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. 4/19

(Certification No.)

Prodotto: *(Product)* **distributed remote Qualified Signature Creation Device (drQSCD) v1.0**

Sviluppato da: *(Developed by)* **I4P-informatikai Kft. (I4P Ltd.)**

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 Rita Forsi)
Rita Forsi

Roma, 15 maggio 2019

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

distributed remote Qualified Signature Creation Device (drQSCD) v1.0

OCSI/CERT/SYS/06/2017/RC

Versione 1.0

15 maggio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	15/05/2019

2 Indice

3 Elenco degli acronimi

AES Advanced Encryption Standard

API Application Programming Interface

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CM Cryptographic Module

CPU Central Processing Unit

DPCM Decreto del Presidente del Consiglio dei Ministri

DTBS/R Data To Be Signed / Representation

EAL Evaluation Assurance Level

ECA External Client Application

eIDAS Electronic IDentification, Authentication and Signature

HDD Hard Disk Drive

IT Information Technology

LCA Local Client Application

LCD Liquid Crystal Display

LED Light Emitting Diode

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza (ITSEF)

MPC Multi-Party Computation

MPCA Multi-Party Cryptographic Appliance

MPCM Multi-Party Cryptographic Module

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto Della Valutazione

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
SO	Sistema Operativo
SOGIS	Senior Officials Group Information Systems Security
SSA	Server Signing Application
SSH	Secure Shell
TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOTP	Time-based One-Time Password (algorithm)
TSF	TOE (Target of Evaluation) 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 4, September 2012

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

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

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

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

[eIDAS] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 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: distributed remote Qualified Signature Creation Device (drQSCD)”, version 0.4a, 23 October 2018

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v0.15, 29 November 2016

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018

[PRE-CM] “MPCM Preparation Guide”, rev3, 17 January 2019

[PRE-SAM] “MPSAM Preparation Guide”, rev3, 17 January 2019

[RFV] “drQSCD v1.0” Evaluation Technical Report, v1, 6 March 2019

[TDS] “distributed remote Qualified Signature Creation Device (drQSCD)” Security Target, v1.2, 2 May 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 "distributed remote Qualified Signature Creation Device (drQSCD) v1.0", nome abbreviato "drQSCD v1.0", sviluppato dalla società I4P-informatikai Kft. (I4P Ltd.).

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 eIDAS 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).

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 AVA_VAN.5 e 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 "drQSCD v1.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

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	distributed remote Qualified Signature Creation Device (drQSCD) v1.0
Traguardo di Sicurezza	"distributed remote Qualified Signature Creation Device (drQSCD)" Security Target, v1.2, 2 May 2019
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5 e ALC_FLR.3
Fornitore	I4P-informatikai Kft. (I4P Ltd.)
Committente	I4P-informatikai Kft. (I4P Ltd.)
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 4
Conformità a PP	prEN 419 221-5, v0.15 [PP-CM], prEN 419 241-2, v0.16 [PP-SAM]
Data di inizio della valutazione	11 luglio 2017
Data di fine della valutazione	27 marzo 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 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 eIDAS n. 910/2014 [eIDAS] e per eseguire ulteriori operazioni crittografiche di supporto.

Per una descrizione dettagliata dell'ODV, si consulti il cap. 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 o tre 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 cosiddetta **Multi-party Configuration**, l'ODV è composto da tre MPCA identiche che operano in modo distribuito come una sola unità logica che, nel suo insieme, soddisfa i requisiti del Traguardo di Sicurezza [TDS]. Nel caso in cui una delle tre MPCA smette di funzionare, le altre due sono in grado di garantire una funzionalità limitata.

Nel caso della configurazione denominata **Standalone Configuration**, 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.

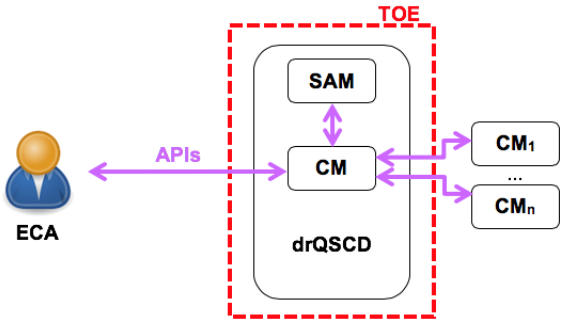

Figura 2 – L'ODV nel caso d'uso "Locale"

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].

