MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Security Target

di

Firma Elettronica Avanzata MPS v. 2.0

REVISIONI DEL DOCUMENTO

Versione	Data	Autore	Descrizione delle modifiche
1.0	13/01/2022	Alberto Monciatti	Prima emissione del documento
1.1	29/01/2022	Alberto Monciatti	Corretto il riferimento ai Common Criteria. Effettuate piccole correzioni testuali

Tabella 1 - Revisioni del documento

Sommario

Indice delle figure

Indice delle tabelle

1 PREMESSA

1.1 Struttura del documento

Il Security Target contiene le seguenti sezioni:

- Introduzione al Security Target [Rif. § 2]: questa sezione fornisce una rappresentazione dell'ODV, ne descrive le caratteristiche e ne definisce l'ambito.
- Dichiarazione di conformità [Rif. § 3]: questa sezione presenta le conformità con i CC.
- Obiettivi di sicurezza per l'ambiente operativo [Rif. § 4]: questa sezione descrive in maniera dettagliata gli obiettivi di sicurezza dell'ambiente operativo dell'ODV.
- Definizione di componenti estese [Rif. § 5]: questa sezione definisce e giustifica l'utilizzo di componenti estese.
- Requisiti di sicurezza [Rif. § 6]: questa sezione definisce i Security Functional Requirements (SFR), i Security Assurance Requirements (SAR) e contiene l'analisi delle dipendenze.
- Specifiche sommarie dell'ODV [Rif. § 7]: questa sezione descrive come gli SFR trovano riscontro nelle funzioni di sicurezza dell'ODV.

1.2 Acronimi

AGB	Applicazione Generica Bancaria
CA	Certification Authority
CC	Common Criteria
CM	Content Manager
CS	Conservatoria Sostitutiva
DB	Data Base
EAL	Evaluation Assurance Level
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MPS	Monte dei Paschi di Siena
ODV	Oggetto Della Valutazione
PAdES	PDFAdvanced Electronic Signatures
CAdES	CMS Advanced Electronic Signatures
PC	Personal computer
PDF	Portable Document Format

PDF/A	Formato standard internazionale (ISO19005), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione di documenti elettronici nel lungo periodo.
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation (ODV)
TSF	TOE Security Function
TSFI	TOE Security Function Interface

Tabella 2 – Acronimi

1.3 Definizioni

Vengono definiti in questa sezione termini specifici utilizzati all'interno del ST con il loro significato nello specifico contesto applicativo. Nel ST quanto i termini qui descritti vengono utilizzati con il significato qui descritto sono evidenziati in "*corsivo*".

Termine	Definizione
FEA MPS	Rappresenta la modalità di applicazione della Firma Elettronica Avanzata scelta da MPS. In particolare, MPS ha scelto la soluzione FEA con firma grafometrica.
Contratto/i	Il testo descrittivo del prodotto sottoscrivibile mediante *FEA MPS* e delle sue condizioni. Il contratto è rappresentato in un file PDF.
Cliente/i	Un soggetto che ha sottoscritto un *"rapporto"* con MPS.
Rapporto	Rappresenta l'accordo scritto intercorso tra un soggetto e MPS mediante il quale il soggetto accetta le condizioni di utilizzo della *FEA MPS*. La firma dell'accordo comporta da parte del soggetto l'accettazione delle condizioni e delle modalità di esecuzione ivi contenute.
Utente/i FEA	Un *"cliente"* MPS che ha sottoscritto i servizi di utilizzo della Firma Elettronica Avanzata MPS v. 2.0
Signature Pad	Trattasi dello strumento (tablet o altro) che il cliente utilizza per apporre la propria firma sul documento e che realizza l'operazione richiesta.
Operatore di sportello	Un dipendente della banca che opera in *Ambiente controllato della banca* per svolgere le *Operazioni bancarie* che vengono richieste da un cliente in presenza.

Termine	Definizione
Ambiente/i controllato/i della banca	Ambiente dove la banca accoglie i propri clienti per consentire loro di svolgere le proprie *Operazioni bancarie* in presenza.
Operazioni bancarie	Disposizioni impartite alla banca dal cliente (ad es. versamenti, bonifici, contratti, etc.).

1.4 Riferimenti

[RF1] Codice dell'amministrazione digitale (DL 7 marzo 2005 n. 82)

[RF2] Codice dell'amministrazione digitale (DL 30 dicembre 2010)

[RF3] DPCM 22 febbraio 2013 – *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71"*.

2 INTRODUZIONE AL SECURITY TARGET (ASE_INT)

2.1 Identificazione del Security Target

Titolo: Security Target di Firma Elettronica Avanzata MPS v. 2.0

Versione ST: 1.1

Data: 29/01/2022

Autore: Alberto Monciatti

2.2 Identificazione dell'ODV

Nome del prodotto: Firma Elettronica Avanzata MPS v. 2.0

Sviluppatore: Banca Monte dei Paschi di Siena S.p.A.

2.3 Panoramica dell'ODV

L'ODV è una componente software, denominata Firma Elettronica Avanzata MPS v. 2.0 (nel seguito per brevità *"FEA MPS"*), di un più ampio progetto, chiamato "Banca Paperless".

La figura seguente fornisce una visione ad alto livello dell'impostazione generale del progetto "Banca Paperless".

