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

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. 8/22

(Certification No.)

Prodotto: Ascertia ADSS Server Signature Activation Module v7.0.2

(Product)

Sviluppato da: Ascertia 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)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da
Eva Spina
Data: 2022.04.29 09:09:46
+02'00'

Roma, 29 aprile 2022

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

Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2

OCSI/CERT/CCL/11/2021/RC

Versione 1.0

29 aprile 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	29/04/2022

2 Indice

3 Elenco degli acronimi

API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CM	Cryptographic Module
CPU	Central Processing Unit
DB	Database
DMZ	Demilitarized Zone
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
eIDAS	Electronic IDentification, Authentication and Signature
GUI	Graphical User Interface
HMAC	Keyed-hash Message Authentication Code
HSM	Hardware Security Module
HW	Hardware
ID	Identifier
IdP	Identity Provider
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One-time Password
PIN	Personal Identification Number
PP	Protection Profile

QES	Qualified Electronic Signatures and Seals
QSCD	Qualified Signature Creation Device
RAS	Remote Application Server
RFV	Rapporto Finale di Valutazione
SAD	Signature Activation Data
SAM	Signature Activation Module
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCAL2	Sole Control Assurance Level 2
SFR	Security Functional Requirement
SIC	Signer's Interaction Component
SSA	Server Signing Application
SO	Sistema Operativo
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
SW	Software
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TW4S	Trustworthy System Supporting Server Signing
XML	eXtensible Markup Language

4 Riferimenti

4.1 Criteri e normative

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

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

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

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

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

[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

[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

[DEL] “ALC_DEL: Delivery Procedures - ADSS Server Signature Activation Module (SAM) v7.0”, v4, Ascertia Ltd., 28 March 2022

[PRE] “AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v5, Ascertia Ltd., 6 April 2022

[RC] “Rapporto di Certificazione Ascertia ADSS Server Signature Activation Module v6.0”, OCSI/CERT/SYS/08/2017/RC, versione 1.0, 13 marzo 2019

[RFV] “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” Evaluation Technical Report, v2, CCLab Software Laboratory, 20 April 2022

[TDS] “Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, v8, Ascertia Ltd., 19 April 2022

[USR] “AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v3, Ascertia Ltd., 28 March 2022

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 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 "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2", nel seguito del documento anche indicato come "ADSS Server SAM", sviluppato da Ascertia Ltd.

L'ODV è un Trustworthy System Supporting Server Signing (TW4S) che offre servizi di firma e sigillo elettronico con accesso da remoto, garantendo che le chiavi di sottoscrizione sono utilizzate sotto il controllo esclusivo del firmatario e soltanto per gli scopi previsti. L'ODV consente la creazione da remoto di firme elettroniche e di sigilli elettronici qualificati (QES) conformi al Regolamento eIDAS [eIDAS].

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 (Ascertia ADSS Server Signature Activation Module (SAM) v6.0), già certificato dall'OCSI (Certificato n. 2/19 del 13 marzo 2019 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore Ascertia Ltd., 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 "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2".

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, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in "AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v5, 6 April 2022 [PRE]

- “AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v3, 28 March 2022 [USR]

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 "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2" 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	Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2
Traguardo di Sicurezza	"Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2", v8 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di AVA_VAN.5
Fornitore	Ascertia Ltd.
Committente	Ascertia Ltd.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419241-2:2019 [PP-SAM]
Data di inizio della valutazione	13 settembre 2021
Data di fine della valutazione	20 aprile 2022

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 "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2" è un Trustworthy System Supporting Server Signing (TW4S) che offre servizi di firma e sigillo

elettronico con accesso da remoto, garantendo che le chiavi di sottoscrizione sono utilizzate sotto il controllo esclusivo del firmatario e soltanto per gli scopi previsti.

L'ODV consente la creazione da remoto di firme elettroniche e di sigilli elettronici qualificati (QES) conformi al Regolamento eIDAS [eIDAS] con Sole Control Assurance Level 2 (SCAL2) conforme a EN 419241-1.

