Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione

Organismo di Certificazione

Glossario di riferimento

Linee Guida Provvisorie - parte 7

LGP7

Dicembre 2004
Versione 1.0

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

L'elenco delle aggiunte e varianti al documento verrà mantenuto aggiornato in modo tale da riportare tutti gli emendamenti effettuati sul presente documento.

Paragrafo e/o linea	Pagine modificate	Modifica effettuata da: nominativo e firma	Data

INDICE

1 Glossario dei termini nell’ambito dello Schema

Accreditamento	Riconoscimento formale dell’indipendenza, dell’affidabilità e della competenza tecnica di un Laboratorio per la Valutazione della Sicurezza
Action	vedi *Azione*
Activity	vedi *Attività*
Addendum al Certificato	Documento che viene allegato al Certificato e che contiene le annotazioni relative alle modifiche apportate ad un ODV iscritto allo Schema di Gestione dei Certificati
Aggiunta	L'operazione di aggiungere uno o più componenti di garanzia tratti dalla parte terza dei CC a un Pacchetto già definito. Ad esempio, è possibile effettuare un'aggiunta di componenti di garanzia ad un EAL.
Algoritmo crittografico	Un insieme di regole matematiche per trasformare i dati di input in un output sulla base di altri parametri di input quali le chiavi crittografiche ed i vettori di inizializzazione
Analisi dell’impatto sulla sicurezza	Analisi delle modifiche apportate all’ODV effettuata al fine di stabilire se le modifiche apportate all’ODV risultino tali da richiedere una ri-valutazione o se possano dare luogo ad un aggiornamento del Certificato nell’ambito del PGC
Analisi di vulnerabilità	Processo che consiste nello svolgere una ricerca sistematica di vulnerabilità nell'ODV, e nel valutare le vulnerabilità eventualmente individuate allo scopo di determinare la loro rilevanza nell'ambiente operativo che è stato previsto per l'ODV.
Assegnazione	Operazione di specificazione libera del valore di un parametro di un elemento (vedi Parametro)
Assets	vedi *Beni*
Assignment	vedi *Assegnazione*
Assistente	Persona formata, addestrata e abilitata dall’Organismo di Certificazione a fornire assistenza
Assistenza	Attività di supporto tecnico, inerente la sicurezza nel settore della tecnologia dell’informazione, fornita durante la fase di preparazione alla valutazione di un sistema/prodotto/PP
Assurance	vedi *Garanzia*
Attack potential	vedi *Potenziale di attacco*
Attività	Termine utilizzato per descrivere l'applicazione di una classe di garanzia definita nella terza parte dei Common Criteria.
Attributo di sicurezza	Informazione associata a Soggetti, Utenti o Oggetti che viene usata per applicare e far rispettare la TSF
Augmentation	vedi *Aggiunta*
Authentication data	vedi *Dati di autenticazione*
Authorized user	vedi *Utente autorizzato*
Azione	Termine utilizzato per descrivere l'applicazione di un elemento di garanzia definito nella terza parte dei Common

	Criteria. All'interno dei componenti di garanzia definiti nella terza parte dei Common Criteria, le azioni possono essere dichiarate in modo esplicito come azioni del Valutatore, oppure essere fatte derivare in modo implicito dalle azioni del Fornitore (azioni del Valutatore di tipo implicito).
Beni	Informazioni o risorse che devono essere protette mediante le contromisure realizzate da un OdV
Canale di comunicazione interno	Un canale di comunicazione tra parti distinte dell'OdV
Canale fidato	Un mezzo mediante il quale una Funzione di Sicurezza dell'ODV e un Prodotto IT remoto e fidato possono comunicare tra loro, assicurando al contempo la realizzazione della Politica di Sicurezza dell'OdV
Certificato	Documento formale e pubblico che conferma i risultati di una valutazione e la corretta applicazione dei Criteri ITSEC e della relativa Metodologia, o dei Common Criteria e della Common Evaluation Methodology
Certificato di Accreditamento	Documento formale e pubblico che attesta l'idoneità di un LVS ad operare all'interno dello Schema nazionale
Certificatore	Persona facente parte dell'organico dell'Organismo di Certificazione e da quest'ultimo formata, addestrata e abilitata a condurre le attività di certificazione
Certificazione	L'attestazione da parte dell'Organismo di Certificazione che conferma i risultati della Valutazione, la corretta applicazione dei criteri adottati e della relativa metodologia
Checksum crittografico	Un valore relativamente corto derivato dai dati per mezzo di un algoritmo crittografico. E' funzione di dati, di una chiave segreta, e eventualmente, di un vettore di inizializzazione ed è generalmente allegato ai dati al fine di permetterne la verifica dell'integrità. Vedere anche "Message Authentication Code" in [ISO1].
Chiave crittografica	Un valore che controlla l'esecuzione di un algoritmo crittografico ed il suo risultato. Vedere anche "Key" in [ISO1].
Chiave privata	E' l'elemento della coppia di chiavi destinato ad essere conosciuto dal solo soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico, o si decifra il documento informatico in precedenza cifrato tramite la chiave pubblica corrispondente
Chiave pubblica	E' l'elemento della coppia di chiavi destinato ad essere reso pubblico, e con il quale si verifica la firma digitale del titolare della coppia di chiavi, o si cifrano i documenti informatici da trasmettere al titolare della coppia delle predette chiavi
Chiave segreta (o simmetrica)	Una chiave utilizzata con un algoritmo crittografico sia per la cifratura che per la decifratura
Class	vedi *Classe*
Classe	Il raggruppamento di ordine gerarchico più elevato di requisiti di sicurezza. I requisiti di sicurezza che appartengono ad una stessa Classe si riferiscono ad uno stesso ambito, ma contribuiscono al raggiungimento di obiettivi di sicurezza che possono essere anche diversi. I requisiti di sicurezza che appartengono ad una stessa Classe sono suddivisi in Famiglie

