MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Firma Grafometrica e dematerializzazione documenti

Rapporto n. 85/2018

Siena,

Direzione Chief Audit Executive
Area Revisione Specialistica
Servizio ICT & Operational Audit

La presente revisione è stata indirizzata a valutare la soluzione di Firma Elettronica Avanzata (FEA) implementata dalla Banca nella forma della Firma Grafometrica e la sua applicazione nell'ambito del servizio di dematerializzazione documenti.

In tale contesto sono stati pertanto esaminati i seguenti ambiti:

- *il rispetto dei requisiti di sicurezza e delle prescrizioni tecniche, stabilite per legge, della soluzione tecnica adottata;*
- *il rispetto dei requisiti di processo, stabiliti per legge, della soluzione adottata;*
- *l'archiviazione e fruibilità dei documenti archiviati;*
- *la cura posta nelle prassi di gestione documentale previste in filiale per l'operatività digitalizzata con la Firma Grafometrica;*
- *l'effettivo impiego del Servizio nell'operatività corrente e il relativo monitoraggio;*
- *il rispetto delle prassi normative agite in fase di negoziazione e di monitoraggio dei fornitori ingaggiati per la fornitura del Servizio.*

La revisione ha interessato le seguenti Funzioni:

- *"Servizio Organization Partner COO e Digital Center", in qualità di owner del processo aziendale cui fa riferimento il Servizio di Firma Grafometrica;*
- *"Servizio Acquisti di Gruppo e Gestione Fornitori", in qualità di funzione deputata all'acquisizione di beni e servizi;*
- *"Servizio Cash Management, ATM e Logistica", in qualità di gestori del servizio di archiviazione e conservazione della documentazione;*
- *"Servizio Sicurezza Informatica e BCM" del Consorzio, in qualità di gestore delle quantità di sicurezza utilizzate;*
- *"Servizio Assisted Banking" del Consorzio, in qualità di gestore della soluzione tecnologica adottata per il Servizio di Firma Grafometrica;*
- *"Servizio Sistemi Tecnologici " del Consorzio, in qualità di gestore del fleet management.*

La revisione è stata svolta mediante:

- *colloqui con i referenti delle Strutture interessate e osservazione delle prassi agite;*
- *esame della normativa e della documentazione operativa correlata;*
- *verifiche a campione.*

In ottemperanza alle disposizioni di Vigilanza ed in conformità agli Standard di Audit del Gruppo, i risultati della revisione sono stati comunicati alle competenti Funzioni in occasione dell'exit meeting e formalizzati nel presente report da audit da inviare agli Organi Aziendali.

Overview

Anagrafica Intervento

Intervento: Firma Grafometrica e dematerializzazione documenti
Obbligatorietà: NO
Unità auditata/e:
- Servizio Acquisti di Gruppo e Gestione Fornitori
- Servizio Cash Management, ATM e Logistica
- Servizio Organization Partner COO e Digital Center
- COG/Servizio Assisted Banking
- COG/Servizio Sicurezza Informatica e BCM
- COG/Servizio Sistemi Tecnologici

Tipologia di intervento: Settoriale – in loco

Date open meeting: 07/05/2018, 08/05/2018, 10/05/2018
Date exit meeting: 19/09/2018, 26/09/2018, 10/10/2018

Responsabili Audit Team:
- Scarponi Erbalisa - IT
- Parigi Giovanni - Operation (CISA)

Audit Team:
- Bonci Andrea
- De Mauro Silvia
- Berlese Paolo Antonello

Esito Intervento

Grade Complessivo Intervento

Rating 1 (VERDE)	Rating 2 (GIALLO)	Rating 3 (ARANCIONE)	Rating 4 (ROSSO)

La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

Fattore Causale	Distribuzione dei Gap per rilevanza		
	Alta	Media	Bassa
Risorse			
Processi	2	2	2
Sistemi	3	1	2
Totale	5	3	4

Precedenti interventi di revisione (se esistenti)

Ambito intervento	Periodo della verifica	N. rapporto	Grade Intervento
Revisione sulle strategie di proposizione e contrattualizzazione alla clientela del Servizio di Firma Elettronica	12/2017 – 02/2018	242/2017	Verde

