Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 5/20

(Certification No.)

Prodotto: Trident version 2.1.3

(Product)

Sviluppato da: I4P-Informatikai Kft. (I4P Informatics Ltd.)

(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+

(AVA_VAN.5, ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 2 settembre 2020

Firmato digitalmente
da Eva Spina
Data: 2020.09.02
10:13:15 +02'00'

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Trident version 2.1.3

OCSI/CERT/CCL/02/2020/RC

Versione 1.0

2 settembre 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	02/09/2020

2 Indice

3 Elenco degli acronimi

3DES Triple Data Encryption Standard

AES Advanced Encryption Standard

API Application Programming Interface

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CD Compact Disc

CEM Common Evaluation Methodology

CM Cryptographic Module

CPU Central Processing Unit

DPCM Decreto del Presidente del Consiglio dei Ministri

drQSCD distributed remote Qualified Signature Creation Device

DTBS/R Data To Be Signed / Representation

EAL Evaluation Assurance Level

ECA External Client Application

ECC Elliptic Curve Cryptography

eIDAS Electronic IDentification, Authentication and Signature

FIPS Federal Information Processing Standards

HDD Hard Disk Drive

ID Identifier

IT Information Technology

JSON JavaScript Object Notation

JWT JSON Web Token

LCA Local Client Application

LCD Liquid Crystal Display

LED Light Emitting Diode

LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MPC	Multi-Party Computation
MPCA	Multi-Party Cryptographic Appliance
MPCM	Multi-Party Cryptographic Module
MPSAM	Multi-Party Signature Activation Module
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PDF	Portable Document Format
PP	Protection Profile
PTRNG	Physical True Random Number Generator
QSCD	Qualified Signature Creation Device
RAD	Reference Authentication Data
RFV	Rapporto Finale di Valutazione
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIC	Signer’s Interaction Component
SOGIS	Senior Officials Group Information Systems Security
SSA	Server Signing Application
SSH	Secure Shell

ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TOTP	Time-based One-Time Password (algorithm)
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
USB	Universal Serial Bus

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “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-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[eIDAS] “Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014

[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

[DEL] “Delivery Documentation, Trident, the distributed remote Qualified Signature Creation Device (Trident or drQSCD)”, version 0.6, I4P-informatikai Kft., 26 May 2020

[DEV-CM] “MPCM Development Guide: distributed remote Qualified Signature Creation Device (drQSCD)”, v1.4, I4P-informatikai Kft., 3 June 2020

[DEV-SAM] “MPSAM Development Guide: distributed remote Qualified Signature Creation Device (drQSCD)”, v1.4, I4P-informatikai Kft., 3 June 2020

[RFVv1] “Trident version 2.1.3” Evaluation Technical Report, v1, CCLab Software Laboratory, 24 July 2020

[RFVv2] “Trident version 2.1.3” Evaluation Technical Report, v2, CCLab Software Laboratory, 5 August 2020

[RFVv3] “Trident version 2.1.3” Evaluation Technical Report, v3, CCLab Software Laboratory, 29 August 2020

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019

[PRE-CM] “MPCM Preparation Guide: distributed remote Qualified Signature Creation Device (drQSCD)”, v1.3, I4P-informatikai Kft., 4 May 2020

[PRE-SAM] “MPSAM Preparation Guide: distributed remote Qualified Signature Creation Device (drQSCD)”, v1.3, I4P-informatikai Kft., 4 May 2020

[RC] “Certification Report distributed remote Qualified Signature Creation Device (drQSCD) v1.0”, OCSI/CERT/SYS/06/2017/RC, version 1.0, 15 May 2019

[TDS] “Trident, the distributed remote Qualified Signature Creation Device (Trident or drQSCD)” Security Target, v2.1, I4P-informatikai Kft., 28 August 2020

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 https://www.sogis.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).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://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 "Trident version 2.1.3", sviluppato dalla società I4P-informatikai Kft. (I4P Informatics Ltd.), nel seguito del documento anche indicato come "Trident" o "drQSCD".

L'ODV è un dispositivo multi-utente e multi-chiave, progettato per essere utilizzato come QSCD per la generazione di firme e sigilli elettronici qualificati in conformità al Regolamento (UE) n. 910/2014 [eIDAS] e per eseguire ulteriori operazioni crittografiche di supporto. L'ODV è composto da un Modulo Crittografico (CM) e da un Signature Activation Module (SAM) ed è adatto all'uso sia in locale, sia da remoto.

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 (drQSCD v1.0), già certificato dall'OCSI (Certificato n. 4/19 del 15 maggio 2019 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore I4P-informatikai Kft. è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS CCLab Software Laboratory 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.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "Trident version 2.1.3".