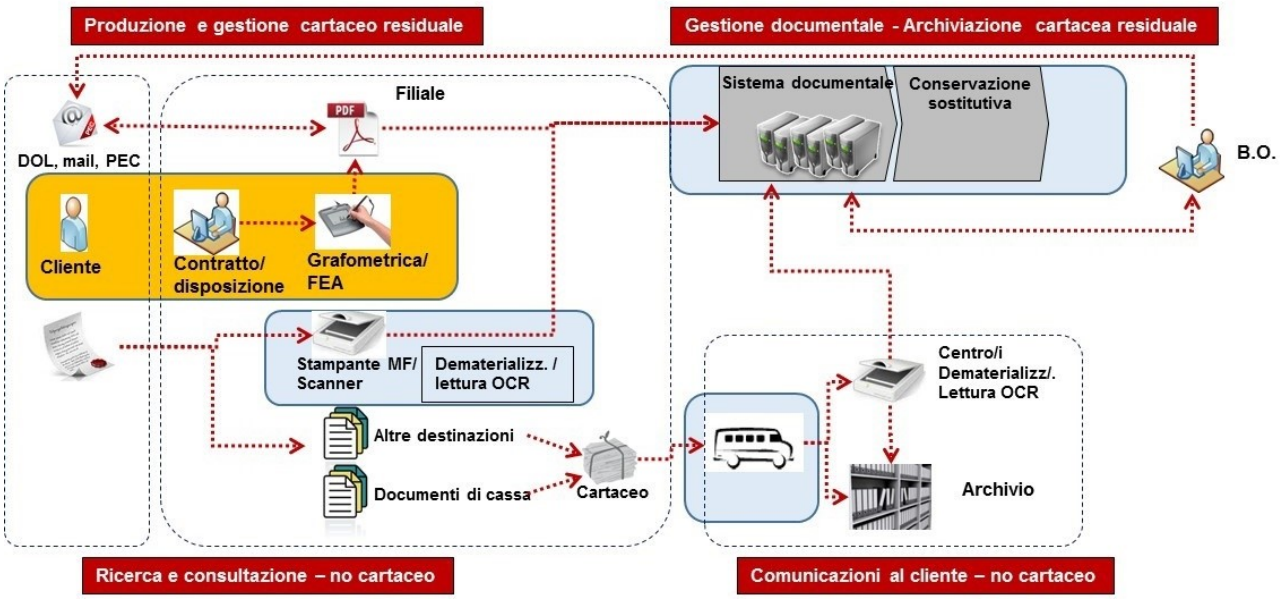

Figura 1 – Architettura generale "Banca Paperless"

Fra i vari obiettivi di questo progetto rientra quello di utilizzare la "Firma Grafometrica" per la firma di documenti all'interno di *Ambienti controllati della banca*. Il cliente della banca che abbia aderito a questo servizio potrà, all'interno degli *Ambienti controllati della banca* stessa, apporre la propria firma mediante appositi dispositivi esterni hardware e software e nel rispetto di leggi e regolamenti in materia. La sua firma così apposta ha la stessa validità di una firma autografa e consente una più efficiente gestione del rapporto e la completa dematerializzazione dei documenti.

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, secondo i formati stabiliti.

L'ambiente operativo che sostiene l'ODV comprende le seguenti componenti:

- una parte server che è ospitata su macchine Linux con application server Tomcat 9. L'insieme di queste macchine rappresenta un raggruppamento dedicato alla gestione della firma da parte di tutte le Filiali della Banca Monte dei Paschi di Siena.
- la macchina client dove è collegato il Signature Pad che è una macchina con S.O. Windows 10 Enterprise a partire dalla quale attraverso l'applicativo Web denominato Digital Branch è possibile attivare la funzionalità l'utilizzo dell'ODV. Il Signature Pad utilizzato è Wacom DTU-1141B.

Il database su cui si appoggia sia l'ODV che il software di Euronovate è Oracle alla versione 11 release 2.0.4.

Per quanto attiene alla archiviazione dei documenti prodotti dall'ODV viene utilizzato il prodotto IBM Content Manager versione 8.6.0.400.

2.4 Descrizione dell'ODV

2.4.1 Ambito fisico

Lo schema seguente illustra il processo di firma grafometrica adottato dalla Banca Monte dei Paschi di Siena nel suo insieme prendendo in considerazione, per dare maggiore chiarezza, tutte quelle componenti che lo costituiscono, all'interno del quale opera anche l'ODV. Le componenti indicate nello schema sono ospitate nel data center della Banca Monte dei Paschi di Siena mentre per alcune è prevista un'interazione con servizi esterni alla stessa ospitati da Intesa (società del gruppo IBM) per la Conservazione Sostitutiva, da Infocert sia per la firma digitale e che per i servizi di Certification Authority. Vengono infine indicati i principali flussi tra le varie componenti.

Le componenti dell'ODV sono chiaramente separate dalle componenti dell'ambiente.