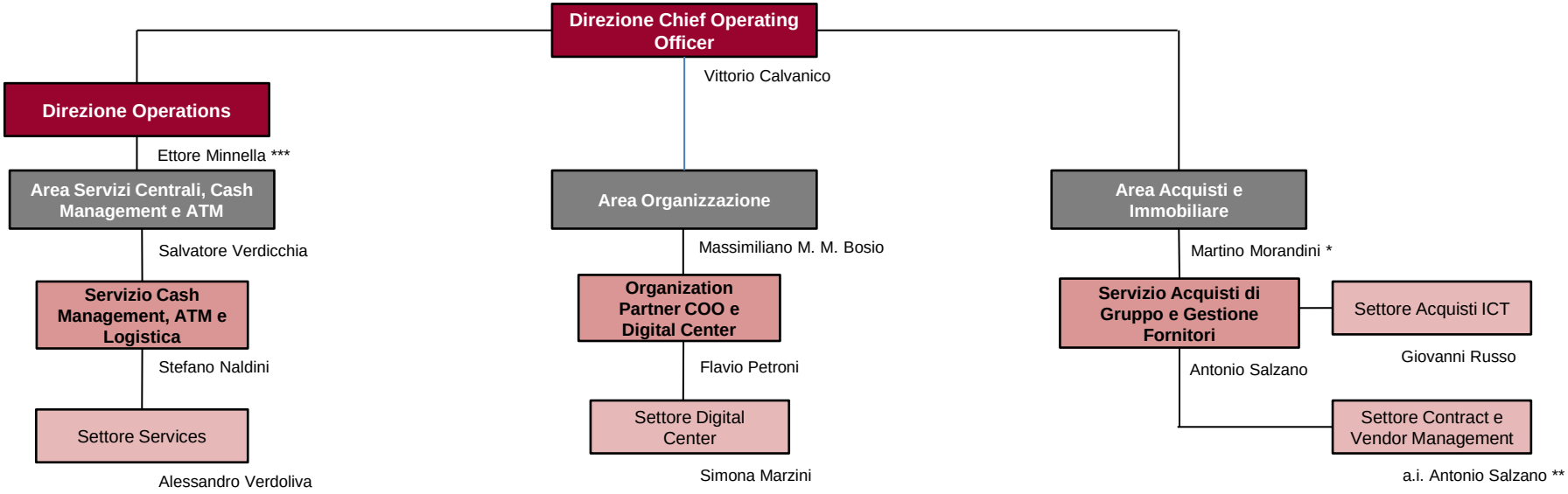
Organi destinatari del presente audit

Legal Entity	Organo Destinatario
BMPS	Presidente del CdA
BMPS	Amministratore Delegato
BMPS	Collegio Sindacale
BMPS	Comitato Rischi
COG	Presidente del CdA, Presidente CS , AD (*)

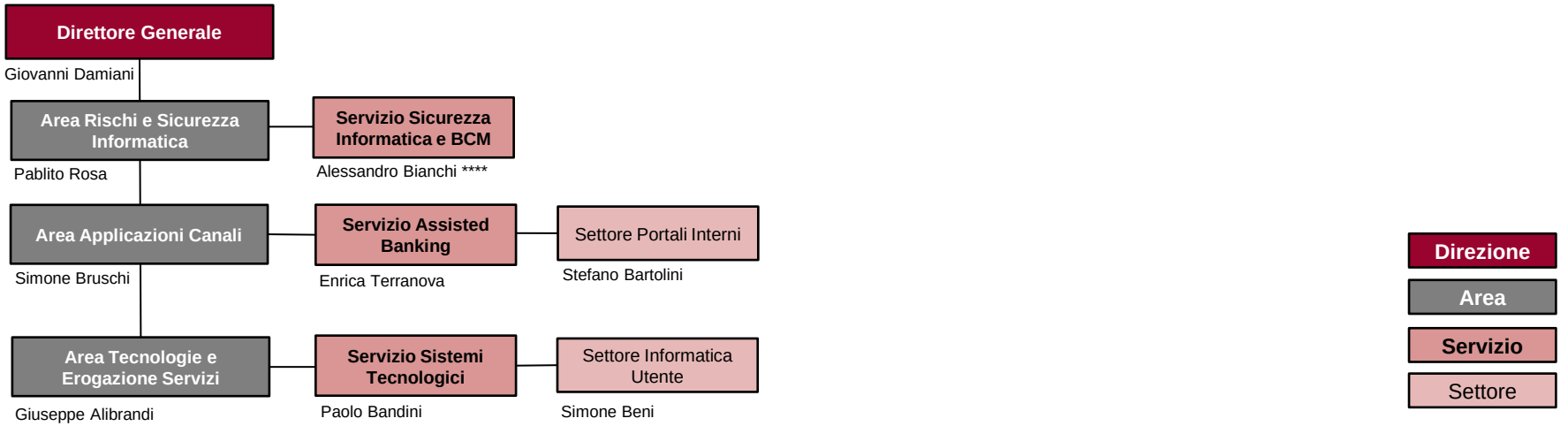
(*) L'attività rientra tra quelle svolte dalla Capogruppo in qualità di Funzione di Audit esternalizzata del Consorzio

Organigramma Strutture Auditate

BMPS - Capogruppo bancaria



Consorzio Operativo Gruppo Montepaschi



Alla data dell'Open Meeting le responsabilità erano cosi delineate:

* Ettore Minnella (ex Area Acquisti, Cost Management Logistica);
** Cesare Limone;
*** Fausto Moreni (ex Dir. Organizzazione e Operations)
**** a.i. Pablito Rosa

Executive Summary (1/3)

CONTESTO DI RIFERIMENTO

A partire dal 2014, con il Servizio di Firma Elettronica Avanzata (FEA) la Banca ha messo a disposizione della propria clientela una tecnologia che consente di firmare in formato elettronico contratti e moduli relativi ad operazioni di sportello che, sul piano giuridico, hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa.

La progressiva trasformazione digitale dei processi di Rete passa attraverso la diffusione di questo Servizio che conta 2,9 mln di adesioni ad ottobre 2018 e 5,77 mln di operazioni nel primo semestre 2018. L'attivazione del Servizio è gratuita e permette alla Banca un abbattimento dei costi (stampa, archiviazione e gestione del cartaceo) ed una riduzione dei rischi di smarrimento/deterioramento dei documenti.