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 e/o utilizzatori. 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 AVA_VAN.5 e ALC_FLR.3, 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 "Trident version 2.1.3" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori 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	Trident version 2.1.3
Traguardo di Sicurezza	"Trident, the distributed remote Qualified Signature Creation Device (Trident or drQSCD)" Security Target, v2.1 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di AVA_VAN.5 e ALC_FLR.3
Fornitore	I4P-informatikai Kft. (I4P Informatics Ltd.)
Committente	I4P-informatikai Kft. (I4P Informatics Ltd.)
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419221-5:2018 [PP-CM] EN 419241-2:2019 [PP-SAM]
Data di inizio della valutazione	27 aprile 2020
Data di fine della valutazione	24 luglio 2020

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 "Trident version 2.1.3" (Trident o drQSCD) è un dispositivo multi-utente e multi-chiave, progettato per essere utilizzato come QSCD per la generazione di firme e sigilli

elettronici qualificati in conformità al Regolamento (UE) n. 910/2014 [eIDAS] e per eseguire ulteriori operazioni crittografiche di supporto.

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

7.3.1 Architettura dell'ODV

A seconda della sua configurazione, l'ODV è costituito da una, due, tre o quattro MPCA (Multi-Party Cryptographic Appliance). Una MPCA si presenta sotto forma di apparato con chassis metallico, montabile su *rack*, come illustrato in Figura 1.

Figura 1 - Aspetto fisico di una MPCA

Nella configurazione denominata **Distributed Configuration** (configurazione distribuita), l'ODV è composto da *n* (con *n* = 2, 3 o 4) MPCA identiche che operano come una sola unità logica che, nel suo insieme, soddisfa i requisiti del Traguardo di Sicurezza [TDS]. Nel caso in cui alcune delle MPCA dovessero smettere di funzionare (ad es., a causa di un errore non recuperabile o per l'indisponibilità della rete), le MPCA rimaste sono in grado di garantire una funzionalità limitata.

Nella configurazione denominata **Standalone Configuration** (configurazione autonoma), l'ODV è costituito da un'unica MPCA che soddisfa i requisiti del Traguardo di Sicurezza [TDS].

L'ODV è formato da due componenti principali, situati all'interno dell'involucro fisico di una MPCA, che operano congiuntamente per soddisfare diversi insiemi di requisiti:

- Il componente **Cryptographic Module (CM)** del drQSCD è un modulo crittografico di uso generico che fornisce il supporto crittografico necessario per i suoi utenti legittimi.

- Il componente **Signature Activation Module (SAM)** del drQSCD è un'applicazione locale installata all'interno del perimetro protetto da manomissione del drQSCD che implementa il Signature Activation Protocol (SAP). Il SAM utilizza i Signature Activation Data (SAD) di un firmatario remoto per attivare la chiave di sottoscrizione corrispondente da utilizzare all'interno di un modulo crittografico.

L'ODV è utilizzabile sia per il caso d'uso "Local Signing", sia per quello "Remote Server Signing", così come descritti nel Protection Profile [PP-CM].

Il caso d'uso "Locale", illustrato in Figura 2, è rivolto ai titolari di chiavi che operano in locale per applicare le proprie firme elettroniche o sigilli elettronici. In questo caso d'uso viene utilizzata la sola funzionalità CM dell'ODV per l'esecuzione in locale delle operazioni crittografiche e per la relativa gestione delle chiavi; a seconda della configurazione, l'ODV può anche fare uso di altri CM esterni.

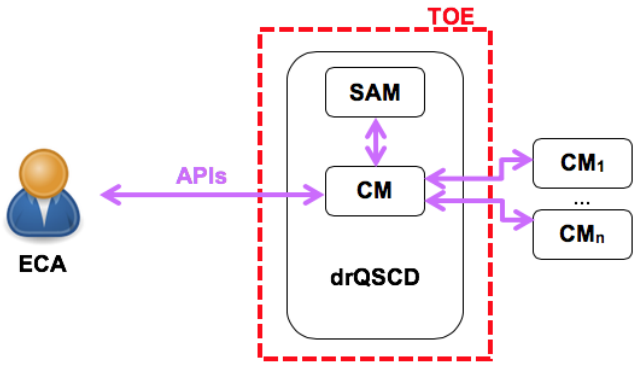

Figura 2 - L'ODV nel caso d'uso "Locale"

Queste operazioni possono essere effettuate in locale dal titolare delle chiavi mediante un'applicazione client esterna (ECA) per creare firme elettroniche e sigilli elettronici qualificati e non qualificati, nonché per eseguire ulteriori operazioni crittografiche di supporto. Esempi d'uso includono i TSP che emettono certificati e marche temporali e che forniscono servizi applicativi come fatturazione elettronica e posta elettronica certificata, in cui il fornitore di servizi utilizza le proprie chiavi per eseguire funzioni crittografiche (ad es., firma elettronica, cifratura, decifratura).