La soluzione di firma remota di ADSS Server SAM consiste di un ambiente locale e di uno remoto, come illustrato in Figura 1. Il firmatario può avviare una transazione di firma interagendo con l'ODV tramite una Business Application.

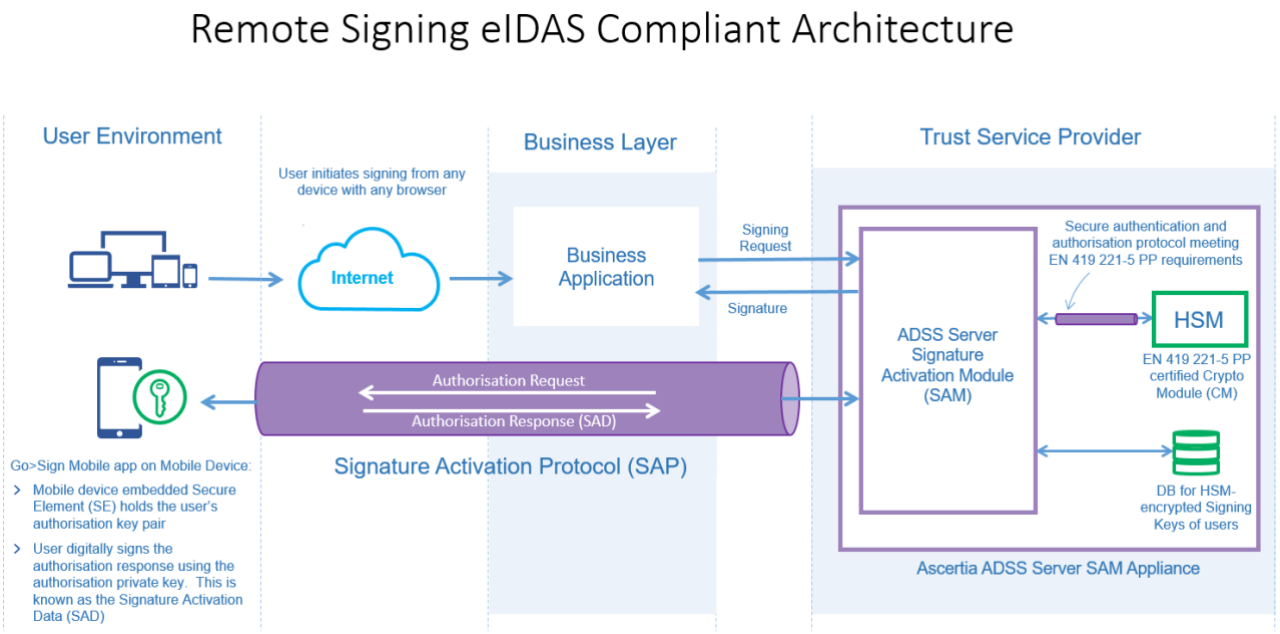

Figura 1 - Soluzione remota per QES conformi al Regolamento eIDAS

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

7.3.1 Architettura dell'ODV

L'ODV consiste dei seguenti tre componenti:

- **ADSS Server SAM Service**: fornisce diversi servizi web per eseguire varie operazioni, quali ad es. registrazione dell'account di un utente, inclusi la chiave di utente e il suo dispositivo mobile, firma delle transazioni e degli *hash*, ecc.

- **ADSS Server SAM Admin Console**: consente agli amministratori di configurare il prodotto, ad es. definizione del controllo di accesso, gestione dell'utente/firmatario, gestione del dispositivo del firmatario, configurazione del dispositivo crittografico (HSM), ecc.

- **ADSS Server SAM Core**: realizza varie operazioni in background, ad es. archiviazione dei log, monitoraggio del DB e dell'HSM, ecc.

L'ODV viene fornito all'interno di un dispositivo hardware protetto da manomissioni che garantisce un ambiente di esecuzione sicuro. L'ODV è costituito dall'hardware anti-manomissione e dai componenti software all'interno del confine logico di ADSS Server SAM mostrato nella Figura 2. Il sistema operativo, il server delle applicazioni, l'HSM, il database, ecc., non appartengono all'ODV.