Committente	La persona fisica, giuridica o altro organismo o associazione che commissiona e sostiene gli oneri economici della valutazione e certificazione e che può anche rivestire il ruolo di Fornitore
Compito (sottocompito)	Termine usato per indicare ogni lavoro di valutazione che è richiesto in modo specifico dalla metodologia di valutazione, e che non deriva in modo diretto dai requisiti definiti dallo standard dei Common Criteria
Component	vedi *Componente*
Componente	Un Componente descrive un insieme specifico di requisiti di sicurezza. Un Componente è l'insieme più piccolo di requisiti di sicurezza che può essere incluso in un Pacchetto, in un PP o in un TDS. I Componenti sono costituiti da un insieme di Elementi. I Componenti sono raggruppati gerarchicamente in Famiglie e Classi
Connectivity	vedi *Connettività*
Connettività	La caratteristica dell'OdV che consente l'interazione tra l'OdV stesso e Entità IT Esterne
Coppia di chiavi pubbliche	Una coppia di chiavi matematicamente correlate, in cui dovrebbe essere computazionalmente impossibile derivare la chiave privata a partire dalla corrispondente chiave pubblica
Cryptographic algorithm	vedi *Algoritmo crittografico*
Cryptographic checksum	vedi *Checksum crittografico*
Cryptographic function	
Cryptographic functionality	vedi *Funzionalità crittografica*
Cryptographic key	vedi *Chiave crittografica*
Cryptographic mechanism	vedi *Meccanismo crittografico*
Cryptographic Variable	vedi *Variabile crittografica*
Dati di utente	Dati creati da e per l'utente che non influenzano il funzionamento delle Funzioni di Sicurezza dell'ODV
Dati delle Funzioni di Sicurezza dell'OdV	Dati creati da e per l'ODV che potrebbero influenzare il funzionamento dell'ODV
Dati di autenticazione	Informazioni utilizzate per verificare l'identità dichiarata da un utente
Dependency	vedi *Dipendenza*
Digital signature	vedi *Firma digitale*
Dipendenza	Una relazione tra Componenti tale per cui il raggiungimento degli obiettivi di sicurezza del Componente dipendente è possibile, in generale, solo nel caso in cui siano soddisfatti i requisiti del Componente da cui dipende. I CC individuano, per ognuno dei Componenti definiti nelle parti seconda e terza, l'elenco completo delle eventuali dipendenze che devono essere rispettate. Eventuali deroghe a una relazione di dipendenza devono essere motivate secondo le modalità stabilite dai CC
Disponibilità delle informazioni	Proprietà tesa a consentire l’accesso e l’utilizzo di informazioni su richiesta di entità autorizzate

Element	vedi *Elemento*
Elemento	Un requisito di sicurezza indivisibile nell'ambito dei CC. Un Elemento costituisce la formulazione dei requisiti di sicurezza a più a basso livello di dettaglio. Un Elemento costituisce l'unità elementare che può essere sottoposta a verifica nel corso del processo di Valutazione
Entità IT esterna	Un qualsiasi Prodotto o Sistema IT, fidato o non fidato, che è esterno all'ODV e interagisce con quest'ultimo
Estensione	L'operazione di aggiungere ad un TDS o ad un PP dei requisiti funzionali non contenuti nella parte seconda dei CC o dei requisiti di garanzia non contenuti nella parte terza dei CC
Estensione del controllo delle funzioni di sicurezza dell'OdV	L'insieme delle interazioni che coinvolgono l'ODV, o che avvengono al suo interno, e che sono soggette alle regole stabilite dalla Politica di Sicurezza dell'ODV
Evaluation authority	vedi *Organismo di certificazione*
Evaluation deliverable	vedi *Risorsa per la valutazione*
Evaluation scheme	vedi *Schema*
Evaluation Tecnical Report (ETR)	vedi *Rapporto Finale di Valutazione*
Exploitable vulnerability	vedi *Vulnerabilità sfruttabile*
Extension	vedi *Estensione*
External IT entity	vedi *Entità IT esterna*
Famiglia	Un insieme di requisiti di sicurezza che sono orientati al raggiungimento dello stesso obiettivo di sicurezza, ma che si possono differenziare per l'enfasi o per il rigore delle specifiche imposte
Family	vedi *Famiglia*
Fiducia	vedi *Garanzia*
Firma digitale	Il risultato di una procedura informatica, che consente: – la sottoscrizione di un documento informatico; – la verifica, da parte dei destinatari, dell'identità del soggetto firmatario; – la sicurezza della provenienza e della ricezione del documento; – la certezza che l'informazione contenuta nel documento non sia stata alterata; – la prova della trasmissione del documento (time stamping). Vedere anche [ISO1].
Formal	vedi *Formale*
Formale	Espresso in un linguaggio dalla sintassi ristretta con una semantica ben definita basate su concetti matematici consolidati
Fornitore	Persona fisica, giuridica o altro organismo o associazione che fornisce l'ODV e che può rivestire il ruolo di Committente
Funzionalità crittografica	Una o più funzioni crittografiche inserite in un ODV
Funzione crittografica	Uno dei calcoli effettuati con un algoritmo crittografico. Esempio: cifratura, decifratura, generazione della firma digitale, verifica della firma digitale, ecc.