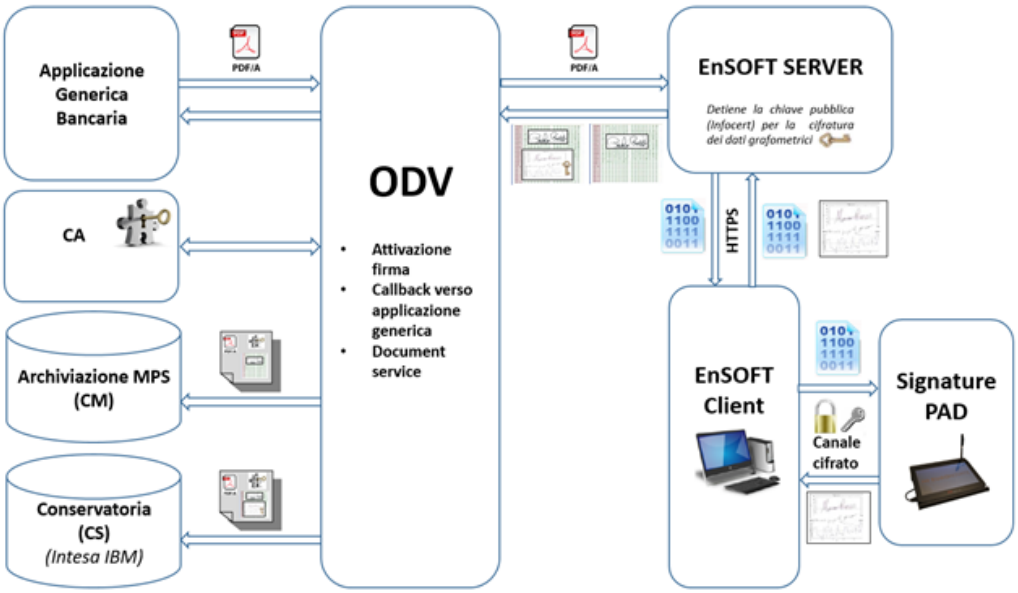

Figura 2 – Componenti del processo di firma grafometrica

Icona	Codice	Descrizione
	Ico1	Chiave pubblica della banca per la cifratura dei dati biometrici di firma (CA INFOCERT). La corrispondente chiave privata è conservata presso notaio per consentire la decifratura ai soli usi forensi
	Ico2	Chiave di cifratura autogenerata da EnSOFT Client per la comunicazione cifrata da e verso il *Signature Pad*
	Ico3	Chiave privata della banca per la firma digitale dei PDF/A generati dall'ODV (CA Infocert)
 PDF/A	Ico4	Documento in formato PDF/A che rappresenta la specifica *Operazione Bancaria* richiesta dall'*Utente FEA*
	Ico5	Dati grafici e grafometrici (biometrici di firma) rilevati mediante il *Signature Pad*
	Ico6	Formato immagine del PDF
	Ico7	Dati biometrici di firma cifrati con chiave pubblica della banca (Ico1).
	Ico8	Ico6 con firme grafiche e dati biometrici di firma Ico7

Icona	Codice	Descrizione
	Ico9	Ico6 con firme grafiche
	Ico10	PDF/A di Ico8 firmato PAdES con chiave privata della banca Ico3
	Ico11	PDF/A di Ico9 firmato PAdES con chiave privata della banca Ico3

Tabella 3 – Tabella Didascalie delle icone del processo di firma grafometrica

Di seguito sono illustrate le componenti proprie dell'ODV e quelle dell'ambiente operativo. Nel testo si farà esplicito riferimento al codice icona (Icoxx) indicato nella Tabella 3 – Tabella Didascalie delle icone del processo di firma grafometrica.

COMPONENTI DELL'ODV

L'ODV comprende le seguenti componenti.

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 (operazione confermata dal cliente, annullata dal cliente o andata in timeout o in errore generico).

Document Service:
componente applicativa software che: invia Ico4 ad EnSOFT SERVER, riceve da EnSOFT SERVER i file binari Ico8 e Ico9, crea i rispettivi file PDF/A e richiede ad Infocert SpA l'apposizione della Firma Digitale della Banca Ico3. Si occupa inoltre dell'invio dei file firmati Ico10 e Ico11 ai rispettivi ambienti di archiviazione.

COMPONENTI DELL'AMBIENTE

Di seguito sono elencate le componenti hardware e software dell'ambiente operativo a supporto dell'ODV, ciascuna con una sintetica descrizione della funzione svolta nell'intero processo di gestione di documenti sottoscritti con FEA MPS.

Applicazione Generica Bancaria:
rappresenta l'insieme delle applicazioni sviluppate dalla banca per consentire ad un *Operatore di sportello* di svolgere l'operazione bancaria richiesta dal cliente. Queste applicazioni sono rese

disponibili all'*Operatore di sportello* all'interno di un contesto applicativo che consente di identificare il cliente e di attivare la specifica applicazione necessaria per l'operazione bancaria richiesta dal cliente stesso. E' questo contesto applicativo che si occupa di verificare se per l'operazione bancaria richiesta il cliente è anche un *Utente FEA* che quindi può utilizzare l'ODV a cui viene inviato Ico4.

EnSOFT SERVER:
è la componente che svolge i compiti di conversione dei file PDF/A in ingresso Ico4 in file immagine Ico6 da inviare alla componente EnSOFT Client. Al ricevimento dei dati grafici e grafometrici di firma Ico5 da EnSOFT Client, su canale sicuro HTTPS, svolge il compito di cifratura dei dati grafometrici mediante la chiave di cifratura Ico1 ottenendo Ico7. Genera quindi i file Ico8 e Ico9 e li invia all'ODV.

