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. 1/19

(Certification No.)

Prodotto: *(Product)* **CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware**

Sviluppato da: *(Developed by)* **Certes Networks, Inc.**

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.3)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 13 marzo 2019

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware

OCSI/CERT/CCL/07/2018/RC

Versione 1.0

13 marzo 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	13/03/2019

2 Indice

3 Elenco degli acronimi

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CEP Certes Enforcement Point

CLI Command Line Interface

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standard

GUI Graphical User Interface

HW Hardware

LAN Local-Area Network

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

NTP Network Time Protocol

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PP Profilo di Protezione

RFV Rapporto Finale di Valutazione

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

SSH Secure Shell

SW Software

TDS Traguardo di Sicurezza

TLS Transport Layer Security

TSF TOE Security Functionality

TSFI TSF Interface

WAN Wide-Area Network

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[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

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

4.2 Documenti tecnici

[CEP] "CEP User Guide v5.3", Revision A, April 2018

[CFNC] "CFNC User Guide v5.3", Revision A, 20 April 2018

[DEL] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Secure Delivery Document, v0.2, 15 November 2018

[INST] "CryptoFlow Net Creator v5.3" Installation Guide, Revision A, April 2018

[RFV] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Evaluation Technical Report, v1, 29 January 2019

[SUP] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Guidance Documentation Supplement, v0.5, 22 January 2019

[TDS] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Security Target, v0.7, 22 January 2019

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 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 EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

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.

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware", nome abbreviato "CryptoFlow Net Creator v5.3", sviluppato dalla società Certes Networks, Inc.

L'ODV è una suite di componenti costituita da dispositivi di cifratura CEP, configurati e gestiti utilizzando il software applicativo personalizzato CryptoFlow Net Creator. Tutte le funzionalità di sicurezza dell'ODV, inclusi gli algoritmi crittografici, sono implementate nel software CryptoFlow Net Creator v5.3 e nel firmware CEP v5.3. Nessuna funzionalità di sicurezza dell'ODV è implementata nell'hardware dell'ODV.

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).

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 aggiunta di ALC_FLR.3, in conformità a quanto indicato 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 riassume l'esito della valutazione di sicurezza del prodotto "CryptoFlow Net Creator v5.3" 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.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione 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	CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware
Traguardo di Sicurezza	"CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Security Target, v0.7, 22 January 2019
Livello di garanzia	EAL4 con aggiunta di ALC_FLR.3
Fornitore	Certes Networks, Inc.
Committente	Corsec Security, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	25 settembre 2018
Data di fine della valutazione	29 gennaio 2019

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 è una suite di componenti costituita dai dispositivi di cifratura CEP e dal software CryptoFlow Net Creator per la gestione della sicurezza e delle politiche. CryptoFlow Net Creator è un'interfaccia grafica GUI basata sul Web che configura e monitora i dispositivI di cifratura CEP, memorizza e distribuisce le politiche (o le regole) e fornisce funzionalità di gestione e controllo delle chiavi. Le politiche create e distribuite da CryptoFlow Net Creator definiscono le azioni che il CEP intraprende sul traffico di rete protetto, sia per cifrarlo e decifrarlo, inviarlo in chiaro o rilasciarlo. Tutto il traffico di gestione remota trasmesso tra il CryptoFlow Net Creator e le dispositivo di cifratura CEP è protetto tramite sessioni TLSv1.2.

Il dispositivo di cifratura CEP offre funzionalità di elaborazione ad alta velocità per proteggere i dati che viaggiano su reti non affidabili durante il transito tra i siti. Ciascun dispositivo di cifratura CEP ha una porta di gestione e due porte dati. Una porta dati locale viene utilizzata per le connessioni LAN alle reti affidabili, mentre una porta dati remota fornisce connessioni WAN su reti non attendibili. Il traffico non cifrato che proviene da una rete locale affidabile viene ricevuto sulla porta dati locale del CEP di origine.

La GUI di CryptoFlow Net Creator è l'interfaccia di gestione principale. Si tratta di un'applicazione basata su Web e di un server di database che supporta l'accesso basato sui ruoli utilizzato per fornire i dispositivi di cifratura CEP, definire le politiche e gestire chiavi e certificati. Le politiche e i dati delle chiavi, utilizzati dai CEP per derivare le chiavi di cifratura, vengono generati e distribuiti in modo sicuro ai dispositivi di cifratura CEP tramite un canale autenticato e cifrato TLS, con l'opzione per l'autenticazione bilaterale basata sui certificati.

