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. 4/18

(Certification No.)

Prodotto: **PassBy[ME] Server System v1.2**
(Product)

Sviluppato da: **Microsec 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:

EAL2

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 8 maggio 2018

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

PassBy[ME] Server System v1.2

OCSI/CERT/SYS/03/2017/RC

Versione 1.0

8 maggio 2018

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	08/05/2018

2 Indice

3 Elenco degli acronimi

2FA	Second Factor Authentication Subsystem
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OCSP	Online Certificate Status Protocol
ODV	Oggetto della Valutazione
PKI	Public Key Infrastructure (Infrastruttura a Chiave Pubblica)
PP	Profilo di Protezione
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SCEP	Certificate Enrollment Server
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
TDS	Traguardo di Sicurezza

TLS	Transport Layer Security
TOE	Target Of the Evaluation
TSA	Time Stamp Authority
TSF	TOE Security Functionality
TSFI	TSF Interface
UI MGMT	User Interface Management

4 Riferimenti

[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

[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

[AGD] PassBy[ME] Server Administrator Guide, Version 1.3, 9 January 2018

[CMS] PassBy[ME] Server Configuration Management Scope, Version 1.1, 6 November 2017

[OPE] PassBy[ME] Server Operational User Guide, Version 1.2, 20 October 2017

[RFV] PassBy[ME] Server Evaluation Technical Report, v1, 12 March 2018

[SIM] PassBy[ME] Appliance System Installation Manual, Version 1.1.21, 29 November 2017

[TDS] PassBy[ME] Server Security Target, v1.7, 11 October 2017

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 per tutti i componenti di garanzia indicati.

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 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 per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "PassBy[ME] Server System v1.2", sviluppato dalla società Microsec Ltd.

L'ODV fornisce il secondo fattore di uno schema di autenticazione, basato su dispositivi mobili, implementato da un provider di servizi online (ad es., il servizio di banking online o di accesso al cloud).

In particolare, l'ODV è una soluzione di ID mobile basata su PKI, che fornisce autenticazione di utente, firma delle transazioni e firma digitale mobile.

Il sistema è composto da due parti:

- il servizio server, chiamato PassBy [ME] Server System (che costituisce l'ODV), che comprende l'amministrazione di utenti e applicazioni, il controllo delle iscrizioni e la memorizzazione dei dati per l'autenticazione e la verifica;

- l'applicazione client in esecuzione su un dispositivo mobile (che non fa parte dell'ODV).

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, 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 "PassBy[ME] Server System v1.2" 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	PassBy[ME] Server System v1.2
Traguardo di Sicurezza	PassBy[ME] Server Security Target, v1.7, 11 October 2017
Livello di garanzia	EAL2
Fornitore	Microsec Ltd.
Committente	Microsec Ltd.
LVS	Systrans Software Laboratory - CCLAB
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	10 maggio 2017
Data di fine della valutazione	12 marzo 2018

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 riassunte le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV fornisce il secondo fattore di uno schema di autenticazione, basato su dispositivi mobili, implementato da un provider di servizi online (ad es., il servizio di banking online o di accesso al cloud).

In particolare, l'ODV è una soluzione di ID mobile basata su PKI, che fornisce autenticazione di utente, firma delle transazioni e firma digitale mobile.

Il sistema è composto da due parti:

- il servizio server, chiamato PassBy [ME] Server System (che costituisce l'ODV), che comprende l'amministrazione di utenti e applicazioni, il controllo delle iscrizioni e la memorizzazione dei dati per l'autenticazione e la verifica;

- l'applicazione client in esecuzione su un dispositivo mobile (che non fa parte dell'ODV).

Ogni utente riceve la propria chiave privata generata sul dispositivo smartphone. Ciò garantisce che la chiave privata esista in una sola copia. In uno scenario di e-Commerce, quando si effettua un acquisto online, il fornitore di servizi a pagamento convaliderà la transazione richiedendo una seconda autenticazione tramite lo smartphone. Il cliente riceverà un avviso sul suo dispositivo mobile e una richiesta di autorizzazione della transazione. Il cliente sarà in grado di confermare o rifiutare la transazione. Il fornitore di servizi a pagamento autorizzerà la transazione solo se l'autenticazione del cliente ha avuto esito positivo e il cliente ha confermato la transazione online.

7.3.1 Architettura dell'ODV

Per una descrizione maggiormente dettagliata dell'ODV, consultare il capitolo 1.5 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti (vedi Figura 1).

