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. 9/22

(Certification No.)

Prodotto: **Firma Elettronica Avanzata MPS v. 2.0**
(Product)

Sviluppato da: **Banca Monte dei Paschi di Siena S.p.A.**
(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:

EAL1

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da Eva Spina
Data: 2022.05.11 09:39:41 +02'00'

Roma, 11 maggio 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

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

Firma Elettronica Avanzata MPS v. 2.0

OCSI/CERT/TEC/02/2022/RC

Versione 1.0

11 maggio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	11/05/2022

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
FEA	Firma Elettronica Avanzata
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NAS	Network Attached Storage
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
PP	Profilo di Protezione
RFV	Rapporto Finale di Valutazione
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Sistema Operativo
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
SHA	Secure Hash Algorithm
ST	Security Target
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation

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

[DPCM] “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”, DPCM del 22 febbraio 2013, Gazzetta Ufficiale Serie Generale n.117 del 21 maggio 2013

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

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

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

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

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

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

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

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

4.2 Documenti tecnici

[CONF] Lista di Configurazione "Applicazione Firma Elettronica Avanzata MPS Versione 2.0", versione 1.0, Banca Monte dei Paschi di Siena S.p.A., 15 febbraio 2022

[GUI1] "Manuale utente di Firma Elettronica Avanzata MPS v. 2.0", versione 1.0, Banca Monte dei Paschi di Siena S.p.A., 1° febbraio 2022

[GUI2] "Installazione ODV di Firma Elettronica Avanzata MPS v. 2.0", versione 1.0, Banca Monte dei Paschi di Siena S.p.A., 15 febbraio 2022

[RC] "Rapporto di Certificazione Firma Elettronica Avanzata MPS v. 1.0", OCSI/CERT/TEC/07/2015/RC, versione 1.0, 8 febbraio 2017

[RFV] Rapporto Finale di Valutazione del prodotto "Firma Elettronica Avanzata MPS v. 2.0", Versione 1.0, Technis Blu S.r.l., 28 aprile 2022

[TDS] "Security Target di Firma Elettronica Avanzata MPS v. 2.0", v. 1.1, Banca Monte dei Paschi di Siena S.p.A., 29 gennaio 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 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 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 per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è l'applicazione software "Firma Elettronica Avanzata MPS v. 2.0", nel seguito del documento anche indicata come "FEA MPS", sviluppata dalla società Banca Monte dei Paschi di Siena S.p.A., nel seguito del documento anche indicata come "Banca MPS".

L'ODV è una componente software dell'infrastruttura di Gestione Documentale di Banca MPS, che consente ai clienti della banca di utilizzare la Firma Elettronica Avanzata (FEA) con tecnologia grafometrica per la firma di documenti all'interno del sistema informativo protetto di Banca MPS, mediante appositi dispositivi esterni hardware e software e nel rispetto di leggi e regolamenti in materia.

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 (Firma Elettronica Avanzata MPS v. 1.0), già certificato dall'OCSI (Certificato n. 1/17 dell'8 febbraio 2017 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore Banca Monte dei Paschi di Siena S.p.A. è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS Technis Blu S.r.l. 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 "Firma Elettronica Avanzata MPS v. 2.0".

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 EAL1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

Inoltre, si precisa che l'emissione del Certificato per l'ODV non costituisce in alcun modo attestazione da parte dell'OCSI di conformità dell'applicazione software denominata "Firma Elettronica Avanzata MPS v. 2.0" ai requisiti generali di sicurezza di cui all'art. 26 del Regolamento (UE) n. 910/2014 [eIDAS] e all'art. 56 del DPCM 22 febbraio 2013 [DPCM].

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Firma Elettronica Avanzata MPS v. 2.0" 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	Firma Elettronica Avanzata MPS v. 2.0
Traguardo di Sicurezza	"Security Target di Firma Elettronica Avanzata MPS v. 2.0", v. 1.1 [TDS]
Livello di garanzia	EAL1
Fornitore	Banca Monte dei Paschi di Siena S.p.A.
Committente	Banca Monte dei Paschi di Siena S.p.A.
LVS	Technis Blu S.r.l.
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	2 febbraio 2022
Data di fine della valutazione	28 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 "Firma Elettronica Avanzata MPS v. 2.0" è una componente software dell'infrastruttura di Gestione Documentale di Banca MPS. Fra i vari obiettivi di questa infrastruttura rientra quello di utilizzare la Firma Elettronica Avanzata (FEA) con tecnologia grafometrica per la firma di documenti all'interno del sistema informativo protetto di Banca MPS. Il cliente della banca che abbia aderito a questo servizio potrà, all'interno del

sistema informativo protetto di Banca MPS, apporre la propria firma mediante appositi dispositivi esterni hardware e software e nel rispetto di leggi e regolamenti in materia. La firma così apposta ha la stessa validità di una firma autografa e consente una più efficiente gestione del rapporto con la banca e la completa dematerializzazione dei documenti.