I dettagli della configurazione di impiego dell'ODV sono illustrati in Figura 1.

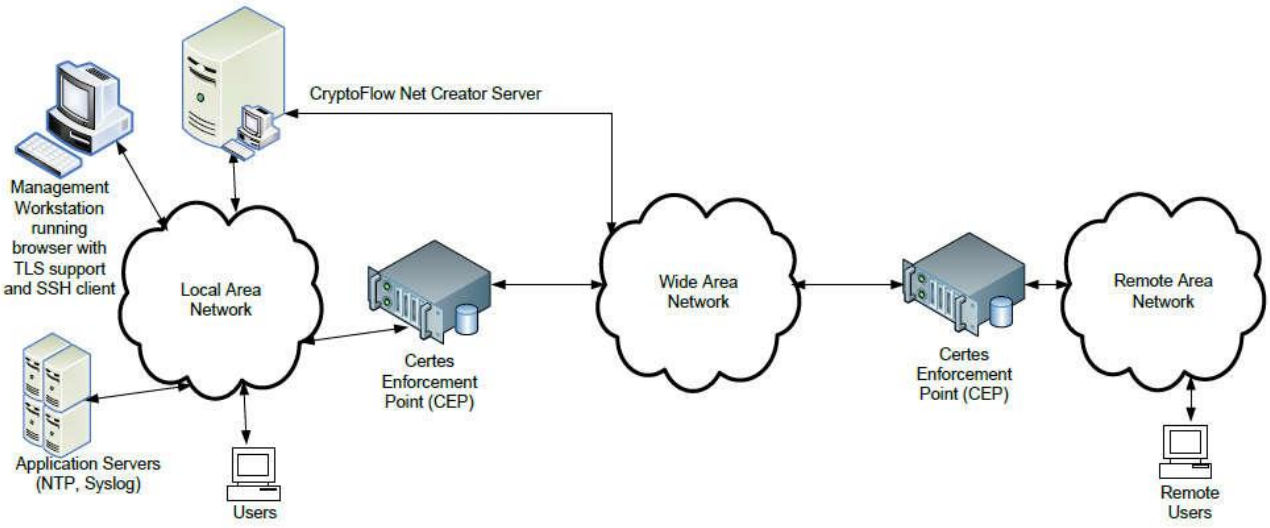

Figura 1 – Configurazione dell'ODV

Per una descrizione dettagliata dell'ODV, si consultino i par. 1.4 e 1.5 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

I dispositivi di cifratura CEP possono essere gestiti da amministratori autorizzati utilizzando l'interfaccia grafica GUI di CryptoFlow Net Creator o quella a linea di comando CLI dei CEP. Utilizzando la GUI di CryptoFlow Net Creator, un amministratore può configurare e gestire più dispositivo da un'unica posizione centralizzata. Inoltre, è possibile creare politiche di sicurezza che definiscono come e dove si verificherà la cifratura. È possibile accedere alla CLI dei CEP dalla workstation di gestione direttamente tramite una porta seriale o tramite una connessione SSH. Ciò consente a un amministratore di eseguire l'installazione iniziale e la risoluzione dei problemi dei CEP.

Una politica definisce le reti da proteggere e raggruppa queste reti per formare gli insiemi di reti. Un criterio può avere uno o più insiemi di reti associati ad esso. Una volta stabiliti gli insiemi di reti, è possibile assegnare i CEP a tali insiemi e definire le politiche di sicurezza che li governano. Ogni CEP in una data rete riceve gli stessi dati della chiave di cifratura del gruppo da utilizzare per derivare le chiavi di cifratura. CryptoFlow Net Creator centralizza la creazione e la distribuzione di politiche e dati delle chiavi. Inoltre, offre una capacità di *rekeying* che garantisce che i CEP generino nuove chiavi di cifratura a intervalli di definiti.