Funzioni di sicurezza (FS)	Contromisure di tipo tecnico di cui è dotato l'ODV sulle quali si fa affidamento per realizzare un sottoinsieme di regole contenute nella politica di sicurezza dell'ODV stesso.
Garanzia	Il termine garanzia (o fiducia), è utilizzato con riferimento alla capacità che l'ODV mostra nel soddisfare i propri obiettivi di sicurezza, considerando le minacce e l'ambiente descritti nel TDS. La garanzia è tipicamente assicurata a vari livelli da un processo di valutazione formale.
Hash	Codice o sequenza di bit che viene utilizzata per verificare se dei dati (una email, un certificato digitale o qualsiasi altra cosa) sono stati in qualche modo alterati
Hash sicuro	Il risultato dell'applicazione ad un messaggio di un algoritmo tale che risulti computazionalmente inattuabile derivare il messaggio dal risultato e tale che sia anche bassa la probabilità che input diversi generino lo stesso valore di hash
Human user	vedi *Utente umano*
Identità	Una rappresentazione (ad esempio una stringa alfanumerica) che identifica in maniera univoca un utente autorizzato
Identity	vedi *Identità*
Impronta	La sequenza di bit di lunghezza predefinita generata mediante l'applicazione sui dati di una opportuna funzione di hash
Informal	vedi *Informale*
Informale	Espresso in un linguaggio naturale
Initialization Vector	vedi *Vettore di inizializzazione*
Interfaccia delle funzioni di sicurezza dell'ODV	L'insieme delle interfacce mediante le quali si accede, tramite le funzioni di sicurezza dell'ODV, alle risorse dell'ODV, o si ottengono informazioni direttamente dalle funzioni di sicurezza dell'ODV. Tali interfacce possono essere o interattive (interfacce uomo-macchina) o di programma (API)
Internal communication channel	vedi *Canale di comunicazione interno*
Internal TOE transfer	vedi *Trasferimento interno all'ODV*
Interpretazione	Un chiarimento o un'estensione di un requisito introdotto dai Common Criteria, dal CEM o da uno Schema.
Inter-TSF transfer	vedi *Trasferimento fra TSF*
Ispettore	Figura abilitata dall'OC per condurre le verifiche previste nella procedura di accreditamento di un LVS.
Iteration	vedi *Iterazione*
Iterazione	L'operazione di utilizzare più di una volta, in un PP o in un TDS, un Componente, associando ad ogni occorrenza una operazione diversa dalle altre occorrenze
Laboratorio per la Valutazione della Sicurezza (LVS)	Organizzazione indipendente che ha ottenuto l'Accreditamento e che pertanto è abilitata ad effettuare