I componenti dell'ODV (blocchi verdi in Figura 1) sono i seguenti:

- PUBLIC Server (Apache), che fornisce l'interfaccia esterna per i seguenti servizi:
    - Web-based management interface: accessibile tramite connessione HTTPS, richiede il secondo fattore, l'autorizzazione di PassBy [ME], per fornire tutte le funzionalità;
    - Authentication and Management service API: accessibile dopo l'autenticazione basata su certificati mutuamente riconosciuti (RFC 5246);
    - Authorization interface for the mobile applications: accessibile dopo l'autenticazione TLS basata su certificati mutuamente riconosciuti.

- Second Factor Authentication Subsystem (2FA): controlla il processo del secondo fattore di autenticazione. Accetta le richieste dal fornitore di servizi e in base all'ID di utente fornito comunica con il dispositivo mobile dell'utente. La decisione dell'utente viene firmata e restituita utilizzando un canale mutuamente autenticato.

- User Interface Management (UI MGMT): elabora tutte le richieste di amministrazione esterna che arrivano attraverso il PUBLIC server. Il suo compito principale è la gestione degli utenti e degli amministratori di un'organizzazione (gestione di un'organizzazione), la convalida delle firme, la gestione dei certificati, la strumentazione di Messaging Server e la memorizzazione dei dati di controllo rilevanti.

- Certificate Enrollment Server (SCEP): utilizzato dai dispositivi mobili per richiedere certificati per le loro chiavi generate a bordo. Oltre alle specifiche SCEP originali, la comunicazione viene instradata attraverso un canale TLS, in cui il server è autenticato. Il processo di registrazione serve per associare un dispositivo mobile a un utente.