Nell'ambito dell'architettura generale del sistema di Gestione Documentale di Banca MPS, l'ODV ha il compito di acquisire i documenti firmati dai clienti della banca tramite il Signature Pad, creare i PDF/A dei documenti stessi, richiedere l'apposizione della firma digitale della banca e inviare i documenti negli archivi della banca ed in Conservatoria Sostitutiva a norma, secondo i formati stabiliti.

Gli utenti dell'ODV, intesi come i soggetti che possono interagire direttamente con l'ODV, sono costituiti dalle applicazioni della banca che prevedono la possibilità di utilizzo della FEA MPS. Non sono previsti altri ruoli utente per l'ODV, in quanto:

- gli Utenti FEA della banca hanno come interfaccia il Signature Pad per le operazioni di sportello e l'applicazione di Internet banking per la consultazione;
- gli operatori di sportello MPS si interfacciano solo con le applicazioni bancarie;
- la gestione e l'amministrazione dell'ODV è di esclusiva pertinenza dell'ambiente operativo.

7.3.1 Architettura dell'ODV

Lo schema mostrato in Figura 1 illustra il processo di FEA con tecnologia grafometrica adottato da Banca MPS nel suo insieme, all'interno del quale opera anche l'ODV.

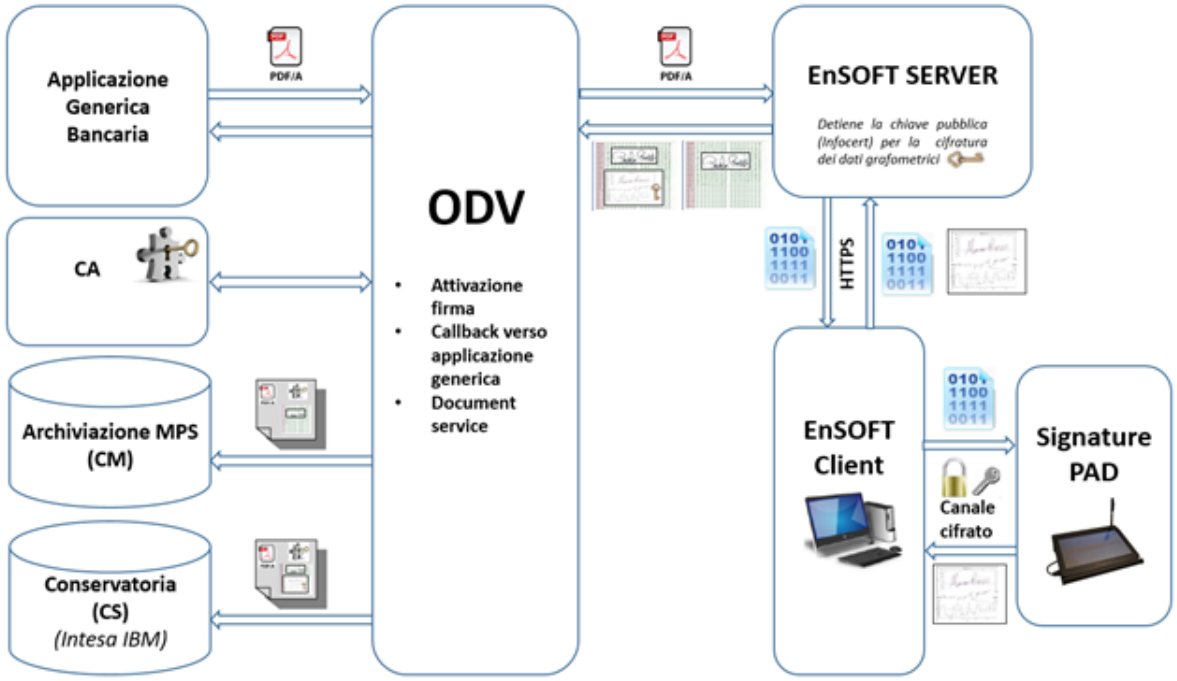

Figura 1 - Schema del processo di firma grafometrica di Banca MPS

Alcune delle componenti indicate nello schema, incluso l'ODV, sono ospitate nel data center di Banca MPS mentre per altre è prevista un'interazione con servizi esterni ospitati da Intesa (società del gruppo IBM) per la Conservazione Sostitutiva a norma e da Infocert sia per la firma digitale, sia per i servizi di Certification Authority.

