Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

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. 2/17

(Certification No.)

Prodotto: **FIN.X RTOS SE V4.0**
(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, 25 luglio 2017

Fino a EAL4 *(Up to EAL4)*

Common Criteria

Fino a EAL4 *(Up to EAL4)*

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

FIN.X RTOS SE V4.0

OCSI/CERT/RES/06/2014/RC

Versione 1.0

25 luglio 2017

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	25/07/2017

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
DSA	Digital Signature Algorithm
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
LUKS	Linux Unified Key Setup
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PAM	Pluggable Authentication Module
POSIX	Portable Operating System Interface for Unix
PP	Profilo di Protezione (Protection Profile)
RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
RSA	Rivest-Shamir-Adleman
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
SSH	Secure Shell
SSL	Secure Sockets Layer
TOE	Target Of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
USB	Universal Serial Bus

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”, July 2014

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

[MAN] FIN.X RTOS SE V4.0 – Software User Manual, ID 1620047582, Rev 02, MBDA, 3 aprile 2017

[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

[RC] Rapporto di Certificazione del prodotto “FINX RTOS Security Enhanced (SE) v3.1”, OCSI/CERT/RES/03/2012/RC, 21 maggio 2014.

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

[RFV] Rapporto Finale di Valutazione del prodotto “FIN.X RTOS SE V4.0”, Versione 1.0, 13 giugno 2017

[SDD] FIN.X RTOS SE V4.0 - Software Design Document, ID 1620047578, Rev 02, MBDA, 3 aprile 2017

[SRS] FIN.X RTOS SE V4.0 - Software Requirements Specification, ID 16200047576, Rev 02, MBDA, 3 aprile 2017

[STD] FIN.X RTOS SE V4.0 - Software Test Description, ID 16200047579, Rev 02, MBDA , 3 aprile 2017

[STP] FIN.X RTOS SE V4.0 - Software Test Plan, ID 16200047577, Rev 02, MBDA , 3 aprile 2017

[STR] FIN.X RTOS SE V4.0 - Software Test Report, ID 16200047580, Rev 02, MBDA , 3 aprile 2017

[SVD] FIN.X RTOS SE V4.0 - Software Version Document, ID 1620047581, Rev 02, MBDA, 3 aprile 2017

[TDS] FIN.X RTOS SE V4.0 - Security Target, ID 16200047415, Rev 03, MBDA, 3 aprile 2017

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia fino a EAL4.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL 4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su http://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Poiché questo processo è la ri-certificazione di una precedente versione dello stesso prodotto il presente certificato è riconosciuto secondo le regole del precedente accordo [CCRA-2000], cioè per tutti i componenti di garanzia fino a EAL4.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "FIN.X RTOS SE V4.0", sviluppato dalla società MBDA Italia S.p.A..

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 di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV ("FINX RTOS Security Enhanced (SE) v3.1"), già certificato dall'OCSI (Certificato n. 1/14 del 21 maggio 2014 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore MBDA, è stato necessario procedere a una ri-certificazione dell'ODV. Le modifiche introdotte nella versione corrente dell'ODV includono: aggiornamento del *kernel* Linux, supporto per le piattaforme a 64 bit, introduzione di un meccanismo di autenticazione a due fattori, aggiornamento dei moduli crittografici.

L'LVS Consorzio RES ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

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 – Configurazione valutata 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 di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) 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.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "FIN.X RTOS SE V4.0" 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.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	FIN.X RTOS SE V4.0
Traguardo di Sicurezza	FIN.X RTOS SE V4.0 - Security Target, ID 16200047415, Rev 03, MBDA, 3 aprile 2017
Livello di garanzia	EAL4 con l'aggiunta di ALC_FLR.1
Fornitore	MBDA Italia S.p.A.
Committente	MBDA Italia S.p.A.
LVS	Consorzio RES
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	17 settembre 2014
Data di fine della valutazione	13 giugno 2017

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].

