Seminario FUB:

"Gestione dell'identità digitale"

Identità digitale e relativi servizi: sicurezza e verifiche sui sistemi ICT

Franco Guida

Responsabile Area "Sicurezza ICT"

Fondazione Ugo Bordoni

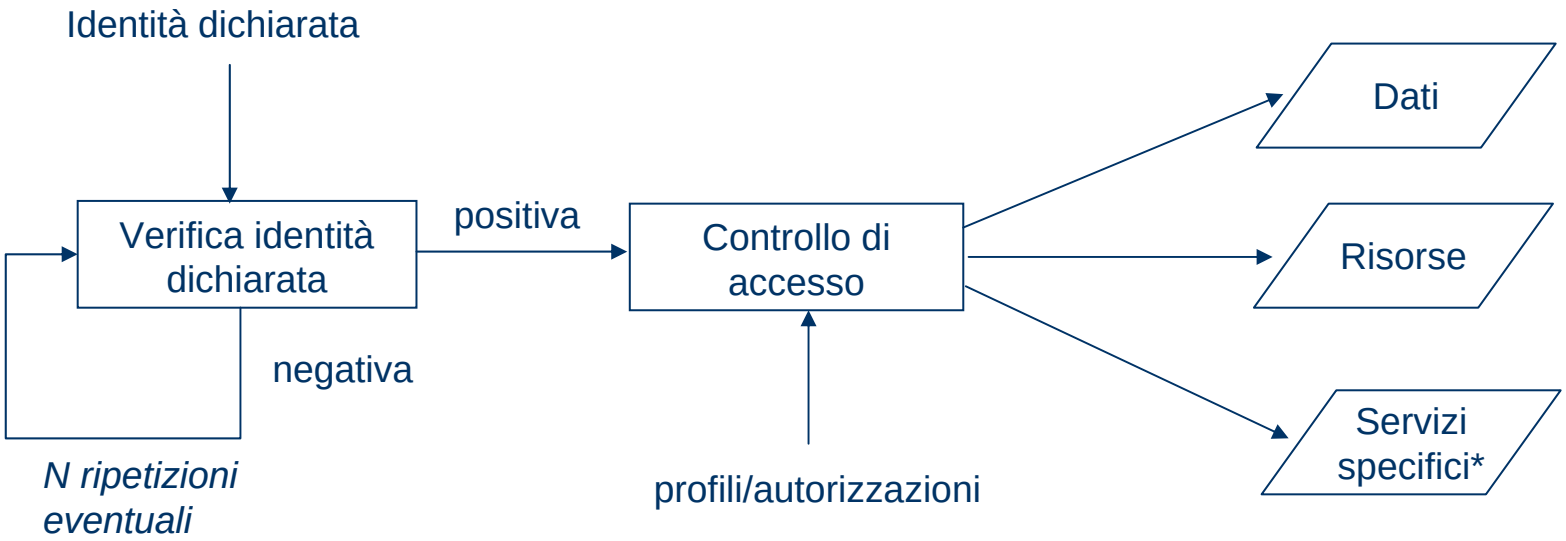
Fondazione Ugo Bordoni

Roma, 18 novembre 2008

Identità digitale, sicurezza ICT, FUB

- Sicurezza ICT ⇔ Identità digitale
  - Accesso dei soli soggetti autorizzati a dati, risorse, servizi ⇒ Garanzia che l'identità dichiarata dei soggetti corrisponda al vero
- La FUB affianca l'ISCOM del Ministero dello Sviluppo Economico – Comunicazioni nelle funzioni istituzionali relative a:
  - certificazione della sicurezza di sistemi ICT e loro componenti in base ai criteri ITSEC e ISO/IEC IS15408 – Common Criteria (DPCM 30 ottobre 2003)
  - verifica del soddisfacimento, da parte dei dispositivi per la generazione delle firme elettroniche avanzate (inclusa la firma digitale italiana), dei requisiti di sicurezza fissati dalla Direttiva europea 1999/93/EC del 13 dicembre 1999 sulla firma elettronica (DL 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale)