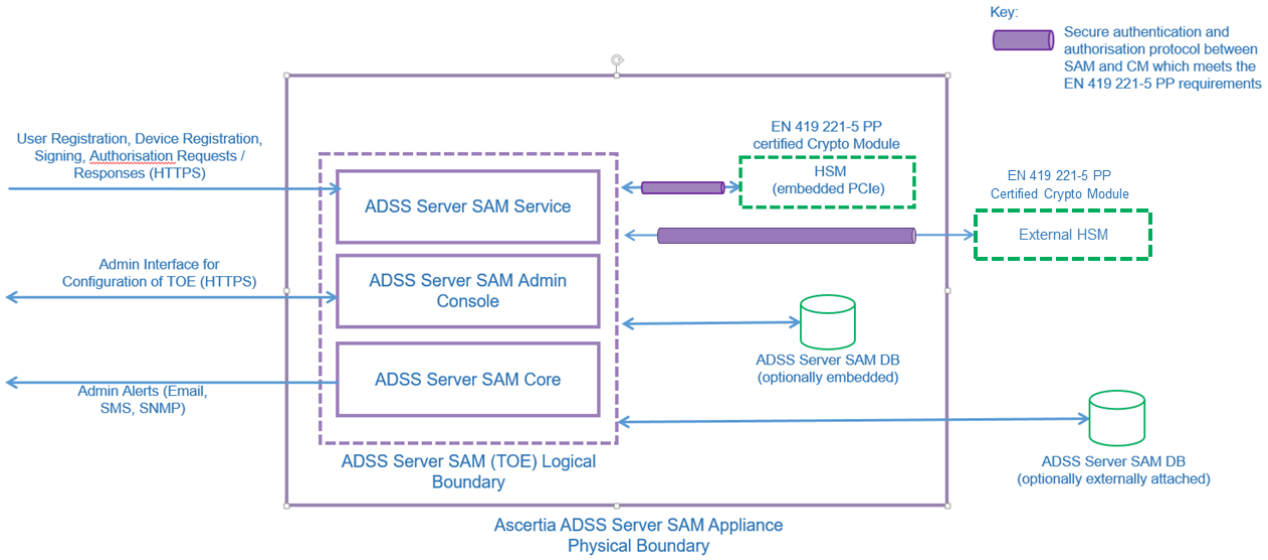

Figura 2 - Confine logico dell'ODV

7.3.1.1 Ruoli e funzioni disponibili

L'ODV prevede i seguenti ruoli:

- *Privileged Users*. Ci sono due tipi di utenti privilegiati che possono eseguire operazioni specifiche dell'ODV tramite l'ADSS Server SAM Admin Console o le ADSS Server SAM API disponibili esternamente:
  - *Ascertia ADSS Server SAM Operators (Operators)*: accedono tramite l'Ascertia ADSS Server SAM Admin Console per eseguire diverse operazioni specifiche dell'ODV, quali ad es. configurazione delle comunicazioni con l'HSM, ecc. Questi operatori affidabili vengono creati nell'ADSS Server SAM Admin Console e ciascun operatore è identificato da un "Operator ID".
  - *Business Applications*: accedono all'ODV mediante API fornite dal servizio RAS per eseguire diverse operazioni specifiche dell'ODV: da un lato gestiscono i *Signers* (Firmatari) (User Module) e dall'altro agiscono come applicazione per la creazione della firma (SCA). Ciascuna Business Application è identificata da un "Client ID".
- *Unprivileged Users.*
  - *Signers* (Firmatari): possono richiedere operazioni di firma da remoto interagendo con le Business Application e quindi autorizzano queste operazioni utilizzando l'app Ascertia Go>Sign Mobile per fornire i dati di autorizzazione richiesti.

