Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/14

(Certification No.)

Prodotto: **FINX RTOS Security Enhanced (SE) v3.1**
(Product)

Sviluppato da: **MBDA Italia S.p.A.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.1)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 21 maggio 2014

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

FINX RTOS Security Enhanced (SE) v3.1

OCSI/CERT/RES/03/2012/RC

Versione 1.0

21/05/2014

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	Federico Filipponi	Prima emissione	21/05/2014

2 Indice

3 Elenco degli acronimi

ACL	Access Control List
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disk - Read-Only Memory
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
DVD-ROM	Digital Versatile Disk - Read-Only Memory
EAL	Evaluation Assurance Level
GB	Gigabyte
IPC	Inter-Process Communication
IT	Information Technology
LGP	Linea Guida Provvisoria
LTP	Linux Test Project
LVS	Laboratorio per la Valutazione della Sicurezza
MD5	Message Digest algorithm 5
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PAM	Pluggable Authentication Module
PP	Profilo di Protezione (Protection Profile)
RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
RHEL	Red Hat Enterprise Linux
RTOS	Real Time Operating System
SAR	Security Assurance Requirement (Requisito di Garanzia)

SATA	Serial Advanced Technology Attachment
SE	Security Enhanced
SFR	Security Functional Requirement (Requisito Funzionale di Sicurezza)
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TDS	Traguardo di Sicurezza (Security Target)
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

4 Riferimenti

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, Version 1.0, May 2000

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[RFV1] Rapporto Finale di Valutazione del prodotto “FINX RTOS SE V3.1”, Versione 1.0, 7 Marzo 2014

[RFV3] Rapporto Finale di Valutazione del prodotto “FINX RTOS SE V3.1”, Versione 3.0, 14 Maggio 2014

[TDS] FINX RTOS SE v3.1 Security Target, ID 16200036572, Rev. 02, 21 Febbraio 2014

[MAN] FINX RTOS SE v3.1 Secure Installation, Configuration & Operations, ID 16200039645, Rev. 02, 21 Febbraio 2014

[BMD] FINX RTOS SE v3.1 – Basic Modular Design, ID 16200036576, Rev. 02, MBDA, 21 Febbraio 2014

[TST] FINX RTOS SE v3.1 – Security Function Verification Test Plan, ID 16200039696, Rev. 02, MBDA, 21 Febbraio 2014

5 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il Sistema Operativo basato su Linux denominato "FINX RTOS Security Enhanced (SE) v3.1", sviluppato dalla società MBDA.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo per la Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G. U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL4, con l'aggiunta di ALC_FLR.1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

6 Riepilogo della valutazione

6.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del Sistema Operativo denominato "FINX RTOS Security Enhanced (SE) v3.1", secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

6.2 Identificazione sintetica della certificazione

Nome dell'ODV	FINX RTOS Security Enhanced (SE) v3.1
Traguardo di Sicurezza	FINX RTOS SE v3.1 Security Target, Rev. 02, 21 Febbraio 2014
Livello di garanzia	EAL4 con aggiunta di ALC_FLR.1
Fornitore	MBDA Italia S.p.A.
Committente	MBDA, FINMECCANICA
LVS	Consorzio RES
Versione dei CC	3.1 (Rev. 4)
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	26 ottobre 2012
Data di fine della valutazione	7 marzo 2014

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

6.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV, denominato "FINX RTOS Security Enhanced (SE) v3.1" (nel seguito anche indicato semplicemente come FINX RTOS o FINX), è un Sistema Operativo di tipo Linux basato sulla distribuzione Gentoo, multi-utente e multi-tasking, adatto ad essere utilizzato sia nel mercato della difesa sia in ambito aerospaziale, industriale, in applicazioni di rete e di elettronica di consumo.

Inoltre, l'ODV è in grado di fornire un contesto di esecuzione predicibile che supporta applicazioni con requisiti real-time. Infatti, FINX RTOS estende il supporto real-time nativo di Linux integrando una *patch* del Kernel Linux denominata PREEMPT_RT. In particolare FINX fornisce le citate caratteristiche real-time in un contesto orientato alla sicurezza.

La valutazione di FINX comprende un insieme potenzialmente distribuito, ma chiuso di sistemi collegati in rete sui quali sia installata la configurazione certificata dello stesso.

I requisiti funzionali di sicurezza dell'ODV sono realizzati dalle seguenti funzioni di sicurezza:

- Identificazione ed autenticazione.
- Controllo Accessi Discrezionale.
- Audit.
- Protezione delle TSF.
- Servizi crittografici.
- Riutilizzo degli oggetti.
- Gestione della sicurezza.

6.3.1 Architettura dell'ODV

6.3.1.1 Hardware

Il Sistema Operativo FINX RTOS SE v3.1 non richiede una specifica piattaforma hardware per operare. Esso può essere installato su una grande varietà di schede e di elaboratori, che comprendono sia workstation e server multi-processore sia singole schede da computer in grado di essere inserite in strutture hardware di tipo dedicato e con particolari caratteristiche di robustezza e resistenza ("ruggedized").