	valutazioni e a fornire assistenza
Linee Guida	Pubblicazione tecnica che fornisce informazioni dettagliate relative alla conduzione ed allo svolgimento delle attività inerenti il processo di Valutazione e Certificazione
Livello di garanzia	La misura della garanzia espressa mediante identificatori alfanumerici la cui parte numerica cresce con il crescere della fiducia (in ITSEC: da E1 a E6; nei Common Criteria: da EAL1 ad EAL7).
Materiale per la Valutazione	Risorse per la valutazione di tipo materiale, cioè, la documentazione tecnica o le componenti software, hardware, firmware realizzati durante lo sviluppo del sistema o del prodotto. Può contenere informazioni riservate.
Meccanismo crittografico	Un processo od una tecnica che coinvolge una o più funzioni crittografiche
Meccanismo di sicurezza	Le specifiche soluzioni hardware, software e firmware che realizzano le funzioni di sicurezza di cui è dotato l'ODV.
Meccanismo di validazione di riferimento	Una implementazione del concetto di Monitor di riferimento che è a prova di manomissione, è sempre richiamata ed è sufficientemente semplice per essere sottoposta ad un'analisi e ad una verifica minuziose
Message Digest	vedi *Impronta*
Metodologia	Il sistema di principi, procedure e processi che è applicato a una valutazione della sicurezza IT
Modello della politica di Sicurezza dell'OdV	Una rappresentazione strutturata della politica di sicurezza che deve essere attuata dall'ODV
Monitor di riferimento	Il concetto di una macchina astratta che applica e fa rispettare le politiche di controllo d'accesso
Non repudiation	vedi *Non ripudio*
Non ripudio	L'impossibilità per una entità di negare di aver preso parte ad una comunicazione
Obiettivo di sicurezza	Una dichiarazione d'intenti, fatta in un PP o in un TDS, al fine di contrastare minacce identificate e/o verificare ipotesi e politiche di sicurezza ben specificate
Object	vedi *Oggetto*
Observation Report	vedi *Rapporto di Osservazione*
Obvious vulnerability	vedi *Vulnerabilità evidente*
Oggetto	Una entità all'interno del TSC che contiene o riceve informazioni e sulla quale i soggetti eseguono operazioni
Oggetto della Valutazione (ODV)	Un prodotto o un sistema IT che, unitamente alla documentazione destinata agli utenti e agli amministratori, è sottoposto al processo di valutazione secondo i criteri e la metodologia adottati.
Organismo di Certificazione (OC)	Organizzazione nazionale indipendente e imparziale che esegue la Certificazione di sistemi, prodotti, PP e l'accreditamento dei Laboratori per la Valutazione della Sicurezza

Organisational security policies (OSP)	vedi *Politiche di sicurezza di un'organizzazione*
Pacchetto	Nei CC, un insieme di Componenti, di tipo funzionale o di garanzia, che si è dimostrato efficace per soddisfare specifici obiettivi di sicurezza. Un pacchetto può essere utilizzato per costruire pacchetti più generali, PP o TDS.
Package	vedi *Pacchetto*
Parameter	vedi *Parametro*
Parametro	Nei CC la definizione completa di alcuni elementi richiede la specificazione di uno o più argomenti. Tali argomenti sono denominati parametri. Il valore di un parametro può essere specificato o in modo libero (sia pure rispettando le regole imposte dai CC), o scegliendo in una lista di valori predefinita. La prima azione è denominata Assegnazione, la seconda Selezione
Penetration testing	vedi *Test di intrusione*
Percorso fidato	Un mezzo mediante il quale un Utente e una Funzione di sicurezza dell'ODV possono comunicare tra loro, assicurando al contempo la realizzazione della Politica di Sicurezza dell'ODV
Piano di Gestione del Certificato (PGC)	Documento che contiene le informazioni, le procedure e l'indicazione dei ruoli necessari per condurre correttamente il mantenimento del Certificato
Piano Di Valutazione (PDV)	Documento che descrive le attività che saranno svolte dall'LVS durante il processo di valutazione, i tempi di esecuzione e le risorse necessarie
Politica della funzione di sicurezza	La politica di sicurezza attuata da una Funzione di Sicurezza
Politica di Sicurezza dell'OdV (PSO)	Un insieme di regole che stabilisce come i Beni debbano essere gestiti, protetti e distribuiti all'interno dell'ODV
Politiche di sicurezza di un'organizzazione (PSO)	Una o più regole, procedure, pratiche o linee guida di sicurezza adottate da un'organizzazione
Potential vulnerability	vedi *Vulnerabilità potenziale*
Potenziale di attacco	Il potenziale di attacco è una stima delle risorse che un attaccante deve possedere per compromettere le funzionalità di sicurezza dell'ODV. Tali risorse devono tenere in conto le conoscenze tecniche, la disponibilità di strumenti hardware e software e le motivazioni dell'attaccante
Private key	vedi *Chiave privata*
Prodotto	Un insieme di elementi software, hardware e/o firmware che svolge una funzione che può essere utilizzata da molti sistemi
Product	vedi *Prodotto*
Profilo di Protezione (PP)	Il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia, definiti secondo i Common Criteria. Un PP ha la finalità di definire un insieme di requisiti che si è dimostrato

