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. 1/17

(Certification No.)

Prodotto: **Firma Elettronica Avanzata MPS v. 1.0**
(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 Rita Forsi)

Roma, 8 febbraio 2017

Common Criteria

SOGIS IT SECURITY CERTIFICATE

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

Firma Elettronica Avanzata MPS v. 1.0

OCSI/CERT/TEC/07/2015/RC

Versione 1.0

8 febbraio 2017

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	08/02/2017

2 Indice

3 Elenco degli acronimi

AGB	Applicazione Generica Bancaria
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
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
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual recognition Arrangement
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179, G.U. n. 214 del 13 settembre 2016

[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

[CCRA-2000] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, May 2000

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

[CONF] “Lista di Configurazione Applicazione Firma Elettronica Avanzata MPS Versione 1.0”, versione 1.0, 10 novembre 2016.

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

[GUI1] “Manuale utente di Firma Elettronica Avanzata MPS v. 1.0”, versione 1.0, 9 febbraio 2016

[GUI2] “Installazione ODV di Firma Elettronica Avanzata MPS v. 1.0”, versione 1.0, 28 ottobre 2016

[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

[RFV] Rapporto Finale di Valutazione del prodotto "Firma Elettronica Avanzata MPS v. 1.0", Versione 1.0, 30 dicembre 2016

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

[TDS] Security Target di "Firma Elettronica Avanzata MPS v. 1.0", v. 1.4, 4 dicembre 2016

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 assurance indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La nuova versione 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).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL 4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

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 secondo le regole dell'accordo [CCRA] in vigore per tutti i componenti di assurance indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto software denominato "Firma Elettronica Avanzata MPS v. 1.0" (nel seguito anche indicato per brevità come "FEA MPS"), sviluppato da Banca Monte dei Paschi di Siena S.p.A. (nel seguito indicato per brevità come "Banca MPS").

Il prodotto FEA MPS è una componente software, parte del più ampio progetto "Banca Paperless", che consente ai clienti della banca di utilizzare la Firma Elettronica Avanzata (FEA) con tecnologia grafometrica per la firma di documenti all'interno di ambienti controllati della banca, mediante appositi dispositivi esterni hardware e software.

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 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 del prodotto FEA MPS ai requisiti generali di sicurezza definiti nelle Regole Tecniche emesse da AgID ([DPCM]) per le soluzioni di FEA.

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. 1.0" 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. 1.0
Traguardo di Sicurezza	Security Target di "Firma Elettronica Avanzata MPS v. 1.0", v. 1.4, 4 dicembre 2016
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. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	24 settembre 2015
Data di fine della valutazione	30 dicembre 2016

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. 1.0", è una componente software di un più ampio progetto di Banca MPS, chiamato "Banca Paperless". Fra i vari obiettivi di questo progetto rientra quello di consentire ai clienti della banca di utilizzare la Firma Elettronica Avanzata (FEA) con tecnologia grafometrica per la firma di documenti all'interno di ambienti controllati della banca, mediante appositi dispositivi esterni hardware e software.

L'ODV opera nell'ambito di applicazioni bancarie utilizzate per servire i clienti all'interno delle filiali della banca. Compito dell'ODV è quello di consentire ad un utente di firmare documenti elettronici e di gestire firma e documenti nel rispetto della vigente normativa italiana in materia:

- Codice dell'Amministrazione Digitale [CAD];
- Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali [DPCM].

L'ODV è un prodotto sviluppato per l'uso esclusivo del Committente Banca MPS e non è quindi destinato ad essere commercializzato.

Nell'ambito dell'architettura generale di "Banca Paperless", l'ODV ha il compito di acquisire i documenti firmati dai clienti della banca tramite un Signature Pad, creare le versioni in formato PDF/A dei documenti stessi, richiedere l'apposizione della firma digitale della banca e inviare i documenti agli archivi della banca ed in Conservatoria Sostitutiva, utilizzando i formati stabiliti.