Sistema ICT che utilizza identità digitali



* Esempio: firma elettronica

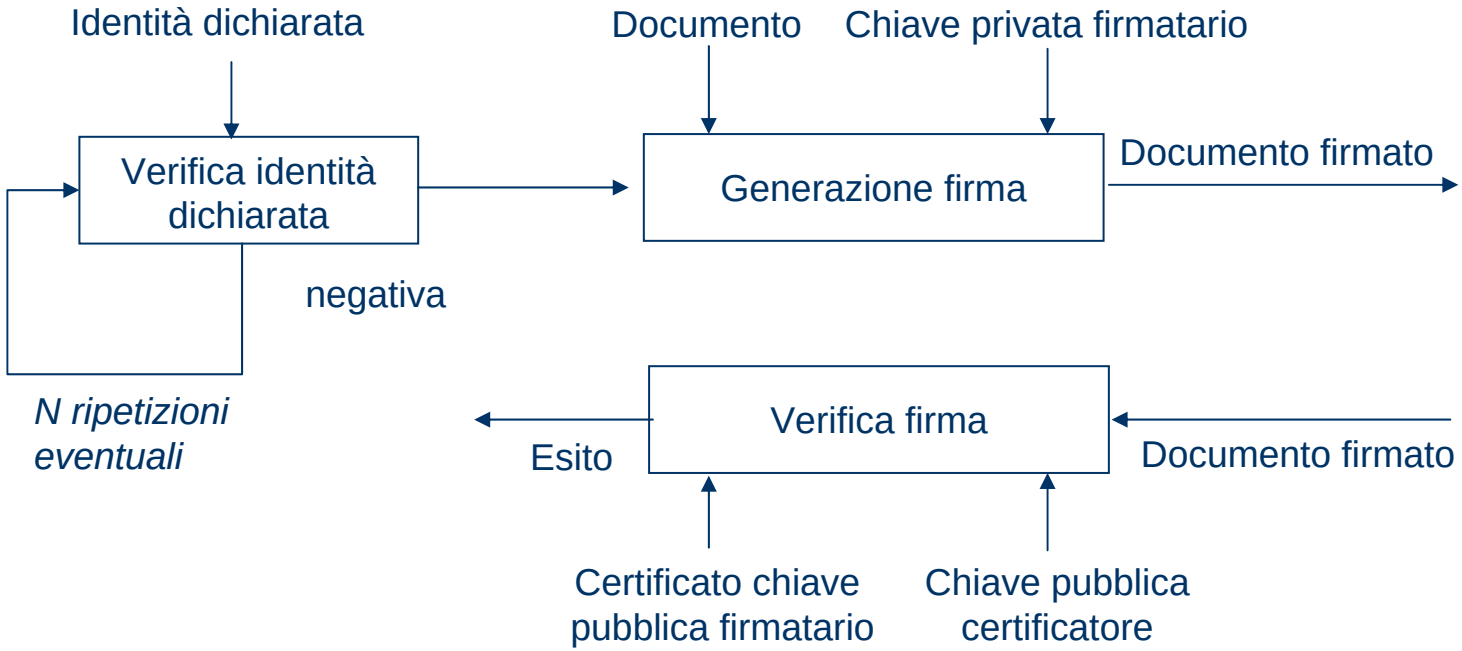
Sistema ICT immerso in un ambiente operativo

- Minaccia: a seguito di eventi accidentali o di azioni intenzionali, l'identità digitale di un individuo potrebbe essere utilizzata da un altro individuo (talvolta con l'inconsapevole collaborazione del legittimo proprietario dell'identità)
- Progettazione di contromisure tecniche e non (procedurali, fisiche, relative al personale)
  - Nel caso delle contromisure tecniche il risultato della progettazione può essere riportato in uno standard internazionale
- Livello di sicurezza adeguato se:
  - viene confermata la validità teorica delle contromisure individuate
  - viene confermato che per tutte le componenti del sistema ICT rilevanti dal punto di vista della minaccia considerata sono state previste le necessarie contromisure
  - nella fase di implementazione (in *hw/sw/fw* se trattasi di contromisure tecniche) e di esercizio delle contromisure non vengono introdotte vulnerabilità sfruttabili nell'ambiente ipotizzato

Come si può verificare l'identità digitale di un soggetto?