In particolare FINX gira su tutte le piattaforme con architettura Intel, che abbiano almeno i seguenti requisiti minimi:

- Microprocessore: Intel Pentium i686
- Disco rigido: SATA, 40 GB
- Memoria RAM: 1 GB
- Adattatore di rete o lettore CD/DVD (richiesto solo per l'installazione)

L'hardware è considerato parte dell'ambiente operativo dell'ODV e come tale fornisce supporto allo stesso tramite meccanismi opportuni.

La valutazione è stata condotta sulle specifiche piattaforme di seguito elencate:

- **VP417/03x** e **VP717/08x**: schede da computer industriali di tipo commerciale le quali possono anche essere adattate ("customizzate") per soddisfare i requisiti di particolari applicazioni critiche che necessitano di girare su un hardware dedicato. Le caratteristiche delle schede citate sono contenute nella documentazione reperibile agli indirizzi seguenti:
  - http://www.gocct.com/sheets/VP/datasheet/vp71708x.pdf
  - http://www.gocct.com/sheets/VP/datasheet/vp41703x.pdf
- **VMWare ESXi v5.1**

Le piattaforme hardware sulle quali gira l'ODV possono essere configurate per supportare sia applicazioni x86 a 32 che a 64 bit. La configurazione certificata prende in considerazione soltanto le applicazioni a 32 bit.

6.3.1.2 Firmware

L'ODV non presenta componenti firmware. Il firmware che realizza l'avvio (boot) ed ogni altro eventuale livello firmware tra l'hardware e FINX è considerato parte dell'ambiente operativo dell'ODV.

6.3.1.3 Software

L'ODV è un Sistema Operativo basato sul Kernel Linux 2.6.33 e derivato dalla distribuzione Gentoo. L'ODV integra la *patch* del Kernel Linux PREEMPT_RT ed una serie di personalizzazioni realizzate per dotare il sistema operativo delle caratteristiche di sicurezza descritte nel Traguardo di Sicurezza [TDS].

L'ODV è costituito dal kernel, da un insieme di processi fidati e da un insieme di file di configurazione.

Il kernel gira nello stato privilegiato del processore e fornisce servizi alle applicazioni. Queste ultime richiedono i servizi del kernel tramite chiamate di sistema. L'accesso diretto all'hardware è ristretto al solo kernel; quando un'applicazione ha l'esigenza di accedere alle componenti hardware, quali i dischi, le interfacce di rete o altre periferiche, deve farlo tramite i servizi messi a disposizione dal kernel. Esso, dopo aver verificato se l'applicazione dispone dei necessari diritti d'accesso e privilegi, esegue il servizio richiesto o rifiuta la richiesta.

Il kernel si occupa anche di garantire la separazione dei diversi processi che fanno capo agli utenti. Ciò è realizzato tramite la gestione della memoria virtuale e reale dell'ODV che assicura che i processi eseguiti con diversi attributi non possono accedere direttamente alle aree di memoria di altri processi ma devono utilizzare i meccanismi di comunicazione tra processi forniti dal kernel e richiamabili tramite opportune chiamate di sistema.

Relativamente ai processi fidati essi sono costituiti da quei processi che quando sono avviati da un utente tramite una chiamata di sistema operano con privilegi estesi. I programmi che rappresentano questi processi fidati nel *file system* sono protetti dalla funzione di sicurezza relativa al controllo accessi discrezionale realizzata dal kernel.

Infine per ciò che riguarda i file di configurazione che fanno parte integrante delle funzioni di sicurezza dell'ODV, essi sono costituiti da quei file che controllano il comportamento dell'ODV e sono identificati come database delle funzioni di sicurezza. Anche tali file sono protetti dal controllo accessi discrezionale realizzato dal kernel.

Dal punto di vista architetturale il kernel è costituito dai seguenti sottosistemi:

- **Sottosistema relativo ai file ed all'input/output**: realizza tutte le funzioni relative agli oggetti del *file system*. In particolare tali funzioni includono quelle che permettono di creare, mantenere, cancellare gli oggetti del *file system* quali i file generici, le cartelle, i link simbolici, i file speciali relativi ai dispositivi, le *pipe* ed i *socket*.

- **Sottosistema relativo ai processi**: realizza tutte le funzioni relative alla gestione dei processi. In particolare, tali funzioni includono quelle che permettono la creazione, la schedulazione, l'esecuzione e la cancellazione dei processi.

- **Sottosistema relativo alla memoria**: realizza le funzioni relative alla gestione delle risorse di memoria del sistema. Tali funzioni includono quelle per creare e gestire la memoria virtuale, gestire le tabelle e gli algoritmi di paginazione.

- **Sottosistema relativo alla rete**: realizza i *socket* UNIX e per il dominio internet. Inoltre realizza gli algoritmi per schedulare i pacchetti di rete.

- **Sottosistema relativo alla comunicazione tra processi (IPC)**: realizza le funzioni relative ai meccanismi di comunicazione tra processi. In particolare tali funzioni includono quelle che permettono la condivisione controllata di informazioni tra processi, permettendo loro di condividere dati e sincronizzare la loro esecuzione al fine di interagire con una risorsa comune.

- **Sottosistema relativo all'audit**: realizza le funzioni del kernel necessarie per intercettare le chiamate di sistema e le registra in accordo con la politica di audit definita dall'amministratore del sistema.