EnSOFT Client:
è la componente che si occupa dell'interfacciamento sicuro su canale cifrato mediante Ico2 con il *Signature Pad*, che è il dispositivo di visualizzazione dell'immagine del documento da firmare Ico6 e della raccolta della/e firma/e previste dallo specifico documento. Alla conferma delle firme apposte dall'*Utente FEA*, EnSOFT Client invia i dati grafici e grafometrici Ico5 ad EnSOFT SERVER, su canale sicuro HTTPS.

Infocert Spa:
è la componente richiamata dall'ODV che riceve i file PDF/A generati dall'ODV (Document Service) e appone ad entrambi i file PDF/A (tipo A e B) la firma digitale della banca in formato PAdES con algoritmo RSA a 2048 bit e hash SHA-256 (Ico10 e Ico11).

Conservazione Sostitutiva:
è la componente applicativa residente presso il data center Intesa IBM dove vengono inviati i documenti in formato PDF/A Ico10 prodotti dall'ODV. Il sistema di Conservazione, alla ricezione dei documenti, applica agli stessi una marca temporale e firma il tutto CaDES, quindi conserva a norma gli stessi.

Archiviazione MPS:
è la componente applicativa della banca che memorizza i documenti prodotti dall'ODV in formato PDF/A Ico11.

2.4.2 Flussi operativi dell'ODV e del suo ambiente

La figura seguente fornisce una rappresentazione del flusso operativo che si svolge attraverso l'ODV ed il suo ambiente, per completare una operazione *FEA MPS*.

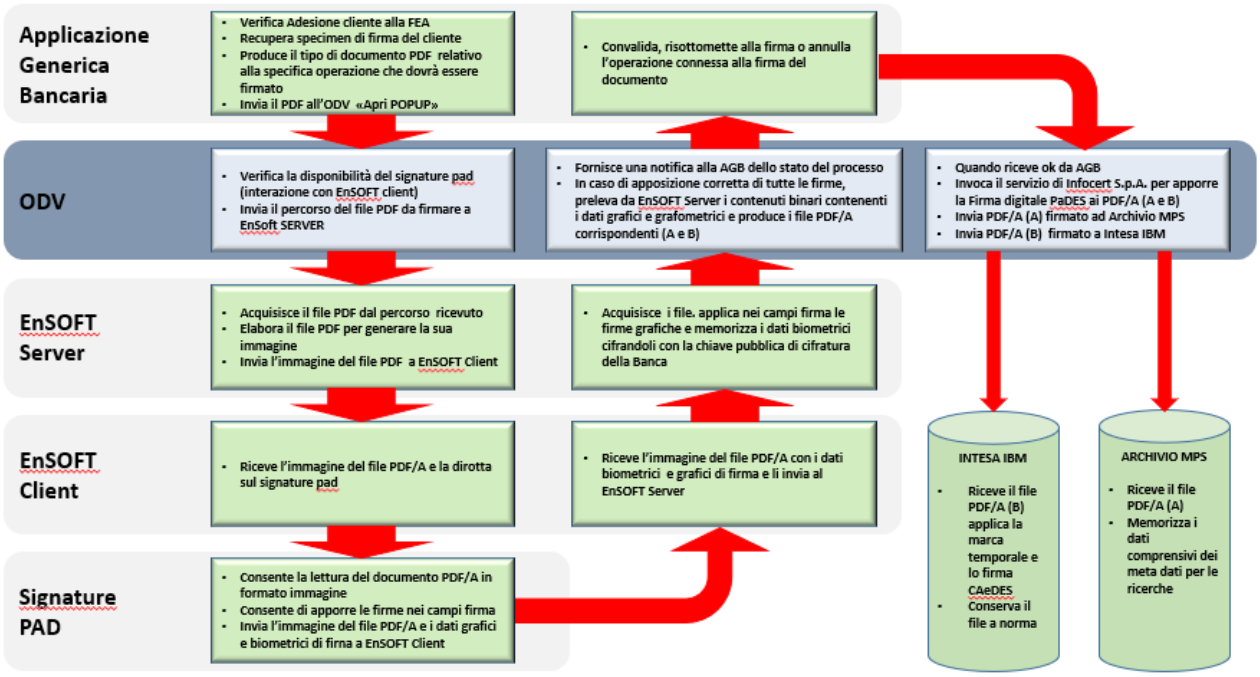

Figura 3 – Flussi operativi del processo di firma grafometrica

La Figura 3 mostra il flusso complessivo del processo di firma grafometrica indicando e distinguendo le elaborazioni che avvengono all'interno delle componenti di ambiente e dell'ODV. Come si vede dalla figura, il processo si articola in un flusso operativo che viene attivato da una applicazione generica bancaria nel caso in cui il cliente della banca, che si è recato personalmente in uno degli *Ambienti controllati della banca* stessa, viene identificato anche come *Utente FEA*. In base al tipo di operazione ed alle informazioni che l'*Utente FEA* fornisce, l'*Operatore di sportello* interagisce con l'applicazione bancaria e produce in modo assistito un documento in formato PDF/A (Ico4) che rappresenta l'*Operazione Bancaria* da effettuare. Questo documento viene quindi inviato all'ODV.

L'ODV, mediante la componente d'ambiente EnSOFT CLIENT, verifica che il *Signature Pad* sia operativo e, ottenuto un riscontro positivo, invia il puntamento al documento (percorso dove si trova il documento) alla componente d'ambiente EnSOFT SERVER.