ADESIONE FEA

Rischi di disconoscimento di operazioni e trattamento non autorizzato di dati biometrici non adeguatamente mitigati

L'iter di contrattualizzazione del Servizio di FEA è un processo regolamentato da norme interne, le cui prassi, agite dagli operatori di Filiale, si concludono con la firma autografa del cliente apposta sul modello di adesione. Tale accettazione consente alla Banca:

- di proporre al cliente la sottoscrizione con firma grafometrica, apposta su *signature-pad*, di tutti i contratti e le disposizioni di sportello su rapporti, presenti e di futura accensione, per i quali sia stata prevista questa modalità di firma e per i quali il cliente abbia i necessari poteri di firma o di rappresentanza;
- di trattare i dati biometrici del cliente, nei termini previsti dal Codice per il trattamento dei Dati Personali.

Le verifiche condotte hanno evidenziato rischi di indisponibilità del modello di adesione completo e firmato, in particolar modo per quelli ante 2016, conservati in Filiale e non accentrati presso il centro documentale. Nello specifico:

- i documenti di adesione ante 21/12/2015***** (circa 1,3 mln di contratti) risultano non accentrati per scelta organizzativa; per tali documenti gli esiti delle verifiche campionarie hanno registrato percentuali che oscillano tra il 65% ed il 99% di documentazione non firmata (**cfr. gap 1**); è già stato avviato un tentativo di raccolta massiva alla fine del 2017 che si è concluso a metà del 2018 senza risultati significativi (solo 12.102 recuperi);
- i documenti di adesione post 20/12/2015 vengono accentrati presso il centro documentale; per tali documenti è stata riscontrata la casistica di pratiche il cui conferimento risulta sospeso o annullato (complessivamente circa 29,5K a luglio 2018) a fronte di motivazioni in gran parte vaghe, assenti o che confermano la mancanza di firma; tali condizioni tuttavia non inibiscono l'operatività con firma grafometrica da parte del cliente (**cfr. gap 2**) .

Quanto sopra dimostra una rilevante esposizione al rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente senza preventiva adesione al Servizio di FEA e al rischio di non conformità per il trattamento non autorizzato di dati biometrici con possibili sanzioni amministrative.

In corso di revisione le funzioni Organizzazione e Rete hanno riconosciuto la necessità di una azione congiunta, già in fase di approntamento, e prioritariamente mirata alla riduzione dello stock di adesioni numericamente più consistente, con precedenza ai clienti che hanno effettivamente concluso almeno una operazione con firma grafometrica (996K a novembre 2018).

(*) Data scelta come spartiacque per il nuovo modello organizzativo basato sull'accentramento documentale.

Executive Summary (2/3)

FIRMA GRAFOMETRICA

Rispetto dei requisiti previsti per la Firma Elettronica Avanzata e delle prescrizioni del Garante in tema di biometria non sempre garantito

Le verifiche condotte sul Sistema di Firma Grafometrica implementato hanno evidenziato carenze nei presidi di controllo tali da non garantire il rispetto dei requisiti tecnici e di processo regolamentati nel 'DPCM del 22/02/2013 - *Regole tecniche in materia di generazione, Apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*'.

Nello specifico si osserva che, allo scopo di garantire *«l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello* stesso *rappresentati»,* la soluzione implementata dalla Banca prevede l'adozione di un formato standard internazionale (ISO 19005-1:2005, PDF/A) per i documenti a Firma Grafometrica. Tuttavia, l'assenza di controlli sul formato dei documenti, in ingresso al sistema di acquisizione delle firma cliente, nonché in uscita dallo stesso, non consente di garantire il rispetto dello standard previsto e quindi dei requisiti di legge (**cfr. gap 3**). Nel corso delle verifiche è stato infatti rilevato come tale carenza abbia consentito la sottoscrizione di documenti, ab origine non conformi al formato PDF/A, che a oggi risultano illeggibili e pertanto privi di qualsiasi validità.

E' stata altresì rilevata l'assenza di un controllo atto a garantire che il documento elettronico sottoscritto grafometricamente del cliente non abbia subito modifiche prima dell'apposizione della firma digitale della Banca e che quindi non vengano archiviati in Conservazione Sostitutiva documenti alterati e pertanto non opponibili in giudizio (**cfr. gap 8**).

Nel corso della revisione è stato inoltre verificato che la soluzione di Firma Grafometrica implementata rispettasse i requisiti funzionali previsti per l'operatività con Firma Elettronica, nell'ambito del processo «*Vendita e Contrattualizzazione prodotti e servizi»*. A tal proposito le verifiche a campione condotte sul perimetro delle operazioni di sportello hanno evidenziato casi di operazioni sottoscritte grafometricamente a fronte delle quali non risultano prodotte e quindi archiviate le relative distinte elettroniche (**cfr. gap 6**) .

ARCHIVIAZIONE DOCUMENTI

Archiviazione dei documenti a Firma Grafometrica presidiata

I documenti elettronici, prodotti nell'ambito del processo di Firma Grafometrica, vengono archiviati all'interno di due distinti sistemi. Nello specifico, il documento contenente il solo segno grafico del cliente viene archiviato all'interno del sistema informativo aziendale (IBM Content Manager); il documento contenente, oltre al segno grafico, anche i dati biometrici criptati del cliente viene inviato in Conservazione Sostituiva, servizio in outosurcing a In.Te.S.A. S.p.A.