- **Sottosistema relativo ai moduli del kernel**: realizza un'infrastruttura per supportare il caricamento di moduli. Tali funzioni includono quelle per caricare e scaricare i moduli del kernel.

- **Sottosistema relativo ai driver dei dispositivi**: implementa il supporto per vari dispositivi hardware attraverso un'interfaccia comune, indipendente dal dispositivo.

I processi fidati includono invece:

- Alcuni demoni che vengono avviati automaticamente allo start-up del sistema o su richiesta dell'amministratore (`auditd`, `init`, `sshd`).

- Una serie di comandi per la gestione di utenti e gruppi (`useradd`, `userdel`, `usermod`, `groupadd`, `groupdel`, `groupmod`, `gpasswd`).

- Alcuni comandi per la gestione delle funzionalità di audit (`auditctl`, `ausearch`).
- Alcuni comandi per la gestione delle caratteristiche delle password e del login (`chage`, `pam_tally2`, `unix_chkpwd`).
- Comandi per effettuare il login locale o remoto (`login`, `ssh`).
- Comandi relativi alla gestione di data e ora e dell'orologio hardware (`date`, `hwclock`).
- Comandi usati dagli utenti per cambiare alcune caratteristiche proprie (`chsh`, `chfn`, `passwd`, `su`).
- Il comando per il blocco della sessione (`vlock`).
- Il comando per l'apertura di porte tty (`agetty`).
- Il comando per l'esecuzione di test dell'hardware (`amtu`).
- Il comando per l'utilizzo delle funzioni crittografiche dei protocolli di rete SSL e TLS (`openssl`).
- Il comando per sollecitare un riscontro da un *host* (`ping`).

Infine, i file di configurazione, noti come database delle funzioni di sicurezza, comprendono le seguenti categorie di file:

- I file che definiscono i filtri e le regole relative alla funzione di audit.
- I file che definiscono le caratteristiche dei gruppi.
- I file che contengono nomi ed indirizzi degli *host* della rete.
- I file che contengono gli script che partono all'avvio del sistema.
- I file che contengono i processi avviati dal programma init ai vari *run level*.
- I file relativi alla configurazione dei moduli PAM.
- I file che contengono le password e le loro caratteristiche.
- I file che definiscono caratteristiche relative al login.
- I file che contengono i parametri di configurazione del server ssh.
- I file che definiscono le informazioni relative alla zona temporale.

6.3.2 Caratteristiche di Sicurezza dell'ODV

6.3.2.1 Politica di sicurezza

La politica di sicurezza dell'ODV è espressa dall'insieme dei Requisiti Funzionali di Sicurezza implementati dallo stesso. Essa copre i seguenti aspetti:

- gli utenti dell'ODV devono essere ritenuti responsabili per le loro azioni rilevanti ai fini della sicurezza che a tal fine devono essere registrate;
- L'accesso ai dati e alle funzioni dell'ODV deve essere concesso solamente agli utenti che sono autorizzati.

6.3.2.2 Ipotesi

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente dell'ODV. In particolare in tale ambito i seguenti aspetti sono da considerare di rilievo:

- le funzionalità di sicurezza dell'ODV sono gestite da uno o più individui competenti. Coloro che sono responsabili per la gestione dell'ODV non sono disattenti, volutamente negligenti o ostili e seguiranno e si atterranno alle istruzioni fornite dalla documentazione di guida;
- si assume che tutti i sistemi IT remoti e fidati sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza siano in grado di realizzare correttamente le funzioni richieste dall'ODV in modo consistente con quanto definito;
- si assume che tutti i sistemi IT remoti e fidati sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza siano sotto lo stesso controllo di gestione e operino sotto vincoli della politica di sicurezza compatibili con quelli dell'ODV;
- si assume che l'ambiente operativo dell'ODV fornisca allo stesso un'appropriata sicurezza fisica, commisurata con il valore dei beni che l'ODV deve proteggere;
- si assume che tutte le connessioni da e verso sistemi IT remoti e fidati e tra parti fisicamente separate delle funzioni di sicurezza dell'ODV, non protette dalle stesse, siano fisicamente o logicamente protette all'interno dell'ambiente dell'ODV, per assicurare l'integrità e la confidenzialità dei dati trasmessi e per assicurare l'autenticità degli estremi della comunicazione;
- si assume che gli utenti autorizzati possiedano le necessarie autorizzazioni per accedere almeno ad alcune delle informazioni gestite dall'ODV e agiscano in maniera cooperativa in un ambiente benevolo;
- si assume che gli utenti siano sufficientemente addestrati e fidati per svolgere alcuni compiti o gruppi di compiti all'interno di un ambiente IT sicuro, esercitando il

completo controllo sui loro dati utente;

- si assume che ogni modifica o corruzione dei file dell'ODV utilizzati dalle funzioni di sicurezza o rilevanti ai fini della sicurezza, dei dati utente o della sottostante piattaforma hardware, causata sia intenzionalmente che accidentalmente, sia rilevata da un amministratore autorizzato.