7.3.1.2 Autenticazione e Autorizzazione

Si verificano I seguenti processi di Autenticazione e Autorizzazione:

- *Operators*: devono connettersi all'ODV utilizzando i certificati client TLS prima di poter eseguire qualunque attività sull'ADSS Server SAM Admin Console. I certificati client TLS degli Operator e le chiavi private associate devono essere memorizzati su *smart card* o *token* USB sicuri, fornendo così un ulteriore livello di sicurezza per la chiave privata oltre l'autenticazione a due fattori degli operatori. L'Ascertia ADSS Server SAM Admin Console garantisce che l'accesso agli oggetti di sistema sia strettamente controllato in base al ruolo dell'utente. Per ogni ruolo viene definito a quali oggetti di sistema può accedere e il tipo di accesso, ad es. sola lettura o modifica/crea/cancella.

- *Business Applications*: devono essere autenticate prima di accedere alle API dell'ODV. Le Business Application devono inoltre autenticarsi utilizzando il rispettivo certificato client TLS poiché tutte le comunicazioni avvengono tramite il canale TLS con autenticazione reciproca. Il termine Business Application si riferisce all'ADSS RAS Service attraverso il quale vengono effettuate tutte le interazioni delle app aziendali con l'ODV.

- *Signers* (Firmatari): sono identificati dall'ID utente e autenticati durante la registrazione del dispositivo da due OTP inviati al numero di cellulare registrato e all'indirizzo Email dell'utente. Durante l'operazione di firma, i Firmatari sono identificati tramite il loro ID utente e autenticati dalla risposta di autorizzazione firmata XML (SAD).

7.3.1.3 Supporto Crittografico

L'ODV non esegue operazioni crittografiche per i suoi utenti (*Signers*): non genera/archivia/distrugge, esporta/importa, esegue il backup/ripristino o usa la chiave di utente. L'ODV richiama il modulo crittografico (CM) con i parametri appropriati ogni volta che è necessaria un'operazione crittografica per l'utente *Signer*, ovvero l'autorizzazione a usare la *Assigned Key*.

L'ODV utilizza diverse chiavi di infrastruttura per proteggere i suoi file archiviati, 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 utente e autenticazione**: l'ODV mantiene i ruoli di *Privileged User* (*Operator* o *Business Application*) e *Unprivileged User* (*Signer*) e associa gli utenti ai ruoli. L'ODV identifica gli utenti mediante un identificativo utente univoco. L'ODV garantisce che ogni utente abbia un solo ruolo, di conseguenza un *Signer* non può essere un *Privileged User*. Questi utenti sono memorizzati e gestiti in diversi

sottosistemi e identificati con ID diversi (Operator ID, Client ID, User ID).
I Privileged User si autenticano con l'ODV tramite il canale TLS. La Business Application si autentica col suo ID cliente e il certificato. L'Operator si autentica con il suo certificato memorizzato su una *smart card* protetta da PIN.
I *Signer*s (Firmatari) utilizzano l'autenticazione tramite impronta digitale all'interno dell'app Go>Sign Mobile (se il Firmatario ha già effettuato l'accesso) per autorizzare una richiesta di firma, ovvero creare il SAD. Questo vale per l'autenticazione diretta. In caso di autenticazione delegata, l'IdP supportato fornisce l'asserzione successivamente all'autenticazione dell'utente e tale asserzione viene aggiunta nel SAD generato al momento dell'autorizzazione.

- **Sicurezza delle chiavi**: l'ODV richiama con parametri appropriati un modulo crittografico (CM) certificato in conformità con il Profilo di Protezione EN 419221-5 [PP-CM] per qualsiasi operazione di gestione delle chiavi o di crittografia e per la generazione di numeri casuali.

- **Controllo degli accessi e del flusso di informazioni**: quando ADSS Server SAM viene installato, viene automaticamente creato un account di tipo Operator con un certificato di operatore predefinito. L'operatore predefinito accede all'ADSS Server SAM Admin Console e crea *Privileged Users*, ad esempio ADSS Server SAM *Operators* e Client Applications.
  L'ODV garantisce che solo una Business Application come *Privileged User* può creare un nuovo utente *Signer* (Firmatario) e avviare la generazione di una coppia di chiavi per conto del Firmatario. Un tipico processo di registrazione del Firmatario prevede la registrazione dei dettagli dell'utente *Signer* e la generazione di una coppia di chiavi per la firma remota e di un certificato digitale. Una volta registrati i dettagli del Firmatario, la Business Application richiede all'ADSS RAS Service di generare la coppia di chiavi di firma per il Firmatario. ADSS Server SAM utilizza il modulo crittografico (CM) per generare e archiviare in modo sicuro la coppia di chiavi di firma per il Firmatario.