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

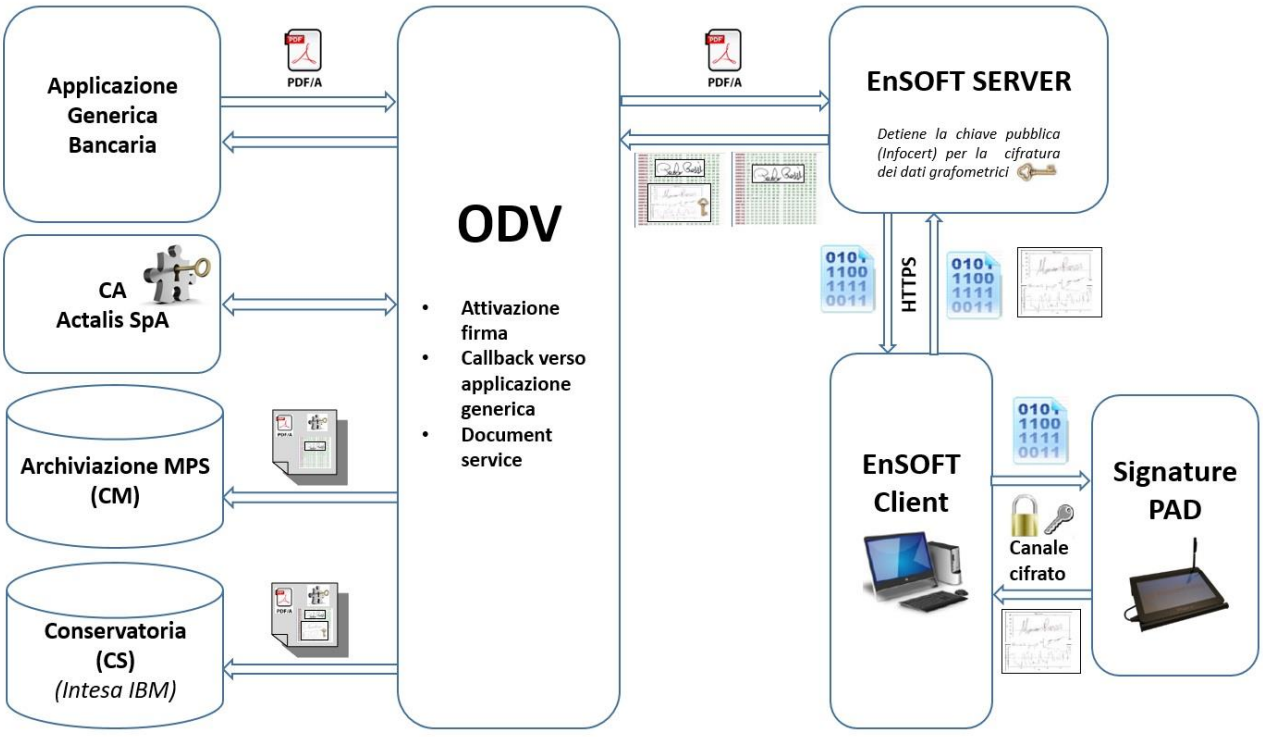

Figura 1 – Schema del processo di firma grafometrica di Banca MPS

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, da Actalis (società del gruppo Aruba) per la firma digitale e da Infocert per i servizi di Certification Authority.

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.

7.3.1 Architettura dell'ODV

7.3.1.1 Hardware

La descrizione delle caratteristiche hardware e software dei server che ospitano l'ODV è fornita in [TDS], par. 2.3. La descrizione dell'ambito fisico dell'ODV è fornita in [TDS], par. 2.4.1.

7.3.1.2 Software

La descrizione dell'ambito logico dell'ODV è fornita in [TDS], par. 2.4.3.

Le principali componenti del prodotto FEA MPS sono:

- **Attivazione Firma**: componente applicativa software per interfacciare l'infrastruttura software della 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.
- **Document Service**: componente applicativa software che gestisce il flusso documentale nell'ambito delle operazioni di FEA.

Per maggiori dettagli sui flussi operativi di gestione documentale mediati dall'ODV si faccia riferimento al [TDS], par. 2.4.1.