6.3.2.3 Funzioni di sicurezza

Le funzionalità di sicurezza implementate dall'ODV sono:

- **Identificazione ed autenticazione**: a tutti gli utenti è assegnato un identificativo univoco all'interno della singola macchina sulla quale è installato l'ODV. Tale identificativo è utilizzato insieme agli attributi ed al ruolo associato all'utente come base per le decisioni relative al controllo accessi. L'ODV autentica l'identità dichiarata dall'utente prima di consentirgli di effettuare altre azioni. L'ODV gestisce internamente un insieme di identificatori associati ai processi. Tali identificatori sono derivati dall'identificativo univoco associato al momento del suo login all'utente che ha lanciato il processo. Alcuni dei citati identificatori possono cambiare durante l'esecuzione di un processo (per esempio tramite il comando `su`) in accordo alla politica realizzata dall'ODV. FINX realizza l'identificazione e l'autenticazione usando i moduli PAM e basandosi sulla password dell'utente. La qualità delle password usate può essere rafforzata attraverso opzioni di configurazione.

- **Audit**: l'ODV fornisce una funzionalità di audit che permette di generare record di audit per gli eventi critici dal punto di vista della sicurezza. L'amministratore autorizzato può selezionare quali eventi devono essere registrati e per quali utenti l'audit è attivo. L'ODV fornisce strumenti che consentono all'amministratore autorizzato di estrarre specifici tipi di eventi di audit, eventi relativi a specifici utenti, eventi relativi a specifici oggetti del *file system*, o eventi che ricadono in un particolare intervallo temporale tra l'insieme di tutti i record di audit registrati dall'ODV stesso. I record di audit sono memorizzati in un formato leggibile da parte dell'uomo. Il sistema di audit rileva quando la capacità del file di audit eccede una soglia configurabile e l'amministratore autorizzato può definire le azioni che devono essere eseguite quando la soglia viene superata. Le possibili azioni includono il passaggio in modalità singolo utente e l'arresto del sistema operativo. Le funzioni di audit assicurano anche che nessun record di audit vada perso in seguito alla saturazione dei *buffer* di audit interni. Infatti i processi che cercano di creare un record di audit mentre i *buffer* di audit interni sono pieni vengono fermati finchè le risorse non sono nuovamente disponibili. Nell'improbabile caso di una saturazione non recuperabile la componente di audit del kernel entra in uno stato che impedisce la generazione di ulteriori eventi da registrare.

- **Controllo Accessi Discrezionale**: l'ODV restringe l'accesso agli oggetti del *file system* basandosi su liste di controllo accessi (ACL) che includono i bit di permesso standard nel mondo UNIX per utenti, gruppi ed altri utenti. I meccanismi di controllo accessi proteggono anche dall'accesso non autorizzato gli oggetti usati per la comunicazione tra processi (IPC). FINX gestisce il *file system* di tipo ext3, il quale supporta le liste di controllo accessi di tipo POSIX. Ciò permette di definire diritti di

accesso ai file appartenenti a questo tipo di *file system* fino alla granularità di un singolo utente. Per gestire il controllo accessi discrezionale per gli oggetti di tipo IPC sono usati i bit di permesso.

- **Riutilizzo degli oggetti**:il contenuto degli oggetti del *file system*, della memoria e degli oggetti usati per la comunicazione tra processi (IPC) è cancellato prima che i citati oggetti possano essere riutilizzati da un processo appartenente ad un altro utente. FINX supporta anche la cancellazione sicura dei dischi (ad esempio tramite lo strumento `shred`), ma tale funzione è esclusa dalla configurazione certificata.

- **Gestione della Sicurezza**: la gestione dei parametri dell'ODV, critici dal punto di vista della sicurezza, è effettuata da amministratori autorizzati. Per la gestione dell'ODV è usato un insieme di comandi che richiedono i privilegi di root. I parametri di sicurezza sono memorizzati in specifici file che sono protetti dai meccanismi di controllo accessi dell'ODV contro accessi non autorizzati da parte di utenti che non sono amministratori autorizzati. Tutti gli utenti autorizzati sono in grado di modificare i propri dati di autenticazione.

- **Servizi crittografici**: forniscono supporto per consentire agli utenti autorizzati ed alle relative applicazioni di cifrare, decifrare, calcolare l'impronta (*hash*) e firmare digitalmente i dati che risiedono all'interno dell'ODV e che sono trasmessi ad altri sistemi. I meccanismi crittografici sono usati specificamente per proteggere la comunicazione con sistemi remoti fidati e l'autenticazione delle parti che sono in comunicazione.

- **Protezione delle funzioni di sicurezza**: i componenti del kernel che gestiscono la memoria ed i processi assicurano che il processo associato ad un utente non possa accedere alla memoria del kernel o a quella associata ad altri processi. Le funzioni di sicurezza non appartenenti al kernel ed i relativi dati sono protetti dai meccanismi di controllo accessi discrezionale e dai meccanismi di isolamento dei processi. In genere i file e le directory contenenti dati interni delle funzioni di sicurezza (per esempio i file di configurazione) sono anche protetti in lettura dai permessi di tipo discrezionale. Inoltre, quando sono in esecuzione il software del kernel ed i dati sono protetti dai meccanismi hardware di protezione della memoria.

6.4 Documentazione

La documentazione specificata nel capitolo 8 (Appendice A) viene fornita al cliente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel capitolo 7.2 di questo rapporto.

6.5 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli SFR sono stati presi o ricavati per estensione dai CC Parte 2 [CC2].