7.3.1.1 Componenti dell'ODV

L'ODV comprende le seguenti componenti:

- **Attivazione Firma**: componente applicativa software per interfacciare l'infrastruttura software di Banca MPS con il prodotto software della società Euronovate.

- **Callback verso applicazione generica**: componente applicativa software che permette di notificare all'applicazione chiamante l'esito dell'operazione di firma (operazione confermata dal cliente, annullata dal cliente o andata in *timeout* o in errore generico).

- **Document Service**: componente applicativa software che gestisce il flusso documentale nell'ambito delle operazioni di FEA.

Per maggiori dettagli sui flussi operativi dell'ODV e del suo ambiente si faccia riferimento al par. 2.4.2 del Traguardo di Sicurezza [TDS].

7.3.1.2 Componenti dell'ambiente operativo

Di seguito sono elencate le componenti dell'ambiente operativo dell'ODV, ciascuna con una sintetica descrizione della funzione svolta nell'intero processo di gestione dei documenti sottoscritti mediante FEA MPS:

- **Applicazione Generica Bancaria (AGB)**: rappresenta l'insieme delle applicazioni sviluppate dalla banca per consentire ad un Operatore di Banca MPS di svolgere l'operazione bancaria richiesta dal cliente.

- **EnSOFT SERVER**: è la componente che svolge i compiti di conversione dei file PDF/A in ingresso in file immagine da inviare alla componente EnSOFT Client.

- **EnSOFT Client**: è la componente che si occupa dell'interfacciamento sicuro su canale cifrato con il Signature Pad e della raccolta della/e firma/e previste dallo specifico documento.

- **Infocert Spa**: è la componente richiamata dall'ODV che riceve i file PDF/A generati dall'ODV (Document Service) e vi appone la firma digitale della banca in formato PAdES con algoritmo RSA a 2048 bit e *hash* SHA-256.

- **Conservazione Sostitutiva**: è la componente applicativa residente presso il data center Intesa IBM dove vengono inviati i documenti in formato PDF/A prodotti dall'ODV.

- **Archiviazione MPS**: è la componente applicativa della banca che memorizza i documenti prodotti dall'ODV in formato PDF/A.

Per maggiori dettagli sull'ambiente operativo dell'ODV si faccia riferimento al par. 2.4.1 del Traguardo di Sicurezza [TDS].

7.3.2 Caratteristiche di Sicurezza dell'ODV

Trattandosi di una valutazione a livello di garanzia EAL1, non viene descritto completamente il problema di sicurezza dell'ODV, ma ci si limita a definire gli obiettivi di sicurezza per l'ambiente operativo, elencati nel cap. 4 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consultino il par. 2.4.3 e il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Immodificabilità e connessione univoca**: l'ODV, a completamento e integrità del documento dopo le firme apposte dal cliente, sull'intero documento provvede a richiedere ad Infocert S.p.A. l'apposizione della firma digitale della banca in modalità PAdES. L'apposizione della firma digitale della Banca costituisce elemento di imbustamento/blindatura del documento. Questa operazione viene fatta per garantire la connessione univoca della firma al documento sottoscritto e per garantirne la non modificabilità.
- **Conservazione Sostitutiva a norma**: l'ODV invia il documento informatico sottoscritto dal cliente comprensivo degli elementi grafometrici cifrati ad un sistema di Conservazione Sostitutiva, come da disposizioni normative.
- **Archiviazione nei sistemi MPS**: L'ODV invia il documento con il solo dato grafico della firma al sistema di archiviazione interna di Banca MPS. Il cliente ha quindi la possibilità di richiamare, tramite l'Internet banking, i documenti da lui firmati, per verifica e controllo, oppure richiederli in filiale.

7.4 Documentazione

Come specificato nel Traguardo di Sicurezza [TDS], l'ODV è un'applicazione sviluppata per l'uso esclusivo di Banca MPS ed inserita in un contesto operativo più ampio. In questo contesto, gli utenti reali dell'ODV sono rappresentati dalle applicazioni che la banca ha sviluppato a sostegno dei servizi offerti ai propri clienti. Nel TDS tali utenti sono identificati con "Applicazione Generica Bancaria" (AGB). Inoltre, l'ODV non richiede attività preparatorie sulle postazioni di utilizzo.