	efficace per raggiungere gli obiettivi individuati, sia per quanto riguarda le funzioni di sicurezza, sia per quanto riguarda la garanzia. Un PP fornisce agli utenti uno strumento per fare riferimento ad uno specifico insieme di esigenze di sicurezza, e facilita lo svolgimento di future valutazioni di Prodotti o Sistemi che soddisfino tali esigenze.
Protection Profile	vedi *Profilo di Protezione*
Public key	vedi *Chiave pubblica*
Public key pair	vedi *Coppia di chiavi pubbliche*
Raffinamento	L'operazione di aggiungere dettagli ad un Componente, seguendo, comunque, i vincoli imposti dai CC
Rapporto di Attività (RA)	Documento che l'LVS invia all'Organismo di Certificazione, nel quale sono indicati dettagliatamente i risultati raggiunti e le attività svolte dal Laboratorio stesso durante le varie fasi della valutazione. Può contenere informazioni riservate
Rapporto di Certificazione (RC)	Documento emesso dall'Organismo di Certificazione, che conferma i risultati della valutazione e la corretta applicazione dei criteri
Rapporto di Certificazione dell'accreditamento	Rapporto redatto dalla Commissione Tecnico-consultiva che, sulla base del Rapporto Finale di Accreditamento, esprime l'esito motivato di una procedura di accreditamento
Rapporto di Classificazione delle Componenti dell'ODV (RCC)	Documento che fornisce una classificazione delle componenti dell'ODV secondo la loro rilevanza in termini di sicurezza.
Rapporto di Mantenimento	Documento che viene allegato al Rapporto di Certificazione al fine di attestare il buon esito dell'attività di mantenimento effettuata
Rapporto di Osservazione (RO)	Rapporto dell'LVS per l'OC e il Committente, finalizzato alla segnalazione di anomalie o errori. Può contenere informazioni riservate.
Rapporto Finale di Accreditamento	Rapporto redatto dal Responsabile della Sezione Accreditamento che, sulla base del Rapporto Finale di Visita Ispettiva, descrive l'iter della pratica di accreditamento di un laboratorio.
Rapporto Finale di Valutazione (RFV)	Rapporto prodotto dall'LVS, contenente i risultati della valutazione, che costituisce la base per la Certificazione dell'ODV o del PP. Può contenere informazioni riservate.
Rapporto Finale di Visita Ispettiva	Rapporto redatto dagli Ispettori contenente la descrizione delle attività ispettive effettuate e il loro esito.
Reference monitor	vedi *Monitor di riferimento*
Reference validation mechanism	vedi *Meccanismo di validazione di riferimento*
Refinement	vedi *Raffinamento*
Requisiti di garanzia	Requisiti su cui si basa la fiducia che l'ODV raggiunga gli obiettivi di sicurezza specificati nel TDS. Normalmente, nel caso dei CC, i requisiti di garanzia sono raggruppati in pacchetti predefiniti (EAL) corrispondenti a livelli di garanzia standard.

Requisiti di sicurezza	L'insieme dei requisiti funzionali e di garanzia specificati in un PP, in un TDS o in un pacchetto.
Requisiti funzionali di sicurezza	I Requisiti funzionali di sicurezza descrivono il comportamento di sicurezza che viene richiesto ad un ODV, ed hanno l'obiettivo, se correttamente realizzati, di consentire il raggiungimento degli obiettivi di sicurezza enunciati in un PP o in un TDS.
Residual vulnerability	vedi *Residual vulnerability*
Responsabile per la Gestione del Certificato (RGC)	Persona (o gruppo di persone) che ha il compito di verificare che i processi e le procedure di gestione del Certificato dichiarate nel PGC siano applicati dal Fornitore.
Riservatezza delle informazioni	Proprietà tesa ad impedire l'accesso e la divulgazione non autorizzata di informazioni
Risorsa per la valutazione	Una risorsa necessaria al Valutatore o al Certificatore per svolgere o verificare una o più attività di valutazione, e che deve essere messa a disposizione dal Committente o dal Fornitore.
Robustezza di una funzione	La misura della capacità di una Funzione di Sicurezza di contrastare attacchi diretti condotti con risorse predefinite.
Ruolo	Un insieme predefinito di regole che stabilisce le interazioni consentite tra l'utente e l'ODV
Schema	L'insieme delle procedure e delle regole nazionali necessarie per la Valutazione e Certificazione, in conformità ai criteri europei ITSEC o agli standard internazionali ISO/IEC IS-15408 (Common Criteria) e alle relative metodologie ITSEM e CEM
Schema di Gestione dei Certificati (SGC)	L'insieme delle procedure che permettono di mantenere nel tempo la validità del Cerificato
Secret	vedi *Segreto*
Secret key	vedi *Chiave segreta*
Secure hash	vedi *Hash sicuro*
Security assurance requirement (SAR)	vedi *Requisito di garanzia*
Security attribute	vedi *Attributo di sicurezza*
Security Function Policy (SFP)	vedi *Politica della funzione di sicurezza*
Security Function (SF)	vedi *Funzione di sicurezza*
Security impact analysis	vedi *Analisi dell'impatto sulla sicurezza*
Security objective	vedi *Obiettivo di sicurezza*
Security requirements	vedi *Requisiti di sicurezza*
Security Target (ST)	vedi *Traguardo di sicurezza*
Segreto	Informazione che deve essere conosciuta solo da Utenti autorizzati o dal TSF al fine di realizzare una specifica SFP
Selection	vedi *Selezione*
Selezione	Operazione di scelta del valore di un parametro all'interno di una lista di valori predefiniti (vedi Parametro)
Semiformal	vedi *Semiformale*