7.3.1.3 Componenti di ambiente

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)**: è l'insieme delle applicazioni sviluppate dalla banca per consentire ad un Operatore di sportello 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.
- **Actalis S.p.A.**: 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 [TDS], par. 2.4.1.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Trattandosi di una valutazione a livello di garanzia EAL1, nel Traguardo di Sicurezza [TDS] non viene descritto completamente il problema di sicurezza, ma ci si limita a definire i Requisiti Funzionali di Sicurezza (SFR), per i quali si rimanda al par. 6.3 del [TDS], gli obiettivi di sicurezza per l'ambiente operativo e le funzioni di sicurezza realizzate dall'ODV, che sono riportati qui di seguito.

7.3.2.1 Obiettivi di sicurezza per l'ambiente operativo

Gli obiettivi di sicurezza per l'ambiente operativo dell'ODV sono riassunti di seguito:

- **OE.Clienti**: L'ambiente operativo deve provvedere a soddisfare la seguente esigenza: identificazione del firmatario del documento e acquisizione dell'adesione dello stesso.

- **OE.Firma**: L'ambiente operativo deve provvedere a soddisfare le seguenti esigenze:

    a. connessione univoca della firma al firmatario;

    b. controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;

    c. possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.

- **OE.Integrity**: L'ambiente operativo deve provvedere a soddisfare la seguente esigenza: possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma.

- **OE.Protect**: L'ambiente operativo deve provvedere a soddisfare la seguente esigenza: assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati.

- **OE.Trust**: L'AGB deve trasmettere i documenti firmati dalla banca all'ODV attraverso canali o *path* sicuri.

Per una formulazione completa degli obiettivi di sicurezza dell'ambiente operativo dell'ODV si veda il Traguardo di Sicurezza [TDS], par. 4.

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza dell'ODV sono le seguenti:

- **ODV_Firma – 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 Actalis 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.

- **ODV_Cons – 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.

- **ODV_Archiv – Archiviazione nei sistemi MPS**: L'ODV invia il documento con il solo dato grafico della firma al sistema di archiviazione interna di MPS. Il cliente ha quindi la possibilità di richiamare, tramite l'*home banking*, i documenti da lui firmati, per verifica e controllo, oppure richiederli in filiale.

Per maggiori dettagli sulle funzioni di sicurezza dell'ODV si veda il Traguardo di Sicurezza [TDS], par. 2.4.3.

7.3.3 Configurazione dell'ODV

L'ODV valutato è identificato in [TDS] come versione 1.0, e corrisponde alla configurazione predisposta dal Committente per i test. Tutti i test (funzionali e di vulnerabilità) sono stati effettuati su questa versione dell'ODV.

7.4 Documentazione

Come specificato in [TDS], l'ODV è un'applicazione sviluppata per l'uso esclusivo di Banca MPS ed inserita in un contesto più ampio, progettata per supportare le operazioni di sportello dei clienti della banca, senza tuttavia interagire direttamente con gli stessi.

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 raccomandazioni contenuti nel par. 8.2 di questo rapporto.

7.5 Requisiti funzionali e di garanzia

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati selezionati dai CC Parte 2 [CC2] e tutti i Requisiti di Garanzia (SAR) dai CC Parte 3 [CC3].

Trattandosi di una valutazione a livello di garanzia EAL1, nel Traguardo di Sicurezza [TDS] non viene descritto completamente il problema di sicurezza, ma ci si limita a definire gli obiettivi di sicurezza per l'ambiente operativo, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza realizzate dall'ODV.

7.6 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 30 dicembre 2016 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 25 gennaio 2017. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.7 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. 1.0" 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
Tests	**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 Dichiarazione di certificazione6 – Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti e/o utilizzatori del prodotto "Firma Elettronica Avanzata MPS v. 1.0" 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 all'ambiente operativo specificato nel capitolo 2.4.1 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 italiana. 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 o la necessità di una rivalutazione.

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 utilizzatori dell'ODV, sono i seguenti:

- Security Target di "Firma Elettronica Avanzata MPS v. 1.0", v. 1.4, 4 dicembre 2016 [TDS];
- "Manuale utente di Firma Elettronica Avanzata MPS v. 1.0", versione 1.0, 9 febbraio 2016 [GUI1];
- "Installazione ODV di Firma Elettronica Avanzata MPS v. 1.0", versione 1.0, 28 ottobre 2016 [GUI2].