7.3 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 "FIN.X RTOS SE V4.0" (nel seguito anche indicato semplicemente come FINX RTOS o FINX), è un sistema operativo multi-utente e *multi-tasking* di tipo Linux derivato dalla distribuzione Gentoo, adatto ad essere utilizzato sia nel mercato della difesa, sia in ambito aerospaziale, industriale, in applicazioni di rete e di elettronica di consumo. Può girare su famiglie di processori Intel x86 e x86-64.

Inoltre, l'ODV è in grado di fornire un contesto di esecuzione predicibile che supporta applicazioni con requisiti *real-time*. 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

7.3.1 Architettura dell'ODV

7.3.1.1 Hardware

Il Sistema Operativo FIN.X RTOS SE V4.0 non richiede una specifica piattaforma hardware per operare.

In particolare, esso opera 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: 1,5 GB
- Adattatore di rete o lettore CD/DVD (richiesto solo per l'installazione dell'ODV)
- Porta USB

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:

- **VP717/08x**, **VP917/08x** e **VPB14/033-41E2-PTG**: 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:

  - VP917/08x: http://www.gocct.com/sheets/VP/vp91xx1x.htm
  - VP717/08x; http://www.gocct.com/sheets/VP/datasheet/vp71708x.pdf
  - VPB14/033-41E2-PTG: http://www.gocct.com/sheets/VP/vpb1xmsd-rc.htm

- **VMWare ESXi v5.1**

L'ODV prevede una procedura di installazione dedicata per ognuna delle piattaforme sopra elencate.

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

Periferiche come *hard disk*, schede di rete, CD/DVD *drive*, interfacce seriali, mouse e tastiera, possono essere usate con l'ODV senza che queste influiscano con le sue funzioni di sicurezza. Le chiavette USB (*USB Token*) possono essere usate per la *dual-factor authentication*.

7.3.1.2 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.

7.3.1.3 Software

L'ODV è un sistema operativo basato sul *kernel* Linux 4.4.53 PREEMP-RT-66 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, di database e di file di configurazione.

Per quanto riguarda il *kernel* esso 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*, quindi 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 principali:

- **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 (*symlink*), 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, inizializzare 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 (*trusted program*) sono raggruppati in sottosistemi come indicato di seguito:

- **System Initialization** (comprende il *boot loader* GRUB): `init`.
- **Identification and Authentication**: `agetty`, `login`, `su`, `passwd`, `vlock`.
- **System Management**: `chage`, `chsh`, `groupadd`, `groupmod`, `groupdel`, `useradd`, `usermod`, `userdel`, `grpck`, `pwck`, `sudo`, `pam_tally2`, `openssl`, `date`, `hwclock`, `chmod`, `chown`, `amtu`, `aide`, `cryptsetup`, `glsa-check`.
- **Network Applications**: `sshd`, `ssk-keygen`, `ssh`, `scp`.
- **User-level Audit**: `auditd`, `auditctl`, `ausearch`.

Infine, database e file di configurazione comprendono i file di seguito elencati (descrizione in lingua Inglese):

- `/etc/audit/audit.rules`: *defines filters for auditable event record generation.*
- `/etc/audit/audit.rules.stop.post`: *filters that are loaded immediately after the audit daemon is stopped.*
- `/etc/audit/audit.rules.stop.pre`: *filters that are loaded immediately before the audit daemon is stopped.*
- `/etc/audit/auditd.conf`: *configuration settings for audit subsystem operation (such as audit trace file location and disk space thresholds).*
- `/etc/group`: *stores group names, supplemental GIDs, and group members for all system groups.*
- `/etc/hosts`: *contains hostnames and their address for hosts in the network. This file is used to resolve a hostname into an Internet address in the absence of a domain name server.*
- `/etc/init.d/*`: *system start-up scripts.*
- `/etc/init.d/auditd`: *defines various configuration options for the audit function.*
- `/etc/inittab`: *describes the process started by init program at different run levels.*
- `/etc/ld.so.conf`: *file containing a list of colon, space, tab, newline, or comma separated directories in which to search for libraries for run-time link bindings.*
- `/etc/localtime`: *defines the local time zone information used for date/time input and display.*
- `/etc/login.defs`: *defines various configuration options for the login process.*
- `/etc/modprobe.d/*`: *configuration files for modprobe. Modprobe automatically loads or unloads a module while taking into account its dependencies.*