EnSOFT SERVER acquisisce il documento e lo elabora al fine di ottenere una rappresentazione binaria (Ico6 - immagine del documento PDF/A ricevuto). Utilizzando il canale sicuro HTTPS comunica il file immagine (Ico6) a EnSOFT Client. EnSOFT Client comunica il file immagine (Ico6) al *Signature Pad*, utilizzando il canale cifrato mediante chiave di cifratura autogenerata (Ico2) per la comunicazione da e verso EnSOFT Client e il *Signature Pad*. Mediante il dispositivo di ambiente *Signature Pad*, l'*Utente FEA* può scorrere e leggere il documento e apporre la/e firma/e richieste e confermare l'operazione. Una volta confermata l'operazione dall'*Utente FEA* i dati grafici e grafometrici (Ico5), unitamente al documento immagine (Ico6) tornano mediante lo stesso canale cifrato ad EnSOFT CLIENT che li inoltra mediante canale HTTPS ad EnSOFT SERVER. EnSOFT SERVER cifra i dati grafometrici (Ico7) con chiave pubblica della banca (Ico1) e quindi genera: il file binario contenente il documento immagine, i dati grafici e quelli grafometrici cifrati (Ico8) e il file binario contenente il documento immagine e i dati grafici (Ico9).

Il controllo torna all'ODV che genera due file PDF/A del documento firmato dall'*Utente FEA*, uno (tipo A nello schema) contenente le sole firme grafiche, l'altro (tipo B nello schema) contenente in più anche i dati grafometrici cifrati. L'ODV dopo convalida da parte dell'*Operatore di sportello*, che può solo vedere e controllare il documento in formato PDF/A prodotto, richiede ad Infocert S.p.A. l'apposizione ad entrambi i file PDF/A (A e B) della firma digitale (Ico3) della banca in formato PAdES. Quindi l'ODV esporta i due PDF/A ottenuti (Ico10 e Ico11) nei rispettivi sistemi di archiviazione.

2.4.3 Ambito logico

MPS, per gli aspetti che riguardano direttamente o indirettamente la firma elettronica di documenti da parte dei propri clienti, intende applicare le regole espresse nel DPCM 22 febbraio 2013 [**RF3**]. Questo obiettivo viene raggiunto attraverso determinazioni di tipo organizzativo, funzioni dell'ambiente operativo e funzioni dell'ODV. Di seguito vengono riportate le funzioni realizzate dall'ODV, mentre nel successivo par. 4 sono esposte le funzioni a carico dell'ambiente operativo.

La tabella sottostante sintetizza le funzioni di sicurezza esposte nel Security Target.

Codice	Funzione di sicurezza	Descrizione
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 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.
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 [**RF1**] e [**RF2**].
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.

Tabella 4 - Funzioni di sicurezza dell'ODV

2.5 Ruoli utente

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 home 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 IT.

2.6 Confini dell'ODV

L'ODV può essere utilizzato solo per gestire la firma di documenti di clienti della Banca che sono anche *Utenti FEA* mediante l'utilizzo della *FEA MPS*, all'interno degli *Ambienti controllati della banca* e dopo il riconoscimento *de visu* da parte dell'*Operatore di sportello* della Banca.

I confini dell'ODV sono rappresentati da:

- interfaccia verso le applicazioni bancarie che permettono l'utilizzo di FEA MPS
- interfaccia verso Ensoft Client e Server per l'attivazione del processo e per il recupero di dati (documenti firmati, stato dell'operazione)
- interfaccia verso le applicazioni di generazione delle chiavi pubbliche e private
- interfaccia verso Infocert S.p.A. per l'apposizione della firma digitale
- interfaccia verso le applicazioni di conservazione dei documenti firmati.

3 DICHIARAZIONE DI CONFORMITÀ (ASE_CCL)

Il ST e l'ODV sono conformi alla versione 3.1 (Revision 5) of the Common Criteria for Information Technology Security Evaluation.

La dichiarazione di conformità si riferisce a:

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 5 april 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 5 april 2017

Il pacchetto di garanzia dichiarato è EAL1.

Questo ST non dichiara la conformità ad alcun Protection Profile.

Nel ST non sono previste estensioni.

4 OBIETTIVI DI SICUREZZA PER L'AMBIENTE OPERATIVO (ASE_OBJ)

Questo paragrafo definisce gli obiettivi di sicurezza per l'ambiente operativo dell'ODV. MPS, per gli aspetti che riguardano direttamente o indirettamente la firma elettronica di documenti da parte dei propri clienti, intende applicare le regole espresse nel DPCM 22 febbraio 2013 [**RF3**]. MPS si riconosce come soggetto di cui all'art. 55 comma 2, lettera a) del DPCM 22 febbraio 2013: *"coloro che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti di cui alla lettera b)"*

L'obiettivo della conformità al DPCM viene raggiunto attraverso le funzioni dell'ODV precedentemente indicate, determinazioni di tipo organizzativo, e funzioni proprie dell'ambiente operativo, in modo da garantire la sicurezza, l'integrità e la non modificabilità del documento firmato dal cliente. Di seguito gli obiettivi per l'ambiente operativo che concorrono, unitamente alle funzioni dell'ODV, al raggiungimento dell'obiettivo di conformità al DPCM citato.