- **Protezione dei dati**: l'ODV implementa funzionalità di sicurezza contro la manomissione fisica. L'ODV rileva quando viene aperto l'involucro dell'ODV e azzera i dati sensibili e interrompe l'alimentazione principale. Ciò garantisce che vengano preservate l'integrità e la riservatezza dei beni protetti. Durante lo stato di manomissione, tutte le funzionalità dell'ODV vengono interrotte e non viene fornito alcun servizio (sia quelli di firma, sia quelli di amministrazione) anche se l'ODV viene riavviato hardware. Quando l'ODV viene riavviato hardware, mantiene lo stato di manomissione in modo tale che la precedente condizione di manomissione possa essere segnalata.

- **Audit**: l'ODV utilizza un database di audit posto al di fuori dei confini dell'ODV. L'ODV registra tutti gli eventi relativi alla sicurezza in questo database. Ogni record di audit contiene la data e l'ora dell'evento (utilizzando un *timestamp* attendibile), il tipo di evento, l'identità del soggetto (l'identità dell'utente che ha causato l'evento se disponibile, ovvero un utente identificato che ha avviato l'evento) e il risultato (successo o fallimento) dell'evento. La traccia di controllo non include alcun dato che consenta il recupero di dati sensibili.
  L'integrità dei dati memorizzati in una qualsiasi delle tabelle del database è protetta da un approccio HMAC sequenziale. La chiave simmetrica HMAC è conservata in modo sicuro nel modulo crittografico (CM).

- **Protezione delle comunicazioni**: l'ODV protegge i dati dell'utente durante il trasporto garantendone riservatezza e integrità. Il SIC comunica in modo sicuro con il modulo RAS Service, la SCA con la SSA e la SSA con l'ODV su un canale TLS v1.2/1.3. La comunicazione con il modulo crittografico (CM) avviene attraverso un canale sicuro utilizzando comandi di API specifiche del produttore. Gli operatori dell'ODV (come *Privileged Users*) accedono alla GUI dell'ADSS Server SAM Admin Console su un canale TLS v1.2/1.3 con autenticazione reciproca.

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* al seguente Profilo di Protezione:

- 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]. Poiché il TDS dichiara conformità *strict* al Profilo di Protezione EN 419241-2:2019 [PP-SAM], sono inclusi anche tutti gli SFR definiti in tale PP.

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 20 aprile 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 22 aprile 2022. 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 "AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v5, 6 April 2022 [PRE]

- "AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v3, 28 March 2022 [USR]

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 "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in "AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v5, 6 April 2022 [PRE]

- "AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v3, 28 March 2022 [USR]

Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5.

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

Classi e componenti di garanzia		Verdetto
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
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 5.1 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di Sicurezza dell'Organizzazione e le ipotesi descritte rispettivamente nel par. 4.2.2.2 e nel par. 4.2.2.3 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([DEL], [PRE], [USR]).

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 dell'ODV

Le fasi di consegna e le procedure necessarie per mantenere la sicurezza durante la distribuzione dell'ODV al cliente sono descritte nel documento Delivery Procedures [DEL].

Ascertia fornisce l'ODV al suo distributore SAM autorizzato tramite download da un sito sicuro. Ascertia consente al distributore l'accesso all'area dedicata del sito di download del prodotto ADSS SAM Appliance. La conferma che il download è pronto viene inviata al distributore SAM via Email. L'Email contiene il *checksum* crittografico del software caricato assieme ai dettagli del cliente a cui deve essere spedita l'ADSS Server SAM Appliance.