Non essendo un prodotto destinato alla commercializzazione, non sono previste guide per l'installazione, la configurazione e l'uso dell'ODV per l'utente finale. Il Committente ha predisposto ai soli fini di valutazione due documenti, elencati in Appendice A – Indicazioni per l'uso sicuro del prodotto, il primo dei quali illustra in maniera dettagliata come le AGB interagiscono con l'ODV per attivarne le funzionalità [GUI1], mentre il secondo descrive gli strumenti di pacchettizzazione, di distribuzione e di installazione in produzione del software che compone l'ODV [GUI2].

Per l'utilizzo sicuro dell'ODV si deve fare riferimento a quanto specificato nel Traguardo di Sicurezza [TDS]. Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti 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 Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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 gli obiettivi di sicurezza per l'ambiente operativo, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza realizzate dall'ODV.

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 e/o utilizzatori. 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 Technis Blu S.r.l.

L'attività di valutazione è terminata in data 28 aprile 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 4 maggio 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 Appendice B – Configurazione valutata. I potenziali acquirenti e/o utilizzatori 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 e/o utilizzatori (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 "Firma Elettronica Avanzata MPS v. 2.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL1, 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 EAL1.

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 for the operational environment	ASE_OBJ.1	Positivo
Stated security requirements	ASE_REQ.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.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
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Test	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability survey	AVA_VAN.1	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 e/o utilizzatori del prodotto "Firma Elettronica Avanzata MPS v. 2.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel cap. 4 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti e/o utilizzatori di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, descritta in Appendice B – Configurazione valutata.

L'ODV è un'applicazione progettata per realizzare, unitamente al proprio ambiente operativo, una soluzione di Firma Elettronica Avanzata (FEA), definita nella vigente normativa ([eIDAS], [DPCM]). Poiché nel tempo tale normativa potrebbe essere soggetta a revisioni, si consiglia il Committente di verificare periodicamente la conformità dell'ODV a tale normativa e, nel caso, valutare l'opportunità di un aggiornamento della certificazione.

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

I documenti di guida rilevanti ai fini della valutazione o referenziati all’interno dei documenti prodotti e disponibili ai potenziali acquirenti e/o utilizzatori dell’ODV, sono i seguenti:

- “Manuale utente di Firma Elettronica Avanzata MPS v. 2.0”, versione 1.0 [GUI1]
- “Installazione ODV di Firma Elettronica Avanzata MPS v. 2.0”, versione 1.0 [GUI2]

10 Appendice B – Configurazione valutata

L'ODV "Firma Elettronica Avanzata MPS v. 2.0", è una componente software del sistema di Gestione Documentale di Banca MPS. Si tratta di un prodotto sviluppato per l'uso esclusivo di Banca MPS, attualmente in esercizio e non destinato alla commercializzazione.

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 alla quale si applicano i risultati della valutazione.

10.1 Ambiente operativo dell'ODV

I componenti software dell'ODV sono installati su macchine con SO Linux (Red Hat Enterprise Linux Server release 7.9) sulle quali sono installati l'*application server* Tomcat versione 9 per la parte di Front End e IBM WebSphere Application Server versione 9 per la parte di Back End.

Gli applicativi di Banca MPS che prevedono l'utilizzo dell'ODV sono installati su macchine client con SO Windows 10 Enterprise sulle quali è presente il prodotto Euronovate ENSoft 2.0 che colloquia con il Signature Pad Wacom DTU-1141B. A partire da queste macchine è possibile attivare le funzionalità dell'ODV mediante un applicativo Web denominato Digital Branch.

Il database su cui si appoggiano sia l'ODV, sia il software di Euronovate è Oracle Enterprise Edition 11g Release 2 (11.2.0.4).

Per l'archiviazione dei documenti prodotti dall'ODV viene utilizzato il prodotto IBM Content Manager versione 8.6.00.400.

Per maggiori dettagli si consulti il par. 2.3 del Traguardo di Sicurezza [TDS].

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 EAL1 tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

I test funzionali di sicurezza sono stati eseguiti presso la sede del Committente situata in Firenze. In tale sede è posto l'ambiente di collaudo utilizzato da Banca MPS per le proprie applicazioni.

Per l'effettuazione dei test è stato riprodotto un ambiente operativo coerente con quanto specificato nel Traguardo di Sicurezza [TDS].

