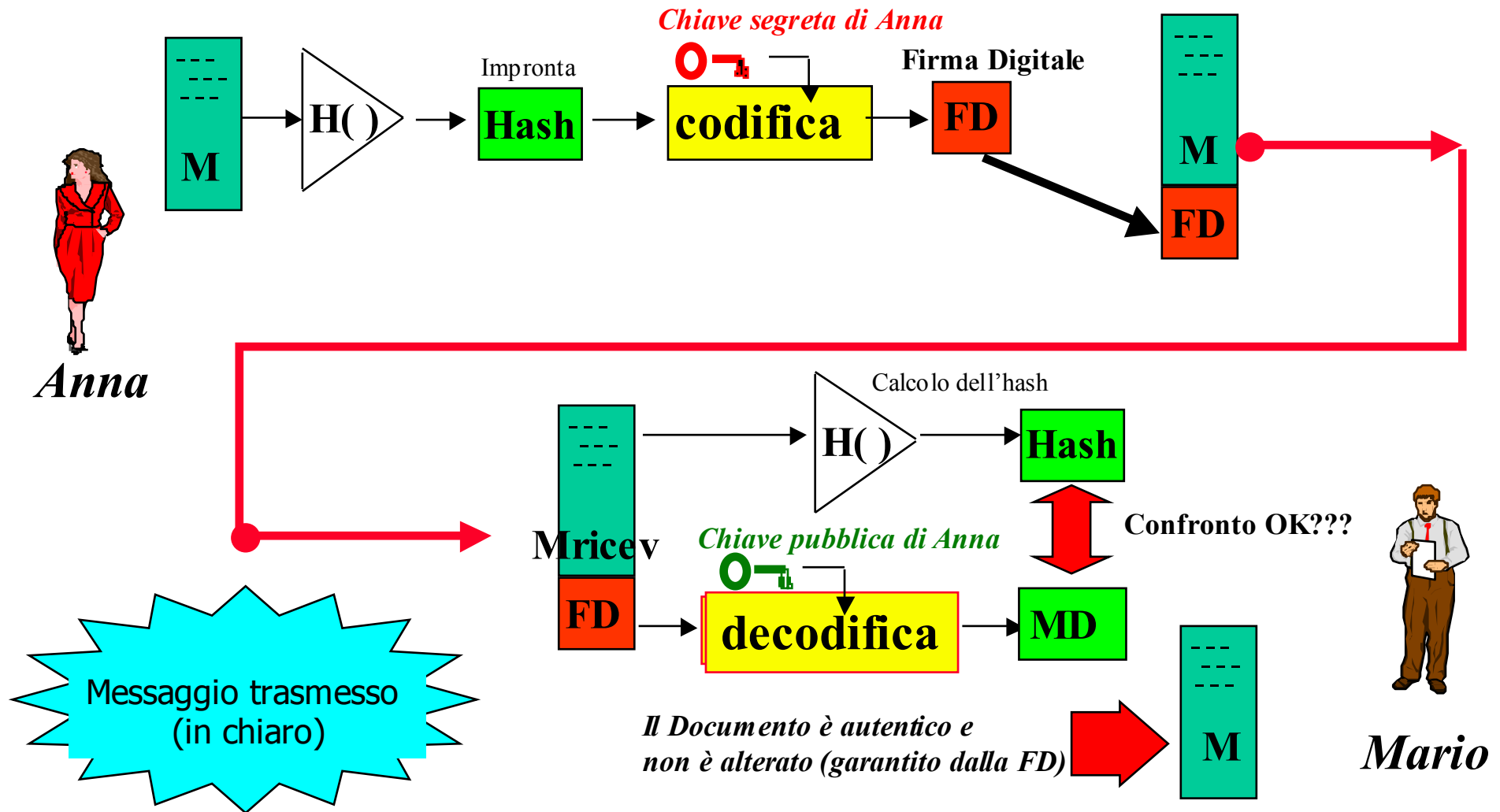


PKI

infrastruttura a chiave pubblica



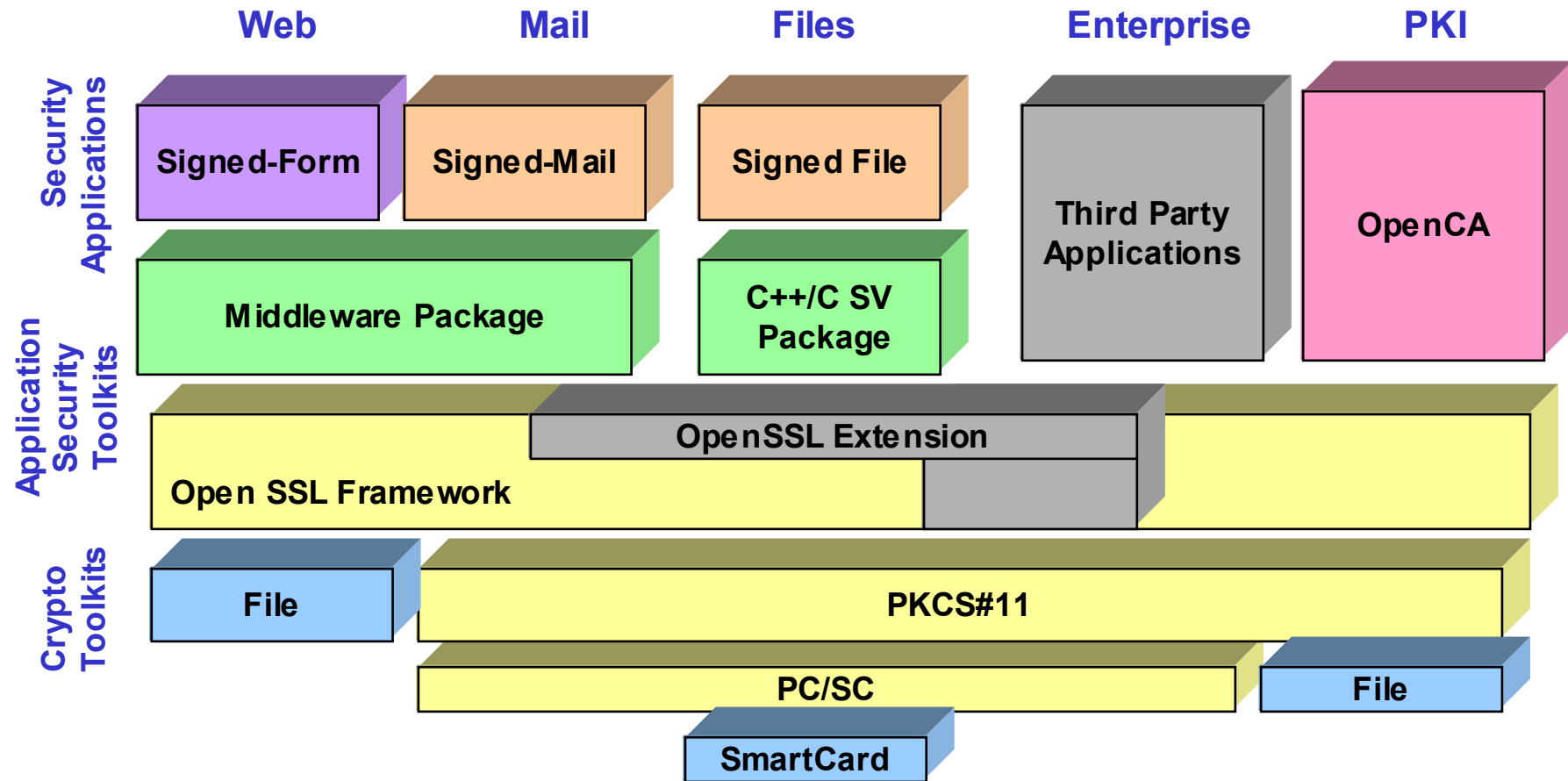
Il processo di firma digitale



Alcune Applicazioni



Security Building Blocks



Un progetto che parte da lontano

Il Comune di Modena fin dal **1998** ha avviato una sperimentazione sull'utilizzo di un sistema di firma digitale in collaborazione con il Politecnico di Torino aderendo al circuito **EuroPKI**.

EuroPKI

*The mission of EuroPKI is to provide public-key certification services for a wide variety of subjects including individuals, organizations and European projects. Currently **EuroPKI** is supporting various initiatives: the most important one is the **ICE-CAR** project.*

ICE-CAR

The ICE-CAR project is intended to

- foster the development of European security technology for the purpose of securing the growing application of open networks, as for instance the internet, for administration, e-commerce, intra-organisation communication, health care applications and research;
- promote the availability of technically compatible and interconnectable public key infrastructures (PKIs) which are necessary to guarantee the authenticity and validity of public keys in use.

Questa sperimentazione che si e' conclusa nel 2000 ha consentendo la verifica delle problematiche tecnico-organizzative e la maturazione di una importante esperienza utile per l'evoluzione del Progetto stesso.

I prodotti rilasciati in questa prima fase sperimentale sono stati:

1. Un'infrastruttura di emissione, gestione, revoca e verifica dei certificati X509
2. Un'infrastruttura di distribuzione dei certificati tramite ldap server
3. Un'infrastruttura composta dai servers web e mail che utilizzano tali certificati, tramite i protocolli SSL (secure socket layer) ed S/MIME (Secure Multipurpose Internet Mail Extension), utilizzati rispettivamente per le transazioni interattive e quelle di tipo store and forward.