- `/etc/pam.d/*`: *this directory contains the configuration of PAM. In it there is one configuration for each application that performs identification and authorization. Each of the configuration file contains the PAM modules that are to be used for this procedure.*

- `/etc/passwd`: *stores user names, user IDs, primary group ID, user real name, home directory, shell for all system users.*

- `/etc/security/opasswd`: *contains the password history for check of reuse of old passwords.*

- `/etc/security/pwquality.conf`: *provides a way to configure the default password quality requirements for LUKS passwords.*

- `/etc/shadow`: *defines user passwords in one-way encrypted form, plus additional characteristics.*

- `/etc/ssh/sshd_config`: *contains ssh configuration parameters for the ssh server.*

- `/etc/sysctl.conf`: *an interface that allows you to make changes to a running CSCI_FINXSE kernel. You can configure various CSCI_FINXSE networking and system settings.*

- `/var/log/btmp`: *stores time and date of last unsuccessful login for each user.*

- `/var/log/lastlog`: *stores time and date of last successful login for each user.*

- `/usr/portage/metadata/glsa/gls a*.xml`: *GLSA notifications managed as XML files.*

- `/root/.dfa/<username>/.user_settings`: *contains user's data for dual-factor authentication.*

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 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 ed alle funzioni dell'ODV deve essere concesso solo agli utenti autorizzati. L'autorizzazione all'accesso alle risorse controllate dall'ODV deve essere garantito solo dopo aver superato con esito positivo meccanismi di identificazione e autenticazione imposti dall'ODV;

- la protezione dei dati dell'utente e delle funzioni di sicurezza deve riguardare sia la confidenzialità, sia l'integrità degli stessi, attraverso meccanismi propri dell'ODV che ne segnalino ogni eventuale modifica.

7.3.2.2 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 operativo 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;

- l'installazione dell'ODV deve essere eseguita seguendo le procedure riportate nelle guide, assicurando in questo modo che tutti i componenti, hardware, software e firmware concorrano a supportare la realizzazione dei meccanismi di sicurezza dell'ODV;

- i responsabili della gestione sicura dell'ODV devono stabilire procedure che assicurino la protezione della confidenzialità e dell'integrità dei dati trasmessi, assicurandosi che tutte le connessioni fisiche siano adeguatamente protette;

- 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 gli utenti siano sufficientemente addestrati e fidati per svolgere alcuni compiti o gruppi di compiti all'interno di un ambiente 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, sia accidentalmente, sia rilevata dai responsabili della gestione dell'ODV.

7.3.2.3 Funzioni di sicurezza

Le funzionalità di sicurezza implementate dall'ODV sono:

- **Identificazione ed autenticazione**: la funzionalità di identificazione ed autenticazione nell'ODV comprende tutte le forme di login interattivo (ad esempio, utilizzando il protocollo SSH o accedendo alla console locale) nonché modifiche di

identità tramite il comando `su` o `sudo`. Tutte queste forme si basano su esplicite informazioni di autenticazione fornite interattivamente da un utente. In particolare, avviene quanto segue:

- A ciascun utente viene assegnato un identificativo utente univoco all'interno del singolo sistema che costituisce l'ODV. Questo identificativo utente viene utilizzato insieme agli attributi e ai ruoli assegnati all'utente come base per le decisioni del controllo accessi.
- L'ODV autentica l'identità dichiarata dell'utente prima di consentire all'utente stesso di eseguire qualsiasi ulteriore azione.
- L'ODV mantiene internamente un insieme di identificatori associati ai processi che sono derivati dall'identificativo utente univoco relativo all'utente collegato. Alcuni di questi identificatori possono cambiare durante l'esecuzione del processo (ad esempio, utilizzando il comando `su`) in base ad una policy implementata dall'ODV.

