



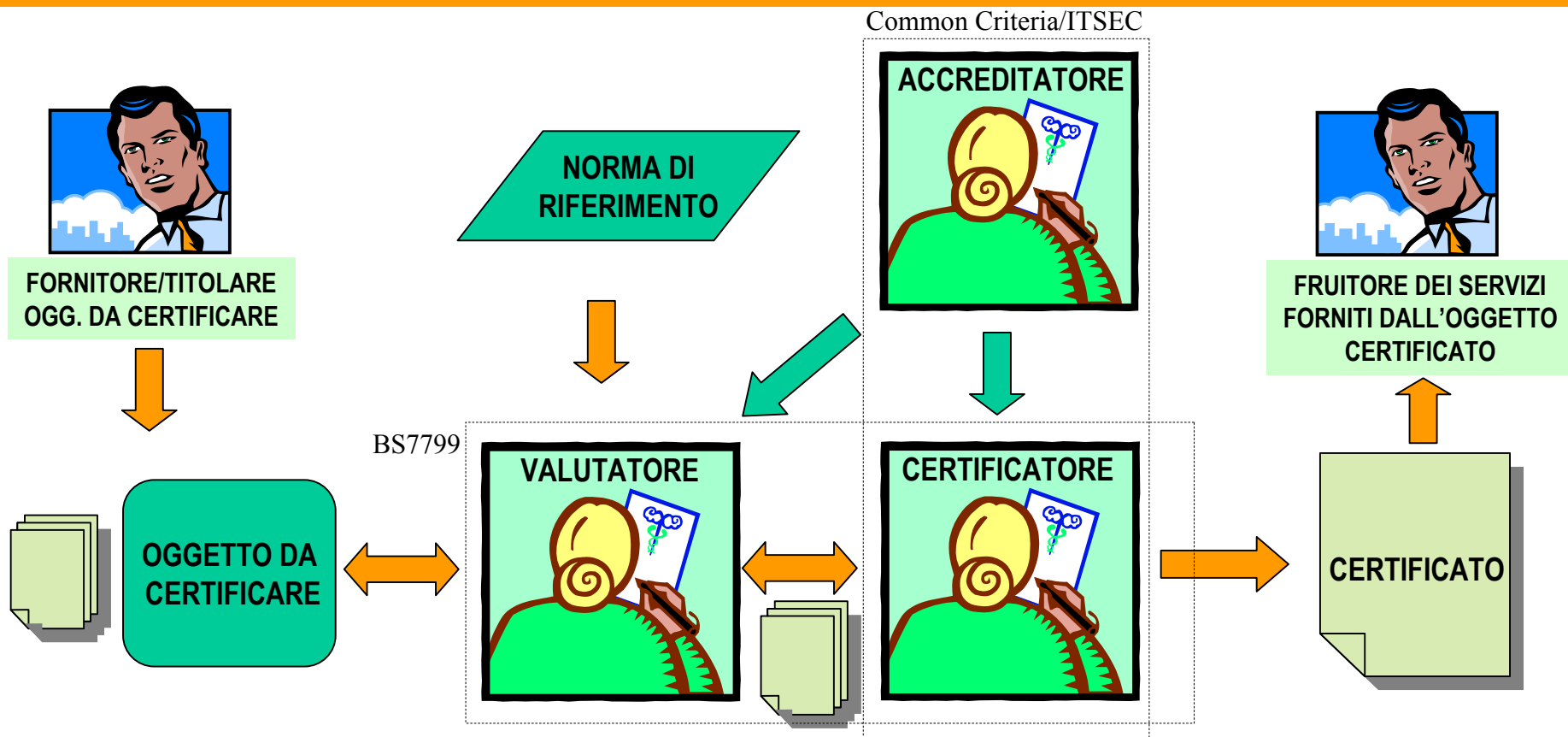
Organismo di Certificazione della Sicurezza Informatica

Apertura lavori del Convegno Le certificazioni di sicurezza in Italia

Franco Guida

Infosecurity 2005 – Fiera di Milano – 11 febbraio 2005

Le entità in gioco



Quando si può parlare di certificazione

La certificazione deve essere eseguita in modo da garantire l'imparzialità, l'oggettività, la ripetibilità e la riproducibilità dell'intero processo di certificazione. A tal fine:

