

RICONOSCIMENTO IN AMBITO INTERNAZIONALE DEI CERTIFICATI DI SICUREZZA EMESSI DALL'OCSI (ORGANISMO DI CERTIFICAZIONE DELLA SICUREZZA INFORMATICA)

INTERNATIONAL RECOGNITION OF COMMON CRITERIA CERTIFICATES ISSUED BY OCSI (ITALIAN CERTIFICATION BODY IN THE FIELD OF IT SECURITY)

Sommario: si è finalmente concluso, con esito positivo per l'OCSI (Organismo di Certificazione della Sicurezza Informatica), l'iter della cosiddetta "valutazione ombra", particolare procedura di controllo definita dagli Schemi internazionali di certificazione nel settore della sicurezza IT aderenti al CCRA (Common Criteria Recognition Arrangement). Conseguentemente, si è ottenuta la "promozione" dell'OCSI al rango di Schema Produttore di certificati, il che consentirà anche alle certificazioni rilasciate in Italia di essere riconosciute in tutti i paesi aderenti al CCRA.

I. Introduzione

Come ormai noto, con il DPCM del 30 ottobre 2003 (GU n.98 del 27-4-2004) "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione" [1], è stato stabilito che l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) del Ministero delle Comunicazioni (oggi Ministero dello Sviluppo Economico - Dipartimento per le Comunicazioni) svolge il ruolo di Organismo di Certificazione della sicurezza nel settore della tecnologia dell'informazione. Tale Organismo sovrintende tutte le attività connesse con la valutazione e certificazione di sistemi/prodotti nell'ambito dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, condotte in conformità ai criteri internazionali ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation*, comunemente noti come Common Criteria) ([2], [3], [4], [5], [6]) e ITSEC ([7], [8]).

In seguito all'approvazione del decreto, in seno

Abstract: the process of the so-called "shadow certification", a particular assessment procedure defined by the international certification Schemes in the field of IT security that joined the CCRA (Common Criteria Recognition Arrangement), has finally come to an end for the OCSI (Organismo di Certificazione della Sicurezza Informatica), with a positive outcome. Consequently, the "status" of OCSI has been improved to the rank of Certificate Authorising Scheme, which implies that the certificates issued in Italy will be also recognized in all countries participating in the CCRA.

all'ISCOM e in collaborazione con la Fondazione Ugo Bordoni (FUB), hanno quindi preso il via le attività dell'Organismo di Certificazione della Sicurezza Informatica (OCSI) [9].

Dopo aver completato tutte le attività propedeutiche all'avvio della normale operatività dello Schema, e cioè la definizione della normativa, Linee Guida Provvisorie (LGP) ([10], [11], [12], [13], [14], [15], [16]) e Note Informative dello Schema (NIS) ([17], [18], [19]), l'accreditamento dei Laboratori per la Valutazione della Sicurezza (LVS) e l'abilitazione degli Assistenti, nel corso del 2007 sono state finalmente avviate le prime tre valutazioni, riguardanti due prodotti per i quali è stata richiesta la certificazione a livello EAL3 ed un prodotto a livello EAL4, secondo la scala in uso nei Common Criteria, che va da EAL1 a EAL7 (EAL: *Evaluation Assurance Level* - Livello di Garanzia della Valutazione).

Nel corso del 2008 si sono poi conclusi i primi processi di certificazione, con la conseguente emissione dei primi due certificati OCSI, secondo lo standard Common Criteria, per due prodotti a livello EAL3.

In particolare, le valutazioni svolte hanno rivestito un ruolo di fondamentale importanza in quanto hanno consentito all'OCSI di accedere alla procedura della cosiddetta "valutazione ombra", descritta in questo articolo. Tale procedura, richiesta per poter beneficiare del "mutuo riconoscimento" delle certificazioni da parte degli altri Organismi di Certificazione internazionali, ha avuto il suo momento culminante dal 15 al 19 dicembre 2008, con la visita di controllo presso la sede dell'ISCOM di un gruppo di ispettori degli Organismi di Certificazione esteri. Il relativo rapporto stilato dagli ispettori è stato approvato proprio di recente dal CCRA (*Common Criteria Recognition Arrangement*) [20], con la conseguente "promozione" dell'OCSI al rango di Schema Produttore di certificati.

