Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 2/19

(Certification No.)

Prodotto: Ascertia ADSS Server Signature Activation Module v6.0
(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 Rita Forsi)
Rita Forsi

Roma, 13 marzo 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

Ascertia ADSS Server Signature Activation Module v6.0

OCSI/CERT/SYS/08/2017/RC

Versione 1.0

13 marzo 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

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

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CM	Cryptographic Module
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
eIDAS	Electronic IDentification, Authentication and Signature
HSM	Hardware Security Module
HW	Hardware
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
PP	Profilo di Protezione
QSCD	Qualified Signature Creation Device
RFV	Rapporto Finale di Valutazione
SAD	Signature Activation Data
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SFR	Security Functional Requirement
SIC	Signer’s Interaction Component
SSA	Server Signing Application
SW	Software
TDS	Traguardo di Sicurezza

TSF TOE Security Functionality

TSFI TSF Interface

4 Riferimenti

4.1 Criteri e normative

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

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

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

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

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

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

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

4.2 Documenti tecnici

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v015, 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

[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

[DEL] “Ascertia ADSS Server Signature Activation Module (SAM)” Delivery Procedures, v2, 24 October 2018

[PRE] “Ascertia ADSS Server Signature Activation Module (SAM)” Preparation Procedure, v4, 30 January 2019

[RFV] “Ascertia ADSS Server Signature Activation Module (SAM) v6.0” Evaluation Technical Report, v1, 7 February 2019

[TDS] “Ascertia ADSS Server Signature Activation Module (SAM) v6.0” Security Target, v18, 1 October 2018

[USR] “Ascertia ADSS Server Signature Activation Module (SAM)” Operational User Guidance, v4, 10 December 2018

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 "Ascertia ADSS Server Signature Activation Module (SAM) v6.0", nome abbreviato "ADSS Server SAM v6.0", sviluppato dalla società Ascertia Ltd.

L'ODV è un Trustworthy System Supporting Server Signing (TW4S) che offre servizi di firma elettronica da remoto, garantendo che la/le chiavi di firma del Firmatario sono utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.

L'ODV fornisce un servizio, con accesso da remoto, per la creazione di firme elettroniche e di sigilli elettronici qualificati conformi al Regolamento eIDAS n. 910/2014 [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).

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, 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 "ADSS Server SAM v6.0" 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	Ascertia ADSS Server Signature Activation Module (SAM) v6.0
Traguardo di Sicurezza	"Ascertia ADSS Server Signature Activation Module (SAM) v6.0" Security Target, v18, 1 October 2018
Livello di garanzia	EAL4 con 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	prEN 419 241-2, v0.16 [PP-SAM]
Data di inizio della valutazione	27 settembre 2017
Data di fine della valutazione	7 febbraio 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 Trustworthy System Supporting Server Signing (TW4S) che offre servizi di firma elettronica da remoto, garantendo che la/le chiavi di firma del Firmatario sono utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.

L'ODV fornisce un servizio, con accesso da remoto, per la creazione di firme elettroniche e di sigilli elettronici qualificati conformi al Regolamento eIDAS n. 910/2014 [eIDAS]. Questa soluzione remota consiste di un ambiente locale e di uno remoto, come illustrato in Figura 1.