..... evolvendo costantemente,

Fin dall'inizio l'obiettivo primario e' stato quello di fornire Servizi ad alto valore aggiunto attraverso connessioni e modalità di accesso sicure in grado di:

- tutelare il cittadino nell'accesso, inoltro, scambio e custodia delle informazioni;
- tutelare la struttura Comunale nell'identificazione (informatica) del cittadino (per es. nell'accettazione di domande) e nella messa a disposizione di informazioni riguardanti la sua sfera personale.

in altri termini:

- **garantire** una **identificazione** dell'utenza e una **non ripudiabilità** delle informazioni trasmesse in ambienti di rete aperti quali Internet,
- **garantire** una **sicurezza** (privacy) nell'inoltro di documenti riservati,
- garantire ai fruitori dei servizi offerti il possesso di una infrastruttura informatica 'sicura' in grado di proteggere e tutelare le informazioni circolanti.

Il Progetto e' articolato in due "momenti":

- Funzionalità di base
- Introduzione della firma digitale nei Sw gestionali



... producendo risultati e

Funzionalità di base

Funzionalità di Servizi

1. Messa in **gestione** dell'infrastruttura di CA per l'emissione di certificati di firma digitale.
2. Realizzazione di un pacchetto (toolkit) in ambiente Windows che assolva le funzioni di:
 - a) sign
 - b) verify
 - c) encrypt
 - d) decryptsu documenti (files in generale) dell'utente attraverso firme digitali su files o su SmartCard.
3. Consentire l'utilizzo di e-mail firmate
4. Consentire l'utilizzo di web-form firmate
5. Consentire l'utilizzo di allegati firmati

Funzionalità infrastrutturali

6. Protezione del colloquio SSL tra Client e Server
7. Protezione del colloquio SSL tra Client e Server con Authentication Client

Gli obiettivi raggiunti in questa prima fase si possono quindi riassumere in:

- creazione di servizi telematici al cittadino in grado di offrire un ulteriore e complementare canale di fruizione accanto a quelli tradizionalmente già presenti e disponibili.
- dotare questi servizi di uno strato di identificazione, di security ecc.. che può spaziare dalla basic auth verso tecnologie di tipo PKI:
 - basic auth
 - PKI su files
 - PKI su smartCard



..... che non ha il *fiato corto* !

Introduzione della firma digitale nei Sw gestionali

Ogni procedimento amministrativo prevede al suo interno la sottoscrizione di qualche modulo, documento. L'opportunità di poter disporre di una tecnologia e un know-how sulla firma digitale (tecnologia di tipo PKI) consente di elevare il grado di sicurezza e tutela informativa, garantendo tutti, Cittadini e Comune nell'Inoltro e nell'interscambio della documentazione.

La mancanza di standard internazionali per i lettori di smartCard e lettori, la lenta diffusione degli stessi nel mercato dei Personal Computer costituiscono oggi un deterrente all'impiego esteso di questa tecnologia, anche se la situazione sta evolvendo verso un'integrazione dei lettori all'interno di portatili e Personal computer.

D'altro canto una realtà quale il Comune di Modena non può né deve restare in attesa ma deve guidare questo processo affiancando soluzioni innovative che precorrano i tempi e le consentano di essere all'altezza di un compito che in futuro ormai prossimo la vedrà protagonista nella scelta di tecnologia PKI

Del resto se per l'utente la firma digitale è un'opportunità che apre la strada a servizi ad alto valore aggiunto forniti dalle diverse parti (Comune, Banche, o altre Aziende) attraverso l'identificazione del cittadino, la sottoscrizione delle proprie informazioni, la trasmissione di dati sensibili (attraverso encrypting delle informazioni stesse), da un punto di vista di chi fornisce servizi (quindi il Comune) costituisce occasione ed opportunità di costruire, consolidando la, un'infrastruttura protetta, esponibile con ragionevole sicurezza in ambienti aperti quali Internet (SSL).

L'integrazione di una tecnologia PKI all'interno degli applicativi gestionali del Comune di Modena consentirà di aumentare notevolmente il valore aggiunto degli applicativi stessi.

- Sportello Unico alle Imprese
- Delibere e Determinazioni Dirigenziali
- Protocollo a Norma AIPA

- Inoltro modulistica che necessita di sottoscrizione



Team di Progetto

Capo Progetto:

- dott. Massimo Ferrari

Team di Sviluppo:

- dott. Stefano Gibellini
- Marco Gessani

Collaboratori esterni:

- ing. Andrea Giacobazzi
- ing. Massimiliano Pala