In questo articolo viene fornito un breve aggiornamento sulle attività svolte dall'OCSI nel 2008 (cap. 1), una descrizione degli scopi e delle attività del CCRA (cap. 2), alle quali l'Italia ha partecipato già a partire dal 2000, e la descrizione dello svolgimento e dei risultati della procedura di "valutazione ombra", alla quale l'OCSI è stato sottoposto alla fine del 2008 (cap. 3).

1. Attività dell'OCSI svolte nel 2008

1.1 Attività preparatorie

Dopo una fase preparatoria, nella quale sono state predisposte le Linee Guida Provvisorie (LGP) dello Schema, che regolamentano tutte le attività svolte nell'ambito dello Schema stesso, nel corso del biennio 2006-2007 le attività dell'OCSI sono entrate nella fase operativa, con il conseguimento dei risultati di seguito brevemente esposti:

- pubblicazione di una serie di Note Informative dello Schema (NIS), con le quali sono state apportate alcune modifiche e integrazioni alle LGP, per renderle più adeguate ad eseguire correttamente ed efficacemente le attività di valutazione e certificazione;
- accreditamento di Laboratori per la Valutazione della Sicurezza (LVS), che effettuano, sotto il diretto controllo dell'OCSI, le valutazioni di prodotti/sistemi o di Profili di Protezione (*Protection Profile* - PP) secondo

le norme previste dallo Schema nazionale e i criteri internazionali (attualmente sono sei gli LVS accreditati);

- abilitazione di Assistenti, che forniscono assistenza alle varie parti coinvolte nel processo di valutazione di un ODV (Oggetto Della Valutazione), Committente, Fornitore o LVS, nella fase di stesura della documentazione richiesta;
- erogazione di corsi su "La certificazione della sicurezza informatica: guida per l'applicazione dei Common Criteria", aventi il fine della formazione, abilitazione e addestramento dei certificatori, del personale dipendente dell'Organismo di Certificazione, nonché dei valutatori degli LVS accreditati e degli Assistenti abilitati.

1.2 Processi di certificazione ed emissione di certificati

Dopo aver completato tutte le attività propedeutiche all'avvio della normale operatività dello Schema, descritte nel paragrafo precedente, nel corso del 2007 sono state finalmente avviate le prime tre valutazioni, riguardanti due prodotti per i quali è stata richiesta la certificazione a livello EAL3 ed un prodotto a livello EAL4, secondo la scala in uso nei Common Criteria, che va da EAL1 a EAL7.

Nel corso del 2008 si sono conclusi i primi due processi di certificazione, con la conseguente emissione dei primi certificati OCSI, secondo lo standard Common Criteria. In particolare, i prodotti oggetto delle certificazioni sono stati i seguenti:

- "ET 500 Plus", un dispositivo che fornisce l'accesso controllato alle periferiche in esso integrate, utilizzato per il rilascio e per la verifica dei nuovi documenti di identità elettronici. Il prodotto è stato realizzato dalla società "Italdata - Ingegneria dell'idea"; la valutazione, a livello di garanzia EAL3, è stata condotta dall'LVS Consorzio RES; il relativo certificato è stato emesso dall'OCSI il 14 luglio 2008
- "Gestione dei dati sanitari, infermerie e CMD", un'applicazione Web di supporto per la gestione dei dati sanitari del personale della Difesa che consente l'accesso ai dati sanitari dei pazienti da parte del personale

medico autorizzato. Il prodotto è stato realizzato dalla società "Blustaff"; la valutazione, a livello di garanzia EAL3, è stata condotta dall'LVS Eutelia; il relativo certificato è stato emesso dall'OCSI il 30 ottobre 2008.