Il caso d'uso "Remoto", illustrato in Figura 3, è rivolto ai TSP che soddisfano i requisiti per la creazione di firme o di sigilli elettronici da remoto, come specificato in [eIDAS]. In questo caso, il CM integrato, eventualmente supportato da altri CM esterni, se presenti e configurati per essere utilizzati, e la funzionalità SAM del drQSCD soddisfano complessivamente i requisiti per i QSCD nel contesto della firma remota, così come descritti nell'Allegato II ad [eIDAS].

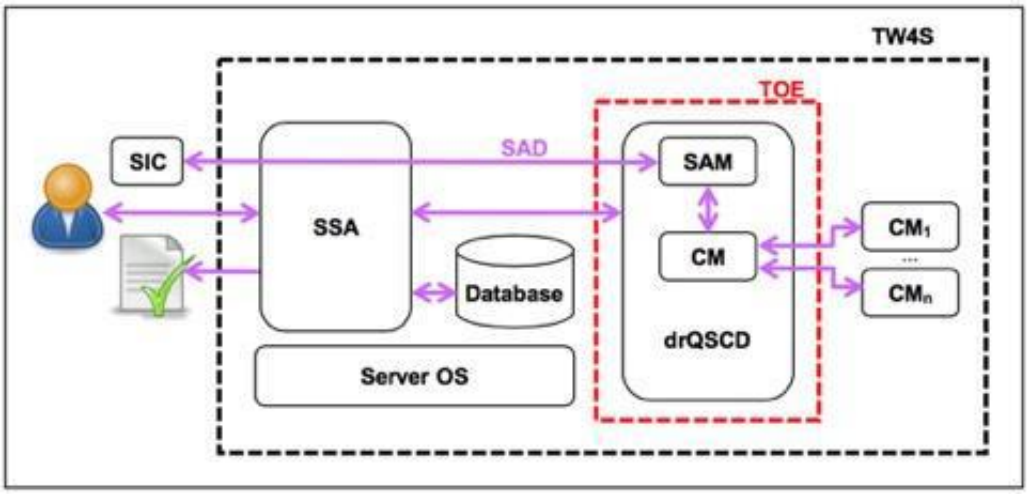

Figura 3 - L'ODV nel caso d'uso "Remoto"

Il Signer's Interaction Component (SIC) è un componente software e/o hardware, gestito nell'ambiente del firmatario sotto il suo esclusivo controllo. La Server Signing Application (SSA) utilizza il drQSCD per generare, memorizzare e utilizzare le chiavi di sottoscrizione.

I componenti CM e SAM dell'ODV forniscono le seguenti funzionalità.

La **funzionalità CM** include, ma non è limitata a:

- generazione, memorizzazione, utilizzo, backup, ripristino e distruzione di chiavi crittografiche simmetriche (AES, 3DES) e asimmetriche (RSA, ECC);
- garanzia della sicurezza, in termini di riservatezza e integrità, delle chiavi simmetriche e delle chiavi private asimmetriche, nonché dei numeri primi pre-generati per le coppie di chiavi RSA;
- generazione di firme elettroniche qualificate e sigilli elettronici qualificati;
- esecuzione di ulteriori operazioni crittografiche di supporto: creazione di firme elettroniche e sigilli non qualificati, verifica di firme elettroniche e sigilli, funzione crittografica di *hash*, *keyed-hash message authentication*, cifratura e decifratura, derivazione di chiavi, verifica di password *one-time* TOTP e di *token* JWT;
- supporto all'autenticazione di applicazioni client o di utenti autorizzati all'uso di chiavi segrete e per l'identificazione elettronica, come definita in [eIDAS];
- supporto all'uso di TOTP o JWT per l'attivazione delle chiavi da parte dei loro titolari.

Il drQSCD può anche essere configurato per generare, memorizzare ed attivare le chiavi del firmatario in uno o più CM esterni, per il miglioramento delle prestazioni o per motivi *legacy*.

La **funzionalità SAM** include, ma non è limitata a:

- autenticazione del firmatario remoto basata su due fattori (una password e una password usa e getta calcolata a partire da un segreto condiviso) o autenticazione delegata ai sensi dell'articolo 9 del Regolamento (UE) n. 910/2014 [eIDAS] utilizzando un *token* JWT;
- autorizzazione dell'operazione di firma;
- attivazione della chiave di sottoscrizione nella funzionalità CM interna (e in CM esterni, se configurati).

La funzionalità SAM dell'ODV garantisce che il firmatario remoto conservi il controllo esclusivo delle proprie chiavi di sottoscrizione per la generazione di firme elettroniche qualificate, come stabilito dall'Allegato II ad [eIDAS].

In caso di **configurazione distribuita**, parti diverse del drQSCD implementano protocolli di calcolo *multi-party* sicuri (MPC). In questa configurazione il drQSCD garantisce quanto segue:

- generazione di coppie di chiavi RSA (e dei numeri primi pre-generati) e di coppie di chiavi ECC in modo distribuito;
- creazione di firme e sigilli elettronici o decifratura di messaggi cifrati RSA utilizzando un metodo di firma/decifratura a più passi;
- autenticazione degli utenti finali in modo distribuito.