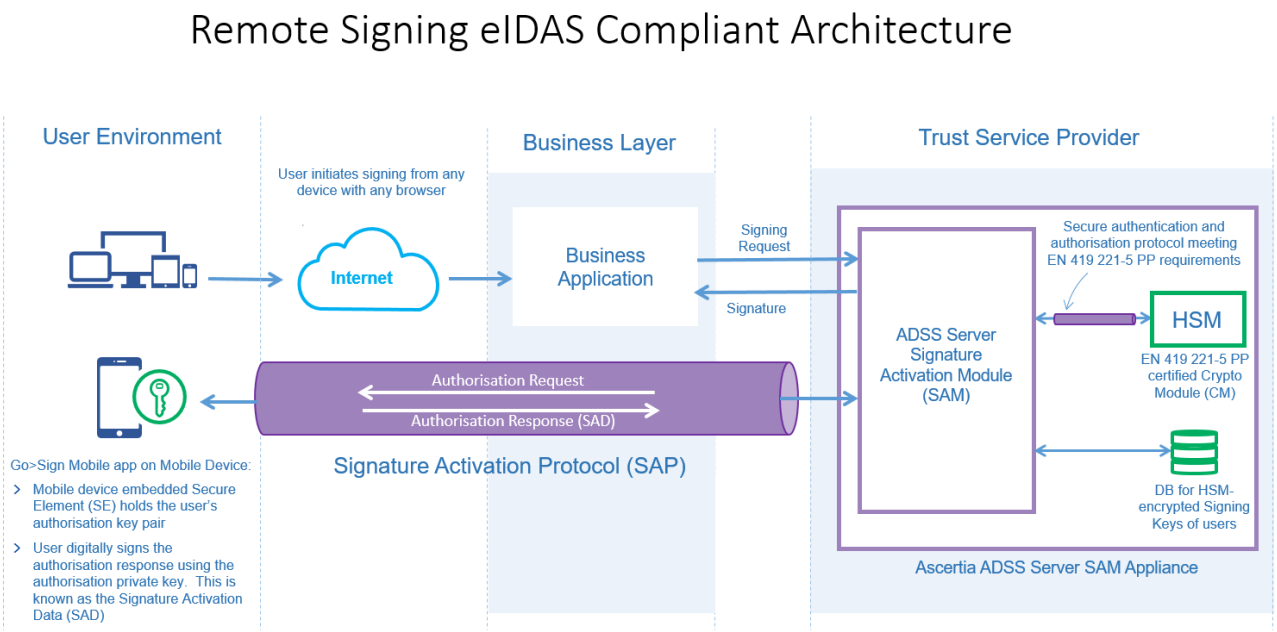

Figura 1 – Soluzione remota per firme elettroniche qualificate conformi al Regolamento eIDAS

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

7.3.1 TOE Architecture

L'ODV "ADSS Server SAM" consiste dei seguenti tre componenti:

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

2. **ADSS Server SAM Admin Console**, che 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.

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

Il confine fisico dell'ODV è un hardware anti-manomissione, all'interno del quale si trovano diversi componenti, quali il sistema operativo, il server delle applicazioni, l'HSM, il database ecc. che non appartengono all'ODV. L'ODV è costituito dall'hardware anti-manomissione e dai componenti software all'interno del confine logico dell'ODV mostrato nella Figura 2.

