Ministero dello Sviluppo Economico Comunicazioni

Istituto Superiore
delle Comunicazioni e Tecnologie dell'Informazione

Identità digitale:
tecnologia e sfide

Ministero dello Sviluppo Economico Comunicazioni

L'Istituto Superiore

- L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, costituito nel 1907, opera nell'ambito del Ministero dello Sviluppo Economico, settore Comunicazioni, in qualità di organo tecnico-scientifico. La sua attività riguarda: la sperimentazione e la ricerca di base e applicata, il supporto tecnico alle imprese, alle istituzioni e ai cittadini anche attraverso l'operatività dei propri laboratori di prova, la formazione, specializzazione e divulgazione nel campo delle comunicazioni elettroniche, la normazione.
- Considerando il suo ruolo di organismo pubblico super partes, il valore aggiunto dell'Istituto, dato in termini di garanzia e competenza, è l'aspetto che contraddistingue i servizi di supporto tecnico e consulenziale forniti alle imprese e ai soggetti coinvolti nel settore delle comunicazioni elettroniche. Tali servizi si sostanziano non solo nelle tradizionali attività di certificazione, realizzate grazie alle competenze e alle strumentazioni dei laboratori che consentono di verificare la conformità di ogni apparato telematico alle varie norme e raccomandazioni di riferimento, ma anche in peculiari campagne di misura per la verifica della qualità del servizio (QoS), della sicurezza delle reti e per l'accertamento delle specifiche tecniche di interoperabilità dei servizi nell'ambito dell'interconnessione delle reti di vari operatori.

Attività relative all'identità digitale

- Biometria e Sicurezza dei dati biometrici - progetto di ricerca congiunto tra ISCOM e COMLAB dell'università degli studi "ROMA TRE".

- L'Istituto ricopre il ruolo di Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali (OCSI), ed è Centro di Valutazione (Ce.Va) di sistemi e prodotti ICT che trattano dati classificati.

- OCSI (conformità Direttiva EU 1999/93CE – allegato III).

Biometria e Sicurezza dei dati biometrici

Obbiettivo: realizzazione database

- Il database biometrico di validazione servirà a fornire una base di dati ampia e statisticamente significativa per tutti gli enti/società che intendono validare i loro algoritmi e sistemi di autenticazione biometrica.

- Verrà inizialmente studiato e proposto per il viso con un approccio innovativo basato sulla sintesi cinematografica che quindi richiederà un esiguo numero di volontari. Verrà poi valutato come e con quali strumenti estendere l'approccio sintetico agli altri parametri biometrici.

- L'obbiettivo finale è rendere disponibile il database a livello europeo come un sistema di validazione per l'autenticazione ed il riconoscimento visuale.

Biometria e Sicurezza dei dati biometrici

Le aree di ricerca congiunte identificate sono tre:

- Costruzione di un database sintetico di dati biometrici.
- Autenticazione e Protezione di dati biometrici basati su sistemi de-centralizzati.
- Steganografica e Data-Hiding per la Sicurezza.

La collaborazione è comunque mirata alla pubblicazione di articoli ed alla partecipazione a progetti internazionali

Biometria e Sicurezza dei dati biometrici

Attività:

- Analisi dei diversi sistemi di autenticazione biometrica: viso, iride retina, palmo, impronta digitale.
- Costruzione di un database sintetico di dati biometrici per il viso. Verranno analizzate diverse alternative:
- Partendo da un database di immagini naturali, verranno introdotte delle modifiche artificialmente;
- Generazione del database sintetico con software di generazione/animazione di immagini sintetiche (tipo cinematografico);
- Costruzione del database sintetico con arricchimento dai campioni naturale;
- Studio e analisi delle caratteristiche statistiche del database: generazione di un database con caratteristiche statistiche significative (distanza desiderata, set di campioni significativo e completo).
- Analisi dei possibili metodi di generazione di Database sintetici per iride, retina, impronta digitale.

Biometria e Sicurezza dei dati biometrici

Scuola Superiore di Specializzazione in Telecomunicazioni

Lo scorso anno e nel nuovo anno accademico 2008-09 è stato attivato presso la Scuola Superiore di Specializzazione in Telecomunicazioni il corso:

- Sistemi di autenticazione multimediali: riconoscimento biometrico visivo, tattile e cartaceo (firma digitale)

Ministero dello Sviluppo Economico Comunicazioni

Ce.Va.

- Presso l'ISCTI opera il Centro di valutazione (Ce.Va.), l'unico centro di questo appartenente tipo alla Pubblica Amministrazione.

- Esegue valutazioni di prodotti e sistemi ICT in base alle norme e alle procedure dello Schema Nazionale di Valutazione e Certificazione della sicurezza informatica riguardante prodotti classificati coordinato dall'Autorità Nazionale per la Sicurezza (ANS).

