Franco Tafini

La firma digitale:

nuove tecnologie per nuovi ambiti di applicazione

La normativa italiana sulla firma digitale

- Dalle novità del DPCM 30/3/09 un forte impulso alla diffusione della firma digitale
- Art.7 Conservazione delle chiavi e dei dati per la creazione della firma. Il titolare…
- …mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma

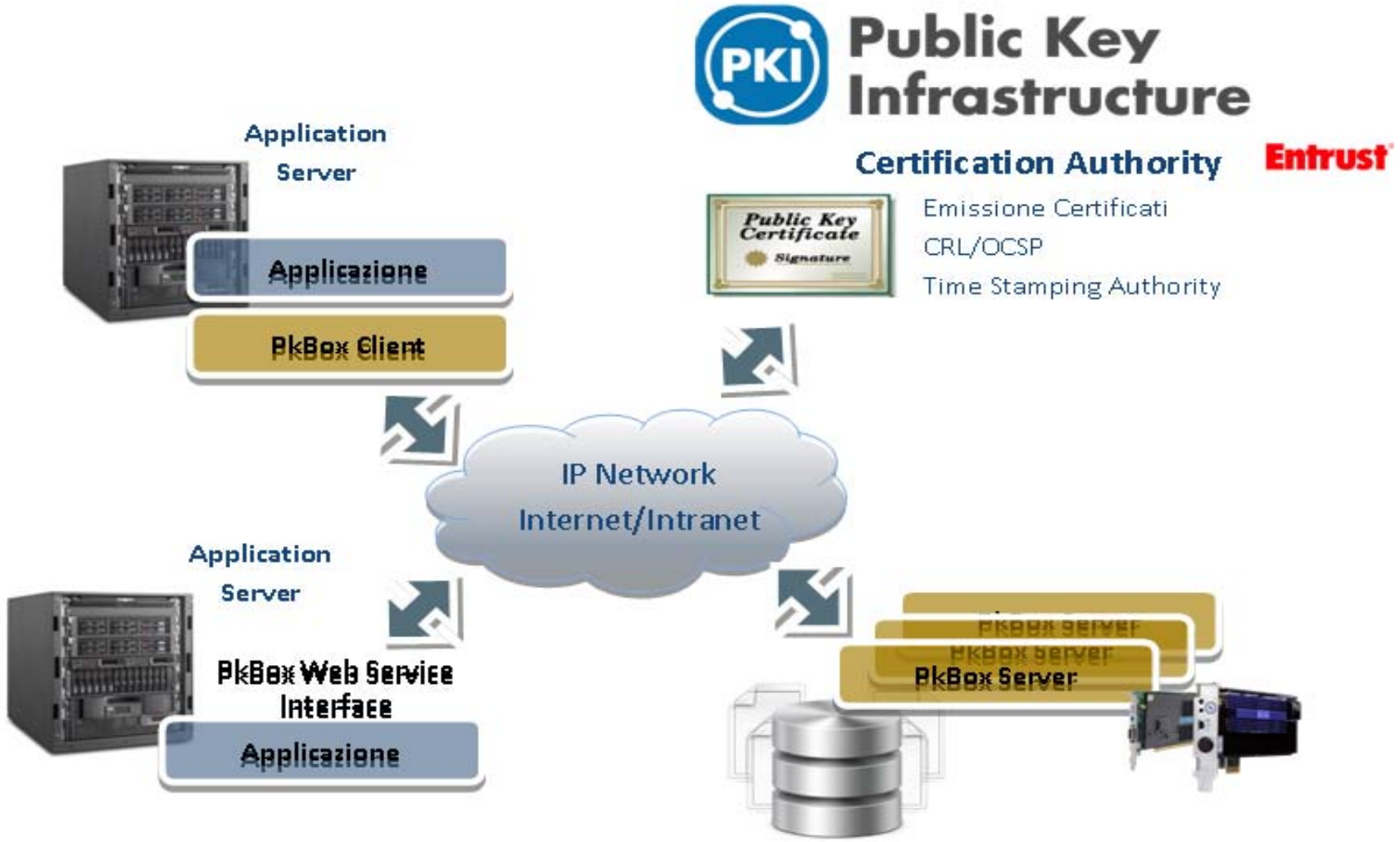
I noti problemi della firma digitale tradizionale