La terza certificazione di prodotto, al livello EAL4, avviata ufficialmente nel novembre del 2007, è stata condotta fino ad una fase avanzata e la sua conclusione è prevista per la metà del 2009.

In particolare, è da ricordare che una delle due certificazioni EAL3, "Gestione dei dati sanitari, infermerie e CMD", e la valutazione EAL4, hanno rivestito un ruolo di fondamentale importanza in quanto oggetto di verifica in sede di valutazione ombra da parte del gruppo di commissari delegati dagli Organismi di Certificazione internazionali, come verrà ampiamente descritto nel cap. 3.

1.3 Attività internazionali

Tra le attività svolte dall'OCSI in ambito internazionale, l'avvenimento senza dubbio più rilevante è stata la partecipazione alla conferenza "9th International Common Criteria Conference" (9ICCC) che si è tenuta a Jeju, in Corea del Sud, dal 23 al 25 settembre 2008.

La conferenza ICC, che si tiene con cadenza annuale, riunisce organismi di certificazione, laboratori di valutazione, esperti, responsabili della sicurezza e sviluppatori di prodotti commerciali che hanno interesse nella specifica, nello sviluppo, nella valutazione e certificazione della sicurezza IT (*Information Technology*).

Inoltre, l'OCSI ha partecipato ad alcune riunioni dei gruppi di lavoro del *Common Criteria Recognition Arrangement* (CCRA), che riunisce tutti gli organismi di certificazione internazionali. In particolare, l'OCSI ha partecipato con un suo rappresentante alle seguenti riunioni dei gruppi di lavoro che verranno descritti nel paragrafo 2.4.

1. (CCMB) 9-11/06/2008, Londra (UK)
2. (CCDB) 1-2/04/2008, Wellington (NZ)
17-18/09/2008, Jeju (KR)
3. (CCES) 3/04/2008, Wellington (KR)
19/09/2008, Jeju (KR)
4. (CCMC) 22/09/2008, Jeju (KR)

2. Panoramica sul CCRA (Common Criteria Recognition Arrangement)

Lo standard dei Common Criteria, unitamente alla metodologia definita nel documento complementare *Common Methodology for Information Technology Security Evaluation* (CEM) [5], costituisce il fondamento tecnico di un gruppo internazionale denominato CCRA (*Common Criteria Recognition Arrangement*), frutto di un accordo di mutuo riconoscimento sottoscritto nel 2000 da dodici Paesi, tra cui l'Italia, che si occupa per l'appunto dell'applicazione, dell'armonizzazione e dell'evoluzione dello standard Common Criteria. Negli anni seguenti, altri Paesi hanno aderito all'accordo, che attualmente comprende 26 partecipanti.

2.1 Scopi del CCRA

Tra gli scopi principali del CCRA vi sono quelli di assicurare che:

- prodotti e sistemi IT vengano valutati da laboratori accreditati competenti ed indipendenti, al fine di determinare il soddisfacimento di specifici requisiti di sicurezza nei limiti dei livelli di garanzia richiesti;
- venga prodotta ed utilizzata documentazione di supporto, in accordo coi Common Criteria, allo scopo di definire come i criteri e le metodologie di valutazione vengono applicati nei processi di certificazione riguardanti specifiche tecnologie;
- le certificazioni di sicurezza di prodotti e sistemi IT vengano emesse da un certo numero di cosiddetti *Certificate Authorising Schemes* (Schemi Produttori di Certificati), sulla base dei risultati della loro valutazione;
- "tali certificati vengano riconosciuti da tutti gli Schemi internazionali aderenti al CCRA.