Obiettivo	Descrizione
OE.Clienti	L'ambiente operativo deve provvedere a soddisfare la seguente esigenza: identificazione del firmatario del documento e acquisizione dell'adesione dello stesso. Il cliente deve essere informato in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso. L'attivazione e l'uso del servizio devono essere subordinate alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente.

Obiettivo	Descrizione
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. Il cliente della banca deve avere la possibilità di verificare il documento che gli viene mostrato sul *Signature Pad* prima di firmarlo. Il *Signature Pad* deve permettere la lettura dell'intero documento da firmare, mediante funzioni di scorrimento, prima e dopo la sottoscrizione. Dopo la firma, il cliente deve avere la possibilità di annullare la firma stessa con apposito comando, oppure di confermare la firma apposta. L'operatore della banca non può in alcun modo intervenire sul documento, né modificarlo successivamente alla firma del cliente. Alla richiesta di una firma cliente **l'ambiente operativo** deve provvedere a generare una chiave casuale di comunicazione e ad inviarla al dispositivo di firma da utilizzare per il trasporto dei dati biometrici acquisiti da inserire nel documento. Una volta acquisiti i dati biometrici il **software di firma (ENSoft)** deve creare il blocco biometrico da cifrare con la Chiave Pubblica della banca (Ico1). Per garantire la non riusabilità del blocco biometrico, all'interno dello stesso deve essere inserito l'HASH del documento originale. Il cliente può richiedere all'operatore una copia cartacea del documento che ha sottoscritto, oppure che il medesimo gli venga inviato al recapito telematico comunicato dal cliente (posta elettronica e/o home banking).

Obiettivo	Descrizione
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. MPS deve mettere a disposizione dei clienti le funzionalità di recupero e verifica del documento elettronico sottoscritto. A tal fine MPS deve provvedere alla conservazione del documento elettronico e all'archiviazione di tutte le evidenze informatiche necessarie a comprovarne l'integrità, la leggibilità, l'assenza di modifiche dopo l'apposizione delle firme e l'autenticità delle firme apposte.
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. L'ambiente IT a supporto dell'ODV deve proteggere i documenti da trattare tramite FEA dall'introduzione e dalla presenza di agenti malevoli (malware). La rete di comunicazione deve realizzare un elevato livello di protezione al fine di garantire l'integrità e la confidenzialità delle informazioni inerenti l'ODV che viaggiano sulla rete. I responsabili dell'ODV devono assicurare che l'infrastruttura tecnologica dell'ODV sia custodita in locali nei quali l'accesso è consentito solamente al personale autorizzato.
OE.Trust	L'AGB deve trasmettere i documenti firmati dalla banca all'ODV attraverso canali o path sicuri.

Tabella 5 - Obiettivi di sicurezza

5 DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST non prevede la definizione di componenti estese.

6 REQUISITI DI SICUREZZA (ASE_REQ)

6.1 Generalità

Questa sezione definisce i requisiti funzionali di sicurezza per l'ODV.

Definisce inoltre i requisiti di garanzia soddisfatti dall'ODV.

Ogni requisito è stato estratto dai Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 5 april 2017 e dai Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 5 5april 2017.

6.2 Convenzioni

Nel presente documento sono state utilizzate le seguenti convenzioni:

Assegnazione L'operazione di assegnazione consente di specificare un parametro all'interno di un requisito. Le assegnazioni sono indicate usando un testo in grassetto all'interno di parentesi quadre **[assegnazione]**.

Iterazione L'operazione di iterazione permette di utilizzare più di una volta un componente per effettuare operazioni diverse. Una iterazione si effettua ponendo uno slash "/" alla fine del componente seguito da una stringa univoca che identifica l'iterazione.

6.3 Requisiti Funzionali di Sicurezza

Functional Requirements		
Classes	**Families**	**Description**
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_ETC.2	Export of user data with security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ITC.2	Import of user data with security attributes

Tabella 6 - ODV Security Function Requirements (SFR)

6.4 Dettaglio dei Requisiti Funzionali

FDP_ACC.1	
Hierarchical to:	No other components
FDP_ACC.1.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] on: [**Soggetti:** • **Document Service** **Oggetti:** • **Contenuti binari del documento** • **PDF/A tipo A (Ico8)** • **PDF/A tipo B (Ico9)** **Operazioni:** • **Riceve da EnSOFT SERVER i contenuti binari del documento e crea i PDF/A (tipo A e B) del documento stesso** • **Invia i documenti PDF/A (tipo A e B) ad Infocert per l'apposizione della firma digitale della banca** • **Riceve i documenti PDF/A (tipo A e B) firmati digitalmente PAdES dalla banca** • **Invia in CS il documento PDF/A B firmato PAdES** • **Invia in CM il documento PDF/A A firmato PAdES**]
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	

FDP_ACF.1	
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] to objects based on the following: **[Attributi Soggetti: nessuno** **Attributi Oggetti: firma digitale PAdES]**.