Semiformale	Espresso in un linguaggio dalla sintassi ristretta con una semantica ben definita
Sistema	Una specifica installazione IT (software, firmware o hardware), caratterizzata da uno scopo e da un ambiente operativo ben definiti.
System	vedi *Sistema*
SOF basic	Il grado di robustezza di una funzione per la quale l'analisi mostra che la funzione stessa fornisce una protezione adeguata contro violazioni casuali della sicurezza dell'ODV provocate da attaccanti che possiedono un basso potenziale d'attacco
SOF high	Il grado di robustezza di una funzione per la quale l'analisi mostra che la funzione stessa fornisce una protezione adeguata contro violazioni della sicurezza dell'ODV pianificate od organizzate deliberatamente, e provocate da attaccanti che possiedono un elevato potenziale d'attacco
SOF medium	Il grado di robustezza di una funzione per la quale l'analisi mostra che la funzione stessa fornisce una protezione adeguata contro violazioni della sicurezza dell'ODV di tipo diretto o intenzionale, e provocate da attaccanti che possiedono un moderato potenziale d'attacco
Soggetto	Una entità all'interno del TSC che provoca l'esecuzione di operazioni
Sottoattività	Termine utilizzato per descrivere l'applicazione di un componente di garanzia definito nella terza parte dei Common Criteria.
Strength Of Function (SOF)	vedi *Robustezza di una funzione*
Sub-activity	vedi *Sottoattività*
Subject	vedi *Soggetto*
Target of evaluation (TOE)	vedi *Oggetto della valutazione*
Task (sub-task)	vedi *Compito*
Test di intrusione	Test che sono eseguiti con l'obiettivo di determinare se le vulnerabilità potenziali dell'ODV possono essere sfruttate nell'ambiente operativo che è stato previsto per quest'ultimo.
TOE Security Functions (TSF)	vedi *Funzioni di Sicurezza dell'ODV*
TOE Security Functions Interface (TSFI)	vedi *Interfaccia delle Funzioni di Sicurezza dell'ODV*
TOE Security Policy (TSP)	vedi *Politica di sicurezza dell'ODV*
TOE security policy model	vedi *Modello di politica di sicurezza dell'ODV*
Traguardo di Sicurezza (TDS)	Il documento, utilizzato come base per la Valutazione di un ODV, che contiene gli obiettivi di sicurezza, la descrizione dell'ambiente in cui l'ODV è utilizzato e le minacce alle quali è soggetto, i requisiti funzionali e di garanzia, la specifica delle funzioni di sicurezza
Transfer outside TSF control	vedi *Trasferimento fuori dal controllo delle Funzioni di Sicurezza dell'ODV*
Trasferimento fra TSF	Comunicazioni di dati tra l'ODV e le funzioni di sicurezza di altri prodotti IT fidati

Trasferimento fuori dal controllo delle Funzioni di Sicurezza dell'ODV	La comunicazione di dati ad entità fuori dal controllo delle Funzioni di Sicurezza dell'ODV
Trasferimento interno all'ODV	Comunicazione di dati tra parti distinte dell'ODV
Trusted channel	vedi *Canale fidato*
Trusted path	vedi *Percorso fidato*
TSF data	vedi *Dati delle Funzioni di Sicurezza dell'ODV*
TSF Scope of Control (TSC)	vedi *Estensione del controllo delle funzioni di sicurezza dell'OdV*
Unità di lavoro	Espressione usata per indicare il livello più granulare di lavoro di valutazione. Ogni azione riportata nel CEM comprende una o più unità di lavoro che devono essere svolte dal Valutatore.
User	vedi *Utente*
User data	vedi *Dati di utente*
Utente	Ogni entità (utente umano o entità IT) esterna all'ODV che interagisce con l'ODV stesso
Utente autorizzato	Un Utente che, in accordo con la Politica di Sicurezza dell'ODV, può eseguire un'operazione
Utente umano	Qualsiasi persona che interagisca con l'ODV
Valutatore	Persona nell'organico dell'LVS formata, addestrata ed abilitata dall'Organismo di Certificazione a condurre le attività di valutazione
Valutazione	L'analisi di un sistema, prodotto, PP condotta in base a predefiniti criteri applicati secondo una predefinita metodologia.
Valutazione concomitante	Valutazione condotta durante lo sviluppo del sistema o del prodotto
Valutazione consecutiva	Valutazione condotta dopo lo sviluppo del sistema, del prodotto o la redazione del Profilo di Protezione.
Variabile crittografica	Un valore o serie di valori richiesti per il funzionamento di un algoritmo di crittografia al fine di trasformare l'input in output. Esempi di variabile crittografica sono le chiavi crittografiche (segrete, pubbliche, private, ecc), i parametri di chiave pubblica ed i vettori di inizializzazione. Si noti che il testo in chiaro ed i valori hash non sono considerati variabili crittografiche
Verdetto	Una dichiarazione di esito positivo, negativo o in sospeso prodotta da un Valutatore e riferita a un elemento che descrive un'azione che deve essere svolta dal Valutatore, a un componente di garanzia o a una classe. Si veda anche la voce verdetto complessivo.
Verdetto complessivo	Una dichiarazione di esito positivo o negativo che viene prodotta dal Valutatore e che riguarda il risultato di una valutazione.
Vettore di inizializzazione	Un vettore (serie di bit) utilizzato per definire lo stato iniziale per la cifratura all'interno di un algoritmo crittografico.
Virdict	vedi *Verdetto*