Il drQSCD garantisce la coerenza dei dati del TSF quando vengono replicati tra le diverse parti dell'ODV (MPCA).

7.3.1.1 Ruoli e funzioni disponibili

La funzionalità CM dell'ODV mantiene i seguenti ruoli e l'associazione degli utenti ai ruoli:

- *Administrator*: soggetto privilegiato che può eseguire, tramite una console locale o le CMAPI disponibili esternamente, operazioni di gestione specifiche del CM, tra le quali:
    - creazione di un nuovo account con attributi di sicurezza per un utente *Administrator* (la creazione dell'amministratore iniziale richiede l'inserimento di un codice di installazione);
    - esportazione della componente pubblica di una chiave asimmetrica;
    - sblocco dell'accesso ad una chiave bloccata;
    - modifica degli attributi delle chiavi;
    - esportazione/cancellazione di dati di audit;
    - funzioni di backup e ripristino (la funzione di ripristino è sotto doppio controllo).
- *Key User*: un soggetto normale non privilegiato che può richiamare le operazioni su una chiave in base ai requisiti di autorizzazione della chiave stessa.
- *Local Client Application* (LCA): applicazione in esecuzione all'interno del perimetro fisico di una MPCA.
- *External Client Application* (ECA): applicazione che comunica da remoto con una delle MPCA attraverso una connessione di rete.

La funzionalità SAM dell'ODV mantiene i seguenti ruoli:

- *Privileged User*: un utente che può eseguire, tramite una console locale o le SAMAPI disponibili esternamente, operazioni specifiche del SAM, tra le quali:
    - creazione di un nuovo account con attributi di sicurezza per un utente *Signer* (firmatario);
    - gestione degli account degli utenti *Signer*;

- creazione di un nuovo account con attributi di sicurezza per un *Privileged User* (la creazione del *Privileged User* iniziale richiede l'inserimento di un codice di installazione);
- creazione e modifica del record di dati di configurazione e del file di configurazione del SAM;
- funzioni di backup e ripristino (la funzione di ripristino è sotto doppio controllo);
- generazione delle coppie di chiavi degli utenti *Signer*.

- *Signer*: un utente che comunica in remoto con il SAM ed è in grado di eseguire le seguenti operazioni:
  - richiedere la generazione di una nuova coppia di chiavi RSA o ECC e assegnarla al proprio account;
  - impostare o modificare i dati di autorizzazione per la propria chiave (Key Authorisation Data);
  - firmare (utilizzando la propria chiave di sottoscrizione nel CM, trasmettendo i dati richiesti, incluso l'ID utente univoco, due diversi fattori di autenticazione, l'ID della chiave, i Key Authorisation Data e uno o più DTBS/R);
  - gestire il proprio account di utente *Signer*.

7.3.1.2 Autenticazione e Autorizzazione

Il componente CM dell'ODV utilizza per l'identificazione e l'autenticazione un metodo comune a tutti i ruoli: un identificativo univoco dell'utente (inviato dall'utente durante l'autenticazione), una password statica e/o un TOTP o JWT. La password statica viene verificata rispetto ai RAD (*hash* cifrato della password + sale) memorizzati nell'account dell'utente come attributo di sicurezza. Il TOTP viene verificato utilizzando un segreto condiviso di lunghezza 256 bit.

Il CM blocca l'account dopo un numero predefinito di tentativi di autenticazione falliti consecutivi, configurabile dall'amministratore in maniera differente per ciascun ruolo.

Prima di concedere l'uso di una chiave segreta in un'operazione crittografica, viene sempre richiesta l'autorizzazione o la ri-autorizzazione del richiedente come utente della chiave. Il CM blocca la chiave segreta dopo un numero predefinito di tentativi di autorizzazione falliti consecutivi.

Il componente SAM dell'ODV utilizza per i *Privileged User* lo stesso metodo di identificazione e autenticazione del CM: un identificativo univoco d'utente, una password statica e/o un TOTP. Per gli utenti *Signer*, il SAM richiede l'autenticazione forte: autenticazione a due fattori integrata (una password come fattore basato sulla conoscenza più un TOTP come fattore basato sul possesso) o autenticazione delegata ai sensi dell'articolo 9 del Regolamento (UE) n. 910/2014 [eIDAS] utilizzando un *token* JWT. Il SAM garantisce che tutti gli utenti abbiano un solo ruolo; di conseguenza, un utente *Signer* non può essere anche un *Privileged User*.

Il SAM blocca l'account dell'utente dopo un numero predefinito di tentativi di autenticazione falliti consecutivi. In caso di blocco dell'account di un utente *Signer*, il SAM sospende anche l'utilizzo di tutte le chiavi di sottoscrizione di cui l'utente è titolare.