Le verifiche hanno confermato, limitatamente al campione analizzato, l'archiviazione nonché la fruibilità delle distinte a Firma Grafometrica prodotte a fronte di operazioni di sportello. Nonostante l'esito positivo delle verifiche a campione, è stata tuttavia rilevata l'assenza di un sistema di monitoraggio a presidio dell'effettiva archiviazione dei documenti elettronici. La carenza, rappresentata in sede di exit meeting, è stata sanata prima della pubblicazione del presente rapporto.

Il servizio di conservazione sostitutiva di documenti digitali del fornitore In.Te.S.A. SpA è stato approfondito anche dal punto di vista della gestione del fornitore, rilevando la necessità di rivedere l'accordo con l'appaltatore, per l'estensione di un periodo massimo di conservazione per alcune tipologie contrattuali, che non è risultato conforme alle disposizioni di legge, e l'introduzione di un periodo di preavviso prima della distruzione documentale. E' stato richiesto inoltre di attivare il monitoraggio sulla qualità della fornitura ricevuta. Anche tali carenze sono state sanate prima della pubblicazione del presente rapporto dalla Funzione Logistica di BMPS.

Executive Summary (3/3)

SICUREZZA LOGICA

Carenze nei presidi di sicurezza logica

Nella gestione dell'archivio documentale della Banca (IBM Content Manager) non sono rispettati i presidi minimi di sicurezza logica, sia in termini di gestione delle utenze che di tracciatura delle relative attività svolte (**cfr. gap 4**). Non è pertanto possibile garantire la riservatezza e l'integrità dei documenti archiviati.

Gli strumenti di amministrazione e accesso ai contenuti del Content Manager non sono integrati con le componenti infrastrutturali del controllo accessi, inoltre le prassi agite per la gestione delle utenze (personali e applicative) sono risultate difformi alle policy aziendali in materia. Si evidenziano a tal proposito casi di accesso con utenze applicative e l'utilizzo condiviso tra più persone di un unico utente con privilegi di amministratore. Infine, l'assenza di un log rende impossibile ricostruire a posteriori le attività svolte dai singoli utenti.

Per quanto attiene il sistema di Conservazione Sostitutiva, è stata accertata l'impossibilità di risalire alle operazioni effettuate sui documenti archiviati (**cfr. gap 7**). Nello specifico, il sistema di tracciatura dello strumento per l'accesso ai documenti, «Portale Documenti», non è in grado di rilevare né il quanto acceduto né le operazioni effettuate (interrogazione/download). Nel corso della revisione sono state riscontrate carenze anche nella gestione delle utenze di accesso al «Portale Documenti» cui ascrivere, tra le altre, la presenza di utenze anonime ovvero non associabili ad alcuna risorsa. La criticità evidenziata in sede di exit meeting è stata sanata prima della pubblicazione del presente rapporto.

Infine, con specifico riferimento alla soluzione di Firma Grafometrica, le verifiche condotte sulle cartelle di rete in cui transitano i documenti elettronici hanno evidenziato la presenza di utenze personali con privilegi di accesso in modifica, rimosse nel corso della revisione su segnalazione della team di audit. Si rileva tuttavia l'impropria archiviazione nelle suddette cartelle dei documenti contenenti i dati biometrici criptati dei clienti; tale circostanza introduce un rischio di accesso non autorizzato ai documenti archiviati al di fuori della Conservazione a norma (**cfr. gap 11**).

ACCESSO DIRETTO AI DATI

Accesso diretto ai dati bypassando tutti i presidi di controllo stabiliti dalle policy aziendali

Nel corso delle verifiche è stato accertato l'utilizzo dell'applicativo "Gestione Tabellare" per condurre attività di accesso diretto in modifica ai dati operativi, eludendo tutti i presidi di controllo ad oggi implementati per garantire il rispetto delle policy di sicurezza logica di Gruppo (**cfr. gap 5**).

Lo strumento in argomento ha peraltro evidenziato evidenti limiti negli aspetti di sicurezza logica tra i quali: l'assenza di meccanismi automatici di attribuzione e/o revoca delle abilitazioni che tengano conto, ad esempio, dell'effettiva assegnazione delle risorse alle strutture aziendali; l'assenza di un log auditabile; l'impossibilità di intercettare gli accessi ai dati attraverso gli strumenti preposti al monitoraggio. Tenuto conto dell'ampia diffusione nell'utilizzo dello strumento all'interno del Consorzio, nonché della rilevanza dell'informazione relativa agli accessi in modifica anche ai fini della corretta valutazione del rischio informatico, è stata da subito avviata una specifica attività finalizzata a ricondurre l'accesso diretto ai dati nell'ambito delle corrette Policy di Gruppo.