- L'ODV realizza l'identificazione e l'autenticazione usando il protocollo SSH V2 o i moduli PAM che si basano sulla password dell'utente o su una coppia di chiavi pubblica/privata (per esempio, autenticazione basata su *token*). La qualità delle password usate può essere rafforzata attraverso le opzioni di configurazione. La funzione di sicurezza dell'autenticazione consente i seguenti metodi di autenticazione:

  1. basato su password: è sempre utilizzato durante il processo di login locale o remoto e dopo comando `su` (e `sudo`);
  2. di tipo *dual-factor*: può essere usato in unione al metodo con password, durante il processo di login locale e dopo comando `su` (e `sudo`);
  3. basato su chiave pubblica: usato in connessioni SSH.

- **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 finché 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). L'ODV gestisce *file system* di tipo ext3 e ext4 i quali supportano 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 tali strumenti sono esclusi 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**: L'ODV fornisce canali di comunicazione protetti da crittografa e primitive di crittografia che gli utenti (sia privilegiati, sia non privilegiati) possono utilizzare per scopi non specificati. L'ODV fornisce comunicazioni protette da crittografia per consentire alle entità remote di collegarsi all'ODV; per l'utilizzo interattivo, viene fornito il protocollo SSH V2. L'ODV è conforme allo standard LUKS per supportare la riservatezza dell'archiviazione dei dati mediante uno spazio di archiviazione protetto da crittografia: i dati cifrati possono essere decifrati (ad esempio per l'accesso ad essi) mediante la chiave di sessione dell'utente.

- **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 cartelle 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.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto 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 8.2 di questo rapporto.

7.5 Requisiti funzionali e di garanzia

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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.

7.6 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 13 giugno 2017 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione l'11 luglio 2017. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.7 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 – Configurazione valutata. 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.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV1] 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 "FIN.X RTOS SE V4.0" 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 – Configurazione valutata.

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
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	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

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione)

Si raccomanda ai potenziali acquirenti del prodotto "FIN.X RTOS SE V4.0" 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 "Software User Manual" [MAN] del prodotto FINX RTOS.

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 – Indicazioni per l'uso sicuro del prodotto 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 hardware 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].

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

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

9.1 Consegna

La consegna del Kit di installazione del Sistema Operativo FIN.X RTOS SE V4.0 può avvenire in due diverse modalità:

- nella forma di file immagine (estensione ".iso") scaricabile direttamente dal sito di MBDA (accesso con username e password);
- memorizzato su supporto ottico di tipo CD-ROM o DVD-ROM.

In Tabella 2 sono elencati i materiali dell'ODV che vengono consegnati al cliente.

Nome	Descrizione
CSCI_FINXSE-X86_64_16100031299_01.iso	FIN.X RTOS SE V4.0 Installation Kit per versione a 64-bit + SHA256 hash per *CSCI_FINXSE-X86_64_16100031299_01.iso*
CSCI_FINXSE-X86_16100031299_01.iso	FIN.X RTOS SE V4.0 Installation Kit per versione a 32-bit + SHA256 hash per *CSCI_FINXSE-X86_16100031299_01.iso*
16200047415_FINX_SE_V4_ST.pdf (Rev. 03)	FIN.X RTOS SE V4.0 - Security Target + SHA256 hash per *16200047415.03_FINX_SE_V4_ST.pdf*
16200047581.02_FINX_SE_V4_SVD.pdf (Rev. 02)	FIN.X RTOS SE V4.0 – Software Version Document + SHA256 hash per *16200047581.02_FINX_SE_V4_SVD.pdf*
16200047582.02_FINX_SE_V4_SUM.pdf (Rev. 02)	FIN.X RTOS SE V4.0 – Software User Manual + SHA256 hash per *16200047582.02_FINX_SE_V4_SUM.pdf*

Tabella 2 - Materiali consegnabili dell'ODV

9.2 Installazione

Il Kit di installazione del Sistema Operativo FIN.X RTOS SE V4.0 consente l'installazione dell'ODV nella sua configurazione certificata su una delle piattaforme hardware e di virtualizzazione elencate nel Traguardo di Sicurezza [TDS] e nel documento "Software User Manual" [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.