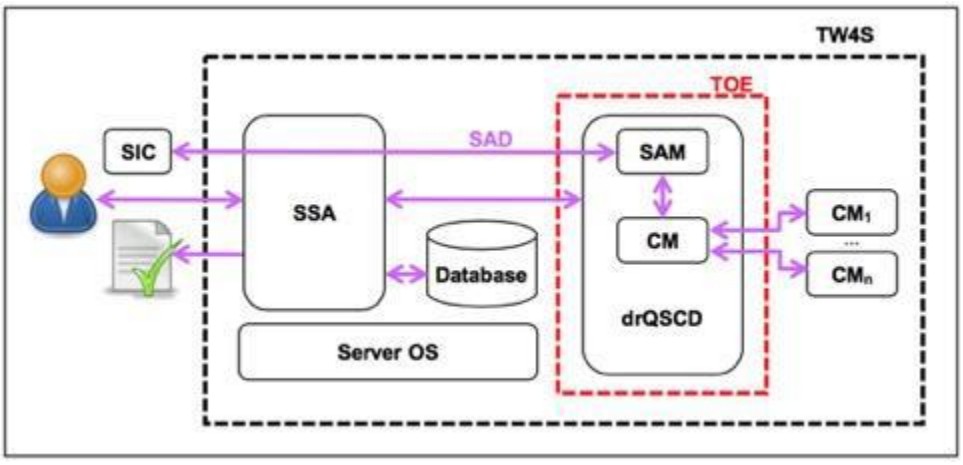

Figura 3 – L'ODV nel caso d'uso "Remoto"

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 e asimmetriche;
- 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 simmetrica e asimmetrica, derivazione di chiavi, verifica di password *one-time* TOTP;
- 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 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 a due fattori del firmatario remoto;
- 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 Multi-party, la **funzionalità MPC** include, ma non è limitata a:

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

Il drQSCD garantisce la coerenza tra le diverse MPCA (ad es., i database e gli stati interni).

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 RSA;
    - 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*;
    - creazione e modifica del record di dati di configurazione e del file di configurazione del SAM;
    - funzioni di backup e ripristino;

- 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 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) e una password statica. La password viene verificata rispetto ai RAD (*hash* cifrato della password + sale) memorizzati nell'account dell'utente come attributo di sicurezza.

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 e una password. Per gli utenti *Signer*, il SAM richiede due diversi fattori di autenticazione: una normale password (fattore basato sulla conoscenza) più una password *one-time* TOTP (fattore basato sul possesso). 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 (*Signer*): 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 cap. 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 capp. 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 distribuite 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 un'operazione crittografica distribuita o la cancellazione di una chiave. Allo stesso tempo, il SAM esegue 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 e assegnarla al proprio account. Solo un *Privileged User* può generare una nuova coppia di chiavi RSA e assegnarla all'account di un utente *Signer*.

  - *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 Multi-party, 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'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 cap. 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:

- Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v0.15, 29 November 2016 [PP-CM]
- Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018 [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 prEN 419 221-5 [PP-CM] e prEN 419 241-2 [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 40 di [PP-SAM])
- FPT_PHP.1 e FPT_PHP.3 (in accordo alla Application Note 67 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 6 marzo 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 27 marzo 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 "drQSCD v1.0" 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 "drQSCD v1.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo 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 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], [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].

Il tipo di protezione applicato corrisponde alla natura del prodotto (software e hardware). Le seguenti procedure garantiscono la sicurezza durante tutte le fasi di consegna:

- L'ODV viene inserito nella sua scatola di spedizione, sigillato con nastro di sicurezza ed etichettato.
- Il servizio di distribuzione sotto contratto spedisce l'ODV al cliente, il quale verifica l'integrità dei sigilli antimanomissione sulla scatola di spedizione.
- Se la scatola non è stata manomessa, il cliente disimballa l'ODV e controlla i sigilli antimanomissione e i cavi sull'apparato.
- Se l'ODV non risulta fisicamente danneggiato, il cliente avvia l'ODV e controlla il *checksum* crittografico e il numero di serie sullo schermo. Il numero di serie e il *checksum* vengono inviati al cliente via Email prima della consegna.
- Il cliente compila la lista di controllo per l'accettazione e la invia firmata al Produttore (I4P), che provvede alla registrazione del cliente per la garanzia e l'assistenza in caso di problemi.
- In caso si riscontrino segni di manomissione o il numero di serie e/o il *checksum* di controllo non corrispondono, l'ODV deve essere restituito a I4P per l'ispezione.