- Installare e aggiornare il software di firma
- Installare e configurare il driver del lettore di smart card
- Ripetere la procedura per ognuno dei computer utilizzati dallo stesso titolare
- Risolvere eventuali conflitti tra driver e applicazioni che richiedono un controllo esclusivo della smart card…
- Ricordarsi di avere sempre con sé non solo la smart card ma anche il lettore e/o necessari dispositivi per effettuare la firma
- Ricordarsi di gestire il rinnovo dei certificati digitali entro la data di scadenza
- Gestire la procedura di sostituzione in caso di furto, smarrimento dei vari dispositivi utilizzati

La firma digitale remota

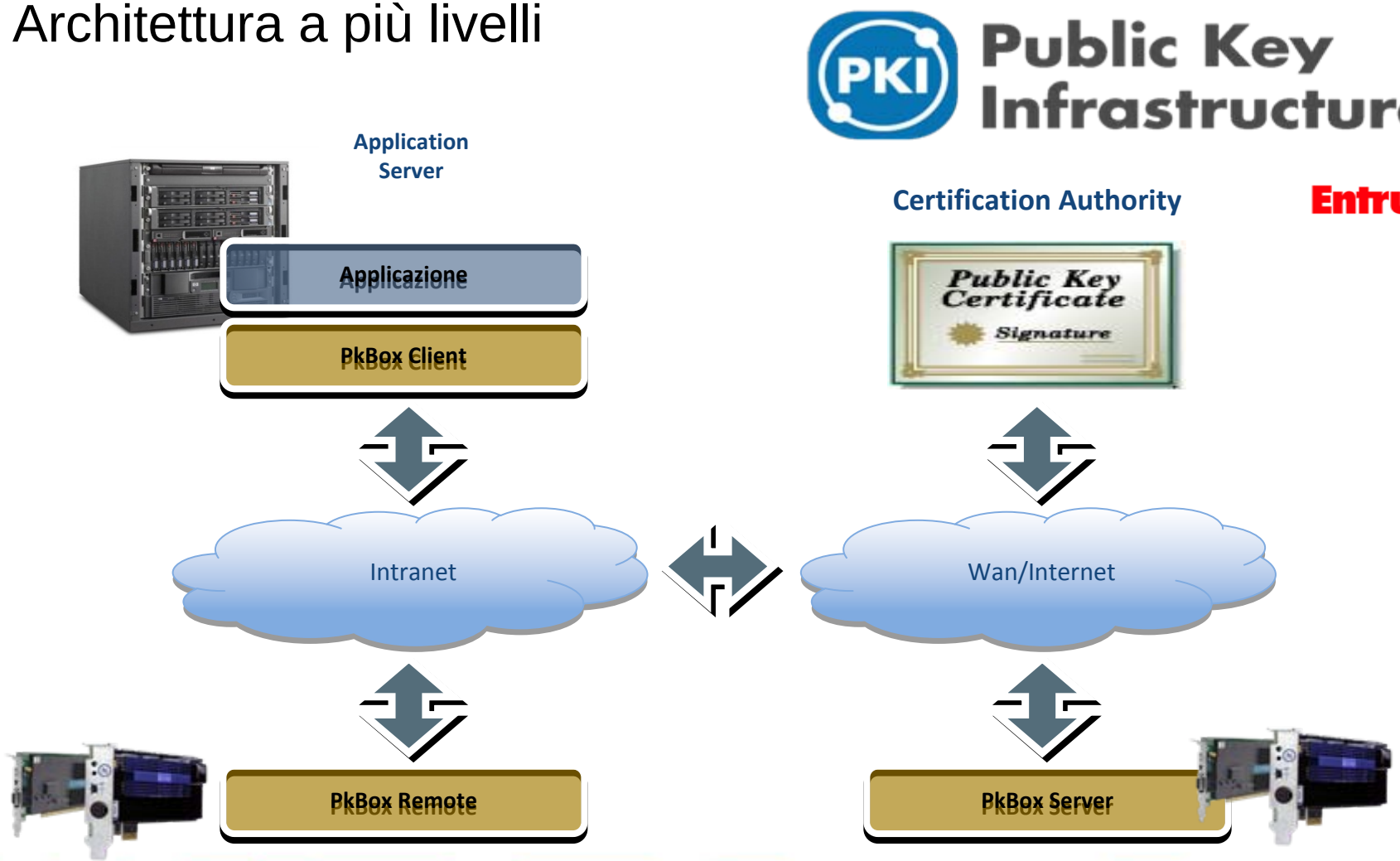
- Proprio l'art. 7. del DPCM 30/3/09 pone le basi normative per il riconoscimento della **Firma Remota**
- Un tipo di firma digitale basata sull'utilizzo di un **dispositivo sicuro centralizzato** (HSM) per la generazione e la conservazione delle chiavi di firma
- Una tipologia di firma che permette di semplificare le modalità operative e di ridurre in modo significativo la dotazione tecnica necessaria per firmare
- Una tipologia di firma che conserva tutte le prerogative di un'operazione di sottoscrizione effettuata in modo tradizionale con una smart card