6.6 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement (CCRA).

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Consorzio RES.

L'attività di valutazione è terminata in data 7 marzo 2014 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV1] che è stato approvato dall'Organismo di Certificazione nella sua versione finale [RFV3] il 15 maggio 2014. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

6.7 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

7 Esito della valutazione

7.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV1, RFV3] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "FINX RTOS Security Enhanced (SE) v3.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con l'aggiunta di ALC_FLR.1, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con l'aggiunta di ALC_FLR.1.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo

Classi e componenti di garanzia		Verdetto
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Basic flaw remediation	*ALC_FLR.1*	*Positivo*
Tests	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: security enforcing modules	ATE_DPT.2	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Focused vulnerability analysis	AVA_VAN.3	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

7.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 5 - Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti del prodotto "FINX RTOS Security Enhanced (SE) v3.1" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 3 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV valutato, le cui modalità di configurazione sono specificate nel documento Guida per l'installazione, la configurazione e l'uso sicuri dell'ODV [MAN].

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione di guida per l'amministratore e per l'utente [MAN] fornita con la configurazione valutata. In particolare, l'Appendice A del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo del prodotto.

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente non-IT, relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV, descritte nel par. 3.3 del documento [TDS]. In particolare, si assume che gli amministratori dell'ODV siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da amministratori inesperti, malfidati o negligenti.

Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento delle piattaforme HW su cui è installato l'ODV e di tutti i sistemi IT esterni fidati sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza. Le specifiche dell'ambiente operativo sono descritte nel documento [TDS].

8 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

8.1 Consegna

La consegna del Kit di installazione del Sistema Operativo FINX RTOS SE v3.1 può avvenire in due diverse modalità:

- nella forma di file ISO scaricabile direttamente dal sito di MBDA;
- memorizzato su supporto ottico di tipo CD-ROM o DVD-ROM.

In entrambi i casi l'operatore addetto all'installazione dovrà verificare preventivamente l'integrità dell'ODV. Nel caso di consegna tramite download i valori di *checksum* del file ISO e della documentazione andranno confrontati con quelli resi disponibili allo stesso indirizzo Internet.

Le tabelle che seguono identificano i materiali consegnabili (*deliverable*) relativi all'ODV valutato. In particolare, in Tabella 2 sono contenuti i materiali che è possibile scaricare dal sito di MBDA qualora il contratto con il cliente preveda questa forma di consegna. In Tabella 3 sono elencati i file/documenti che il cliente riceve in caso di consegna manuale tramite CD-ROM/DVD-ROM e formato cartaceo per i materiali per i quali lo stesso è applicabile (documento di guida).

Nome file	Contenuto	Vers.
FIN.X-RTOS_SE_v3.1-16100021323.01.iso	-	01
FIN.X-RTOS_SE_v3.1-16100021323.01.iso.md5 o FIN.X-RTOS_SE_v3.1-16100021323.01.iso.sha256	-	N/A
ST_FINXSE_RTOS_V3.1_16200036572.02.pdf	FINX RTOS SE v3.1 – Security Target – ID 16200036572	02
ST_FINXSE_RTOS_V3.1_16200036572.02.pdf.md5 o ST_FINXSE_RTOS_V3.1_16200036572.02.pdf.sha256	-	N/A
OPE-PRE_FINXSE_RTOS_V3.1_16200039645.02.pdf	FINX RTOS SE v3.1 – Secure Installation, Configuration & Operations – ID 16200039645	02
OPE-PRE_FINXSE_RTOS_V3.1_16200039645.02.pdf.md5 o OPE-PRE_FINXSE_RTOS_V3.1_16200039645.02.pdf.sha256	-	N/A

Tabella 2 - Materiali consegnabili dell'ODV (file scaricabili dalla rete)

Identificativo	Titolo	Vers.	Modalità di consegna
NC/M/CPS-MBDA/DVD6426	FINX-RTOS SE V3.1 Installation Kit	N/A	CD-ROM/ DVD-ROM
NC/M/CPSMBDA/CDR6427	FINX RTOS SE v3.1 – Secure Installation, Configuration & Operations - ID 16200039645	N/A	CD-ROM
NC/M/CPS-MBDA/CDR6431	Hash MD5 e SHA256	N/A	CD-ROM
16200039645	FINX RTOS SE v3.1 – Secure Installation, Configuration & Operations - ID 16200039645	02	Cartaceo

Tabella 3 - Materiali consegnabili dell'ODV (consegna manuale)

8.2 Installazione

Il Kit di installazione del Sistema Operativo FINX RTOS SE v3.1 consente l'installazione dell'ODV nella sua configurazione certificata su una delle piattaforme hardware e di virtualizzazione elencate nel Traguardo di Sicurezza [TDS] e nella Guida per l'installazione, la configurazione e l'uso sicuri dell'ODV [MAN]. In ogni caso dovrà essere effettuata un'installazione ex novo dell'ODV e il Sistema Operativo FINX RTOS dovrà risultare l'unico sistema operativo installato sulla piattaforma.