2.2 Obiettivi comuni degli Schemi aderenti al CCRA

Gli Schemi e gli Organismi di Certificazione che aderiscono al CCRA, incluso lo Schema italiano, rappresentato dall'OCSI, condividono i seguenti obiettivi:

- a) assicurare che le valutazioni di

prodotti/sistemi IT e Profili di Protezione (*Protection Profiles* - PP) vengano condotte applicando i Common Criteria in maniera coerente e rigorosa, in modo da contribuire in maniera sostanziale ad aumentare il livello di fiducia nell'effettiva sicurezza di tali prodotti e PP;

- b) incrementare il numero di prodotti/sistemi IT e Profili di Protezione certificati disponibili;
- c) eliminare l'onere della duplicazione delle certificazioni di sicurezza nei diversi ambiti nazionali;
- d) aumentare costantemente l'efficienza ed il rapporto costo-efficacia delle certificazioni di sicurezza.

Lo scopo ultimo del CCRA, attraverso il perseguimento dei succitati obiettivi, è quello di giungere alla situazione in cui un qualsiasi prodotto/sistema IT o Profilo di Protezione che abbia ottenuto una certificazione Common Criteria possa essere adottato ed utilizzato in ambito internazionale senza che sia necessario procedere ad ulteriori valutazioni. Questo in virtù di una piena condivisione di giudizio da parte degli Organismi di Certificazione aderenti sul livello di affidabilità degli altri partecipanti, sulla base del mutuo riconoscimento degli elevati standard di applicazione dei Criteri di valutazione adottati.

2.3 I diversi ruoli all'interno del CCRA

I partecipanti al CCRA sono organizzazioni o agenzie governative rappresentative degli Schemi di certificazione dei rispettivi paesi. I partecipanti possono essere produttori di certificati, semplici "consumatori", ossia utilizzatori di certificati emessi in altri paesi, oppure avere entrambe le funzioni.

I già citati partecipanti definiti come *Certificate Authorising* (Produttori di Certificati), sono rappresentativi di Organismi di Certificazione operanti nei rispettivi paesi ed hanno la funzione di autorizzare i certificati emessi da tali Organismi. Nel caso in cui un *Certificate Authorising Participant* sia anche direttamente responsabile dell'organizzazione e della gestione delle risorse e delle competenze che costituiscono un Organismo di Certificazione, viene definito come *Qualified Participant* (Partecipante Accreditato).

Naturalmente, al di là delle riconosciute capaci-

tà intrinseche dei diversi Organismi di produrre certificazioni affidabili e di indubbia qualità, va tenuto conto del fatto che il riconoscimento della validità di una certificazione condotta in un'altra nazione non può prescindere dalle prerogative dei singoli governi, qualora si tratti di Organismi di diretta espressione governativa, come è il caso dell'OCSI, che possono essere chiamati ad esprimere pareri e a prendere decisioni che coinvolgono attori appartenenti alla sfera pubblica, sotto il diretto controllo dello Stato. Anche per questo motivo, gli accordi del CCRA considerano nettamente distinta la funzione di semplice produzione di certificati da quella di autorizzazione, che sottintende il mutuo riconoscimento.

2.4 Gruppi di lavoro

I rappresentanti degli Schemi nazionali aderenti al CCRA si riuniscono periodicamente, di norma due volte l'anno, per verificare da un lato la corretta applicazione dello standard e dall'altro per migliorarne l'efficacia attraverso integrazioni e aggiornamenti.

In particolare, le riunioni del CCRA si articolano in diversi gruppi di lavoro:

- il DB (*Development Board*) è un gruppo di lavoro prettamente tecnico che ha il compito di coordinare le attività di lavoro sui vari temi ritenuti di interesse generale, quali ad esempio le politiche di gestione e mantenimento delle certificazioni, la strategia di marketing, la gestione del sito web, ecc. Una volta individuato il tema di interesse, si istituisce un gruppo di lavoro che procede alla definizione di un documento specifico su quel tema, da sottoporre all'approvazione nella successiva riunione. Naturalmente fra queste attività è compresa quella che riguarda la revisione e l'aggiornamento dei criteri di valutazione. Anzi, data la particolare importanza dell'argomento, è stato istituito un gruppo di lavoro permanente al riguardo, denominato MB (*Maintenance Board*).
- l'ES (*Executive Subcommittee*) è un organo strategico-decisionale che si occupa di programmare le principali attività di interesse comune, quali ad esempio l'organizzazione dell'annuale conferenza internazionale sui Common Criteria (ICCC), ospitata a rota-

zione da tutti i Paesi aderenti; inoltre, ha il compito di vagliare le richieste dei nuovi Schemi candidati a diventare Schemi Produttori, attraverso la cosiddetta "valutazione ombra", pianificando il calendario e le modalità operative di tali valutazioni

- l'MC (*Management Committee*) si riunisce di norma solo una volta l'anno e comprende i Direttori di tutti gli Schemi aderenti al CCRA. Questo gruppo ha essenzialmente un compito di ratifica dei risultati ottenuti dai gruppi precedenti, nonché di coordinamento tra tutti gli Schemi, anche di quelli che in tali gruppi non sono rappresentati.

2.5 Condizioni per il mutuo riconoscimento

Gli accordi del CCRA stabiliscono che ogni partecipante riconosca la validità dei certificati Common Criteria emessi dai partecipanti *Authorising* (o *Qualified*). L'autorizzazione dei certificati emessi dagli Organismi rappresentati da tali partecipanti vale quale conferma del fatto che i processi di valutazione e certificazione sono stati condotti in maniera professionale, in osservanza dei requisiti richiesti dal CCRA stesso.

Tali requisiti prevedono che i Laboratori che svolgono materialmente le valutazioni siano stati accreditati nei rispettivi paesi da un Ente accreditante in accordo con la norma europea EN 45001 (od una sua interpretazione approvata da tutti i partecipanti) o che siano stati abilitati da un Organismo di Certificazione riconosciuto, responsabile della gestione e applicazione del corrispondente Schema nazionale. Per quanto riguarda gli Organismi di certificazione stessi, questi debbono essere stati accreditati similmente ai Laboratori oppure istituiti per legge, o secondo procedure amministrative equivalenti, valide nel paese di appartenenza (questo è ad esempio il caso dell'OCSI, istituito per decreto).

Allo scopo di assicurare l'applicazione coerente ed armonica dei Common Criteria da parte di tutti gli Schemi e Organismi di Certificazione, gli accordi del CCRA prevedono che i partecipanti collaborino attraverso lo scambio di informazioni e lo svolgimento regolare di discussioni volte a risolvere dubbi e differenze di interpretazione dei Criteri stessi.

Inoltre, è responsabilità degli Organismi di Certificazione provvedere ad una costante verifica

dei processi di valutazione in corso nell'ambito degli Schemi di appartenenza, onde assicurare che i Laboratori di Valutazione accreditati lavorano secondo gli standard qualitativi e professionali richiesti e, in particolare:

- a) conducono le valutazioni in modo imparziale;
- b) applicano i Common Criteria e la CEM correttamente e in maniera coerente con gli altri Schemi aderenti;
- c) proteggono in maniera adeguata la confidenzialità delle informazioni riservate relative agli ODV valutati.

Allo scopo di verificare che tutti i partecipanti continuano nel tempo a soddisfare i requisiti e gli scopi del CCRA, gli accordi prevedono che vengano effettuate, ad intervalli regolari di tempo, delle verifiche di controllo, da parte di rappresentanti di *Qualified Participant*, degli Organismi di Certificazione riconosciuti. Queste verifiche includono la procedura cosiddetta di "valutazione ombra" (*Shadow Certification/Evaluation*).

3. La valutazione ombra

Come già accennato in precedenza, per accedere pienamente al mutuo riconoscimento delle proprie certificazioni, ciascuno Schema aderente al CCRA deve sottoporsi ad una particolare procedura di controllo, la cosiddetta "valutazione ombra".