L’architettura del sistema di firma remota

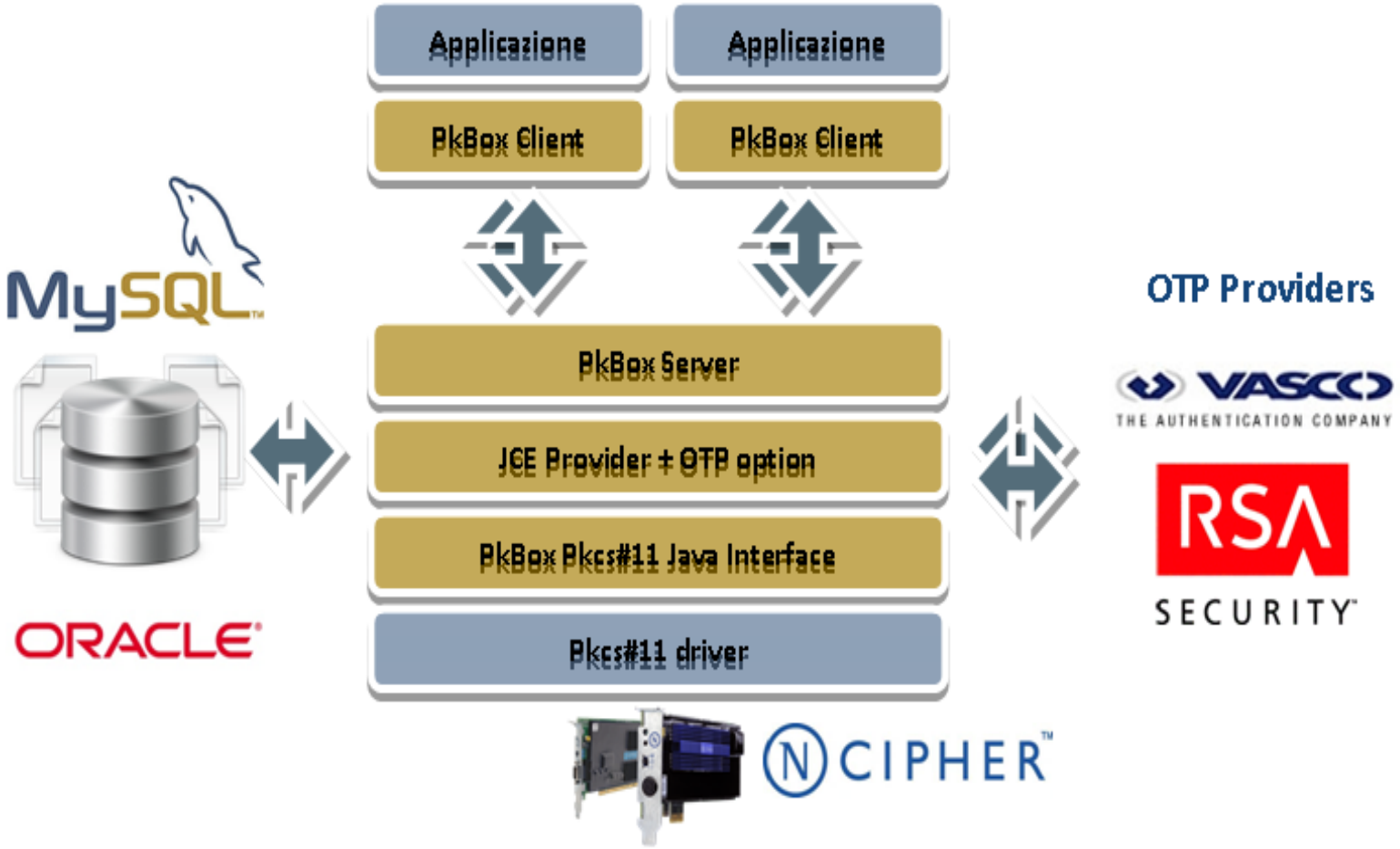


Riservatezza e sicurezza

Architettura a più livelli

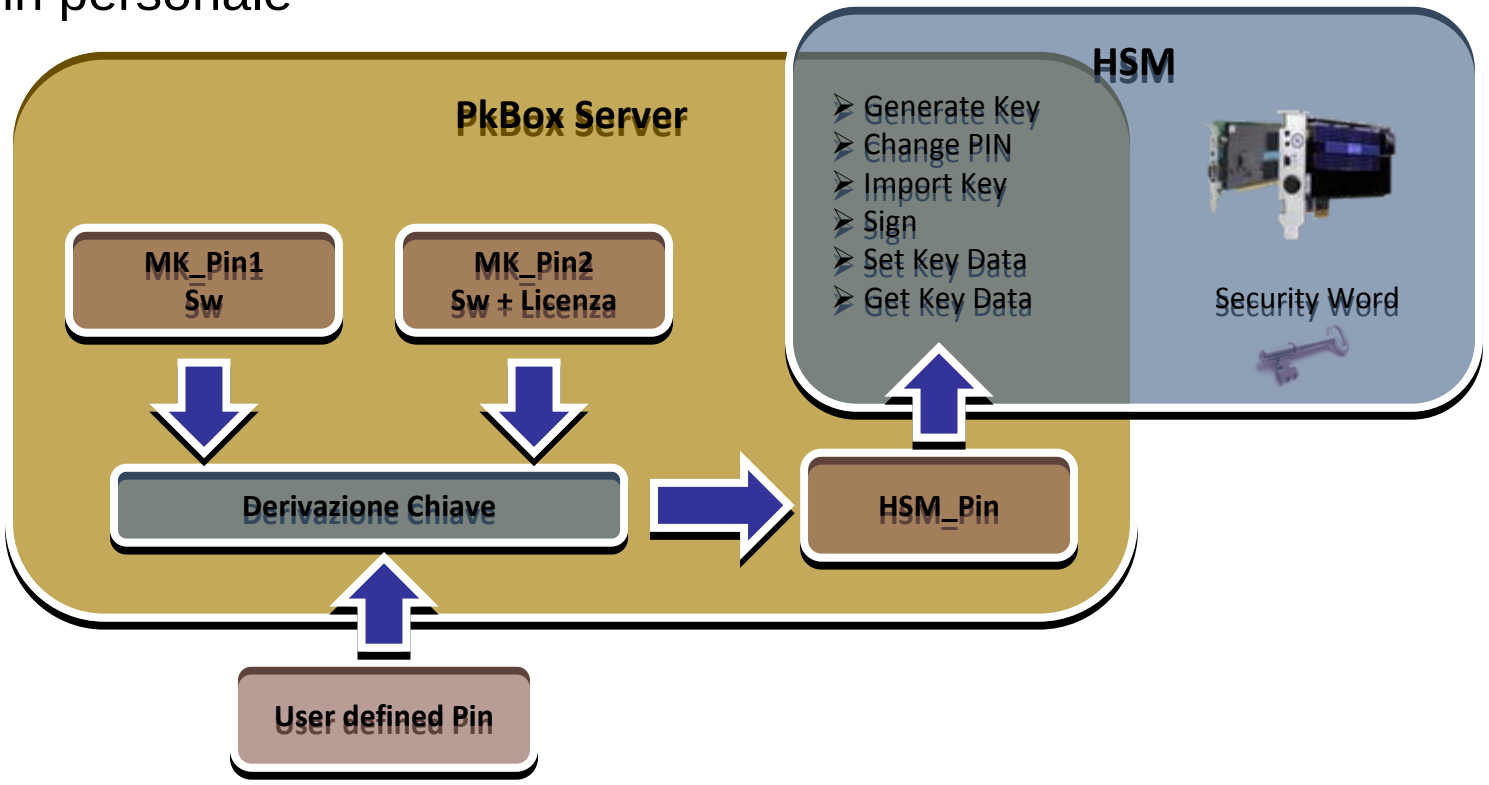


Le operazioni di autenticazione tramite OTP



Derivazione HSM PIN

L'accesso ai dati e alle funzionalità dell'HSM è vincolato alla conoscenza di un Pin personale