L'ODV è progettato per essere installato in un cabinet o in un centro dati fisicamente sicuro con il livello appropriato di controllo di accesso fisico e protezione fisica (ad es., controllo antincendio, serrature, allarmi). L'ODV è destinato alla gestione da parte degli amministratori che operano secondo una politica di sicurezza coerente.

L'ODV è inteso a fornire servizi di riservatezza e integrità delle informazioni che viaggiano attraverso una rete non sicura. L'ambiente dell'ODV dovrebbe garantire una connettività di rete stabile per l'ODV per svolgere la sua funzione prevista.

L'ODV richiede timestamp affidabili per controllare gli eventi rilevanti per la sicurezza. L'ODV richiede che gli orologi sui diversi componenti del TOE siano sincronizzati in modo che l'ora in cui si è verificato ciascun evento possa essere accuratamente verificata. L'ambiente dell'ODV è responsabile della fornitura di un server NTP per la sincronizzazione dell'ora.

È possibile accedere alla funzionalità di gestione dell'ODV tramite un client SSH di terze parti indipendente o un browser Web.

La Figura 2 illustra l'ambito fisico e il confine fisico della soluzione globale e collega insieme tutti i componenti dell'ODV. L'ODV è un dispositivo di cifratura CEP (sia hardware che software) configurato e gestito utilizzando il software applicativo personalizzato CryptoFlow Net Creator.

Solo il CEP (hardware e software) e CryptoFlow Net Creator (solo software) sono inclusi nell'ODV. L'hardware CEP include dispositivi appositamente progettati inclusi con l'acquisto dell'ODV. Il software è personalizzato per fornire funzionalità crittografiche e la capacità di gestire i dispositivi di cifratura CEP.