7.3.1.3 Supporto Crittografico

Il componente CM dell'ODV garantisce la sicurezza delle chiavi durante il loro intero ciclo di vita. Il normale ciclo di vita di una chiave comprende le modalità con cui la chiave può arrivare all'interno del drQSCD (importazione, generazione o ripristino da un backup), con conseguente associazione di un insieme di attributi alla chiave, la memorizzazione della chiave e, infine, i modi in cui la chiave memorizzata può essere elaborata (esportazione, uso in una funzione crittografica, backup, distruzione).

Il componente SAM dell'ODV non esegue direttamente operazioni crittografiche per i suoi utenti: in particolare, non genera/memorizza/distrugge, esporta/importa, esegue il backup/ripristino o usa la chiave d'utente.

Il SAM richiama il CM interno (o un CM esterno, se configurato) con i parametri appropriati ogni volta che è richiesta un'operazione crittografica per il firmatario.

Il SAM utilizza diverse chiavi di infrastruttura per proteggere i propri file memorizzati, i record del database e i dati trasmessi o ricevuti tramite i canali di comunicazione.

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].

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:

- **Ruoli, Autenticazione e Autorizzazione (CM e SAM)**: per la descrizione di queste funzioni si rimanda ai parr. 7.3.1.1 e 7.3.1.2.

- **Security management (CM)**: l'amministratore del CM (*CM Administrator*) è in grado di sbloccare un account utente bloccato o una chiave bloccata, specificare un valore iniziale alternativo per l'attributo di sicurezza "Key Usage" ("General" o "Signing"), esportare e cancellare i dati di audit locali e il file Errorlog, effettuare il backup e il ripristino dello stato del TSF del CM. L'utente della chiave (*Key User*) è in grado di modificare gli attributi della sua chiave.

- **Security management (SAM)**: Il SAM implementa le seguenti funzioni di gestione della sicurezza: gestione degli utenti *Signer*, gestione dei *Privileged User*, gestione della configurazione, funzioni di backup e ripristino.

- **Key Security (CM)**: Il CM implementa le seguenti funzioni di sicurezza relative all'intero ciclo di vita delle chiavi:

    - importazione di chiavi;

    - generazione di chiavi;

- ripristino di chiavi da un backup;
- associazione di un insieme di attributi ad una chiave;
- memorizzazione delle chiavi;
- esportazione di chiavi;
- uso delle chiavi;
- backup delle chiavi;
- distruzione delle chiavi.

- **Key Security (SAM)**: Il SAM non esegue operazioni crittografiche con la chiave dell'utente *Key User* e non cancella la chiave dell'utente *Key User*. Il SAM richiama il CM con i parametri appropriati ogni volta che è richiesta l'esecuzione di un'operazione crittografica, la generazione o la cancellazione di una chiave. Il SAM esegue altresì operazioni crittografiche non distribuite con le chiavi di infrastruttura.

- **Access and information flow control (CM)**: Il CM applica le seguenti Politiche della Funzione di Sicurezza (SFP):
  - *Key Basics*: L'importazione di chiavi segrete non è consentita. L'esportazione di chiavi segrete è consentita solo per le chiavi non assegnate con Export Flag = "yes". Le chiavi pubbliche vengono sempre esportate con protezione dell'integrità del valore e degli attributi. Lo sblocco dell'accesso ad una chiave non consente di accedere alla chiave a soggetti diversi da quelli che risultavano autorizzati nell'istante in cui la chiave è stata bloccata. Nessun soggetto è autorizzato ad accedere direttamente al valore di testo in chiaro di una chiave segreta o ad accedere a valori intermedi durante qualsiasi operazione che utilizza una chiave segreta.
  - *Key Usage*: Gli attributi della chiave "Unprotected Flag" e "Operational Flag" possono essere modificati solo dall'utente *Key User*. I dati di autorizzazione (*Authorisation Data*) possono essere modificati solo dall'utente *Key User*. Solo i soggetti con autorizzazione in vigore per una specifica chiave segreta possono eseguire operazioni utilizzando il valore di testo in chiaro di quella chiave. Possono essere eseguite solamente le funzioni crittografiche consentite dall'attributo *Key Usage* associato alla chiave segreta.
  - *Backup*: Solo gli utenti *Administrator* sono in grado di eseguire le funzioni di backup e ripristino (la funzione di ripristino è sotto doppio controllo). Tutti i backup sono firmati e cifrati a protezione della loro integrità e riservatezza.

- **Access and information flow control (SAM)**: Il SAM applica le seguenti SFP aggiuntive:
  - *Privileged User Creation*: Solo un *Privileged User* è in grado di creare un nuovo account per un *Privileged User*.