Schema dell'applicazione di Firma Remota

User Web Application

Internet

Web & Application Server

Internet

PkBox Server

PkBox Server

Rete Inter/Intranet

Web PkBox Proxy

PkBox Remote

PkBox Remote

Application Server

La biometria come alternativa al PIN

Un'identificazione certa del sottoscrittore

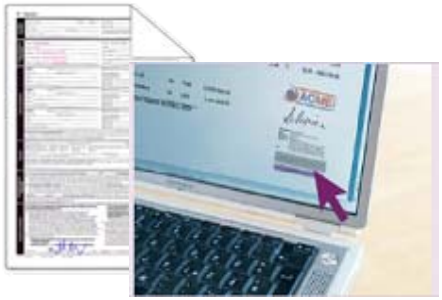
Accesso

Acquisizione **Firma**

Verifica & accesso ai servizi/programmi

Firma Documenti

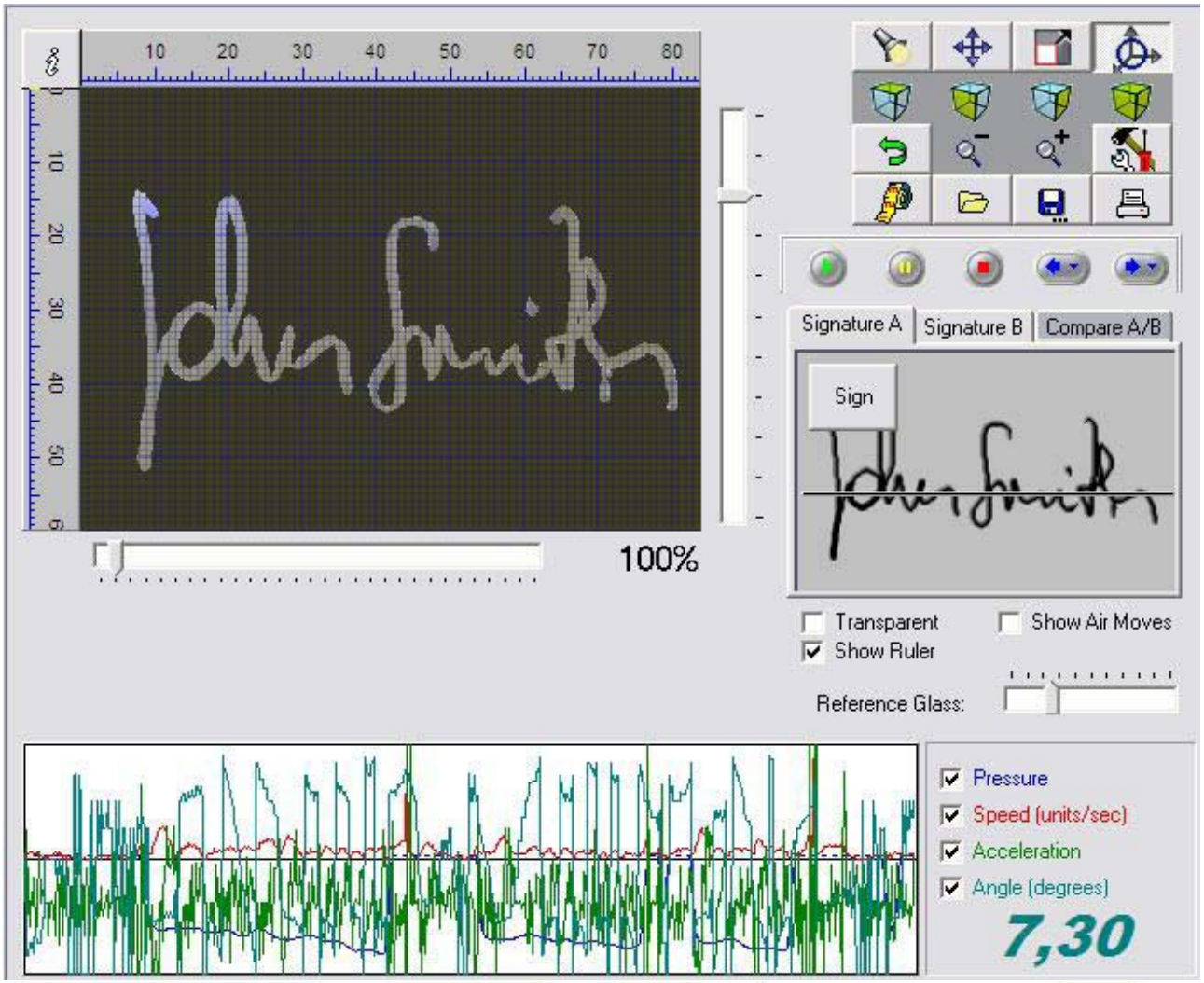
Acquisizione **Firma**



Firma & Marca Temporale

Verifica

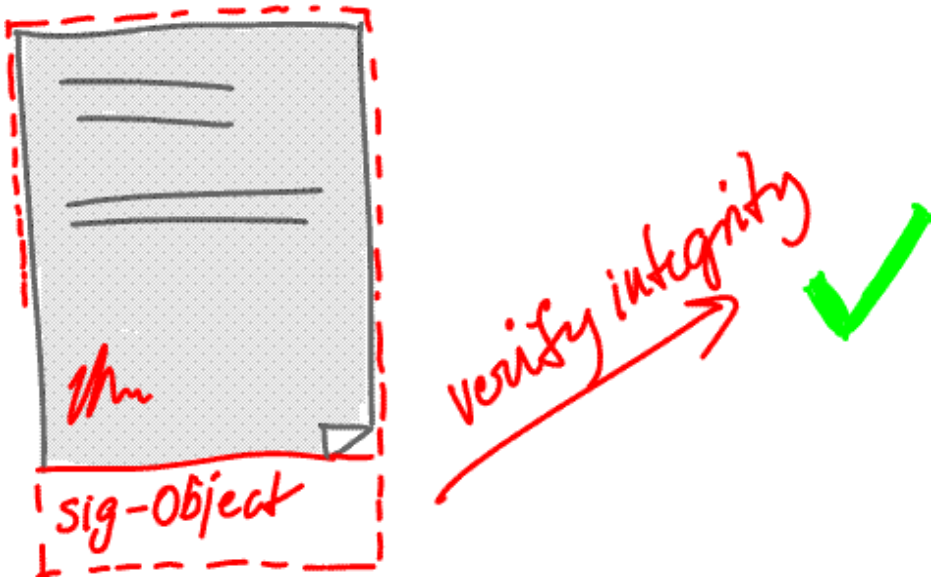
La Biometria applicata alla Firma Digitale