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", rev3, 17 January 2019 [PRE-CM]
- "MPSAM Preparation Guide", rev3, 17 January 2019 [PRE-SAM]

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "distributed remote Qualified Signature Creation Device (drQSCD) v1.0", sviluppato dalla società I4P-informatikai Kft. (I4P Ltd.).

L'ODV è identificato nel Traguardo di Sicurezza [TDS] come "drQSCD version 1.0".

La configurazione valutata dell'ODV include i seguenti elementi:

- una o tre MPCA;
- la documentazione di guida, che fornisce informazioni sulla configurazione valutata e consente di installare e utilizzare correttamente l'ODV.

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;
    - 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 supportate dal sistema operativo (SO) certificato;
    - 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* (basato su Red Hat Enterprise Linux versione 7.1 certificato CC);
    - *shell* ristretta;
    - Multi-Party Cryptographic Module (in caso di configurazione Multi-party, le tre MPCA forniscono congiuntamente la funzionalità CM);
    - applicazione client locale del Signature Activation Module (in caso di configurazione Multi-party, le tre 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 cap. 1.4 del [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

Per l'esecuzione delle attività di test, il Committente/Fornitore ha messo a disposizione l'ODV ai Valutatori nelle seguenti due configurazioni:

- tre MPCA fisiche per i test indipendenti e la valutazione delle vulnerabilità;
- una vMPCA virtuale per la ripetizione dei test del Fornitore.

I Valutatori hanno installato l'ODV applicando le procedure di installazione descritte in [PRE-CM] e [PRE-SAM] ("Setting up the system") 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 utilizzato i seguenti strumenti e *suite* di test:

- Maven
- Java
- Red Hat Linux

Il Fornitore ha eseguito test approfonditi sull'ODV, a livello di sottosistemi, moduli e interfacce dei moduli. 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 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.

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:

- Test delle autorizzazioni alla generazione di firme mediante esecuzione del comando di firma con parametri corretti e non corretti, con una o più chiavi proprietarie e con diversi utenti nei ruoli *Administrator* e *User*.

- Test della funzione di decifratura del modulo MPCM con parametri di input validi e non validi, con particolare attenzione al *padding*. La cifratura è effettuata con OpenSSL.

- Test del comando `mpc_passwd` con parametri corretti e non corretti.

- Test del comando `login` con parametri e password corretti e non corretti.

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 sulle stesse configurazioni dell'ODV già utilizzate per le attività dei test funzionali, verificando che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno effettuato delle ricerche in libri e articoli disponibili pubblicamente, riferibili alle minacce documentate nel Traguardo di Sicurezza [TDS], al fine di individuare possibili vulnerabilità dell'ODV. I Valutatori hanno quindi confrontato le informazioni reperite con le minacce contrastate dall'ODV, identificando alcune potenziali vulnerabilità applicabili all'ODV nel suo ambiente operativo.

In una seconda fase, i Valutatori hanno effettuato delle ricerche sulla rete Internet allo scopo di individuare tutte le vulnerabilità note applicabili a tipologie di prodotti simili all'ODV. In questa ricerca i Valutatori hanno utilizzato parole chiave specifiche (versioni di componenti software vulnerabili) per selezionare i risultati migliori, concentrandosi in particolare su pubblicazioni specialistiche, documenti di ricerca e atti di conferenze reperibili su siti professionali.

I Valutatori hanno altresì sottoposto l'ODV a scansioni di vulnerabilità utilizzando strumenti software commerciali.

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:

- gestione delle sessioni;
- gestione dei comandi e validazione dell'input da parte delle interfacce delle API;
- gestione dei ruoli;
- uscita dalla *shell* ristretta;
- vulnerabilità di SSH;
- funzione di backup/ripristino.

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, cioè vulnerabilità che potrebbero essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.