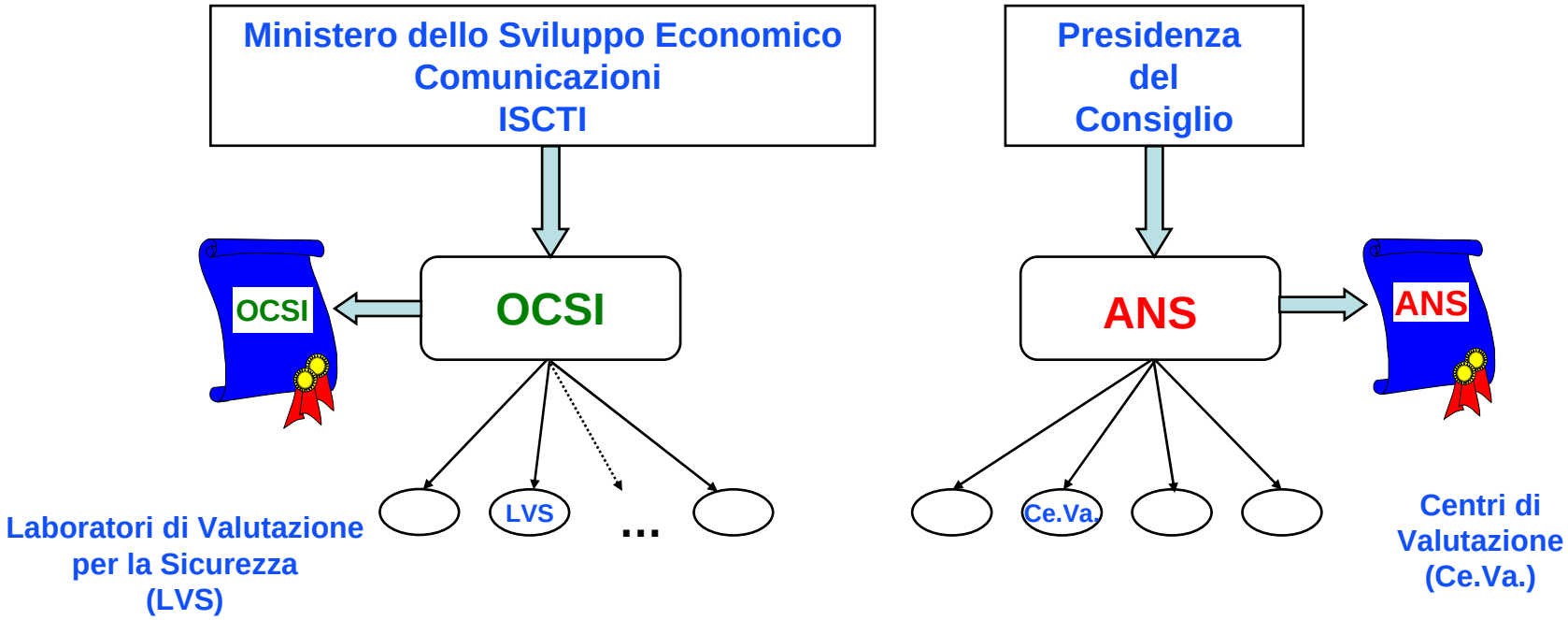
OCSI

- L'ISCTI è anche l'Organismo di Certificazione della Sicurezza Informatica (OCSI), istituito dal DPCM del 30 ottobre 2003 (G.U. n. 98 del 27 aprile 2004) per la valutazione e certificazione della sicurezza di sistemi e prodotti commerciali nel settore ICT.

- L'OCSI è attualmente impegnato nella procedura della "Valutazione ombra", al termine della quale, entro il 2008, potrà ottenere il riconoscimento dello status di "Certificate Producer" ed accedere così al mutuo riconoscimento delle certificazioni rilasciate in Italia anche in tutti i paesi aderenti al CCRA (Common Criteria Recognition Arrangement.)

Ministero dello Sviluppo Economico Comunicazioni

OCSI – Ce.Va.



Prodotti/sistemi IT commerciali (informazioni non classificate)

Prodotti/sistemi IT (informazioni classificate)

Direttiva EU 1999/93/CE

- L'OCSI è stato designato, ai sensi del comma 4 dell'articolo 3 della direttiva EU sulla firma digitale (1999/93/CE), e notificato , ai sensi del punto b) del comma 1 dell'articolo 11 della direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma ai requisiti di sicurezza espressi nell'allegato III alla suddetta direttiva

- In Italia l'affidamento all'OCSI dell'accertamento è specificato dal comma 5 dell'articolo 35 del Codice dell'Amministrazione Digitale.

  Il comma 6 dello stesso articolo indica che l'accertamento non è necessario in Italia se già eseguito con esito positivo da un organismo designato e opportunamente notificato da un altro stato membro

Procedure di accertamento (1)

- ***Accertamento standard***

  L'accertamento è eseguito controllando che il dispositivo di firma sia dotato di certificazione ISO/IEC 15408 (Common Criteria) EAL 4+, rilasciata in conformità a uno dei Protection Profile (e.g. CWA 14169) definiti nella Decisione della Commissione delle Comunità Europee del 14 luglio 2003, e che tale certificazione sia valida in Italia.

  Si applica ai dispositivi di firma tradizionali, ad es. smart card.

Procedure di accertamento (2)

- ***Accertamento per dispositivi di firma HSM***

  Per i dispositivi da usarsi come dispositivi propri dei certificatori italiani per l'apposizione di firme elettroniche con procedure automatiche (HSM), come definite dal DL 7 marzo 2005 n. 82 e dal DPCM 12 ottobre 2007, non è utilizzabile uno dei Protection Profile definiti nella Decisione della Commissione delle Comunità Europee del 14 luglio 2003.

  Per tali dispositivi OCSI ha definito una specifica:

- **Procedura provvisoria** di accertamento di conformità

Validità procedura di accertamento

- Considerando che l'accertamento di conformità dei dispositivi HSM non presenta precedenti simili, l'OCSI ha inteso comunque procedere all'accertamento di conformità di tali dispositivi, definendo una propria specifica procedura, nell'ottica di non arrecare danno al mercato del settore e nel contempo tutelare gli utilizzatori.

- L'accertamento eventualmente rilasciato potrà essere considerato valido fino a quando non si renderà disponibile una procedura codificata di rilevanza europea, analogamente a quanto avvenuto con la Decisione della Commissione delle Comunità Europee del 14 luglio 2003.