8.3 Documentazione per l'utilizzo sicuro dell'ODV

I documenti di guida rilevanti ai fini della valutazione o referenziati all'interno dei documenti prodotti e disponibili ai potenziali acquirenti, sono i seguenti:

- FINX RTOS SE v3.1 Security Target, Rev. 02, 21 Febbraio 2014 [TDS];
- FINX RTOS SE v3.1 Secure Installation, Configuration & Operations, Rev. 2.0, 21 Febbraio 2014 [MAN].

9 Appendice B - Configurazione valutata

L'ODV, denominato "FINX RTOS SE V3.1", è costituito dal kernel Linux 2.6.33 e da un insieme di pacchetti software elencati nel documento [MAN].

L'ODV deve essere installato ed utilizzato sulle seguenti piattaforme, i cui dettagli sono riportati nel cap. 6.3.1.1, come specificato nel Traguardo di Sicurezza [TDS]:

- VP417/03x;
- VP717/08x;
- VMWare ESXi v5.1.

Il documento di guida [MAN], che costituisce parte integrante dell'ODV, specifica un insieme di vincoli, come per esempio valori specifici di parametri contenuti nei file di configurazione, passi che devono essere eseguiti durante l'installazione e informazioni rivolte all'amministratore relativamente a come gestire in modo sicuro l'ODV.

10 Appendice C - Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4+ tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

10.1 Configurazione per i Test

Le piattaforme sulle quali sono stati condotti i test sia dal Fornitore che dai Valutatori sono le seguenti:

- VP417/03x;
- VP717/08x;
- VMWare ESXi v5.1.

Inoltre, i Valutatori hanno condotto alcuni test anche su:

- VMWare ESXi v5.0.

Sono state utilizzate 2 versioni beta dell'ODV durante le varie sessioni di test:

- FINX-RTOS-3.1.0-SE-beta130725.iso
- FINX-RTOS-3.1.0-SE-beta140124.iso

A seguito della conclusione con esito positivo dei test, la ISO FINX-RTOS-3.1.0-SE-beta140124 è diventata la versione ufficiale del prodotto.

Prima dell'esecuzione dei test il software è stato installato e configurato come descritto nel documento di guida [MAN].

10.2 Test funzionali svolti dal Fornitore

10.2.1 Approccio adottato per i test

Il piano di test presentato dal Fornitore e la definizione dei casi di test necessari sono stati predisposti come segue:

- si è partiti dall'identificazione di tutti i requisiti funzionali (sia quelli rilevanti ai fini della sicurezza sia quelli che non rientrano in questa categoria);

- ogni requisito funzionale è realizzato da una funzionalità e pertanto tutte le funzionalità, con particolare riferimento alle funzionalità di sicurezza, sono state testate in relazione alle loro interfacce;
- tali interfacce sono descritte in termini di specifiche funzionali, quindi tutte le funzionalità, ed in particolare quelle che realizzano funzioni di sicurezza, sono state testate rispetto alle relative specifiche funzionali;
- per ogni specifica funzionale è stata condotta una ricerca all'interno della comunità *open source* al fine di verificare l'esistenza di un test opportuno. Se tale ricerca ha dato esito positivo è stato usato tale test, eventualmente apportandovi modifiche per soddisfare esigenze specifiche. In caso contrario è stato sviluppato un nuovo test.

10.2.2 Strumenti utilizzati

Per l'esecuzione dei test funzionali proposti dal Fornitore, e per la riesecuzione degli stessi da parte dei Valutatori, è stata utilizzata una opportuna test suite messa a disposizione dal Fornitore stesso.

Tale test suite, denominata FINX RTOS SE v3.1 Test Suite v.1.0, è derivata dalla test suite sviluppata nell'ambito del progetto Linux Test Project™ (LTP) e da quella predisposta per la certificazione Common Criteria del sistema operativo RedHat Enterprise Linux (RHEL) 5.

Il progetto LTP è nato con lo scopo di predisporre una test suite per la comunità open source al fine di poter validare l'affidabilità, la robustezza e la stabilità di Linux. FINX RTOS è basato su Kernel Linux e pertanto alcuni test appartenenti alla test suite LTP sono stati utilizzati per le attività di test di FINX, in particolar modo per quanto riguarda le verifiche funzionali ed i test di non regressione. La suite LTP è una collezione di test studiati per verificare vari aspetti dei sistemi operativi Linux ma non è mirata espressamente ai test di sicurezza e pertanto, a questo fine, alcuni test sono stati tratti dalla test suite di RHEL 5.

I test facenti parte della test suite di FINX sono in gran parte automatizzati. Soltanto un piccolo numero di casi di test (meno di 10) deve essere eseguito manualmente a causa del fatto che, per esempio, è richiesta la connessione (login) diretta da parte dell'utente.

Durante la valutazione sono state messe a disposizione tre versioni della test suite, una per ogni sessione di test effettuata presso la sede del Fornitore. La modifica della test suite si è resa necessaria per correggere alcuni problemi in essa riscontrati durante la prima sessione di test e per consentire di allineare la test suite alla seconda versione beta di FINX, creata per risolvere alcune vulnerabilità riscontrate durante la seconda sessione di test.