- l'accreditatore, il certificatore ed il valutatore (qualora sia presente) devono essere terza parte indipendente rispetto al:
 - Fornitore/titolare dell'oggetto da certificare
 - Fruitore della certificazione
- la certificazione deve basarsi su criteri o standard di riferimento comunemente accettati
- deve essere verificata la competenza di chi applica la norma di riferimento (valutatore/certificatore)

Soggetto di riferimento

- Per facilitare il mutuo riconoscimento delle certificazioni in vari Paesi, normalmente chi accredita i certificatori/valutatori è un'**Organismo pubblico** o un'**Associazione altamente rappresentativa**



La sicurezza ICT in un'Organizzazione



Tipi di certificazione

Oggetto certificato	Norme di riferimento
Processo di gestione della sicurezza ICT (ISMS)	BS7799:2
Sistema/prodotto ICT	Common Criteria (ISO/IEC IS15408) ITSEC
Competenza del personale	CISSP/SSCP, CISA/CISM, ecc.

Chi può richiedere la certificazione e perché (1)

- Il soggetto fornitore dell'oggetto certificato
 - perché conta su un incremento delle vendite (es: oggetto certificato=sistema/prodotto ICT)
- Il soggetto titolare dell'oggetto certificato (es: ISMS)
 - perché vuole dimostrare anche verso terzi di aver curato adeguatamente la gestione della sicurezza

Chi può richiedere la certificazione e perché (2)

- Il soggetto fruitore dei servizi offerti dall'oggetto certificato
 - perché desidera garanzie che vadano oltre le dichiarazioni del fornitore (nel caso l'oggetto sia un sistema/prodotto ICT)
 - perché vuole dimostrare anche verso terzi di fare uso di “oggetti” affidabili (ISMS, sistemi ICT, personale) eventualmente utilizzati:
 - per fornire servizi di cui la clientela non si fida (aspettativa di incremento della clientela)
 - per eseguire trattamenti disciplinati da norme di legge (es: trattamento di dati personali)

Le certificazioni in Italia regolate da DPCM

- **Certificazione di prodotto/sistema ICT**
 - Schema Nazionale del 1995 aggiornato nel 2002 (DPCM 11 aprile 2002 – GU n. 131 del 6 giugno 2002) applicabile nel contesto della sicurezza interna e esterna dello Stato
 - Ente di Certificazione/Accreditamento (EC): ANS/UCSi
 - Centri di Valutazione (Ce.Va.): 3 privati, 2 pubblici (tra cui ISCOM ex ISCTI)
 - Schema Nazionale del 2003 (DPCM 30 ottobre 2003 – GU n. 98 del 27 aprile 2004) applicabile in tutti i contesti non coperti dal primo Schema
 - Organismo di Certificazione/Accreditamento (OCSI): ISCOM ex ISCTI (Ministero Comunicazioni) che si avvale del supporto della FUB
 - Laboratori di Valutazione (LVS): da accreditare nei prossimi mesi

Le altre certificazioni in Italia

- **Certificazione del processo di gestione (ISMS)**
 - Schema Sincert per l'accreditamento BS7799
 - Organismo di Accredimento: Sincert
 - Organismi di certificazione accreditati: 4 privati
- **Certificazione del personale**
 - Criteri di verifica della competenza sviluppati per lo più in ambito internazionale (es. CISP/SSCP sviluppati da (ISC)², CISA/CISM sviluppati da ISACA, ecc.)
 - Soggetti operanti anche in Italia (es. Clusit, come Education Affiliate nell'ambito delle certificazioni CISP/SSCP)

Tre aree

- Profili giuridici
- Certificazione di sistema prodotto ICT (esponenti dei due Organismi di certificazione/accreditamento nazionali)
- Certificazione del processo di gestione (ISMS) (rappresentante dell'Organismo di accreditamento e dell'Ente normatore italiano)

Obiettivi Convegno

- Evidenziare le differenze di base dei due tipi di certificazione
- Evidenziare la loro complementarità e quindi l'utilità di entrambe per migliorare il livello di sicurezza globale
- Individuare le poche aree per le quali potrebbe esservi sovrapposizione specificando interpretazioni/accordi che possono evitarle
- Illustrare, nel caso della certificazione di sistema/prodotto ICT, alcune proposte innovative che l'Organismo di Certificazione (OCSI) intende promuovere

Grazie dell'attenzione

e-mail: guida@fub.it