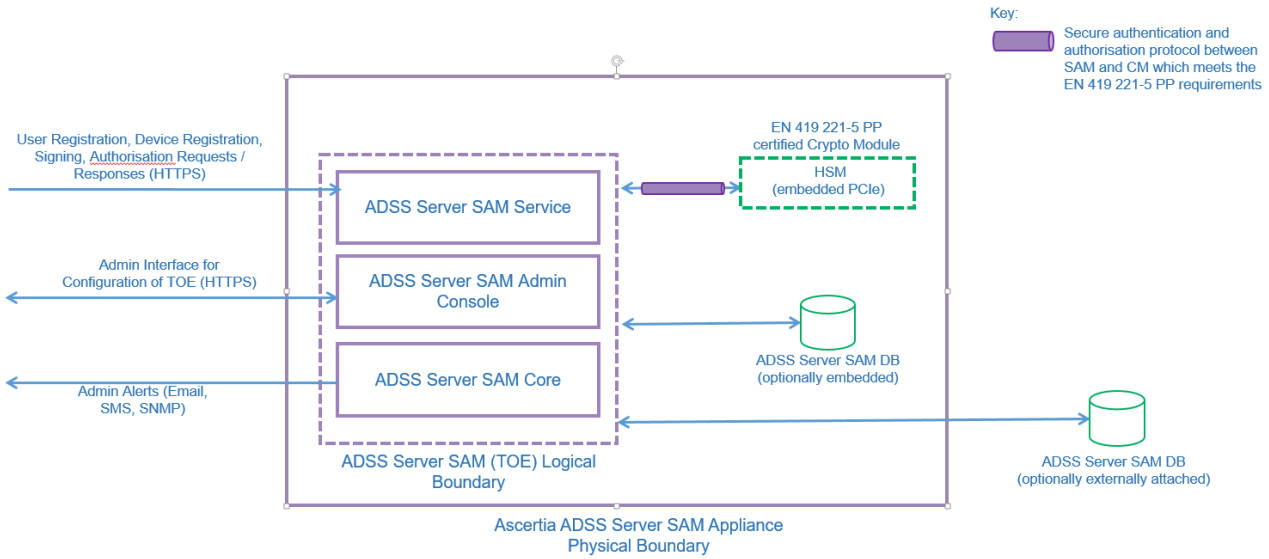

Figura 2 – Confine logico dell'ODV

7.3.1.1 Ruoli e funzioni disponibili

L'ODV prevede i seguenti ruoli:

- *Privileged Users*. Ci sono due tipi di questi utenti che possono eseguire specifiche operazioni dell'ODV tramite l'ADSS Server SAM Admin Console o delle interfacce API disponibili esternamente:
  - *Operators*, che accedono tramite l'Admin Console per eseguire diverse operazioni specifiche dell'ODV, quali ad es. configurazione delle comunicazioni con l'HSM, ecc. questi operatori fidati sono creati nell'Admin Console e ciascun operatore è identificato da un "Operator ID".
  - *Business Applications*, che accedono tramite interfacce 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*, che possono richiedere da remoto operazioni di firma interagendo con le Business Applications 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 sulla Admin Console. I certificati client TLS degli Operators e le chiavi private associate devono essere memorizzate su smart

card/token USB sicure, fornendo così un ulteriore livello di sicurezza per la chiave privata oltre l'autenticazione a due fattori degli Operators. Lo stato di revoca dei certificati TLS degli Operators può anche essere verificato al momento dell'accesso configurandolo nell'Admin Console. Tuttavia, si consiglia di aggiornare immediatamente gli account degli Operators sull'ODV al momento della revoca di un certificato. L'Admin Console garantisce che l'accesso agli oggetti di sistema sia strettamente controllato. Gli utenti vengono prima identificati e autenticati come spiegato sopra, e una volta completato questo processo e l'utente ha effettuato correttamente l'accesso, l'accesso agli oggetti di sistema viene 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 Applications devono inoltre autenticarsi utilizzando il rispettivo certificato client TLS poiché tutte le comunicazioni avvengono tramite il canale TLS reciprocamente autenticato. Si noti che qui il termine Business Applications si riferisce al Servizio RAS di ADSS attraverso il quale tutte le interazioni delle app aziendali sono effettuate 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 e-mail dell'utente. Durante l'operazione di firma, i firmatari sono identificati tramite il loro ID utente e autenticati dalla risposta di autorizzazione firmata (SAD).

7.3.1.3 Supporto Crittografico

L'ODV non esegue operazioni crittografiche per i suoi utenti (Signers): in modo esplicito 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 di crittografia per il firmatario, ovvero l'autorizzazione a usare la chiave assegnata.

L'ODV utilizza diverse chiavi di infrastruttura per proteggere i suoi file archiviati e 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.

- **User Roles and Authentication (TSF_AUTH)**. L'ODV provvede i ruoli di Privileged User (Operator o Business Application) and 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 utente privilegiato. Questi utenti sono memorizzati e gestiti in diversi sottosistemi e identificati con ID diversi (ID operatore, ID client, ID utente).

- **Key Security (TSF_CRYPTO)**. L'ODV richiama con parametri appropriati un modulo crittografico (CM) certificato in conformità con il Profilo di Protezione prEN 419 221-5 [PP-CM] per qualsiasi operazione di gestione delle chiavi o crittografia, generazione di numeri casuali.