Il Comitato Direttivo (*Management Committee*) del CCRA, l'organo gestionale del gruppo, in cui sono presenti rappresentanti di tutti gli Schemi partecipanti, ha facoltà di incaricare uno o più *Qualified Participants* (Partecipanti Accreditati) a sottoporre alla verifica di controllo uno degli Organismi di Certificazione non ancora riconosciuti come *Authorising*. Di norma la verifica avviene dietro esplicita richiesta dei rappresentanti dello Schema corrispondente, che sottopongono volontariamente la propria candidatura.

La valutazione ombra si svolge secondo regole omogenee stabilite dal Comitato Direttivo con lo scopo di assicurare che i controlli vengano eseguiti secondo uno standard uniforme. I partecipanti coinvolti nelle verifiche nominano una squadra di ispettori (*assessment team*) composta da due

membri, ai quali possono aggiungersi altri esperti in rappresentanza di altri partecipanti, con la sola qualifica di osservatori.

In una prima fase, che precede di un mese la visita degli ispettori presso la sede di competenza, l'Organismo sotto controllo deve fornire tutta la documentazione dello Schema in vigore al momento. Gli ispettori esaminano la documentazione allo scopo di verificare che l'Organismo esaminato persegua effettivamente gli scopi del CCRA. La documentazione, che deve essere fornita in lingua inglese, deve comprendere, tra l'altro:

1. una descrizione completa degli scopi, dell'organizzazione e delle funzioni dello Schema, incluso il Manuale di Qualità dell'Organismo di Certificazione e tutte le procedure che governano i processi di Valutazione e Certificazione;
2. la lista aggiornata dei prodotti certificati;
3. una dichiarazione riguardante gli eventuali effetti sulla conduzione delle valutazioni/certificazioni e sull'imparzialità dell'Organismo di leggi e vincoli di tipo amministrativo in vigore nel Paese di appartenenza.

Successivamente, ha inizio la valutazione ombra vera e propria, che prevede la disamina della documentazione prodotta durante le valutazioni di due prodotti IT, condotte secondo lo standard Common Criteria ai livelli di garanzia EAL3 e EAL4. Almeno una delle due valutazioni deve necessariamente essere di livello EAL4. Non è strettamente necessario che entrambe le valutazioni siano state portate a termine: è ritenuto sufficiente per una delle due che sia stato condotto almeno un primo ciclo completo di tutte le attività previste nel Piano di Valutazione, in accordo con il livello di valutazione richiesto (le attività svolte debbono includere anche le attività di analisi delle vulnerabilità, i test funzionali e di penetrazione).

Per ognuna delle valutazioni sottoposte a verifica, l'Organismo deve mettere a disposizione del *team* di verifica il seguente materiale

- a) il Traguardo di Sicurezza (*Security Target*);
- b) il Rapporto Finale di Valutazione (se disponibile);
- c) la documentazione intermedia prodotta, quali i Rapporti di Attività dei Laboratori ed eventuali commenti dell'Organismo su parti-

- colari aspetti della valutazione;
- d) il Rapporto di Certificazione (se disponibile).

Tutta la documentazione prodotta deve essere resa disponibile in lingua inglese, con l'eccezione dei Rapporti di Attività e del rapporto Finale di Valutazione, la cui traduzione, anche parziale, può essere richiesta a discrezione del *team* di verifica. In ogni caso, i rappresentanti dell'Organismo sotto esame sono tenuti a compiere ogni sforzo necessario per agevolare la comprensione della documentazione da parte dei membri del *team* di verifica, evitando di porre ostacoli o resistenze allo svolgimento della valutazione ombra.

La scelta delle valutazioni da sottoporre ad esame deve essere preventivamente concordata tra i partecipanti direttamente coinvolti nella procedura di verifica ed è prevista la stipula di un contratto di non divulgazione di eventuali informazioni sensibili contenute nella documentazione messa a disposizione degli ispettori.