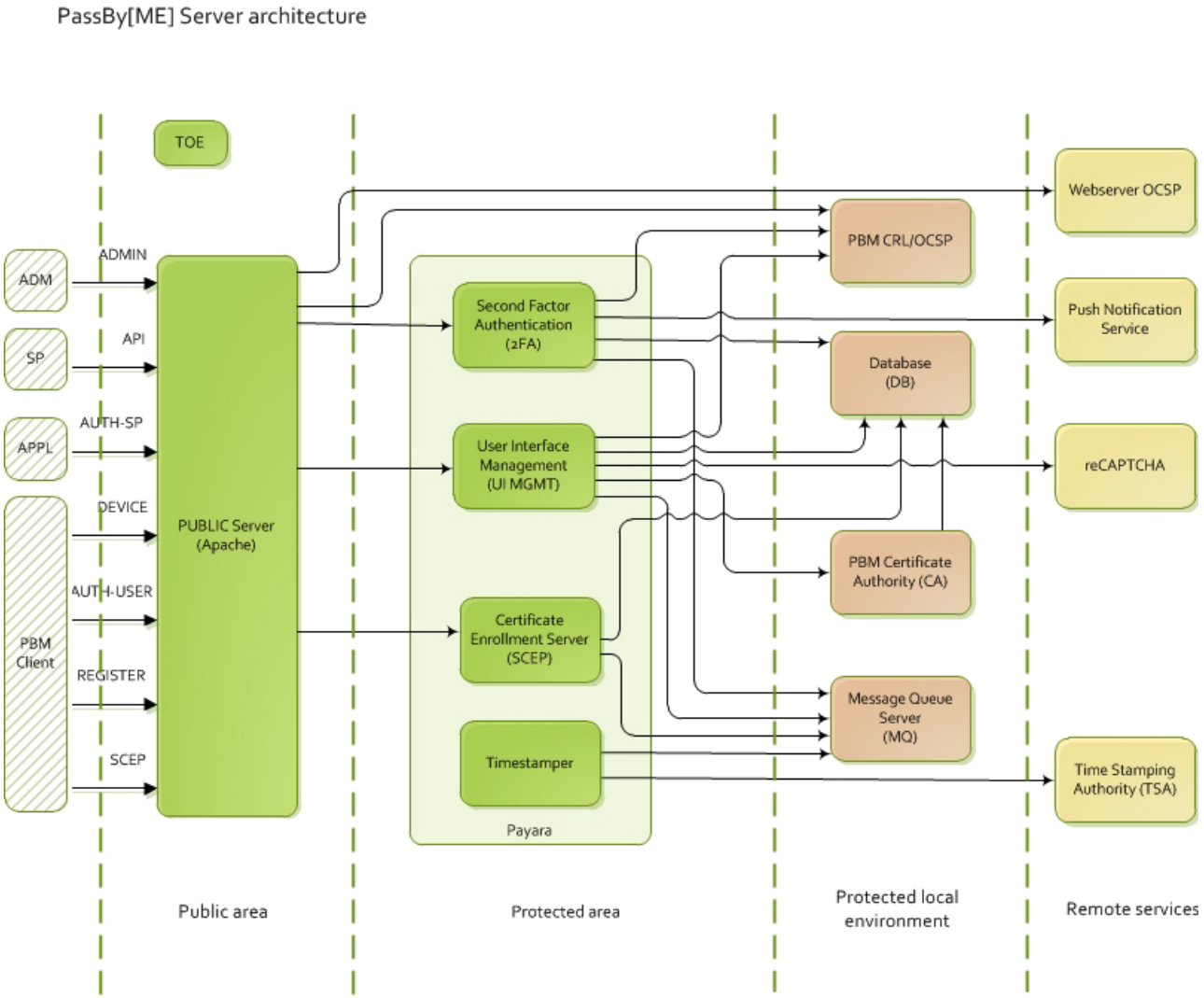

Figura 1 – Confini dell'ODV

- Timestamper: per garantire la validità a lungo termine delle prove generate, il sistema PassBy [ME] applica le marche temporali sulle prove firmate. Il sottosistema Timestamper crea le marche temporali utilizzando il servizio di una Time Stamp Authority (TSA).

Tutti gli altri componenti non fanno parte dell'ODV, ma del suo ambiente operativo.

L'interfaccia esterna dell'ODV è il PUBLIC server. Questa interfaccia consente al dispositivo mobile e al fornitore di servizi di comunicare con il server PassBy [ME]. Per la comunicazione verranno utilizzati canali HTTPS sicuri. Il PUBLIC server contiene più host virtuali, specializzati per un determinato tipo di messaggio o attività. A seconda dell'attività richiesta, il messaggio verrà inviato all'interfaccia utente del sottosistema MGMT, 2FA o SCEP. Per convalidare il certificato degli utenti verrà utilizzato il servizio OCSP o CRL.

I messaggi degli utenti, che contengono una risposta o una decisione, verranno marcati temporalmente e memorizzati nel sistema. Per le funzioni PKI verranno utilizzati i servizi OCSP, CA, Time stamping. Per le funzioni PKI interne, come SSL e la gestione dei certificati, verranno utilizzate le funzioni e le librerie integrate Java di OpenSSL e BouncyCastle.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Nell'utilizzo operativo dell'ODV verranno applicate le seguenti funzionalità di sicurezza:

- PKI Based Entity Authentication: ogni connessione in entrata all'ODV utilizza TLS per proteggere la comunicazione. Laddove applicabile, viene utilizzata l'autenticazione TLS basata su certificati mutuamente riconosciuti per fornire un'autenticazione forte del client.

- PKI Signature Verification: l'autorizzazione alla transazione si basa sulle firme digitali. Il dispositivo mobile dell'utente che riceve un messaggio invia automaticamente al server una prova firmata per ricevuta. La decisione dell'utente di accettare o rifiutare una transazione verrà firmata con la chiave privata memorizzata nel dispositivo mobile e verrà inviata anche al server.

- Certificate Path Validation: l'autenticità di tutti i certificati utilizzati deve essere verificata nel server. Un certificato può essere accettato solo se è possibile convalidare l'intero percorso del certificato di origine. Per la convalida, verranno utilizzati i servizi OCSP o CRL.

- Online Certificate Status Protocol Client: per ottenere lo stato effettivo di un certificato verrà utilizzato il servizio di un risponditore OCSP. È configurabile quale metodo verrà applicato (OCSP o CRL) per il controllo dei certificati.

- Certificate Revocation List (CRL) Validation: la convalida CRL è una delle possibilità per verificare lo stato di un certificato.

- Audit: genera un registro di controllo sulle attività degli amministratori di un'organizzazione, sugli eventi di comunicazione e sulle transazioni firmate dall'utente. Per estendere la validità delle prove firmate dall'utente, l'ODV marca temporalmente tutte le prove firmate utilizzando una TSA.

7.3.2.1 Funzioni di sicurezza

I requisiti funzionali di sicurezza implementati dall'ODV sono raggruppati per comodità nelle seguenti classi di funzioni di sicurezza:

- **Security Audit**. L'ODV tiene traccia di tutti gli eventi importanti verificatisi nel sistema. Le attività degli amministratori di un'organizzazione verranno registrate nel database con un indicatore temporale. Le transazioni dell'utente verranno registrate con la marca temporale e archiviate nel formato PKCS # 7 (Cryptographic Message Syntax Standard).