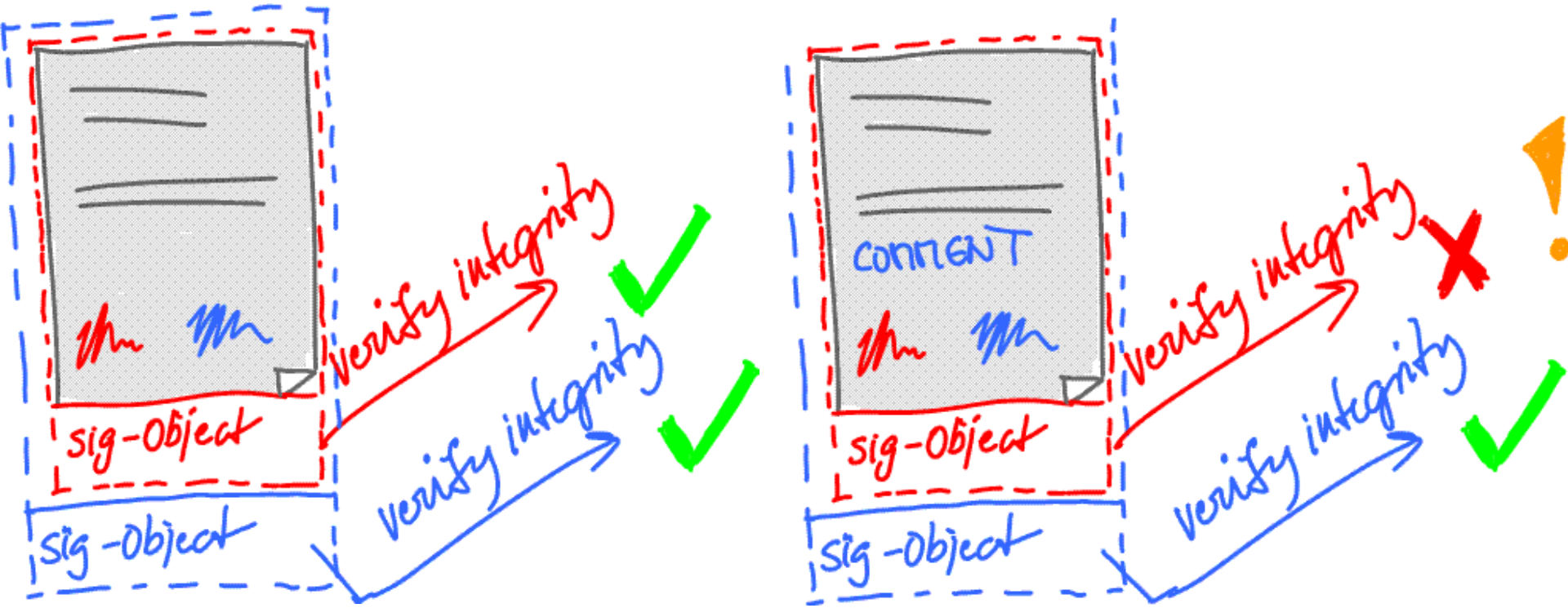
Acquisizione e verifica della firma

Il riconoscimento della firma non avviene in modo grafico (facilmente falsificabile) ma in modo biometrico e più precisamente la valutazione e gestione contemporanea dei seguenti fattori:

La biometria è utilizzata per accedere alle chiavi di firma, il documento viene poi firmato secondo la normativa vigente



Sono gestibili anche controfirme e firme parallele



Riduzione sensibile costi

- Meno stampe
- Meno carta
- Archiviazione
- Sicurezza
- Armadi
- Faldoni

Miglioramento sevizio

- Possibilità di realizzare documenti a distanza
- Disponibilità degli originali da ogni postazione connessa alla rete
- Consegna e invio documenti immediato

Processo di firma dei documenti

Domande & Conclusioni

Grazie per l’attenzione !

Franco.tafini@intesa.it