Per quanto riguarda i test automatici, la test suite è caratterizzata da un'infrastruttura comune in cui i singoli casi di test rispettano un modello condiviso per le fasi di preparazione, esecuzione e pulizia effettuata dopo il test. Ogni caso di test può contenere

vari test della stessa funzione, che riguardino aspetti differenti (ad esempio la funzionalità di base, il comportamento in caso di parametri con valori non ammessi e la reazione nel caso in cui manchino i necessari privilegi). Ogni test all'interno del caso di test riporta un verdetto che può assumere i valori "PASS" o "FAIL" ed il sommario del caso di test eseguito in *batch* riporta la voce "PASS" solo se tutti i test all'interno del caso di test sono stati superati con successo, la voce "FAIL" in caso contrario.

Per quanto riguarda i test manuali, che ricoprono funzionalità che non possono essere facilmente testate in modo automatico, quali il login da console, sono forniti dei *template* costituiti da file di testo che dettagliano tutti i passi richiesti insieme ai risultati attesi. Chi esegue il test crea una copia del *template*, inserisce i risultati effettivi e li confronta manualmente con quelli attesi.

Tutti i risultati dei test in tutti gli ambienti (piattaforme) analizzati hanno mostrato che i risultati attesi sono identici ai risultati effettivi dei test, considerando anche i risultati negativi previsti nel piano di test.

10.2.3 Risultati dei test

I Valutatori hanno verificato che i test proposti dal Fornitore sono stati eseguiti su piattaforme conformi a quanto dichiarato nel Traguardo di Sicurezza [TDS].

I Valutatori sono stati in grado di seguire e comprendere pienamente l'approccio seguito per i test dal Fornitore utilizzando le informazioni dallo stesso messe a disposizione nel documento *Security Function Verification Test Plan* [TST].

I Valutatori hanno analizzato la copertura ed il livello di approfondimento dei test proposti dal Fornitore tramite la revisione di tutti i casi di test. I Valutatori hanno rilevato che i test eseguiti sulle funzioni di sicurezza sono estensivi e coprono le TSFI come identificato nelle specifiche funzionali e nei sottosistemi/interfacce interne identificate nel documento di progetto dell'ODV (*Basic modular design* [BMD]).

I Valutatori hanno revisionato i risultati dei test messi a disposizione dal Fornitore e li hanno trovati consistenti con i risultati attesi previsti nel piano di test.

10.2.4 Copertura dei test

Le specifiche funzionali hanno preso in considerazione le seguenti interfacce delle funzioni di sicurezza (TSFI):

- le chiamate di sistema;
- i file di configurazione critici dal punto di vista della sicurezza (database delle funzioni di sicurezza);
- i programmi fidati.

La mappatura presentata dal Fornitore mostra che i test coprono tutte le singole TSFI identificate per l'ODV.

Oltre alla tracciabilità rispetto alle specifiche funzionali messa a disposizione dal Fornitore, lo stesso ha fornito una mappatura dei casi di test rispetto ai sottosistemi ed alle interfacce interne descritte nel documento di progetto dell'ODV (*Basic modular design* [BMD]). Tale mappatura ha evidenziato che tutti i sottosistemi e tutte le interfacce interne sono coperti dai casi di test.

10.3 Test funzionali ed indipendenti svolti dai Valutatori

I Valutatori, oltre ad aver partecipato presso la sede del Fornitore all'esecuzione di tutti i test automatizzati proposti dallo stesso, hanno condotto per proprio conto due tipologie di test sull'ODV:

- riesecuzione dei test proposti dal Fornitore
- esecuzione di test indipendenti.

Per quanto riguarda la prima categoria di test i Valutatori non hanno adottato alcuna strategia di campionamento, ripetendo la totalità dei test presentati dal Fornitore nella documentazione.

Relativamente ai test indipendenti, i Valutatori hanno individuato dei test mirati ad approfondire alcuni aspetti del comportamento dell'ODV.

In particolare i Valutatori hanno creato casi di test per verificare alcuni aspetti funzionali nelle situazioni in cui i test proposti dal Fornitore non sono stati considerati dai Valutatori sufficientemente ampi. Nella fase di analisi da parte dei Valutatori dei casi di test proposti dal Fornitore i Valutatori hanno acquisito confidenza circa l'impegno profuso dal Fornitore per definire i test e la profondità e copertura degli stessi. Tale analisi ha evidenziato una copertura molto ampia delle funzioni di sicurezza dell'ODV e pertanto i Valutatori hanno ritenuto sufficiente individuare soltanto un piccolo numero di casi di test.

I test effettuati dai Valutatori sono stati eseguiti in due distinte fasi. La prima fase è stata la partecipazione all'esecuzione dei test proposti dal Fornitore nella sede dello stesso. La seconda fase invece ha riguardato i test eseguiti dai Valutatori presso il proprio laboratorio. In tale ambito sono stati sia rieseguiti i test automatici e semi-automatici proposti dal Fornitore, sia eseguiti i test appositamente definiti dai Valutatori per approfondire alcuni aspetti e comportamenti dell'ODV.

Per i test eseguiti presso la sede del Fornitore sono state utilizzate le piattaforme hardware messe a disposizione dal Fornitore ed elencate nel cap. 6.3.1.1. In tali occasioni il sistema operativo che costituisce l'ODV e gli strumenti di test sono stati installati dal Fornitore sulle piattaforme di test in accordo alle istruzioni fornite nel documento di guida [MAN] e tali istruzioni sono state verificate dai Valutatori.