- **User Data Protection**. La protezione dei dati dell'utente definisce in che modo gli utenti dell'ODV possono eseguire operazioni sugli oggetti. I dati dell'utente si trovano nei messaggi, nel database, nel filesystem. L'amministratore di sistema ha un ruolo fidato ed è responsabile dell'intero sistema. Ogni amministratore di un'organizzazione può gestire solo i dati della propria organizzazione. PassBy [ME] gestisce solo una minima quantità di dati relativi all'utente e non richiede l'utilizzo di dati riservati. La maggior parte dei dati utilizzati durante l'operatività viene generata all'interno del sistema e non ha alcun significato al di fuori del contesto dei sistemi PassBy [ME].

- **Identification and Authentication**. Tutti gli utenti, i dispositivi mobili e i fornitori di servizi sono identificati e autenticati tramite certificati emessi da una Certification Authority (CA) configurata di PassBy [ME]. Per la convalida, verranno utilizzati i servizi OCSP o CRL. Gli amministratori di un'organizzazione utilizzano nome utente/password e devono passare un'autenticazione a due fattori utilizzando PassBy [ME] per accedere all'interfaccia di amministrazione basata sul Web. Solo i fornitori di servizi in possesso di un certificato di autenticazione valido possono eseguire operazioni di gestione tramite API. Il sistema PassBy [ME] utilizza segreti condivisi per rafforzare la sicurezza dei processi in cui la PKI non è applicabile.

- **Security Management**. Nel sistema PassBy [ME] tutti i parametri di sicurezza importanti sono regolabili per soddisfare i requisiti dell'ambiente di hosting. Il principale componente di sicurezza del sistema PassBy [ME] è l'infrastruttura PKI sottostante, i cui parametri sono tutti configurabili. Il sistema PassBy [ME] applica periodi di validità ai diversi processi per proteggerli. Questi timeout dipendono dalla configurazione fornita o dai parametri di input. Il sistema PassBy [ME] utilizza segreti condivisi per rafforzare la sicurezza dei processi in cui la PKI non è applicabile. La lunghezza della chiave di questi segreti è configurabile dall'amministratore di sistema.

Per maggiori dettagli vedi il par. 1.5.2 del [TDS].

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita ai clienti insieme al prodotto. La documentazione indicata contiene tutte le informazioni richieste per l'installazione, 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] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

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

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. In particolare, sono inclusi anche i seguenti componenti estesi (vedi [TDS], par. 5):

- FDP_DAU_CPV_EXT.1 Certificate processing
- FDP_DAU_CPI_EXT.1 Certification path initialization
- FDP_DAU_CPD_EXT.1 Certification path development
- FDP_ITC_SIG_EXT.1 PKI Signature Verification
- FDP_DAU_OCS_EXT.1 Basic OCSP Client

- FDP_DAU_CRL_EXT.1 Basic CRL Checking
- FIA_UAU_SIG_EXT.1 Entity Authentication

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

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Systrans CCLAB.

L'attività di valutazione è terminata in data 12 marzo 2018 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 17 aprile 2018. 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 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 "PassBy[ME] Server System v1.2" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, 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 EAL2.

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
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	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
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo

Classi e componenti di garanzia		**Verdetto**
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	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 "PassBy[ME] Server System v1.2" 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 organizzative e le ipotesi descritte nel TDS.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto include 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 ([AGD] e [OPE]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per i potenziali acquirenti del prodotto.

9.1 Consegna

Le componenti dell'ODV, PassBy[ME] Server System v1.2, sono consegnate in forma di archivi compressi memorizzati su supporto elettronico (DVD o USB-token). Il supporto è registrato in formato standard leggibile su sistemi Linux.

Il pacchetto consegnato può essere accettato dal cliente se contiene i seguenti elementi:

- Pacchetto di installazione in forma compressa
- Note di rilascio firmate elettronicamente con firma qualificata da Microsec Ltd.
- Note di installazione
- PassBy[ME] Server Operational User Guide [OPE]
- PassBy[ME] Server Administrator Guide [AGD]

La procedura di accettazione dell'ODV è eseguita dall'Amministratore di Sistema, seguendo le indicazioni fornite nella Guida per l'Amministratore [AGD].