- **Access and information flow control (TSF_CTRL).** Quando l'ODV viene installato, viene automaticamente creato un account operatore con un certificato Operatore predefinito. L'operatore predefinito accede alla Admin Console e crea Utenti Privilegiati, ad esempio Operatori e Applicazioni Client. Quando l'operatore accede alla Admin Console utilizzando il certificato dell'operatore predefinito, viene visualizzata una finestra di avviso all'operatore per indicare come modificare il certificato predefinito con il nuovo certificato dell'operatore. Se l'operatore non configura un nuovo certificato entro 7 (sette) giorni, l'accesso dell'operatore alla Admin Console viene bloccato e sarà necessaria la reinstallazione completa dell'ODV. Solo gli operatori possono gestire gli utenti privilegiati dopo l'autenticazione avvenuta con successo.

- **Data protection (TSF_DP)**. L'ODV implementa funzionalità di sicurezza contro la manomissione fisica. L'ODV rileva quando viene aperto il contenitore dell'ODV e azzera i dati sensibili e interrompe l'alimentazione principale. Ciò garantisce che l'integrità e la riservatezza delle risorse siano preservate. Durante lo stato di manomissione, tutte le funzionalità dell'ODV vengono interrotte e non viene fornito alcun servizio (sia quelli firmatari sia quelli amministrativi) anche se l'ODV viene riavviato dall'hardware. Quando l'ODV viene riavviato, l'hardware manterrà lo stato di manomissione in modo tale da potersi riportare alla condizione precedente la manomissione.

- **Audit (TSF_AUDIT)**. L'ODV utilizza un database di controllo al di fuori dei confini dell'ODV. L'ODV registra tutti gli eventi relativi alla sicurezza nel Database. Ogni record di audit contiene la data e l'ora dell'evento (utilizzando un timestamp affidabile), il tipo di evento, l'identità del soggetto (l'identità dell'utente che ha causato l'evento se applicabile, ovvero un utente identificato che ha avviato l'evento) e il risultato (successo o fallimento) dell'evento. L'audit trail 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).

- **Communication protection (TSF_COMM)**. L'ODV fornisce protezione dei dati dell'utente durante il trasporto. Garantisce sia la riservatezza che l'integrità. Il componente di interazione col Signer/Firmatario (SIC) comunica in modo sicuro con il modulo del servizio RAS, la SCA con SSA e la SSA con il ODV sul canale TLS v1.2. La comunicazione con il modulo crittografico (CM) avviene attraverso un canale sicuro utilizzando comandi API specifiche del fornitore. Gli operatori dell'ODV (come Privileged Users) accedono alla GUI della Admin Console su un canale TLS v1.2 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'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *strict* al seguente Profilo di Protezione:

- 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].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. In particolare, poiché il TDS dichiara stretta conformità al Profilo di Protezione prEN 419 241-2, v0.16 [PP-SAM], sono inclusi anche gli SFR definiti in tale PP.

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 7 febbraio 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 26 febbraio 2019. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLab Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "ADSS Server SAM v6.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di AVA_VAN.5, 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.

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
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 "ADSS Server SAM v6.0" 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 par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel [TDS].

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

Ascertia fornirà l'ODV al suo distributore SAM autorizzato. Il software viene cifrato utilizzando un file zip protetto con password e caricato in un'area FTP protetta ospitata da Ascertia. Le credenziali per l'accesso all'area FTP verranno fornite al distributore SAM autorizzato in modo sicuro tramite posta elettronica cifrata. L'e-mail conterrà anche il checksum crittografico del software caricato. La stessa e-mail conterrà anche i dettagli del cliente a cui deve essere spedito l'ODV. Ascertia fornirà dettagli al suo distributore SAM su come verificare il checksum crittografico.

Il distributore SAM verifica il checksum del software ADSS Server SAM dopo averlo scaricato dal sito FTP Ascertia. Il distributore SAM costruirà l'appliance SAM Server ADSS installando i componenti richiesti, vale a dire:

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

Quindi il software ADSS Server SAM verificato tramite checksum verrà inserito nell'appliance dal distributore SAM.

Il distributore SAM garantirà che l'appliance SAM sia adeguatamente sigillata/protetta e la consegnerà in modo sicuro al cliente e informerà Ascertia e il cliente sullo stato (ETA).