Vulnerabilità	Elemento di debolezza che è presente nell'ODV e che può essere sfruttato, in un determinato ambiente operativo, per violare una politica di sicurezza.
Vulnerability	vedi *Vulnerabilità*
Vulnerability analysis	vedi *Analisi di vulnerabilità*
Vulnerabilità evidente	Vulnerabilità che può essere sfruttata disponendo di un livello minimo di comprensione dell'ODV, di competenza tecnica minima e di risorse minime.
Vulnerabilità potenziale	Vulnerabilità di cui, postulando la disponibilità di un percorso d'attacco, si sospetta l'esistenza nell'ODV, ma la cui effettiva presenza non è stata confermata.
Vulnerabilità residua	Vulnerabilità che potrebbe essere sfruttata da un attaccante che fosse in possesso di un potenziale d'attacco superiore a quello che è stato previsto nell'ambiente operativo che è stato ipotizzato per l'ODV. Si tratta, quindi, di un particolare tipo di vulnerabilità che non può essere sfruttata.
Vulnerabilità sfruttabile	Vulnerabilità che può essere sfruttata nell'ambiente operativo che è stato previsto per l'ODV.
Work unit	vedi *Unità di lavoro*

2 Termini di uso specifico in [CCI3]

Nel seguito è riportata una lista dei termini di uso comune che vengono usati secondo un'accezione precisa in [CCI3]. Per ogni termine è riportata la traduzione Italiana e l'accezione con cui è utilizzato.

Assicurare (*Ensure*)	Questo termine, usato da solo, implica una forte relazione di causalità tra un'azione e le sue conseguenze. Questo termine è tipicamente preceduto dall'espressione "contribuisce a", che indica che la conseguenza non è completamente certa, sulla base di quell'unica azione.
Coerente (*Coherent*)	Questo termine è usato per indicare che un'entità è caratterizzata da un ordine logico ed ha un significato comprensibile. Un documento può essere definito coerente se è caratterizzato da una struttura e da un contenuto che risultano adeguati ad assicurare una corretta comprensione delle informazioni contenute nel documento stesso da parte degli utenti a cui quest'ultimo è destinato.
Completo (*Complete*)	Questo termine è usato per indicare che sono state fornite tutte le parti necessarie di una entità. In termini di documentazione, questo significa che la documentazione comprende tutte le informazioni pertinenti, ad un livello di dettaglio tale da non rendere necessari ulteriori chiarimenti a quel livello di astrazione.
Confermare (*Confirm*)	Il verbo confermare è utilizzato per indicare la necessità di eseguire un'operazione di revisione dettagliata, che richiede l'esecuzione, da parte del valutatore, di una determinazione di sufficienza di tipo indipendente. Il livello di rigore richiesto dipende dalla natura dell'oggetto che deve essere sottoposto all'operazione di conferma. Il verbo confermare trova applicazione esclusivamente nella descrizione delle azioni che devono essere svolte dal valutatore.
Congruente (*Consistent*)	Questo termine descrive una relazione tra due o più entità, e indica che non ci sono contraddizioni evidenti tra queste entità.
Contrastare (*Counter*)	Questo termine è utilizzato con riferimento ad una particolare minaccia, per indicare che l'impatto della minaccia stessa è stato in qualche modo attenuato, ma non necessariamente rimosso in modo completo.
Descrivere (*Describe*)	Questo termine indica che devono essere forniti certi specifici dettagli di un'entità.
Determinare (*Determine*)	Questo termine richiede che sia condotta un'analisi indipendente, con l'obiettivo di raggiungere una particolare conclusione. L'uso di questo temine si differenzia da "confermare" o "verificare", dato che questi due termini implicano che sia già stata effettuata un'analisi che deve essere revisionata, mentre l'uso di "determinare" implica un'analisi effettivamente indipendente, solitamente senza che sia stata effettuata alcuna analisi in precedenza.
Dimostrare (*Demonstrate*)	Questo termine si riferisce ad una analisi che conduce ad una conclusione, che è meno rigorosa di una "prova".
Esaustivo (*Exhaustive*)	Questo termine può essere utilizzato per caratterizzare lo svolgimento di un'analisi o di un'altra attività. Il significato è