FDP_ACF.1	
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**il soggetto può inviare il PDF/A tipo B in CS se l'oggetto è:** • firmato digitalmente dalla banca in formato **PAdES** **il soggetto può inviare il PDF/A tipo A in CM se l'oggetto è:** • firmato digitalmente dalla banca in formato **PAdES**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	Le operazioni di ricezione da EnSOFT SERVER e da Infocert non sono sostenute da attributi di sicurezza

FDP_ITC.1	
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	L'ODV riceve da EnSOFT server il contenuto binario dei dati biometrici di firma, della firma e del documento convalidato da AGB

FDP_ETC.1	
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Notes:	L'ODV prepara i PDF/A A e B del documento da firmare e li invia ad Infocert per l'apposizione della firma digitale della banca

FDP_ITC.2	
Hierarchical to:	No other components.
FDP_ITC.2.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path FPT_TDC.1 Inter-TSF basic TSF data consistency
Notes:	L'ODV riceve da Infocert il documento firmato dalla banca in modalità PAdES. L'ambiente operativo si fa carico di trasmettere il documento in

FDP_ITC.2	
	maniera protetta.

FDP_ETC.2/CS	
Hierarchical to:	No other components.
FDP_ETC.2.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [**none**].
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Notes:	Si applica all'invio in Conservazione Sostitutiva (CS) del documento tipo B firmato digitalmente dalla banca

FDP_ETC.2/CM	
Hierarchical to:	No other components.
FDP_ETC.2.1	The TSF shall enforce the [**politica di sottoscrizione documenti**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [**none**].

FDP_ETC.2/CM	
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Notes:	Si applica all'invio nel sistema di archiviazione della banca (CM) del documento tipo A firmato digitalmente dalla banca

6.5 Requisiti di Garanzia

I requisiti di garanzia per l'ODV sono quelli previsti al livello EAL1, come specificato nella Parte 3 dei Common Criteria, senza potenziamenti.

EAL1 è stato scelto come livello di garanzia in quanto l'ODV opera in un ambiente protetto, con amministratori competenti e con utenti controllati. In questo contesto si assume che eventuali attaccanti avranno un potenziale di attacco limitato, di conseguenza il livello EAL1 è appropriato per fornire la garanzia necessaria a contrastare attacchi a limitato potenziale.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the ODV
	ALC_CMS.1 TOE CM coverage
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Tabella 7 - Security Assurance Requirements (SAR)

ADV_FSP.1 Basic functional specification		
Dependencies:	None	
Developer action elements:	ADV_FSP.1.1D	The developer shall provide a functional specification.
	ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
AGD_OPE.1 Operational user guidance		
Dependencies:	ADV_FSP.1 Basic functional specification	
Developer action elements:	AGD_OPE.1.1D	The developer shall provide operational user guidance.
AGD_PRE.1 Preparative procedures		
Dependencies:	None	
Developer action elements:	AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
ALC_CMC.1 Labeling of the TOE		
Dependencies:	ALC_CMS.1 TOE CM coverage	
Developer action elements:	ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMS.1 TOE CM coverage		
Dependencies:	None	
Developer action elements:	ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
ASE_INT.1 ST introduction		

Dependencies:	None	
Developer action elements:	ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_CCL.1 Conformance claims		
Dependencies:	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements	
Developer action elements	ASE_CCL.1.1D	The developer shall provide a conformance claim.
	ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_OBJ.1 Security objectives for the operational environment		
Dependencies:	None	
Developer action elements	ASE_OBJ.1.1D	The developer shall provide a statement of security objectives.
ASE_ECD.1 Extended components definition		
Dependencies:	None	
Developer action elements	ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
	ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_REQ.1 Stated security requirements		
Dependencies:	ASE_ECD.1 Extended components definition	
Developer action elements:	ASE_REQ.1.1D	The developer shall provide a statement of security requirements.
	ASE_REQ.1.2D	The developer shall provide a security requirements

	rationale.
ASE_TSS.1 TOE summary specification	
Dependencies:	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements:	ASE_TSS.1.1D The developer shall provide a TOE summary specification.
ATE_IND.1 Independent testing – conformance	
Dependencies:	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements:	ATE_IND.1.1D The developer shall provide the TOE for testing.
AVA_VAN.1 Vulnerability survey	
Dependencies:	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements:	AVA_VAN.1.1D The developer shall provide the TOE for testing.

Tabella 8 - Dettaglio dei singoli componenti di garanzia

6.6 Analisi delle dipendenze

La seguente Tabella mostra le dipendenze richieste dai Common Criteria per ogni SFR e SAR al livello di garanzia scelto.

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
SFR		
FDP_ACC.1	FDP_ACF.1 Simple security attributes	FDP_ACF.1 Simple security attributes
FDP_ACF.1	FDP_ACC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_ACC.1 Subset information flow control **NOTA 1**
FDP_ITC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 Subset access control **NOTA 1**
FDP_ETC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Subset access control
FDP_ITC.2	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1 Subset access control **NOTA 1** **NOTA 2** **NOTA 3**
FDP_ETC.2/CS	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Subset access control
FDP_ETC.2/CM	FDP_ACC.1 Subset access control, or	FDP_ACC.1 Subset access control

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
	FDP_IFC.1 Subset information flow control	
SAR		
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1 Basic functional specification
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1 TOE CM coverage	ALC_CMS.1 TOE CM coverage
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
AVA_VAN.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Tabella 9 - Tabella delle analisi delle dipendenze

NOTA 1 – Per i requisiti funzionali FDP_ACF.1, FDP_ITC.1/Doc e FDP_ITC.1/Firma, la dipendenza con FMT_MSA.3 non è rispettata poiché l'ODV non possiede funzioni di management e non gestisce gli attributi di sicurezza, in quanto gli stessi sono definiti a livello di inizializzazione del sistema e sono gestiti dall'ambiente IT della banca.