9.3 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:

- FIN.X RTOS SE V4.0 - Security Target, Rev 03, 3 aprile 2017 [TDS];
- FIN.X RTOS SE V4.0 – Software User Manual, Rev 02, 3 aprile 2017 [MAN];
- FIN.X RTOS SE V4.0 – Software Version Document, Rev 02, 3 aprile 2017 [SVD].

10 Appendice B – Configurazione valutata

L'ODV, denominato "FIN.X RTOS SE V4.0", è costituito dal *kernel* Linux 4.4.53 PREEMP-RT-66 e da un insieme di pacchetti software elencati nel documento "Software Version Document" [SVD]. La versione dell'ODV valutata è la *issue* 4.0 per architetture a 32-bit e a 64-bit.

L'ODV deve essere installato ed utilizzato sulle seguenti piattaforme, i cui dettagli sono riportati nel cap. 7.3.1.1, come specificato nel Traguardo di Sicurezza [TDS]:

- VP717/08x
- VP917/08x
- VPB14/033-41E2-PTG
- VMWare ESXi v5.1

Il documento "Software User Manual" [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.

La guida riporta indicazioni su come configurare il meccanismo per la *dual-factor authentication*, fornendo istruzioni dettagliate per la preparazione delle chiavette USB (*USB Token*) da assegnare agli utenti finali.

11 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.

11.1 Configurazione per i Test

Le attività di test sono state svolte sia presso il laboratorio dell'LVS Consorzio RES, sia presso il *test bed* allestito dal Fornitore.

L'ambiente su cui sono stati svolti i test presso il sito del Fornitore era costituito dalle seguenti piattaforme:

- VP717/08x
- VP917/08x
- VPB14/033-41E2-PTG
- VMWare ESXi v5.1 (installato su un PC *desktop* messo a disposizione dal Fornitore per l'uso degli ambienti virtuali).

Il Fornitore ha messo a disposizione dei Valutatori anche i seguenti strumenti:

- Laptop/PC per la "remote installation" e l'installazione su VMware.
- Chiavette USB (*USB Token*) per l'autenticazione tramite *token*.

Per l'effettuazione dei test presso il Laboratorio dell'LVS, i Valutatori hanno allestito un proprio *test bed* basato su macchine virtuali.

Prima dell'esecuzione dei test il software è stato installato e configurato come descritto nel documento "Software User Manual" ([MAN]).

Durante l'attività di test i Valutatori hanno ripetuto tutti i test funzionali proposti dal Fornitore. I Valutatori hanno altresì svolto una serie di test indipendenti.

A seguito della conclusione con esito positivo dei test, i file immagine dell'ODV identificati come CSCI_FINXSE-X86_64_16100031299_01.iso per l'architettura a 64 bit e CSCI_FINXSE-X86_16100031299_01.iso per quella a 32 bit sono divenuti la versione ufficiale del prodotto valutato.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Il Fornitore ha presentato per il Prodotto “FIN.X RTOS SE V4.0” i documenti “Software Test Plan” [STP], “Software Test Description” [STD] e “Software Test Report” [STR] che coprono tutte le evidenze richieste dai Common Criteria per la classe ATE.

Scopo dell’attività di ripetizione dei test funzionali del Fornitore è stato quello di verificare che tali documenti di test per l’ODV fossero adeguati nel fornire:

- la conferma che le funzioni di sicurezza dell’ODV operino in accordo con quanto descritto nella documentazione di progetto (“Software Design Document” [SDD]);
- la dimostrazione che i test proposti dal Fornitore siano completi sia dal punto di vista della copertura di tutte le funzioni di sicurezza dell’ODV, con riferimento al documento di specifiche funzionali (“Software Requirements Specification” [SRS]), sia dal punto di vista del dettaglio con cui i test stessi sono stati ideati dal Fornitore;
- la possibilità di ri-esecuzione dei test da parte dei Valutatori al fine di verificare la correttezza dei risultati ottenuti.