- *Signer Creation*: Solo un *Privileged User* è in grado di creare un nuovo account per un utente *Signer*.
- *Signer Maintenance*: Solo un *Privileged User* o l'utente proprietario *Signer* è in grado di eliminare l'identificativo di una chiave e una chiave pubblica dall'account di un utente *Signer*.
- *Supply DTBS/R*: Solo un *Privileged User* autorizzato è in grado di fornire i DTBS/R per conto dell'utente *Signer*.
- *Signer Key Pair Generation*: Solo un utente *Signer* può richiedere la generazione di una nuova coppia di chiavi RSA o ECC e assegnarla al proprio account. Solo un *Privileged User* può generare una nuova coppia di chiavi RSA o ECC e assegnarla all'account di un utente *Signer*.
- *Signer Key Pair Deletion*: Solo un utente *Signer* può richiedere la cancellazione di una coppia di chiavi asimmetriche.
- *Signing*: Solo un utente *Signer* può richiedere al SAM di eseguire un'operazione di firma con la propria chiave.
- *SAM Maintenance*: Solo un *Privileged User* può eseguire i comandi relativi alla gestione del SAM, trasmettendo informazioni al SAM per gestire i ruoli e la configurazione.
- *Signer*: L'ordine dei comandi relativi al "Signer" è regolato e controllato.
- *Privileged User*: L'ordine dei comandi relativi al "Privileged User" è regolato e controllato.

- **Data protection (CM)**: Il CM garantisce la protezione dei propri dati del TSF mediante le seguenti misure di sicurezza:
  - *Self-test*: per dimostrare la corretta operatività del TSF.
  - *Secure failure*: la capacità di preservare uno stato sicuro quando si verificano i diversi tipi di errori.
  - *Tamper protection*: rilevamento di manomissioni e capacità di risposta alle manomissioni.
- **Data protection (SAM)**: Il SAM è implementato come applicazione locale all'interno dello stesso perimetro fisico del CM. Di conseguenza, il CM fornisce i suoi servizi di sicurezza anche a protezione del SAM.
- **Audit (CM e SAM)**: Il CM e il SAM registrano tutti gli eventi relativi alla sicurezza. Ogni record di audit include una marcatura temporale affidabile, l'identità del soggetto (ove applicabile), l'identificativo del CM o del SAM correlato e una stringa leggibile dall'uomo che descrive l'evento specifico.
- **Communication protection (CM)**: Il CM implementa e applica:

- un canale sicuro basato sul protocollo TLS per la comunicazione con le ECA;
- un canale sicuro basato sul protocollo TLS per la comunicazione con l'utente *Administrator*, attraverso la SSA;
- un canale sicuro basato sul protocollo SSH per la comunicazione con gli utenti *Administrator*, utilizzando l'interfaccia di comando della console nella *shell* ristretta fornita;
- un canale diretto per la comunicazione con gli utenti *Administrator*, utilizzando l'interfaccia di comando della console con una tastiera fisica;
- un canale sicuro basato sul protocollo TLS, per la comunicazione interna tra le MPCA.

- **Communication protection (SAM)**: Il SAM implementa e applica:
  - un canale sicuro basato sul protocollo TLS per la comunicazione con i *Privileged User*, attraverso la SSA;
  - un canale sicuro basato sul protocollo SSH per la comunicazione con i *Privileged User*, utilizzando l'interfaccia di comando della console nella *shell* ristretta fornita;
  - un canale sicuro basato sul protocollo SAP proprietario;
  - un canale diretto per la comunicazione con i *Privileged User*, utilizzando l'interfaccia di comando della console con una tastiera fisica.

- **Distributed structure**: In caso di configurazione distribuita, questa funzione di sicurezza, basata sulla struttura distribuita del drQSCD, garantisce quanto segue:
  - crittografia distribuita;
  - condivisione dei segreti;
  - protezione della coerenza;
  - tolleranza ai guasti.

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'inizializzazione, 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] dichiara conformità *strict* ai seguenti Profili di Protezione:

- EN 419221-5:2018, Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services [PP-CM]
- EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing [PP-SAM]

7.6 Requisiti funzionali e di garanzia

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

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Considerando che il TDS dichiara conformità *strict* ai Profili di Protezione EN 419221-5:2018 [PP-CM] e EN 419241-2:2019 [PP-SAM], sono inclusi anche tutti gli SFR di tali PP, ad eccezione dei seguenti SFR presenti in [PP-SAM]:

- FCS_RNG.1. (in accordo alla Application Note 39 di [PP-SAM])
- FPT_PHP.1 e FPT_PHP.3 (in accordo alla Application Note 69 di [PP-SAM])

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, gli 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 24 luglio 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFVv1]. Due versioni aggiornate dell'RFV ([RFVv2], [RFVv3]) contenenti solo modifiche di lieve entità sono state approvate dall'Organismo di Certificazione rispettivamente il 5 ed il 31 agosto 2020.

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 [RFVv1] (e successivi aggiornamenti) 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 "Trident version 2.1.3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di AVA_VAN.5 e 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 AVA_VAN.5 e 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
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Systematic flaw remediation	*ALC_FLR.3*	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
Advanced methodical vulnerability analysis	AVA_VAN.5	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 "Trident version 2.1.3" 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 cap. 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 rispettivamente nel par. 3.3 e nel par. 3.4 del [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], [DEV-CM], [DEV-SAM], [PRE-CM], [PRE-SAM]).