Tabella dei gap (1 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
1	Vendita/contrattualizzazione Prodotti e Servizi / Gestione contratto per servizio di Firma Elettronica Avanzata e Dematerializzazione Documenti	**Operatività con firma grafometrica a rischio disconoscimento e/o trattamento di dati biometrici non autorizzato** Prima dell'accentramento obbligatorio (dicembre 2015) le istruzioni operative prevedevano la conservazione in filiale dell' adesione al servizio di FEA (circa 1,3M di documenti). Questa condizione espone ad una minore certezza di recupero della documentazione e non ne garantisce la correttezza formale (es. presenza delle firma). Quanto detto è stato confermato da una ricognizione compiuta presso un campione di filiali, i cui esiti hanno rilevato un'elevata percentuale (99% in un caso e 65% nell'altro) di documentazione non firmata e/o archiviata in maniera non appropriata. Quanto sopra non tutela efficacemente dal rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente senza preventiva adesione al Servizio di FEA, né dal rischio di non conformità per il trattamento non autorizzato di dati biometrici con possibili sanzioni amministrative.	A	Compliance/ Operativo	Processo	**Recupero documentazione presente in filiale**. Recuperare tale documentazione riconfigurando un Piano di accentramento sul modello dell'iniziativa 2017 che ha centralizzato solo 12.102 documenti. Per quanto non immediatamente recuperabile, inibire ai clienti l'operatività mediante firma grafometrica.	Dir Rete con il contributo del Servizio Organization Partner COO e Digital Center e Servizio Controlli, Conformità e Operations	31/12/2019

Tabella dei gap (2 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
2	Vendita/contrattualizzazione Prodotti e Servizi / Gestione contratto per servizio di Firma Elettronica Avanzata e Dematerializzazione Documenti	**Ritardato o mancato invio del documento di adesione al servizio FEA al Centro Documentale** Gli accertamenti hanno riguardato quei clienti per i quali le Filiali/Centri Specialistici non hanno trasmesso al Centro Documentale il documento di adesione al Servizio di FEA tramite procedura PARDO: ▪ documenti “sospesi” (n. 9.671 al 30/04/18, su un totale di 1.360.697 prodotti). L’analisi sui suddetti documenti ha rilevato sospesi datati (il 60% originato ante 2018) e giustificativi per la sospensione in gran parte vaghi, assenti o che confermano la mancata firma del cliente; ▪ documenti “annullati” (n. 16.839 al 30/04/18). Per questi è stato verificato su un campione di 30 unità che fosse stata inibita l’operatività con firma grafometrica o in caso contrario non vi fossero altri documenti Pardo collegati. Il test è fallito per tutti i casi analizzati. Sospendere o annullare la pratica PARDO non esclude l’operatività con firma grafometrica del cliente e, al contempo, non consente l’effettuazione dei controlli da parte del Centro Documentale (presenza firma e completezza della documentazione di adesione). Come rappresentato nel gap precedente anche questa condizione espone al rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente e al rischio di non conformità per il trattamento non autorizzato di dati biometrici.	A	Compliance / Operativo	Processo	**Limitare l’incidenza di documentazione sospesa/annullata in PARDO** Al fine di limitare i rischi indotti da «documentazione sospesa/annullata», prevedere una serie di misure di controllo per limitarne la proliferazione, richiamando la Rete alla sistemazione di quanto non regolarizzato.	Servizio Organization Partner COO e Digital Center con il contributo del Servizio Controlli, Conformità e Operations	30/06/2019

Tabella dei gap (3 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (gg/mm/aa)
3	Vendita / contrattualizzazione Prodotti e Servizi / Operatività con firma elettronica	**Assenza di controlli sul formato del documento digitale** Il DPCM del 22 febbraio 2013 «*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*» include tra i requisiti della soluzione di Firma Elettronica Avanzata (FEA): ▪ *«l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati»;* ▪ *«la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma»*. Allo scopo di rispettare tali requisiti, la soluzione FEA implementata dalla Banca prevede l'adozione del formato standard internazionale ISO 19005-1:2005, PDF/A*, per i documenti a firma grafometrica. Si osserva tuttavia che non sono presenti controlli atti a garantire che i documenti prodotti dalle diverse applicazioni bancarie e sottoposti alla firma del cliente siano conformi al suddetto formato. Questa carenza ha consentito la sottoscrizione di documenti ab origine non conformi al formato PDF/A, circostanza questa che ne ha determinato l'alterazione del contenuto che ad oggi risulta illeggibile. I documenti della specie risultano pertanto privi di qualsiasi validità. A tal proposito, con riferimento alla sottoscrizione di operazioni su Fondi Anima si osserva che: ▪ in data 12/06 sono stati rilasciati in produzione 5 modelli non conformi che hanno determinato l'archiviazione di 165 documenti illeggibili su un totale di 429 sottoscritti. ▪ In data 28/06 sono stati rilasciati in produzione 2 modelli non conformi che hanno determinato l'archiviazione di 18 documenti illeggibili su un totale di 41 sottoscritti. (*) Standard ISO 19005-1:2005, Document management -- Electronic document file format for long-term preservation, https://www.iso.org/standard/38920.html	A	Operativo	Sistemi	**Implementare controlli per verificare la consistenza del documento digitale al formato PDF/A** Allo scopo di garantire l'aderenza ai requisiti regolamentari definiti per la Firma Elettronica Avanzata, implementare controlli che consentano di accertare la conformità al formato PDF/A, del documento elettronico sottoposto alla firma del cliente. Assicurare la conformità al suddetto formato anche in uscita dal sistema di acquisizione della firma cliente.	COG Servizio Assisted Banking	30/04/2019