- Generalmente in uno o più dei seguenti modi:
  - verificando che il soggetto conosca o possa accedere a dati ignoti o inaccessibili a chiunque altro (ad esempio un PIN, una password o una chiave di firma)
  - verificando che il soggetto sia in possesso di un oggetto che nessun altro dovrebbe possedere (ad esempio una carta magnetica o una smart-card opportunamente configurate e consegnate con una procedura affidabile)
  - verificando che il soggetto che si sottopone alla verifica possegga alcune caratteristiche biometriche o comportamentali (ad esempio le modalità di apposizione di una firma autografa) preventivamente acquisite sul soggetto legittimo

Sistema ICT per la firma elettronica avanzata europea

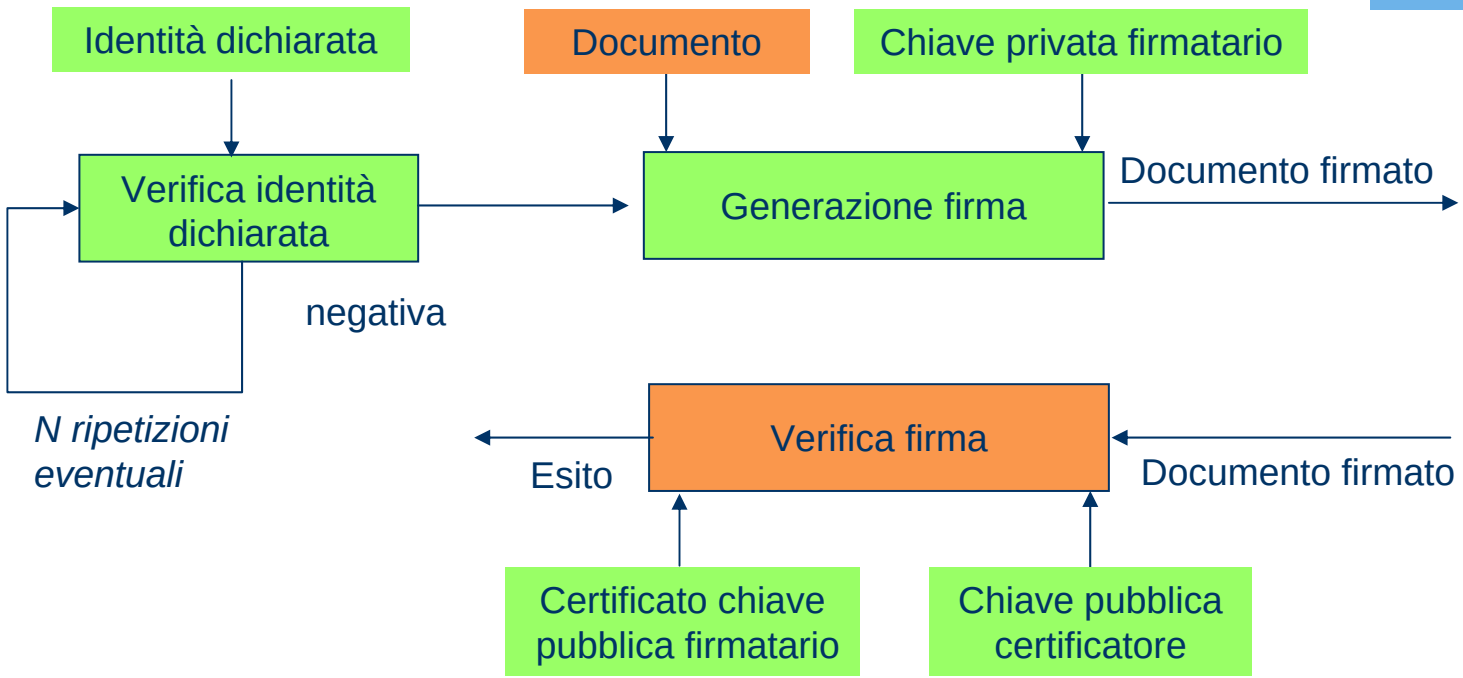


- Assenza blocco di controllo d'accesso per la presenza di un unico servizio
- La firma digitale è un servizio con due peculiarità:
  - il non ripudio, in base al quale, in caso di esito positivo della verifica, al firmatario è attribuito in modo incontestabile il documento firmato (accresciuta esigenza di assenza di errori e violazioni)
  - può essere usata per verificare l'identità oltre che come servizio per la firma di documenti

Verifica dell'identità digitale e servizio "firma elettronica"

- La verifica dell'identità digitale può fare uso della firma elettronica:
  - alcuni protocolli di verifica dell'identità digitale (autenticazione) richiedono al soggetto che si sottopone alla verifica di firmare dati di prova generati da chi verifica, dimostrando così la conoscenza o la capacità di accesso alla chiave segreta di firma
- La firma elettronica ha normalmente bisogno della verifiche di identità in vari passi. Ad esempio:
  - Occorre avere garanzia che chi usa un dispositivo di firma ne sia il legittimo titolare (ad esempio verificando il possesso del dispositivo e la conoscenza di un PIN, consegnati inizialmente previa ulteriore verifica di identità del titolare e con procedure affidabili)

Sistema ICT per la firma elettronica avanzata europea



- Per gli oggetti arancioni sono formulati solo requisiti di alto livello nella Direttiva europea 1999/93/EC