Il cliente finale che riceve l'appliance garantirà che i sigilli dell'appliance ADSS Server SAM non siano stati manomessi.

Maggiori dettagli su tale procedura sono contenuti nelle "Procedure di consegna" [DEL] del Modulo di Attivazione del server di firma ADSS Ascertia (SAM)".

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

Il software ADSS Server SAM verrà quindi installato dal cliente finale seguendo la documentazione di distribuzione definita.

- "Ascertia ADSS Server Signature Activation Module (SAM)" Preparation Procedures [PRE]. La preparazione richiede che la copia consegnata dell'ODV sia accettata, configurata e attivata dall'utente per mostrare le proprietà di protezione necessarie durante il funzionamento dell'ODV. Le procedure preparatorie forniscono la certezza che l'utente sarà a conoscenza dei parametri di configurazione dell'ODV e di come possono influenzare le TSF.

- “Ascertia ADSS Server Signature Activation Module (SAM)” Operational user guidance [USR]. Questo documento aiuta a garantire che tutti i tipi di utenti siano in grado di utilizzare l’ODV in modo sicuro. La guida operativa dell'utente è il principale veicolo a disposizione dello sviluppatore per fornire agli utenti dell’ODV il background necessario e le informazioni specifiche su come utilizzare correttamente le funzioni di protezione dell’ODV.

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Ascertia ADSS Server Signature Activation Module (SAM) v6.0", nome abbreviato "ADSS Server SAM v6.0", sviluppato dalla società Ascertia Ltd.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 6.0. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

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

10.1 Ambiente operativo dell'ODV

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

Per maggiori dettagli, consultare il par. 1.4.3 del [TDS].

Component	Requirement
ADSS Server SAM (a Java EE 8 application supported on the listed platforms)	Operating System: • Red Hat Enterprise Linux 7.4
	Hardware: • AIC-TB116-AN A modern multi-core CPU such as the Xeon E3-xxxx or E5-xxxx series is recommended, with 8GB RAM (minimum 4GB RAM) and 2GB disk space. Consider 12 GB RAM if the database is deployed on the same host as ADSS Server SAM or for high performance or throughput systems.
	Database: • Percona-XtraDB-Cluster 5.7.21 (A variant of MySQL)
Client systems (system sending service request to ADSS Server)	Any reasonable system: • ADSS Client SDK for Java API requires JRE v1.6 or above • ADSS Client SDK for .NET requires Microsoft .NET Framework 4.0 or above
Operator browsers	The following browsers are supported for ADSS Server SAM Operators: • Google Chrome 30+ • Firefox 25+ • Edge 38+ • Internet Explorer (IE) 9+

HSM	The following Hardware Security Modules are supported: • Utimaco HSMs (CP5 Se500 or Se1500)
Optional DMZ Proxy machine	If required, a DMZ proxy server can be configured. The following DMZ proxy machines are supported: • Windows Server + IIS or Apache or IBM HTTP Server • Linux + Apache or IBM HTTP Server Use a reasonable CPU, 2GB RAM,100 MB disk space
Mobile Devices OS	For authorised remote signing, the native apps (iOS and Android) of Go>Sign Mobile will require the following OS versions: • iOS 9.0 or above • Android 6 (Marshmallow) or above

Tabella 2 – Componenti dell'ambiente operativo dell'ODV

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4, con aggiunta di AVA_VAN.5, tali attività prevedono tre passi successivi:

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

11.1 Configurazione per i Test

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

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

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

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

11.2.2 Risultati dei test

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

11.3 Test funzionali ed indipendenti svolti dai Valutatori

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

A parte il già citato Postman per le interfacce API, non sono stati utilizzati altri strumenti di test particolari, oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

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

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

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

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.3.

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

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

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

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco High, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi. Per l'esecuzione dei test i Valutatori hanno utilizzato diversi strumenti (Kali Linux, Burp Suite Pro, boofuzz, TLS Attacker 1.2 e tlsfuzzer).

Dall'esecuzione dei test di intrusione, i Valutatori hanno effettivamente riscontrato 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 neanche vulnerabilità residue, cioè vulnerabilità che potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.