A tale scopo, dopo aver verificato la copertura dei test del Fornitore, i Valutatori hanno ripetuto tutti i test del Fornitore, verificando il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.2.2 Strumenti utilizzati

Per la ri-esecuzione dei test del Fornitore i Valutatori hanno utilizzato una *test suite* prodotta e resa disponibile ai Valutatori dal Fornitore stesso. Di tale *test suite* sono state utilizzate due differenti versioni identificate come segue, per entrambe le architetture a 32 e a 64 bit:

- Release: 01 beta-version 2016-09-29_1042
- Release: 01 beta-version 2016-11-08_1623

Per ciò che concerne la ripetizione dei test del Fornitore e l’effettuazione dei test indipendenti presso il Laboratorio dell’LVS, i Valutatori hanno allestito un proprio *test bed* su ambiente virtuale vSphere 5.1 all’interno del quale sono state create diverse macchine virtuali su cui è stato installato l’ODV. Su ciascuna di esse sono stati ripetuti i test del Fornitore utilizzando le immagini “.iso” dell’ODV e le *test suite* scaricate dal sito indicato dal Fornitore stesso.

11.2.3 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 analizzare e comprendere pienamente l’approccio seguito per i test dal Fornitore utilizzando le informazioni dallo stesso messe a

disposizione nei documenti “Software Test Description” [STD], “Software Test Plan” [STP] e “Software Test Report” [STR] in cui si riportano:

- l’insieme dei test funzionali svolti dal Fornitore ed i risultati ottenuti;
- le evidenze circa la copertura dei test svolti dal Fornitore e cioè che tutte le TSF sono state testate in relazione alle loro specifiche funzionali (“Software Requirements Specification” [SRS]);
- le evidenze circa la profondità con cui i test del Fornitore sono stati condotti e cioè che tutti i moduli presentati nella documentazione di progetto (“Software Design Document” [SDD]) siano stati tenuti in considerazione durante lo svolgimento dei test.

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.

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.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Sono state svolte due sessioni di test presso il sito del Fornitore in data 29-30 novembre e 2 dicembre 2016 (I Sessione) e 4 aprile 2017 (II Sessione). Durante tali sessioni sono stati ripetuti tutti i test funzionali predisposti dal Fornitore e svolti i test indipendenti dei Valutatori.

Nell’ambito dei test indipendenti, i Valutatori hanno effettuato verifiche puntuali circa l’implementazione delle funzioni crittografiche in relazione al programma `ssh` e alla *dual-factor authentication*.

Per ciò che riguarda l’applicazione `ssh`, i Valutatori hanno eseguito le seguenti prove:

- uso di `ssh` con password;
- verifiche della funzione `ssh-keygen`;
- Uso di `ssh` con chiavi RSA e DSA. Tutte le lunghezze permesse per le chiavi sono state testate.
- Uso di `ssh` e invocazione del comando `su`.

Per ciò che riguarda la *dual-factor authentication*, i Valutatori hanno eseguito le seguenti prove:

- preparazione del *token* con uso della funzione `cryptsetup`;
- verifica della cancellazione delle chiavi simmetriche;

- creazione di utenti e assegnazione chiavi (la chiave privata resta nel *token*);
- uso della funzione `sync` per agganciare la password alla *passphrase* del *token*;
- uso di configurazione non di default (ad esempio, chiavi DSA con lunghezza 2048);
- cambio password utente e *dual-factor authentication*.

Al termine dell'ultima sessione di test, sia le verifiche sui test funzionali del Fornitore, sia quelle scaturite da test dei Valutatori, hanno dato esito positivo (risultati coerenti con i risultati attesi).