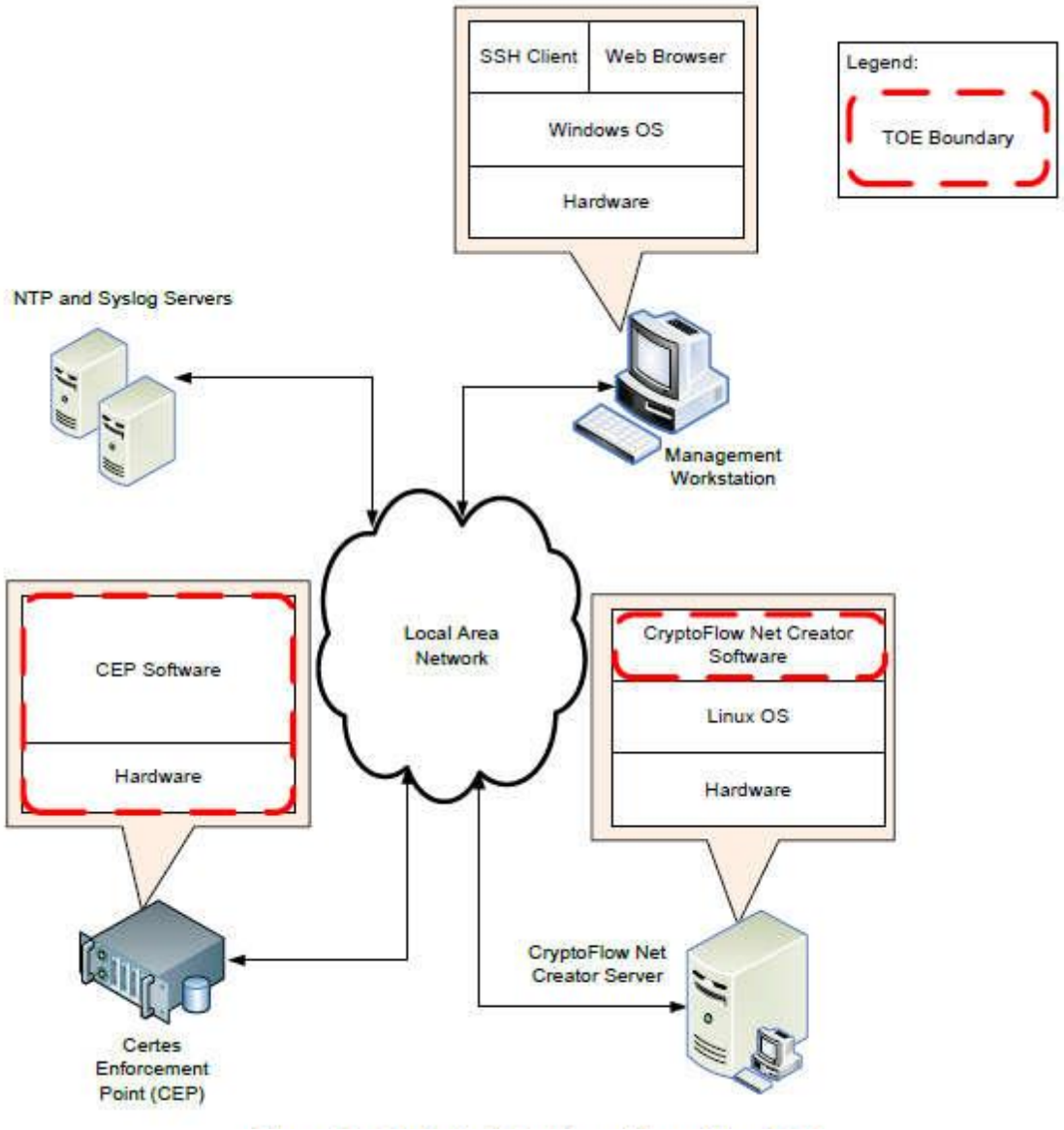

Figura 2 – Confine fisico dell'ODV

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Tutte le funzionalità di sicurezza dell'ODV, inclusi gli algoritmi crittografici, sono implementate nel software CryptoFlow Net Creator v5.3 e nel firmware CEP v5.3. Nessuna funzionalità di sicurezza dell'ODV è implementata nell'hardware. Inoltre, le funzionalità di sicurezza sono le stesse per tutti i modelli di dispositivi di cifratura CEP.

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

- **Security Audit.** L'ODV fornisce funzionalità per la generazione e la visualizzazione di record di controllo. Poiché gli amministratori gestiscono e configurano l'ODV, questo tiene traccia delle proprie attività registrando i record di controllo nei registri di controllo. L'ODV registra tutte le impostazioni e le modifiche di configurazione rilevanti per la sicurezza per verificare la responsabilità delle azioni dell'amministratore. Gli amministratori autorizzati possono visualizzare i record di controllo, mostrando l'identità dell'utente che ha attivato l'evento.

- **Cryptographic Support.** L'ODV utilizza due moduli crittografici certificati FIPS 140-2 per eseguire operazioni crittografiche, utilizzate per proteggere le comunicazioni dagli amministratori remoti alla GUI di CryptoFlow Net Creator e alla CLI dei CEP. Vengono inoltre utilizzati per cifrare i dati utente, creare un canale di comunicazione sicuro per il trasferimento dei dati utente tra CEP e proteggere i dati TSF (ad es., dati delle chiavi, politiche) trasmessi tra CryptoFlow Net Creator e i CEP.

- **User Data Protection.** L'ODV applica il controllo del flusso di informazioni SFP che adotta una serie di regole al traffico che passa attraverso l'ODV. A seconda dell'operazione identificata nell'SFP, l'ODV determinerà se instradare il traffico degli utenti in chiaro, scartarlo o cifrarlo/decifrarlo. Gli amministratori dell'ODV autorizzati configurano l'SFP impostando gli attributi di sicurezza utilizzando la GUI CryptoFlow Net Creator o la CLI dei CEP.

- **Identification and Authentication.** Tutti gli amministratori dell'ODV devono essere identificati e autenticati prima di eseguire qualsiasi azione sulla GUI di CryptoFlow Net Creator o sulla CLI dei CEP. L'accesso all'ODV richiede un nome utente e un ruolo autorizzati. Ciò garantisce che solo gli amministratori legittimi dell'ODV possano accedere alle impostazioni di configurazione e gestione. L'ODV nasconde le password alla GUI di CryptoFlow Net Creator e alla CLI dei CEP durante l'autenticazione.