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

Le fasi di consegna e le procedure necessarie per mantenere la sicurezza durante la distribuzione dell'ODV all'utente finale sono descritte nel cap. 4 di [DEL].

Quando l'ODV viene spedito dal servizio di distribuzione, il cliente riceve anche un'Email con le seguenti informazioni:

- numeri di serie dei sigilli antimanomissione posti sulla confezione;
- numero di serie dell'MPCA;
- numeri di serie dei cavi di sicurezza antimanomissione posti sull'involucro fisico dell'MPCA;
- *checksum* crittografico dell'MPCA;
- nome utente e password per il primo accesso all'MPCA;
- password iniziale del dispositivo PTRNG.

Una volta ricevuto l'ODV, il cliente deve eseguire i passaggi descritti di seguito per assicurarsi che l'MPCA non sia stata manomessa e sia funzionante:

- verificare che i sigilli antimanomissione che proteggono il pacco siano integri e che i loro numeri di serie corrispondano a quelli indicati nell'Email;
- dopo aver disimballato l'MPCA, assicurarsi che tutti i cavi di sicurezza antimanomissione indicati nell'Email siano intatti e controllare anche che il numero di serie dell'MPCA (scritto su un adesivo sul retro dell'unità) e i numeri di serie dei cavi di sicurezza antimanomissione corrispondano a quelli indicati nell'Email;
- collegare l'MPCA ad una fonte di alimentazione adatta, connettere tastiera e display e accenderla (in questa fase non collegare l'MPCA alla rete, in quanto potrebbe costituire un rischio per la sicurezza fino a quando le credenziali dell'utente amministratore non verranno modificate);
- accedere con il nome utente e la password forniti nell'Email e ottenere le informazioni sull'MPCA digitando il comando "getstatus" (senza virgolette) seguito da Invio; il comando fornisce sia il numero seriale, sia il *checksum* crittografico dell'MPCA; controllare che entrambi corrispondano esattamente a quelli indicati nell'Email.

Nel caso uno o più dei controlli sopra descritti dovesse dare esito negativo, l'ODV deve essere restituito al Produttore (I4P) per l'ispezione. Altrimenti, il cliente deve compilare la

lista di controllo per l'accettazione e inviarla firmata a I4P, che provvede alla registrazione del cliente per la garanzia e l'assistenza in caso di problemi.

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- "MPCM Preparation Guide", v1.3, 4 May 2020 [PRE-CM]
- "MPSAM Preparation Guide", v1.3, 4 May 2020 [PRE-SAM]
- "MPCM Development Guide", v1.4, 3 June 2020 [DEV-CM]
- "MPSAM Development Guide", v1.4, 3 June 2020 [DEV-SAM]

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Trident version 2.1.3", sviluppato dalla società I4P-informatikai Kft. (I4P Informatics Ltd.).

La configurazione valutata dell'ODV include i seguenti elementi:

- una, due, tre o quattro MPCA;
- un CD contenente la documentazione di guida in formato PDF.

Ogni MPCA include i seguenti elementi:

- un apparato con chassis metallico, montabile su *rack*, con alimentatore esterno;
- interfacce fisiche:
    - interfacce di rete (3 interfacce Ethernet con TCP/IP);
    - due interfacce USB per l'amministrazione tramite la console locale e per scopi di backup;
    - connettore video per un display locale;
    - singolo o doppio connettore di alimentazione;
    - alloggio per batteria ricaricabile con LED di stato;
    - pulsanti Power/Reset e Tamper/Confirm;
    - indicatori LED;
    - display LCD per informazioni sulla versione.
- hardware interno:
    - scheda madre e CPU;
    - dischi rigidi (HDD) su cui sono memorizzati il software e i dati dell'MPCA (file e record di dati);
    - un Tamper Detection Module che cancella automaticamente le informazioni sensibili e spegne l'apparato quando si tenta di aprirlo;
    - diversi sensori di manomissione;
    - un PTRNG che fornisce un seme casuale generato in hardware per svariate operazioni crittografiche (ad es., generazione di chiavi).
- software interno:

- sistema operativo *hardened* (Red Hat Enterprise Linux versione 7.7, basato sulla versione 7.1 certificata CC);
- *shell* ristretta;
- Multi-Party Cryptographic Module (in caso di configurazione distribuita, le *n* MPCA forniscono congiuntamente la funzionalità CM);
- applicazione client locale del Signature Activation Module (in caso di configurazione distribuita, le *n* LCA SAM forniscono congiuntamente la funzionalità SAM);
- OpenSSL FIPS Object module v2.0.16 (versione validata FIPS 140-2 di OpenSSL).

Per maggiori dettagli, consultare il par. 1.4 del Traguardo di Sicurezza [TDS] e il cap. 2 di [DEL].