Tabella dei gap (4 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
4	Gestione dei processi operativi di sicurezza logica / Gestione documenti in formato digitale della clientela	**Mancato rispetto dei presidi minimi di sicurezza logica nella gestione dell'archivio documentale della Banca, IBM Content Manager (CM)** a) Il governo e la gestione delle utenze applicative che accedono al CM nonché dei relativi profili abilitativi vengono condotti difformemente dalle policy aziendali in materia*. Si rileva altresì che non è possibile, allo stato attuale, ricostruire l'associazione delle utenze ai corrispondenti asset di riferimento e strutture responsabili dell'utilizzo. b) Con riferimento alle modalità di accesso agli strumenti nativi a supporto del CM**, si osserva che: ▪ le applicazioni non sono integrate con il sistema di autenticazione *Single Sign-On* (SSO) e non risultano implementati i processi di gestione centralizzati delle credenziali e dei profili abilitativi*; ▪ la consolle di amministrazione, utilizzata anche per il censimento delle utenze, è accessibile esclusivamente tramite un'utenza generica (*icmadmin*) condivisa tra più risorse afferenti a strutture consortili diverse; ▪ l'applicazione web per l'accesso diretto ai contenuti del CM è acceduta da risorse della Banca e del Consorzio utilizzando le utenze applicative. c) Gli strumenti a supporto del CM non sono auditabili non essendo disponibili né log degli accessi né delle operazioni effettuate. Non è pertanto possibile ricostruire a posteriori l'operatività degli utenti. (*) D 02026 «*Regole in materia di Gestione e Controllo Accessi: Accesso ad Applicazioni e Sistemi ICT*» D 00150 «*Processo Gestione Accessi Logici*» del Consorzio (**) *IBM System Administration Client*, consolle di amministrazione del CM *IBM Content Navigator*, applicazione web per l'accesso diretto ai contenuti del CM	A	Operativo	Sistemi	**Ricondurre la gestione del CM alle Policy di sicurezza logica** a) Ricondurre la gestione delle utenze applicative e dei relativi profili abilitativi nell'ambito delle policy aziendali in materia. Eseguire un assessment sulle utenze applicative attualmente censite finalizzato a ricondurre ciascuna utenza al proprio asset di riferimento, affinché sia sempre chiaramente identificabile la Struttura responsabile del loro corretto utilizzo. b) Implementare i corretti presidi di sicurezza per l'accesso agli strumenti a supporto del CM: ▪ valutare l'opportunità di integrare gli strumenti a supporto del CM nell'ambito del sistema di autenticazione SSO. Da subito, ricondurre le richieste di accesso logico nell'ambito del processo di Gruppo; ▪ creare le necessarie utenze nominative di tipo gestionale da assegnare agli utenti della consolle di amministrazione del CM, disattivando contestualmente l'utenza generica; ▪ inibire l'utilizzo interattivo delle utenze applicative tramite Content Navigator. Implementare inoltre le necessarie modifiche affinché la parte segreta delle credenziali (password) sia gestita in modo sicuro. c) Implementare per gli strumenti a supporto del CM un sistema di tracciatura degli accessi e dell'operatività svolta in modo da garantirne la verificabilità.	COG Servizio Sistemi Tecnologici con il contributo del Servizio Assisted Banking	28/02/2019

Tabella dei gap (5 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
5	Gestione dei processi operativi di sicurezza logica	**Accesso diretto ai dati eludendo i presidi di controllo definiti** Nel corso delle verifiche è stato accertato l'utilizzo, diffuso e trasversale nell'ambito del Consorzio, dell'applicativo "Gestione Tabellare" per condurre attività di accesso diretto in modifica ai dati operativi, eludendo tutti i presidi di controllo ad oggi implementati per garantire il rispetto delle policy di sicurezza logica di Gruppo. Tale situazione espone a elevati rischi, non presidiati, d'integrità, riservatezza e disponibilità dei dati aziendali. Si osserva infine che tutte le modifiche condotte direttamente sui dati tramite Gestione Tabellare non sono state, fino ad oggi, oggetto di monitoraggio e rilevazione. Questo pertanto può aver indotto anche a valutazioni non corrette del rischio informatico sottostante le singole applicazioni interessate.	A	Operativo	Sistema	**Ricondurre l'accesso diretto ai dati nell'ambito delle Policy di Gruppo** Circoscrivere l'utilizzo dell'applicativo alle sole tabelle di dominio, escludendo pertanto tutte le tabelle operative contenenti dati di business e/o informazioni riconducibili ai clienti. Ricondurre la gestione dei profili abilitativi e della tracciatura delle operazioni svolte a quanto previsto dalle policy aziendali (panieri abilitativi/Log Unico). Nelle more, adottare i necessari presidi a mitigazione dei rischi individuati.	COG Servizio Credito	Processo rafforzato Studio fattibilità entro 31/01/2019
6	Vendita / contrattualizzazione Prodotti e Servizi / Gestione documenti in formato digitale della clientela	**Disallineamento tra Log Unico e contenuto degli archivi documentali** Con riferimento alle operazioni di sportello, non è assicurata la coerenza tra la modalità di sottoscrizione (grafometrica/cartacea) registrata nel Log Unico ed il contenuto degli archivi documentali. Le verifiche condotte su un campione di operazioni di sportello hanno infatti evidenziato la presenza di operazioni che dal Log Unico risultano sottoscritte grafometricamente, per le quali non risulta tuttavia archiviata alcuna distinta elettronica. In particolare, con riferimento alle operazioni di sportello disposte il 18/06/2018, che da Log Unico risultano sottoscritte grafometricamente, si osserva che su un totale di 878 disposizioni di cambio a/b non sono presenti negli archivi 143 distinte elettroniche. Casi della specie, benché numericamente meno rilevanti, sono stati riscontrati anche su operazioni di versamento in cc e bonifico.	M	Operativo	Sistemi	**Assicurare la coerenza tra Log Unico e contenuto degli archivi documentali** Con riferimento alle operazioni di sportello, assicurare la coerenza della modalità di sottoscrizione registrata nel Log Unico ed il contenuto degli archivi documentali.	COG Servizio Assisted Banking	31/01/2019