- **Security Management.** L'ODV è gestito dagli amministratori in uno degli otto ruoli: Amministratore di piattaforma, Amministratore, Amministratore di dispositivo, Operatore di dispositivo, Creatore di politiche, Attuatore di politiche, Utente e Ops. L'ODV è in grado di eseguire le seguenti funzioni di gestione: gestione degli attributi di sicurezza SFP di controllo del flusso di informazioni e gestione dei dati TSF. L'ODV limita l'accesso alle funzioni di gestione in base al ruolo dell'amministratore. L'SFP di controllo del flusso di informazioni è permissivo per impostazione predefinita, consentendo il passaggio delle informazioni tra CEP in chiaro; tuttavia, gli amministratori autorizzati sono in grado di modificare l'SFP di controllo del flusso di informazioni per eseguire operazioni alternative, ad es. l'eliminazione o la cifratura delle informazioni.

- **Protection of TOE Security Functionality.** L'ODV protegge i dati delle TSF dalla divulgazione e modifica quando vengono trasmessi tra parti separate dell'ODV. L'ODV utilizza TLSv1.2 per proteggere la comunicazione tra CryptoFlow Net Creator e un dispositivo di cifratura CEP. L'ODV e il suo ambiente forniscono timestamp affidabili per il dispositivo di cifratura CEP e il software CryptoFlow Net Creator, rispettivamente. I timestamp vengono utilizzati per registrare l'ora esatta per i record di controllo. Il tempo per tutti i componenti dell'ODV è sincronizzato utilizzando un server NTP nell'ambiente dell'ODV.

- **TOE Access.** L'ODV termina una sessione di amministratore inattiva della GUI di CryptoFlow Net Creator o della CLI dei CEP dopo un periodo di tempo preconfigurato. Gli amministratori devono eseguire nuovamente l'autenticazione dopo essere stati disconnessi. Ciò impedisce a una persona non autorizzata di accedere alle funzioni di gestione dell'ODV attraverso una sessione non presidiata. Gli amministratori possono anche terminare le proprie sessioni interattive. Prima di stabilire una sessione utente, l'ODV visualizza un banner di accesso contenente un messaggio di avviso relativo all'utilizzo non autorizzato dell'ODV.

- **Trusted Path/Channels.** L'ODV (dispositivo di cifratura CEP) fornisce un canale affidabile tra se stesso e un altro prodotto affidabile (un altro dispositivo di cifratura CEP in questo caso) cifrando, decifrando e autentificando tutti i dati trasmessi utilizzando algoritmi crittografici forniti da un modulo crittografico certificato FIPS 140-2. Utilizza questo canale fidato per trasferire i dati dell'utente tra i dispositivi di cifratura CEP. Utilizzando un browser Web compatibile, un amministratore remoto avvia una connessione sicura alla GUI di CryptoFlow Net Creator.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata 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 seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 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.

7.7 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 CCLab Software Laboratory.

L'attività di valutazione è terminata in data 29 gennaio 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 26 febbraio 2019. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 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 [RFV] prodotto dall'LVS CCLab Software Laboratory 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 "CryptoFlow Net Creator v5.3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di ALC_FLR.3, 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 aggiunta di ALC_FLR.3.

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

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Systematic flaw remediation	ALC_FLR.3	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.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 "CryptoFlow Net Creator v5.3" 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 agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([DEL], [INST], [SUP], [CFCN], [CEP]).

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

Per mantenere la sicurezza dell'ODV durante la fase di distribuzione al cliente, sono seguite da parte del fornitore Certes diverse procedure.

Prima della spedizione sono svolye alcune attività preliminari:

- attività di pre-distribuzione per software, hardware e documentazione dell'ODV;
- etichettatura dell'ODV, che include il numero di serie, il numero del modello e logo;
- imballaggio dell'ODV.

Per la spedizione ai clienti, Certes utilizza corrieri internazionali, quali UPS, FedEx o DHL.

I clienti possono utilizzare i documenti di spedizione e ricezione per verificare l'ODV. L'etichetta di spedizione apposta sulla confezione identifica il cliente in base al nome e all'indirizzo della società e indica un singolo dipendente specifico della società a cui è destinata il dispositivo. La lista di imballaggio può anche essere controllata per assicurarsi che i numeri di serie (indicati come S/N sulla lista) su ciascun componente corrispondano a quelli sulla lista di imballaggio.

Durante il processo di avvio iniziale, gli hash per il software installato vengono automaticamente confrontati con gli hash nella lista di spedizione firmata consegnata al cliente; eventuali modifiche al codice o alla lista comporteranno un codice di rifiuto. Questo controllo avviene automaticamente all'avvio e non richiede alcuna azione da parte dell'utente.