Nella fase di preparazione, i Valutatori hanno sottoposto l'ambiente di test a verifica di conformità con l'ambiente di produzione, così come descritto nel TDS e nel documento Lista di Configurazione [CONF] fornito dal Committente. Inoltre, prima dell'effettuazione delle singole sessioni di test i Valutatori hanno verificato che l'ODV, nelle sue diverse componenti, fosse installato e configurato nell'ambiente di test come dichiarato dal Fornitore e riportato in Appendice B – Configurazione valutata.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Nella predisposizione dell'insieme dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto le funzioni di sicurezza dell'ODV, così come rappresentate nel Traguardo di Sicurezza [TDS], le TSFI descritte nel documento di Specifiche Funzionali con i relativi parametri e la documentazione di guida ([GUI1], [GUI2]).

I Valutatori hanno quindi predisposto un insieme di test, con l'obiettivo di verificare l'adeguatezza delle funzioni di sicurezza dell'ODV, nel rispetto di quanto previsto dalla CEM.

In particolare, i test funzionali progettati ed eseguiti dai Valutatori sono stati mirati a verificare che l'ODV svolge le funzioni di sicurezza dichiarate all'interno dei seguenti processi:

- firma dei documenti;
- invio in Conservazione Sostitutiva dei documenti firmati;
- archiviazione nei sistemi di Banca MPS dei documenti firmati.

I test funzionali effettuati dai Valutatori hanno consentito di verificare che l'ODV realizza le funzioni di sicurezza dichiarate, estendendo le verifiche al sistema nel suo complesso, comprensivo di tutti i componenti coinvolti, sia dell'ODV, sia dell'ambiente operativo.

Tutti i test effettuati dai Valutatori hanno dato esito positivo, dimostrando che l'ODV si comporta come descritto nella documentazione tecnica fornita dal Committente e realizza correttamente i requisiti funzionali di sicurezza descritti nel Traguardo di Sicurezza [TDS].

11.3 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. Le fasi di verifica dell'ambiente operativo e della corretta installazione e configurazione dell'ODV sono state ripetute anche in sede di test di intrusione.

Per la predisposizione delle attività di analisi delle vulnerabilità, in considerazione del livello di garanzia richiesto per la valutazione e della natura dell'ODV, i Valutatori hanno preso in considerazione vulnerabilità note dei server e dei client presenti nell'ambiente operativo, oltre che dei protocolli di comunicazione utilizzati per lo scambio dei dati, che potrebbero essere sfruttate per aggirare od interferire con le funzioni di sicurezza dell'ODV.

In particolare, gli elementi sui quali si è concentrata l'analisi dei Valutatori sono stati i seguenti:

- parte server ospitata su macchine Linux con *application server* Tomcat;
- parte client su macchine con sistema operativo Windows 10 connessa a dominio Microsoft;
- archiviazione dei documenti prodotti dall'ODV tramite il prodotto IBM Content Manager;
- invocazione della Conservazione Sostitutiva;
- conservazione su archivio di Banca MPS:
    - contenuto binario del file mantenuto su una share NAS;
    - motore batch di schedulazione.
- sorgenti software su *repository*;
- binari compilati su NAS;
- verifica che il documento firmato non possa essere sostituito o manipolato da parte dell'operatore, prima della conferma da parte del cliente.

Inoltre, sono state analizzate possibili falle nei flussi logici gestiti direttamente dall'ODV allo scopo di escludere che questo possa essere utilizzato in modo da sovvertire le regole che governano la Firma Elettronica Avanzata (FEA), come definita nella normativa italiana, con particolare riferimento al non ripudio.

I Valutatori hanno esaminato le vulnerabilità potenziali così individuate e determinato un insieme di prove di intrusione appropriato per il livello di valutazione EAL1, cioè

assumendo che l'ODV deve resistere ad un ipotetico attaccante con potenziale di attacco Basic.

Al termine delle sessioni di test di intrusione, i Valutatori hanno potuto verificare che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state individuate vulnerabilità residue.

L'analisi condotta dai Valutatori ha comunque rilevato la presenza di una serie di vulnerabilità note in alcuni componenti software dell'ambiente operativo. Anche se tali vulnerabilità non risultano facilmente sfruttabili nell'ambiente protetto di Banca MPS e non rappresentano rischi reali per l'ODV, si raccomanda al Fornitore di provvedere all'aggiornamento periodico dei software che costituiscono l'architettura generale del sistema di Gestione Documentale di Banca MPS, all'interno della quale opera l'ODV.