Affinché l'Organismo di Certificazione sottoposto alla valutazione ombra superi la verifica con successo, gli esperti facenti parte del *team* di verifica debbono ottenere evidenze sufficienti a convincerli che tale Organismo ha agito in maniera coerente ed aderente ai requisiti imposti dai Common Criteria e dal CCRA in tutte le fasi e per tutti gli aspetti concernenti i processi di valutazione e certificazione. A tal fine, l'Organismo sotto esame è tenuto a collaborare fattivamente e costruttivamente con gli ispettori.

Oltre alla parte puramente tecnica, riguardante l'applicazione dei Criteri di valutazione, la verifica riguarda anche tutti gli aspetti procedurali e di qualità concernenti la corretta applicazione da parte dell'Organismo di Certificazione delle regole che governano lo Schema nazionale, nel rispetto delle norme di qualità previste nello standard UNI CEI EN 4501 I. Particolare enfasi viene data alle procedure messe in atto per assicurare la confidenzialità delle informazioni riservate conservate presso i locali dell'Organismo e dei Laboratori accreditati. Queste includono tutta la documentazione di valutazione prodotta dai Committenti e dai Fornitori degli ODV certificati o in fase di certificazione, tutta la documentazione prodotta dai Laboratori e dall'Organismo stesso e, infine, gli stessi ODV che possono essere completamente o in parte installati presso i Laboratori di Valutazione.

Al termine della visita ispettiva, che di norma dura una settimana (cinque giorni lavorativi), gli esperti inviati dal CCRA riferiscono le loro conclusioni al Comitato Direttivo, eventualmente corredate da raccomandazioni volte a correggere o a migliorare gli aspetti rivelatisi non completamente conformi ai requisiti. Il Comitato Direttivo del CCRA visiona il rapporto con le risultanze della valutazione ombra e, una volta verificata la correttezza delle conclusioni, in relazione alle evidenze prodotte, lo trasmette all'Organismo che è stato sottoposto a verifica.

3.1 I risultati della valutazione ombra dell'OCSI

Come già detto in precedenza, l'OCSI ha da tempo richiesto il cambiamento di status per divenire Schema Produttore di certificati e accedere così al riconoscimento delle proprie certificazioni in tutti i Paesi che applicano uno Schema nazionale di certificazione della sicurezza di prodotti e sistemi IT aderenti al CCRA (*Common Criteria Recognition Arrangement*). Conseguentemente sono state avviate le attività relative alla "valutazione ombra", che ha avuto il suo momento culminante dal 15 al 19 dicembre 2008 con la visita ispettiva presso la sede dell'ISCOM di un gruppo di commissari degli organismi di certificazione esteri: Spagna (Presidente) e Germania in qualità di ispettori, mentre Norvegia e Turchia hanno ricoperto il ruolo di osservatori. Gli ispettori hanno controllato i processi di certificazione svolti dall'OCSI, unitamente al rispetto delle norme di qualità. Al termine, hanno stilato un rapporto finale della visita ispettiva, che è stato trasmesso al gruppo ES del CCRA per la discussione e l'approvazione.

Nel rapporto gli ispettori, oltre a ringraziare tutto il personale dell'OCSI per la fattiva collaborazione fornita nel corso della visita, al fine di rispondere a tutte le loro richieste e offrire solu-

zioni ai problemi sollevati, hanno rimarcato alcuni punti di forza da loro riscontrati nelle attività svolte dall'OCSI, che prevedono un continuo scambio di informazioni e di esperienze tra i certificatori durante lo svolgimento dei processi di certificazione. In particolare, è stata molto apprezzata la procedura adottata dall'OCSI per l'accreditamento dei propri Laboratori di Valutazione, che viene rilasciato solo dopo aver sottoposto i candidati valutatori di ogni laboratorio ad accurate verifiche di competenza preliminari, che consentono di ottenere una dettagliata matrice delle loro competenze.