Inoltre, presso il proprio laboratorio l'LVS ha effettuato anche una serie di test atti a verificare particolari comportamenti delle funzioni di sicurezza dell'ODV e la rispondenza con quanto indicato nel documento di guida [MAN]. In particolare, sono stati eseguiti test specifici atti a verificare il comportamento dell'ODV in relazione alle seguenti TSFI:

- `auditctl`
- `ausearch`
- `aureport`
- `/etc/audit/audit.rules`
- `/etc/pam.d`
- gruppi `admin`/`wheel`
- `/var/log/mail.log`

Inoltre, sono stati verificati i seguenti aspetti:

- configurazione dell'allarme generato dall'ODV in relazione a quanto dichiarato in FAU_STG.3 e FAU_STG.4;
- configurazione in relazione alla generazione chiavi RSA (FCS_CKM.1(3)) e DSA (FCS_CKM.1(4));
- verifica del programma `cryptsetup`, utilizzato per la *dual-factor authentication*;
- verifica dell'uso dei protocolli SSL V2 e SSL V3;
- verifica di *tool* di sviluppo all'interno della configurazione dell'ODV;
- verifica dei permessi associati ai file di configurazione rilevanti ai fini della sicurezza;
- verifica della generazione degli *hash* delle password tramite SHA-256.

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

11.4 Analisi delle vulnerabilità e test di intrusione

Le attività di analisi delle vulnerabilità e di test di intrusione sono state svolte presso i laboratori del Fornitore in tre sessioni distinte:

- I Sessione (29-30 novembre e 2 dicembre 2016): in queste giornate sono state lanciate le prime scansioni di vulnerabilità mediante *tool* automatici.
- II Sessione (22 dicembre 2016): ha avuto come obiettivo sia la verifica di alcune delle vulnerabilità riscontrate tramite *tool* automatici, sia l'esecuzione dell'attacco all'ODV tramite link simbolico (*symlink attack*).
- III Sessione (4 Aprile 2017): in questa giornata sono state ripetute scansioni delle piattaforme per verificare la risoluzione di tutte le vulnerabilità riscontrate sia con *tool* automatici che manuali.

Per l'effettuazione delle scansioni i Valutatori hanno utilizzato i seguenti *tool* di analisi:

- Nmap
- OpenVAS
- Armitage (ambiente grafico per l'utilizzo di Metasploit)
- ShellCheck

Questi *tool* sono stati eseguiti da un PC portatile con sistema operativo Kali Linux.

Le prove tramite *tool* automatici hanno evidenziato diverse vulnerabilità, le principali delle quali riguardavano:

- utilizzo di algoritmi di cifratura non robusti;
- utilizzo di pacchetti non aggiornati;
- utilizzo improprio di alcuni strumenti per la scrittura del codice relativo allo script che ha in carico l'automazione del processo di *dual-factor authentication* (`dfa.sh`).

Le anomalie riscontrate sono state prontamente segnalate al Fornitore. Inoltre, attraverso l'uso di Armitage è stato possibile dimostrare che l'ODV non è vulnerabile ad attacchi al servizio SMTP e alla funzione `ssh`.

Durante la II Sessione di test i Valutatori hanno dimostrato la vulnerabilità dello script `dfa.sh` ad un *symlink attack*, che ha consentito di portare l'ODV in uno stato non sicuro (condizione di *Denial of Service*) mediante sovrascrittura del file `/etc/passwd`. I Valutatori hanno messo a disposizione del Fornitore opportune indicazioni circa i metodi di mitigazione/risoluzione di tale vulnerabilità.

Nella III Sessione di test i Valutatori hanno rieseguito tutti i test di intrusione su una nuova versione della ISO dell'ODV (CSCI_FINXSE-X86_64_16100031299_01.iso), prodotta dal

Fornitore sulla base delle risultanze delle precedenti sessioni. Nessuno dei test ha evidenziato ulteriori debolezze dell'ODV.

La ri-esecuzione dei test di intrusione sulla versione aggiornata dell'ODV ha permesso ai Valutatori di verificare che le anomalie precedentemente riscontrate non erano più presenti nell'ODV e che questo è privo di vulnerabilità residue sfruttabili nel contesto operativo dichiarato, consentendo quindi di concludere questa attività con esito positivo.