10 Appendice B – Configurazione valutata

L'ODV "Firma Elettronica Avanzata MPS v. 1.0", è una componente software di un più ampio progetto di Banca MPS, chiamato "Banca Paperless". Si tratta di un prodotto sviluppato per l'uso esclusivo di Banca MPS, attualmente in esercizio e non destinato alla commercializzazione. L'ODV è progettato per supportare le operazioni di sportello dei clienti della banca, senza tuttavia interagire direttamente con gli stessi.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 1.0.

Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, come riportata in [CONF], verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa riportati nel Rapporto Finale di Valutazione [RFV].

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 da parte dei Valutatori.

11.1 Configurazione per i Test

Poiché l'ODV è un prodotto in esercizio, in accordo con il Committente i test funzionali di sicurezza, le attività di analisi delle vulnerabilità e i test di intrusione sono stati eseguiti presso una delle sedi di Banca MPS di Siena, direttamente sull'ambiente di collaudo abitualmente utilizzato dalla banca.

Il *test bed* è stato realizzato presso l'infrastruttura del Committente ed è costruito mediante l'integrazione di più componenti, alcuni dei quali a carico di diversi Fornitori esterni. Per la verifica dell'allestimento del *set up* i Valutatori hanno tenuto conto di quanto descritto nel Traguardo di Sicurezza [TDS], nel documento Lista di Configurazione [CONF] predisposto dal Committente e nelle Guide dei fornitori coinvolti.

Nella fase di preparazione del piano dei test, i Valutatori hanno esaminato la descrizione dell'ODV riportata nel TDS ed hanno verificato che la configurazione proposta dal Committente per i test fosse coerente con quanto specificato nel TDS stesso e nelle specifiche funzionali.

Inoltre, prima dell'effettuazione delle singole sessioni di test i Valutatori hanno verificato che l'ODV, assieme alle diverse componenti del suo ambiente operativo, fosse installato e configurato come dichiarato dal Committente e riportato in Appendice B – Configurazione valutata. Questo a garanzia della ripetibilità e riproducibilità dei test.

11.2 Test funzionali indipendenti svolti dai Valutatori

Nella predisposizione del programma dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS] e le specifiche funzionali.

I Valutatori hanno quindi esaminato le funzioni di sicurezza dell'ODV, così come rappresentate nel TDS e, sulla base della propria esperienza, hanno 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 di funzionalità pianificati e svolti dall'LVS sono stati mirati a verificare che l'ODV:

- svolge le funzioni di sicurezza dichiarate all'interno del processo di firma dei documenti (funzione di sicurezza ODV_Firma);
- svolge le funzioni di sicurezza dichiarate all'interno del processo di invio in Conservazione Sostitutiva dei documenti firmati (funzione di sicurezza ODV_Cons);
- svolge le funzioni di sicurezza dichiarate all'interno del processo di archiviazione nei sistemi di Banca MPS dei documenti firmati (funzione di sicurezza ODV_Archiv);

I test di funzionalità 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.

L'esito dei test ha mostrato il pieno rispetto di quanto previsto nel TDS e nelle specifiche funzionali.

L'ODV ha quindi superato con verdetto positivo la fase di test indipendenti.

11.3 Analisi delle vulnerabilità e test di intrusione

I test di analisi delle vulnerabilità sono stati condotti sullo stesso *test bed* utilizzato per i test funzionali.

Per la predisposizione delle attività di analisi delle vulnerabilità, in considerazione del livello di garanzia richiesto per la valutazione e della natura dell'ODV, il team di valutazione ha 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 7 SP1;
- archiviazione dei documenti prodotti dall'ODV tramite il prodotto IBM Content Manager versione 8.4.3;
- invocazione della Conservazione Sostitutiva (CS):
    - apertura della connessione VPN con il sito del fornitore da parte dell'ODV;
    - trasferimento dati tramite FTP;
    - gestione dei *batch*.
- conservazione su archivio di Banca MPS:
    - contenuto binario del file mantenuto su una *share* NAS;
    - motore *batch* di schedulazione.
- 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 quindi esaminato le vulnerabilità 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, nel rispetto di quanto previsto dalla CEM (cfr. [CEM], appendice B.4).

Le prove di intrusione condotte dai Valutatori hanno confermato l'assenza di vulnerabilità sfruttabili con un basso potenziale di attacco nell'ambiente operativo dell'ODV.