Tabella dei gap (6 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
7	Gestione dei processi operativi di sicurezza logica	**Sistema di Conservazione Sostitutiva – Accountability non garantita** Non risultano garantite l'accountability e la ricostruibilità delle operazioni effettuate tramite Portale Documenti*. Il sistema di loggatura, benché in grado di rilevare l'utenza che ha effettuato l'accesso, non tiene traccia dei documenti acceduti né delle operazioni effettuate (visualizzazione e/o download). (*) *Portale Documenti*: applicazione web di In.Te.S.A. s.p.a messa a disposizione di BMPS per la consultazione on line dei documenti in Conservazione Sostitutiva - https://mps.tdocgold.intesa.it/	M	Operativo	Processo	**Garantire l'accountability del Sistema di Conservazione Sostituiva** Assicurare che il sistema di tracciatura del Portale Documenti garantisca l'accountability e la ricostruibilità degli accessi ai documenti del Gruppo MPS.	Servizio Cash Management, Atm e Logistica	31/05/2019
8	Vendita / contrattualizzazione Prodotti e Servizi / Operatività con firma elettronica	**Assenza controlli su l'integrità dei documenti inoltrati in Conservazione Sostitutiva (CS)** La soluzione di Firma Elettronica Avanzata implementata dalla Banca non garantisce l'integrità, e pertanto la validità, dei documenti inoltrati in CS. Non sono infatti, presenti punti di controllo finalizzati a garantire che il documento informatico sottoscritto grafometricamente non abbia subito modifiche successivamente all'apposizione della firma da parte del cliente e prima della firma digitale della Banca.	M	Operativo	Sistemi	**Implementare controlli che garantiscano l'integrità dei documenti inoltrati in CS** Implementare gli opportuni controlli finalizzati ad assicurare che il documento non sia stato alterato successivamente all'apposizione della firma da parte del cliente e prima della firma digitale della Banca.	COG Servizio Assisted Banking	30/04/2019

Tabella dei gap (7 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
9	Gestione adempimenti prescrittivi in materia di tutela dei dati personali	**Assenza di una relazione tecnica aggiornata di cui al Provvedimento del Garante in tema di biometria** Il «*Provvedimento generale prescrittivo in tema di biometria*» n. 513 del 12/11/2014 in relazione alla sottoscrizione di documenti informatici, punto 4.4. lettera k), richiede la predisposizione e l'aggiornamento nel continuo di «*...una relazione che descriva gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità...*». Tale relazione non è necessaria qualora la Banca sia dotata della certificazione SGSI secondo la norma tecnica ISO/IEC 27001 «*...potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico*». Le verifiche condotte rilevano, tuttavia, l'assenza di una relazione tecnica aggiornata sul sistema attualmente in esercizio pur non essendo la Banca in possesso della certificazione SGSI secondo la norma ISO/IEC 27001.	B	Compliance	Processo	**Redigere la relazione tecnica di cui al Provvedimento del Garante in tema di biometria** Predisporre una relazione tecnica aggiornata inerente il sistema di Firma Elettronica Avanzata attualmente in esercizio.	Servizio Organization Partner COO e Digital Center con il contributo del Servizio Assisted Banking COG	31/01/2019

Tabella dei gap (8 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
10	Vendita / contrattualizzazione Prodotti e Servizi / Operatività con firma elettronica	**Annullamento operazioni di sportello: inoltro in Conservazione Sostitutiva di documenti non validi** La procedura informatica di annullamento delle operazioni di versamento in conto corrente prevede che vengano clonati tutti i documenti prodotti in corrispondenza dell'operazione originaria, compreso quello contenente i dati biometrici criptati (blocco grafometrico) e che sui cloni venga quindi apposta una marcatura di annullamento. Il documento clonato, contenente i dati biometrici, viene poi inoltrato in Conservazione Sostitutiva. Si osserva tuttavia che: ▪ il documento clone risulta alterato dalla marcatura e pertanto privo di qualsiasi valore legale; ▪ lo stesso blocco grafometrico viene associato a due documenti differenti, la distinta originale e il corrispondente clone, in contrasto ai requisiti regolamentari*. (*) DPCM del 22 febbraio 2013 «*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*», Art. 56, lettera h).	B	Operativo	Sistemi	**Modificare il processo di annullamento delle operazioni di sportello.** Nell'ambito della procedura di annullamento delle operazioni di sportello, escludere dalla clonazione il documento contente il blocco grafometrico**.**	COG Servizio Assisted Banking	31/01/2019
11	Vendita / contrattualizzazione Prodotti e Servizi / Gestione documenti in formato digitale della clientela	**Archiviazione dei documenti contenenti i dati biometrici dei clienti all'interno del sistema informativo della Banca** Il Processo di Firma Elettronica Avanzata prevede il transito dei documenti generati, ivi compresi quelli contenenti i dati biometrici, all'interno di specifiche cartelle di rete condivise, sottoposte a politiche di backup che ne garantiscono la conservazione da 60 giorni fino a 5 anni. La conservazione dei documenti contenenti i dati biometrici della clientela presso la Banca introduce un rischio di accesso non autorizzato, non giustificato da un reale beneficio. Si osserva a tal proposito come i documenti archiviati al di fuori della Conservazione a norma non siano opponibili in giudizio.	B	Operativo	Sistemi	**Rivedere il processo di backup delle cartelle di rete condivise** Eliminare dal processo di backup delle cartelle di rete condivise i documenti contenenti i dati biometrici.	COG Servizio Assisted Banking	31/12/2018