- Per gli oggetti verdi, oltre ai requisiti di alto livello indicati nella Direttiva, sono definite nella Decisione della commissione delle comunità europee del 14 luglio 2003 possibili contromisure per le minacce di interesse nonché modalità di validazione della implementazione delle contromisure stesse

Firma elettronica avanzata in Europa

- Le verifiche sull'implementazione non sono fatte sull'intera catena del sistema ICT ma solo su una parte dei dispositivi che consentono di firmare un documento
- Queste verifiche consentono di avere elevate garanzie circa il fatto che l'emissione di firme possa essere controllata esclusivamente dal titolare (requisito di fondamentale importanza)
- L'incompletezza o assenza di specifiche e verifiche sulle rimanenti parti dei dispositivi di generazione della firma non consente invece di avere garanzie elevate circa il fatto che il documento firmato sia effettivamente quello che il titolare della firma si aspetta (requisito critico, anche se meno del precedente)
- L'incompletezza o assenza di specifiche e verifiche sui dispositivi di verifica delle firme non consente di avere garanzie elevate circa la correttezza del responso fornito (requisito importante, ma meno stringente dei precedenti se si può contare su dispositivi di riferimento).

Proposte migliorative

- L'attuale disomogeneità circa le garanzie di sicurezza per le varie componenti del sistema ICT fornitore del servizio di firma sembra giustificarsi solo in parte con le differenti criticità delle operazioni svolte dalle componenti
- Le differenti criticità potrebbero influenzare il rigore con il quale eseguire le verifiche di sicurezza sulle varie componenti ma non dovrebbero portare in taluni casi all'assenza di verifiche (le relative minacce non possono considerarsi trascurabili)
- Sembra quindi utile uno sforzo per garantire un livello minimo di verifica sull'intero sistema ICT (ad esempio, per alcune componenti, certificazioni Common Criteria ai primi livelli: EAL1 o EAL2)
- In assenza di questo sforzo sarà naturale attendersi che le eventuali violazioni prenderanno di mira gli anelli deboli della catena, vanificando almeno in parte quanto di buono è stato fatto per gli altri anelli

Grazie per l’attenzione

guida@fub.it