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 AVA_VAN.5 e 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

Tutte le attività di test sono state eseguite presso la sede dell'LVS su un campione dell'ODV messo a disposizione dei Valutatori dal Fornitore.

I Valutatori hanno verificato l'integrità dell'ODV, quindi hanno inizializzato e configurato il sistema applicando le procedure di installazione descritte in [PRE-CM] e [PRE-SAM] che forniscono informazioni dettagliate sui requisiti minimi di sistema e sui passi necessari per l'installazione sicura dell'ODV.

Successivamente, i Valutatori hanno verificato che l'ODV fosse installato correttamente e in uno stato noto.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Per la verifica delle funzionalità dell'ODV, il Fornitore ha eseguito test sia manuali, sia automatizzati. I test coprono tutte le funzioni di sicurezza e tutti gli aspetti del TSF.

Il Fornitore ha creato casi di test automatici e manuali. I test vengono effettuati dal Fornitore mediante l'esecuzione di script di test, utilizzando un sistema automatizzato e distribuito. Gli strumenti di test e gli script vengono utilizzati in maniera estesa ed approfondita per verificare che i test restituiscano i valori previsti.

11.2.2 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.

Tutte le possibili scelte dei parametri, anche a livello delle interfacce dei moduli, sono state prese in considerazione almeno una volta. Tutte le operazioni crittografiche, con chiavi di tutte le dimensioni consentite, sono state sottoposte a test almeno una volta. Tutti i casi limite identificati sono stati testati esplicitamente. Le condizioni vicine al limite sono state coperte in maniera probabilistica.

11.2.3 Risultati dei test

I Valutatori hanno selezionato un gran numero di test tra quelli effettuati dal Fornitore per poter coprire una porzione più ampia possibile del TSF, 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 creato i propri casi di test per poter meglio verificare funzionalità dell'ODV che risultavano meno coperte dai test del Fornitore.

I Valutatori hanno selezionato i test con lo scopo di verificare l'ODV in profondità e hanno creato i propri casi di test per aumentare ulteriormente le funzionalità testate, risultando in una copertura più rigorosa delle funzionalità di sicurezza dell'ODV.

Per la selezione dei casi di test del Fornitore da ripetere, i Valutatori si sono concentrati sui seguenti aspetti delle funzioni di sicurezza dell'ODV e delle TSFI:

- funzionalità di creazione e cancellazione dell'utente tramite le API;
- gestione delle chiavi;
- blocco dell'utente.

I Valutatori hanno verificato i risultati effettivi dei test e ne hanno riscontrato la coerenza con i risultati attesi.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso campione dell'ODV già utilizzato per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno effettuato una raccolta di informazioni approfondita sull'ODV al fine di identificare potenziali vulnerabilità dell'ODV.

Le azioni dei Valutatori hanno altresì incluso una scansione completa delle porte e l'esecuzione di diversi attacchi di tipo aggiramento della *shell* e attraversamento delle directory. I Valutatori hanno anche utilizzato lo script LinEnum per verificare la presenza di problemi di elevazione dei privilegi e di enumerazione. Questi passaggi sono stati eseguiti al di fuori del contesto della *shell* limitata, poiché il loro scopo principale è ottenere informazioni e scoprire potenziali vulnerabilità nel sistema operativo e nel software sottostante, piuttosto che direttamente nei servizi MPCM e MPSAM.

I Valutatori hanno quindi eseguito un'analisi metodica avanzata delle vulnerabilità dell'ODV utilizzando la documentazione di guida, le specifiche funzionali, i documenti di progetto dell'ODV, la descrizione dell'architettura di sicurezza e la rappresentazione dell'implementazione al fine di identificare potenziali vulnerabilità nell'ODV.

L'analisi dei Valutatori si è concentrata sui seguenti aspetti, portando all'identificazione di diverse vulnerabilità potenziali:

- exploit di *buffer overflow* sul demone Network Time Protocol (ntpd);
- exploit di elevazione dei privilegi su sudo;
- vulnerabilità di tipo esecuzione di codice da remoto in Docker;
- aggiramento della *shell* ristretta;
- manomissione della gestione delle sessioni;
- *buffer overflow* in MPCM;
- enumerazione degli utenti.

I Valutatori hanno analizzato in dettaglio le potenziali vulnerabilità identificate nelle fasi precedenti allo scopo di verificarne l'effettiva sfruttabilità nell'ambiente operativo dell'ODV.

Sulla base delle potenziali vulnerabilità identificate nella precedente analisi, i Valutatori hanno progettato diversi scenari di attacco e test di intrusione per tentare di sfruttare queste vulnerabilità nell'ambiente operativo dell'ODV, considerando un potenziale di attacco High.

Al termine di tutte le sessioni di test di intrusione svolte, i Valutatori hanno potuto concludere che nessuno scenario di attacco con potenziale High o inferiore 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. Non sono state individuate vulnerabilità residue.