Il distributore SAM verifica il *checksum* del software ADSS Server SAM dopo averlo scaricato dal sito sicuro di Ascertia. Il distributore SAM assembla l'ADSS Server SAM Appliance installando i componenti richiesti, vale a dire:

- sistema operativo;
- database;
- l'HSM certificato EN 419221-5 approvato (contattando il produttore dell'HSM e assicurandone la consegna in modo sicuro secondo le procedure definite).

Successivamente il distributore SAM inserisce nel dispositivo il software ADSS Server SAM verificato tramite *checksum*.

Il distributore SAM si accerta che la SAM Appliance sia adeguatamente sigillata/protetta e la consegna in modo sicuro al cliente, informando Ascertia e il cliente sullo stato.

Il cliente finale che riceve il prodotto deve verificare che i sigilli dell'ADSS Server SAM Appliance non siano stati manomessi.

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]:

- "AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0", v5, 6 April 2022 [PRE]

- “AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v3, 28 March 2022 [USR]

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2", sviluppato dalla società Ascertia Ltd.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 7.0.2. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

La configurazione valutata utilizza le impostazioni di sicurezza della modalità certificata Common Criteria e un CM certificato. I passaggi per l'installazione sicura dell'ODV secondo la configurazione valutata CC sono descritti nel cap. 5 del documento Preparation Procedure [PRE].

10.1 Ambiente operativo dell'ODV

In Tabella 2 sono riportati sinteticamente i requisiti minimi hardware e software dei componenti dell'ambiente operativo dell'ODV.

Per maggiori dettagli sulla predisposizione dell'ambiente operativo dell'ODV si rimanda al cap. 4 del documento Preparation Procedure [PRE].

Componente	Requisiti
ADSS Server SAM (un'applicazione Java EE 8 supportata sulle piattaforme elencate)	**Sistema operativo** Sono supportati i seguenti sistemi operativi a 64 bit: • Red Hat Enterprise Linux 8.4
	Hardware AIC-TB116AN con FIPS 140-2 Level 3 Protection Intel Xeon CPU RAM 32GB ECC DIMM e SSD da 960GB
	Database ADSS Server SAM salva la sua configurazione e i dati di log transazionali in un database. Sono supportati i seguenti database: • Percona-XtraDB-Cluster v8.x (Una variante di MySQL)
Browser dell'operatore	I seguenti browser sono supportati per gli operatori di ADSS Server SAM: • Google Chrome 70.x o superiore • Firefox 60.x o superiore • Edge 35.x o superiore • Internet Explorer (IE) 11.X+
HSM	Sono supportati i seguenti HSM certificati CC EN 419221-5: • Utimaco HSMs (CP5 Se500 o Se1500) • Thales Luna K7 HSMs • Entrust nShield Solo XC HSMs
Macchina Proxy DMZ opzionale	Se necessario, è possibile configurare un server proxy DMZ. Sono

Componente	Requisiti
	supportate le seguenti macchine proxy DMZ: • Windows Server + IIS o Apache o IBM HTTP Server • Linux + Apache o IBM HTTP Server Utilizzare una CPU adeguata, 8 GB di RAM, 40 GB di spazio su disco
SO per dispositivi mobili	Per la firma remota autorizzata, le app native (iOS e Android) Go>Sign Mobile richiedono le seguenti versioni di SO: • iOS 11 o superiore • Android 6 (Marshmallow) o superiore

Tabella 2 - Componenti dell'ambiente operativo dell'ODV e requisiti di sistema

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 l'aggiunta di AVA_VAN.5, tali attività tali attività prevedono tre passi successivi:

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

11.1 Configurazione per i Test

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

Prima dell'esecuzione dei test, l'ODV è stato installato e configurato seguendo le istruzioni contenute nella documentazione di guida ([PRE], [USR]). Dopo la configurazione dell'ODV i Valutatori hanno verificato che l'ODV fosse stato installato correttamente e che tutti i servizi necessari funzionassero come previsto.