Maggiori dettagli su tale procedura sono contenuti in "Secure Delivery Document" [DEL].

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

Il software CryptoFlow Net Creator 5.3 verrà quindi installato dal cliente finale seguendo la documentazione di distribuzione definita.

- "CryptoFlow Net Creator 5.3 Installation Guide" [INST]. Questo manuale descrive come dev'essere installato l'ODV da parte di un System Administrator.
- "CryptoFlow Net Creator v5.3 Dispositivos Guidance Documentation Supplement" [SUP]. Il documento descrive le istruzioni aggiuntive necessarie a far funzionare l'ODV in modo sicuro, secondo la certificazione CC.
- "CFNC User Guide v5.3 [CFCN] e "CEP User Guide v5.3" [CEP]. Questi manuali descrivono come un System Administrator deve configurare e mantenere l'ODV e le zone di sicurezza che sono connesse all'ODV.

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware", nome abbreviato "CryptoFlow Net Creator v5.3", sviluppato dalla società Certes Networks, Inc.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 5.3. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

Per maggiori dettagli, consultare il par. 1.5 del [TDS].

10.1 Ambiente operativo dell'ODV

In Tabella 2 sono riportati sinteticamente i requisiti minimi dei componenti dell'ambiente operativo dell'ODV per consentirne la corretta operatività.

Per maggiori dettagli, consultare i par. 1.4.2 e 1.5.1.1 del [TDS].

Component	Requirement
Web browsers	One of the following types of Web browsers should be used: • Microsoft Internet Explorer (IE v11+) • Mozilla Firefox (v64+) • Google Chrome (v71+) • Apple Safari (v12+)
OS	CentOS 6.7 (with the current released updates applied)
CPU	Intel Xeon E3-1270 v5, 3.6 GHz
Memory	8 GB
Disk Space	500 GB minimum

Tabella 2 – Componenti dell'ambiente operativo dell'ODV

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, con aggiunta di ALC_FLR.3, 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

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie.

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nei documenti ([INST], [SUP], [CFCN], [CEP]), come indicato nel par. 9.2. Dopo la configurazione dell'ODV i valutatori hanno verificato che l'ODV è stato installato correttamente e tutti i servizi previsti funzionavano correttamente.

L'ambiente di test così realizzato è lo stesso utilizzato dal Fornitore per testare le TSFI.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

I valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura dei requisiti funzionali (SFR) e delle TSFI descritte nelle specifiche funzionali.

11.2.2 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari per sollecitare le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.2.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, comprese le varie edizioni dell'ICCC, documenti JIL e CCDB, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV. In questa ricerca è stato considerato anche il sistema operativo Linux, facente parte dell'ambiente operativo, ma comunque necessario al corretto funzionamento dell'ODV. Sono state così individuate alcune vulnerabilità potenziali.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza, documentazione operativa, rapporto della visita al sito di sviluppo) al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, congiuntamente a quella del codice sorgente, i Valutatori hanno effettivamente determinato la presenza di altre vulnerabilità potenziali

I Valutatori hanno analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare diverse effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco Enhanced-Basic, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi. Per l'esecuzione dei test i Valutatori hanno utilizzato gli strumenti Kali Linux e Burp Suite Pro.

L'esecuzione dei test di intrusione ha confermato la presenza di vulnerabilità potenzialmente sfruttabili da un attaccante con potenziale di attacco Enhanced-Basic. Tali risultati sono stati prontamente segnalati al Fornitore, tramite un Rapporto di Osservazione. Il Fornitore ha replicato, recependo le osservazioni dei Valutatori e rilasciando una nuova versione dell'ODV. I Valutatori hanno quindi installato questa nuova versione dell'ODV nell'ambiente di test, e hanno potuto verificare che le soluzioni proposte dal Fornitore hanno risolto tutti i problemi sollevati con le precedenti osservazioni.

Sulla base di tali risultati, i Valutatori hanno così concluso che nessuno scenario di attacco con potenziale Enhanced-Basic può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Sono state invece individuate tre vulnerabilità residue, cioè vulnerabilità che potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a Enhanced-Basic.