NOTA 2 – La dipendenza di FDP_ITC.2 con FTP_ITC.1 oppure con FTP_TRP.1 non è rispettata in quanto viene demandato all'ambiente operativo il compito di trasmettere i documenti all'ODV in maniera protetta.

NOTA 3 – La dipendenza di FDP_ITC.2 con FPT_TDC.1 non è rispettata in quanto le TSF non condividono dati con altri prodotti IT.

7 SPECIFICHE SOMMARIE DELL'ODV (ASE_TSS)

Questa sezione fornisce le specifiche sommarie dell'ODV, una definizione ad alto livello delle funzioni di sicurezza soddisfatte dai requisiti funzionali e di garanzia.

7.1 Riepilogo delle funzioni di sicurezza

Le funzioni di sicurezza rappresentate nel Security Target sono le seguenti:

ODV_Firma **Immodificabilità e connessione univoca**

ODV_Cons **Conservazione Sostitutiva a norma**

ODV_Archiv **Archiviazione nei sistemi MPS**

7.1.1 ODV_Firma – Immodificabilità e connessione univoca

Al termine del processo di firma da parte dell'*Utente FEA*, se l'*Operatore di sportello* conferma la validità del documento prodotto, e solo in questo caso, viene fornita notifica dall'EnSOFT Client all'ODV, il quale provvederà ad invocare la componente applicativa atta a prelevare da EnSOFT SERVER i documenti binari contenenti rispettivamente i dati grafometrici (Ico8) e grafici (Ico9) e conseguentemente a salvarli su file system creando così i due file PDF/A (tipo A e B, come definito al § 2.4.2 "Flussi operativi dell'ODV e del suo ambiente"). L'ODV fornisce quindi sempre una notifica del completamento dell'operazione alla AGB, corredandola dello stato della stessa (processo completato correttamente, annullamento da parte dell'operatore, errore, etc.). E' cura dell'AGB, previa verifica interna finale, l'invocazione della componente applicativa Document Service dell'ODV che, a sua volta, richiede ad Infocert S.p.A. l'apposizione ad entrambi i file PDF/A della firma digitale della banca (fornita dalla CA Infocert SpA) in formato PAdES con algoritmo RSA a 2048 bit e hash SHA-256. I due file PDF/A sono in questo modo immodificabili e sono univocamente connessi all'*Utente FEA* che ha apposto le firme, alla banca che ha firmato a sua volta il file generando il formato PAdES e all'*Operazione Bancaria* connessa.

Le operazioni sopra riportate realizzano le SFR **FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FDP_ETC.1, FDP_ITC.2.**

7.1.2 ODV_Cons – Conservazione Sostitutiva a norma

La componente applicativa dell'ODV Document Service dopo aver ricevuto il file PDF/A di tipo B (quello contenente anche i dati grafometrici cifrati come descritto al precedente § 7.1.1 "ODV_Firma – Immodificabilità e connessione univoca") firmato in formato PAdES, invia la busta informatica al conservatore Intesa S.p.a.(Gruppo IBM). Questo file PDF/A contiene il documento con le firme grafiche apposte dall'*Utente FEA* e i dati grafometrici delle firme cifrati mediante la chiave pubblica della banca, rilasciata da CA Infocert, la cui corrispondente privata è custodita

presso notaio (questo a garanzia della possibilità di decifratura solo in caso di uso forense). Quando il conservatore riceve il file applica allo stesso una marca temporale e firma digitale, portando lo stesso in formato CaDES. Quindi si occupa della sua conservazione a norma. Questo documento potrà essere richiesto alla conservatoria in caso di uso forense.

Le operazioni sopra riportate realizzano le SFR **FDP_ACC.1, FDP_ACF.1, FDP_ETC.2/CS.**

7.1.3 ODV_Archiv – Archiviazione nei sistemi MPS

La componente applicativa dell'ODV Document Service, dopo aver ricevuto il file PDF/A di tipo A (quello contenente le sole firme grafiche come descritto al precedente § 7.1.1 "ODV_Firma – Immodificabilità e connessione univoca") firmato in formato PAdES, invia il file all'archivio MPS per l'archiviazione e la messa a disposizione dei clienti. Dato il formato PAdES il documento è facilmente visibile all'*Utente FEA*, così come all'interno della banca, mediante un semplice Reader Acrobat, mediante il quale viene anche verificata l'integrità dello stesso (controllo dello SHA256 del documento) e validità della firma della banca.

Le operazioni sopra riportate realizzano le SFR **FDP_ACC.1, FDP_ACF.1, FDP_ETC.2/CM.**

7.1.4 SFR e funzioni di sicurezza dell'ODV

La tabella seguente fornisce la mappatura dei SFR con le funzioni di sicurezza dell'ODV.

	ODV_Firma	ODV_Cons	ODV_Archiv
FDP_ACC.1	**X**	**X**	**X**
FDP_ACF.1	**X**	**X**	**X**
FDP_ITC.1	**X**		
FDP_ETC.1	**X**		
FDP_ITC.2	**X**		
FDP_ETC.2/CS		**X**	
FDP_ETC.2/CM			**X**

Tabella 10 - Mappatura dei SFR con le funzioni dell'ODV