Per quanto riguarda i test eseguiti presso il laboratorio dei Valutatori è stata utilizzata la piattaforma virtuale e le installazioni dell'ODV e della suite di test sono state eseguite dai Valutatori, sempre prendendo come riferimento le istruzioni del documento di guida [MAN].

Pertanto, in entrambi i casi, il sistema sotto test è stato configurato in accordo al

Traguardo di Sicurezza [TDS] ed alle istruzioni del documento di guida [MAN].

Durante i test presso la sede del Fornitore, i Valutatori hanno osservato quest'ultimo mentre eseguiva i casi di test ed hanno analizzato i file di *log* generati dai test al fine di verificarne la completezza e rilevare eventuali problemi riscontrati nell'esecuzione dei test. Tutti i risultati dei test eseguiti presso il Fornitore, nell'ultima sessione di test, hanno dato esiti conformi ai risultati attesi previsti nel piano di test.

I test indipendenti definiti dai Valutatori hanno riguardato:

- la verifica dei permessi associati ai file di configurazione rilevanti ai fini della sicurezza;
- la verifica della creazione dell'impronta delle password tramite SHA-256;
- la verifica dei tempi tra immissione identificativo d'utente e fine immissione password in diverse situazioni (login locale e remoto);
- la verifica del comando `useradd` con opzione `-p`;
- la verifica della creazione di cartelle personali da parte di utenti, dei permessi ad esse associati e l'uso dello *sticky bit*;
- la verifica di alcuni aspetti particolari del comando `vlock`;
- la verifica di alcune regole di *audit* e dei contenuti dei relativi file in situazioni specifiche;
- la verifica sul *path* completo che deve essere utilizzato per richiamare alcuni comandi;
- la verifica degli esiti dell'utilizzo del comando `useradd` da parte di un utente di tipo non amministrativo.

Tutti i test, nell'ultima sessione di test eseguita, hanno avuto esito positivo.

10.4 Analisi delle vulnerabilità e test di intrusione

Per definire i test di intrusione per l'ODV i Valutatori hanno seguito il seguente approccio.

Prima di tutto sono state verificate le comuni sorgenti accessibili tramite internet che riportano le vulnerabilità dei sistemi operativi Linux in generale ed in particolare della versione del kernel utilizzata dall'ODV. Tale indagine ha avuto lo scopo di determinare:

- se le vulnerabilità riportate erano presenti nella configurazione valutata dell'ODV, considerando l'ambiente operativo di utilizzo. In caso affermativo i Valutatori hanno eseguito un'analisi delle vulnerabilità per stabilire se le stesse potevano essere considerate sfruttabili;
- se le vulnerabilità riportate erano già state risolte nella configurazione valutata

dell'ODV.

In seguito a tale analisi i Valutatori hanno consegnato al Fornitore, durante la seconda sessione di test, un elenco delle vulnerabilità del kernel 2.6.33 che potevano essere applicabili all'ODV e rispetto alle quali il Fornitore era chiamato a decidere come e se risolvere le stesse.

Oltre alla ricerca nei siti che riportano le vulnerabilità note dei sistemi operativi di tipo Linux i Valutatori hanno considerato utile eseguire un'analisi del codice sorgente tramite opportuni strumenti automatizzati. Le motivazioni di tale scelta sono le seguenti:

- essendo l'ODV basato su software *open source*, che è analizzato in modo estensivo dalla comunità *open source* alla ricerca di vulnerabilità ovvie, lo sviluppo di test di intrusione semplici e ad alto livello risulta essere piuttosto inutile;
- essendo l'ODV basato su software *open source*, il cui codice sorgente è pubblicamente disponibile, i Valutatori ipotizzano che potenziali attaccanti possano utilizzare tale codice per generare potenziali attacchi.

L'analisi effettuata non ha evidenziato vulnerabilità sfruttabili.

Infine, per la ricerca di vulnerabilità note sono state effettuate scansioni delle piattaforme di test mediante opportuni strumenti software.

I *report* prodotti da tali strumenti durante la prima sessione di test hanno evidenziato una serie di vulnerabilità, molte delle quali ascrivibili alla distribuzione Gentoo su cui FINX si basa. I Valutatori hanno quindi eseguito una serie di test mirati ad approfondire alcune delle vulnerabilità evidenziate, potenzialmente critiche per l'ODV, ed a verificarne la sfruttabilità.

Al fine di risolvere queste ultime vulnerabilità e quelle del kernel, il cui elenco è stato predisposto e consegnato dai Valutatori nella seconda sessione di test, il Fornitore ha deciso di generare una nuova versione dell'ODV sostituendo i pacchetti risultati vulnerabili con le versioni degli stessi che non presentano più la vulnerabilità riscontrata o eliminando quei pacchetti non ritenuti espressamente necessari al corretto funzionamento dell'ODV.

Nella terza ed ultima sessione di test la scansione sulla nuova versione dell'ODV ha permesso ai Valutatori di verificare che le vulnerabilità precedentemente riscontrate non erano più presenti nell'ODV. Pertanto, a seguito della conclusione con esito positivo dei test di intrusione, tale versione aggiornata dell'ODV è diventata la versione ufficiale del prodotto.