	affine a quello dell'aggettivo sistematico, ma il termine esaustivo è notevolmente più forte, in quanto, oltre ad indicare che l'analisi o l'attività in oggetto sono state svolte seguendo un piano d'azione non ambiguo e adottando un approccio di tipo metodico, comporta anche che il piano d'azione seguito è sufficiente ad assicurare che sono state esplorate tutte le strade percorribili.
Giustificazione (*Justification*)	Questo termine si riferisce al raggiungimento di una conclusione mediante lo svolgimento di un'operazione di analisi, che richiede un notevole rigore nel fornire la spiegazione accurata e completa di ogni passo del ragionamento logico. Una giustificazione è, quindi, più rigorosa di una semplice dimostrazione.
Internamente congruente (*Internally consistent*)	Questa espressione è utilizzata per indicare l'assenza di contraddizioni evidenti tra i diversi aspetti di un'entità. In particolare, quando è riferita alla documentazione, l'espressione indica che la documentazione stessa non contiene affermazioni che risultano in contrasto tra loro.
Mutuo supporto (*Mutually supportive*)	Questa espressione è impiegata per caratterizzare una relazione tra un insieme di entità, relazione nella quale ogni entità è caratterizzata da proprietà che non ostacolano lo svolgimento dei compiti propri delle altre entità, ma che anzi possono contribuire allo svolgimento di questi ultimi. La determinazione della condizione di mutuo supporto non richiede necessariamente la determinazione del fatto che ciascuna delle entità in esame fornisce un supporto diretto alle altre entità che fanno parte dell'insieme, ma può semplicemente consistere in una determinazione di tipo più generale.
Provare (*Prove*)	Svolgere un'analisi formale in senso matematico, in modo completamente rigoroso. Di solito il termine provare è utilizzato quando si vuole mostrare in modo molto rigoroso la corrispondenza che esiste tra due livelli logici di rappresentazione delle TSF.
Specificare (*Specify*)	Fornire alcuni particolari dettagli che riguardano un'entità, in modo più rigoroso e preciso rispetto a quanto indicato dal verbo descrivere.
Spiegare (*Explain*)	Motivare la linea di condotta tenuta senza cercare di dimostrare che quest'ultima fosse necessariamente quella ottimale. Il verbo spiegare possiede un significato diverso da quello dei verbi descrivere e dimostrare.
Tracciare (*Trace*)	Illustrare la relazione di corrispondenza tra due entità in modo informale, impiegando un livello di rigore minimo.
Verificare (*Verify*)	Eseguire un'operazione di revisione dettagliata, in modo più rigoroso di quanto richiesto dal verbo confermare. Nell'ambito delle azioni che devono essere svolte dal valutatore, il verbo verificare indica la necessità che il valutatore stesso esegua un lavoro di tipo indipendente.

3 Riferimenti bibliografici

[CCI1] CCIMB-2004-01-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, version 2.2, gennaio 2004

[CCI2] CCIMB-2004-01-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, version 2.2, gennaio 2004

[CCI3] CCIMB-2004-01-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, version 2.2, gennaio 2004

[CCR1] CCIMB-2004-02-09 “Assurance Continuity: CCRA Requirements”; febbraio 2004

[CEM1] CEM-97/017, “Common Evaluation Methodology for Information Technology Security Evaluation, Part 1 – Introduction and general model”; version 0.6, gennaio 1997

[CEM2] CCIMB-2004-01-004, “Common Evaluation Methodology for Information Technology Security Evaluation, Part 2 – Evaluation Methodology”, version 2.2, gennaio 2004

[ISO1] ISO/IEC 2382-8 “Information technology – Vocabulary” – Part 8: Security, 1998

[ISO2] ISO/IEC TR 15446 “Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets”, dicembre 2003

[ITS1] Information Technology Security Evaluation Criteria, version 1.2, giugno 1991

[ITS2] Information Technology Security Evaluation Manual, version 1.0, settembre 1993

[UNI1] UNI/CEI EN ISO/IEC 17025 Requisiti generali per la competenza dei laboratori di prova e di taratura, 2000.

4 Lista degli acronimi

EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
IT	=	Information Technology
LVS	=	Laboratorio di Valutazione della Sicurezza
NIL	=	Notifica di Inizio Lavori
NIS	=	Nota Informativa dello Schema
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
OSP	=	(Organisational Security Policy) Politica di Sicurezza di un'Organizzazione
PGC	=	Piano per la Gestione del Certificato
PDV	=	Piano Di Valutazione
PP	=	Profilo di Protezione
RA	=	Rapporto di Attività
RAL	=	Riunione di Avvio dei Lavori
RC	=	Rapporto di Certificazione
RCC	=	Rapporto di Classificazione delle Componenti dell'ODV
RFV	=	Rapporto Finale di Valutazione
RGC	=	Responsabile per la Gestione del Certificato
RM	=	Rapporto delle Metodologie
RO	=	Rapporto di Osservazione
ROA	=	Rapporto di Osservazione: Anomalia
ROE	=	Rapporto di Osservazione: Errore
ROS	=	Rapporto di Osservazione sullo Schema
SAR	=	(Security Assurance Requirement) Requisito di Garanzia
SGC	=	Schema di Gestione dei Certificati
SFP	=	(Security Function Policy) Politica della Funzione di Sicurezza
SFR	=	(Security Functional Requirement) Requisito Funzionale di Sicurezza
SOF	=	(Strength of Function) Robustezza di una Funzione di Sicurezza
TDS	=	Traguardo di Sicurezza (ST – Security Target)
TSF	=	(TOE Security Function) Funzione di Sicurezza dell'ODV
TSP	=	(TOE Security Policy) Politica di Sicurezza dell'ODV
UL	=	Unità di Lavoro