L'ambiente di test così realizzato è lo stesso utilizzato dal Fornitore per testare le TSFI. In particolare, per il test delle interfacce API è stato usato lo strumento Postman, insieme a un breve documento esplicativo sul suo utilizzo predisposto dal Fornitore.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Il Fornitore ha utilizzato un approccio ai test che ha portato a coprire tutte le TSFI con almeno un caso di test. Il Fornitore ha creato diversi casi di test fornendone una descrizione dettagliata, con tutte le informazioni necessarie per la loro corretta ripetizione, inclusi i prerequisiti per i test, le procedure di test passo-passo, i risultati attesi e quelli ottenuti per ciascun test.

I Valutatori hanno verificato che i risultati ottenuti dei test riportati nella documentazione di test del Fornitore fossero coerenti con i risultati attesi.

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.

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.

I Valutatori hanno rieseguito i casi di test indipendenti selezionati in occasione della valutazione della precedente versione certificata CC dell'ODV, con alcune correzioni dovute a modifiche nei casi di test del Fornitore. Per ottenere una migliore copertura, i Valutatori hanno selezionato casi di test aggiuntivi al fine di incrementare ulteriormente il numero di casi di test ripetuti.

I casi di test aggiuntivi eseguiti dai Valutatori hanno riguardato i seguenti aspetti del TSF:

- Riavvio di tutti i servizi
- Registrazione di un nuovo client
- Configurazione della funzione di Import/Export
- Login ad ADSS Server SAM
- Logout da ADSS Server SAM
- Registrazione di un utente
- Modifica della password

Questi casi di test sono stati realizzati usando come base i casi di test creati durante la precedente valutazione; i Valutatori hanno effettuato alcune modifiche per poterli applicare alla versione corrente dell'ODV, basandosi sul pacchetto Postman ricevuto.

Sebbene siano state rilevate anomalie durante l'esecuzione di alcuni casi di test, il Fornitore ha provveduto a correggerle e i Valutatori sono stati infine in grado di ripetere tutti i casi di test senza alcun problema.

Tutti i test indipendenti eseguiti dai Valutatori hanno avuto esito positivo, ovvero tutti i risultati dei test sono risultati conformi a quelli previsti.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso ambiente di test 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 condotto ricerche su fonti pubbliche per identificare potenziali vulnerabilità dell'ODV, concentrandosi sulle vulnerabilità scoperte

successivamente alla precedente valutazione. I Valutatori hanno utilizzato il motore di ricerca Google e vari database di vulnerabilità, tra cui Snyk Open Source Vulnerability Database, CVE Details e NIST National Vulnerability Database (NVD), per cercare vulnerabilità nei pacchetti utilizzati dall'ODV. Questa attività ha portato ad individuare due potenziali vulnerabilità.

In una seconda fase, i Valutatori hanno condotto un'analisi metodica del Traguardo di Sicurezza, della documentazione di guida, delle specifiche funzionali, del progetto dell'ODV, della descrizione dell'architettura di sicurezza e della rappresentazione dell'implementazione al fine di evidenziare ulteriori potenziali vulnerabilità nell'ODV. I Valutatori hanno individuato un'altra potenziale vulnerabilità su cui indagare, ma la successiva analisi ha mostrato che la sua non applicabilità all'ODV. Non sono state identificate ulteriori vulnerabilità potenzialmente sfruttabili.

I Valutatori hanno quindi progettato dei possibili scenari di attacco e condotto test di intrusione per verificare l'effettiva sfruttabilità delle vulnerabilità potenziali individuate nell'ambiente operativo dell'ODV, considerando un potenziale d'attacco di livello High.

Le due vulnerabilità riscontrate sono risultate effettivamente sfruttabili durante la prima sessione di test. Il Fornitore ha rilasciato un aggiornamento minore dell'ODV contenente le correzioni relative a questi problemi. I Valutatori hanno ripetuto i test di intrusione e hanno verificato che le due vulnerabilità fossero state effettivamente corrette.

Sulla base dei risultati della seconda sessione di test di intrusione, i Valutatori hanno quindi concluso che nessuno scenario di attacco con potenziale High 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.