Ciò si differenzia dalla procedura seguita dalla maggior parte degli altri Schemi, che preferiscono invece controllare direttamente i nuovi valutatori durante l'esecuzione delle prime valutazioni, considerate per questo come valutazioni di prova. Tale procedura è stata ulteriormente apprezzata perché condivisa anche dai rappresentanti di alcuni laboratori, intervistati dagli ispettori durante la visita.

Il rapporto stilato dagli ispettori sulla valutazione ombra dell'OCSI è stato discusso a lungo e infine approvato proprio di recente, nella riunione del CCRA tenutasi dal 24 al 27 marzo 2009 a Baltimora (USA). Con l'approvazione del rapporto stilato dagli ispettori si è finalmente concluso l'iter della valutazione ombra con la conseguente "promozione" dell'OCSI al rango di Schema Produttore di certificati, che consentirà anche alle certificazioni rilasciate in Italia di essere riconosciute in tutti i paesi aderenti al CCRA.

Tale promozione costituisce il raggiungimento di un obiettivo strategico non solo dell'OCSI, ma anche delle Istituzioni italiane nell'ambito della sicurezza (ANS e Ministero della Difesa), degli enti pubblici interessati a certificare i loro prodotti informatici e delle aziende private che operano a livello nazionale e internazionale negli ambiti della sicurezza.

Riferimenti

- [1] DPCM - "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione", 30 ottobre 2003 (GU n. 98 del 27 aprile 2004)
- [2] CCMB-2006-09-001, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model", versione 3.1, settembre 2006
- [3] CCMB-2007-09-002, "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components", versione 3.1, settembre 2007
- [4] CCMB-2007-09-003, "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components", versione 3.1, settembre 2007
- [5] CCMB-2007-09-004, "Common Evaluation Methodology for Information Technology Security Evaluation", versione 3.1, settembre 2007
- [6] Sito Web dei Common Criteria: www.commoncriteriaportal.org
- [7] Information Technology Security Evaluation Criteria, versione 1.2, giugno 1991
- [8] Information Technology Security Evaluation Manual, versione 1.0, settembre 1993
- [9] Sito Web dell'OCSI: www.ocsi.isticom.it
- [10] OCSI - Linea Guida Provvisoria LGP1, "Descrizione generale dello Schema nazionale di valutazione e certificazione della sicurezza", versione 1.0, dicembre 2004
- [11] OCSI - Linea Guida Provvisoria LGP2, "Accreditamento degli LVS e abilitazione degli Assistenti", versione 1.0, dicembre 2004
- [12] OCSI - Linea Guida Provvisoria LGP3, "Procedure di valutazione", versione 1.0, dicembre 2004
- [13] OCSI - Linea Guida Provvisoria LGP4, "Attività di valutazione secondo i Common Criteria", versione 1.0, dicembre 2004
- [14] OCSI - Linea Guida Provvisoria LGP5, "Il Piano di Valutazione: indicazioni generali", versione 1.0, dicembre 2004
- [15] OCSI - Linea Guida Provvisoria LGP6, "Guida alla scrittura dei Profili di Protezione e dei Traguardi di Sicurezza", versione 1.0, dicembre 2004
- [16] OCSI - Linea Guida Provvisoria LGP7, "Glossario e terminologia di riferimento", versione 1.0, dicembre 2004
- [17] OCSI - Nota Informativa dello Schema N. 1/07, "Modifiche alla LGP1", versione 1.0, marzo 2007
- [18] OCSI - Nota Informativa dello Schema N. 2/07, "Modifiche alla LGP2", versione 1.0, marzo 2007
- [19] OCSI - Nota Informativa dello Schema N. 3/07, "Modifiche alla LGP3", versione 1.0, marzo 2007
- [20] CCRA - "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", maggio 2000