9.2 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'installazione dell'ODV si compone di due fasi.

1. Preparazione dell'ambiente operativo, che consiste nell'installazione del sistema operativo Linux (RHEL or CentOS), con Web Server (Apache) installato e connessione di rete attiva. Il pacchetto dell'ODV consegnato, controllato e accettato, contiene degli script per predisporre l'ambiente operativo. Tutto il lavoro di preparazione, dalla decompressione del pacchetto all'esecuzione degli scripts, viene eseguito dall'Amministratore di Sistema. Indicazioni utili per l'installazione dell'ambiente operativo (switches, routers, servers) possono essere trovate nel documento pubblico:
    - PassBy[ME] Appliance System Installation Manual [SIM]
2. L'installazione e la configurazione dell'ODV devono essere realizzate seguendo le indicazioni contenute negli appositi paragrafi della documentazione fornita ai clienti insieme al prodotto, e in particolare in:
    - PassBy[ME] Server Administrator Guide [AGD]

10 Appendice B – Configurazione valutata

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 1.2. 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.

I componenti della configurazione valutata sono elencati dettagliatamente nella Lista di Configurazione, fornita dallo sviluppatore ai Valutatori nel documento [CMS].

10.1 Componenti dell'ODV

I sottosistemi dell'ODV, con i loro numeri di versione, sono riportati sinteticamente in Tabella 2. Si noti che tutti i sottosistemi hanno lo stesso numero di versione, che corrisponde alla versione rilasciata e distribuita dell'ODV.

Per maggiori dettagli, consultare anche il par. 1.5.1 del [TDS].

Nome	Riferimento	Versione	Data
2FA subsystem	microsec-pbm-2nd-factor-web-1.2.war	1.2	November 2017
UI MGMT subsystem	microsec-pbm-ui-web-1.2.war	1.2	November 2017
Timestamper subsystem	microsec-pbm-timestamper-web-1.2.war	1.2	November 2017
SCEP subsystem	microsec-pbm-scep-web-1.2.war	1.2	November 2017

Tabella 2 – Sottosistemi dell'ODV

10.2 Ambiente operativo dell'ODV

In Tabella 3 sono riportati sinteticamente i requisiti minimi dell'ambiente operativo dell'ODV per consentirne la corretta operatività.

Per maggiori dettagli, consultare anche il par. 1.5.2 del [TDS].

Nome	Sviluppatore	Versione	Data
Operating System CentOS x86_64	The CentOS Project	7.4.1708	December 2016
Operating System RHEL	Red Hat Inc.	7.4.x	July 2017
Apache HTTP Server	The Apache Software Foundation	2.4.6	July 2017
Payara Application Server	Payara Services Ltd.	4.1.2.173	August 2017
Java Standard Edition for Linux x64	Oracle Corporation	1.8.0_152	July 2017
OpenSSL *(part of Linux operating system)*	OpenSSL Software Foundation	1.0.1efips	February 2013
PostgreSQL	The PostgreSQL Global Development Group	9.6.6	November 2017
OpenMQ Server	Oracle Corporation	5.1	September 2017
Online Certificate Status Protocol (OCSP)	Microsec Ltd.	1.2.15	November 2017
Certification Authority (CA)	Microsec Ltd.	1.2	November 2017

Tabella 3 – 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 EAL2 tali attività prevedono tre passi successivi:

- valutazione in termini di copertura 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.

L'installazione dell'ambiente di test è avvenuta seguendo le istruzioni contenute nella documentazione di supporto ([AGD], [OPE], [SIM]), come indicato in Appendice A – Indicazioni per l'uso sicuro del prodotto. Dopo la configurazione dell'ODV i valutatori hanno verificato che l'ODV è stato installato correttamente e tutti i servizi previsti funzionavano correttamente.

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

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

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

11.2.2 Risultati dei test

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

11.3 Test funzionali ed indipendenti svolti dai Valutatori

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

Non sono stati utilizzati strumenti di test particolari, 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, 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.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) ed utilizzato strumenti di scansione automatica (Nessus, Acunetix e BurpSuite Pro), al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, 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 Basic, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

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

I Valutatori hanno così concluso che nessuno degli scenari di attacco ipotizzati con potenziale Basic può essere portato a termine con successo nell'ambiente operativo dell'ODV. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Non sono state individuate neanche vulnerabilità residue, cioè vulnerabilità che, pur non essendo sfruttabili nell'ambiente operativo dell'ODV, potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a Basic.