Tabella dei gap (9 di 9)

N.	Processo	Gap	Rilevanza (A/M/B)	Rischio	Fattore Causale	Raccomandazione	Struttura Owner	Scadenza (GG/MM/AA)
12	Gestione beni strumentali IT	**Inaffidabilità delle informazioni relative all'ubicazione delle tavolette grafometriche** Il dato sull'ubicazione delle 13.725 tavolette grafometriche in esercizio al 26/06/2018 contenuto nello strumento di enterprise asset management «Maximo», non è risultato attendibile. Dalle verifiche effettuate su un campione di n. 30 filiali, è infatti emersa la presenza di tavolette ancora in carico a filiali chiuse/oggetto di spin-off (76% del campione), o tavolette collegate da filiali in numero superiore a quello effettivamente assegnato (13% del campione). Ciò comporta il rischio di non avere sotto controllo il parco completo delle tavolette gestite, di non poter monitorare l'effettivo utilizzo e di non conoscerne con esattezza l'ubicazione.	B	Operativo	Processo	**Mantenere aggiornate le informazione relative all'ubicazione delle tavolette.** Aggiornare i dati relativi all'ubicazione delle tavolette grafometriche, prevedendo per il futuro un più puntuale meccanismo di segnalazione di eventuali spostamenti.	COG Servizio Sistemi Tecnologici	31/01/2019

Agenda

1. Contesto di riferimento
2. Attività svolta

Allegati

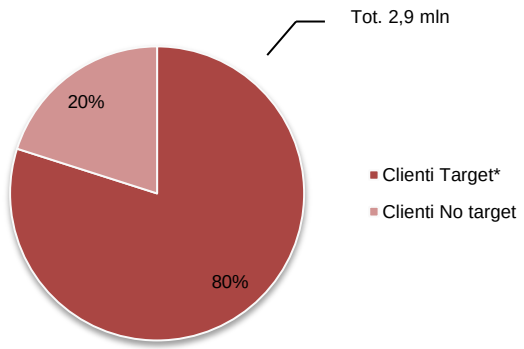
1 Contesto di riferimento – Perimetro FEA

Elenco delle operazioni/documenti sottoscrivibili con FEA

AMBITO DI OPERATIVITA'	TIPO OPERAZIONE
Anagrafe e Antiriciclaggio	Consenso Privacy in Variazione/Censimento Dati Cliente
	Autorizzazione utilizzo Recapiti (in Censimento e variazione dati cliente)
	Comunicazione variazione Indirizzi (in Variazione dati cliente)
	Questionario KYC
Poteri di firma - POFI (post vendita)	Poteri di firma (specimen) e deleghe
Contratti	Carte di debito, credito e prepagate, Conto Italiano ZIP base, Conto Corrente MPS One, Conto Corrente Ordinario Consumatore, Conto MPS MIO, Digital Banking, Conto MPS MIO Business, Conto Corrente Ordinario non Consumatore
Finanza	Questionario MIFID
	Fondi Anima
	Proposte di Consulenza Advice e proposte di gestione con preventivo assenso
Sportello	Emissione Singola/Multipla AC/FAD
	Cambio Assegni
	Ricarica Singola Carte Prepagate
	Incassi Commerciali
	Versamento
	Cambio Contanti
	Introiti Valori
	Bonifici Singoli

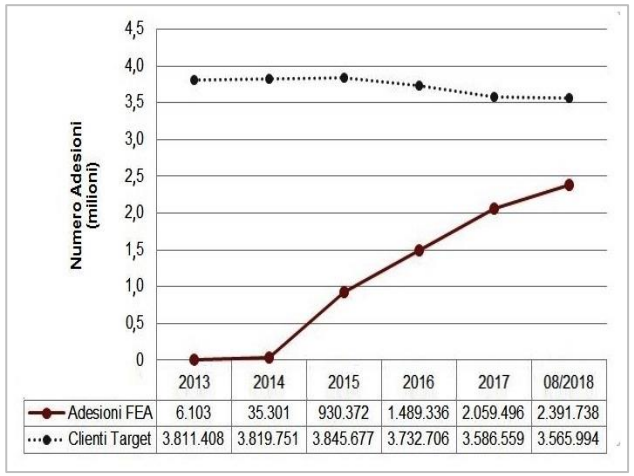
Fonte Allegato al documento 1030D01747 aggiornato al 24/09/2018

Adesioni FEA



Ottobre 2018 - Ripartizione adesioni FEA per tipologia clientela

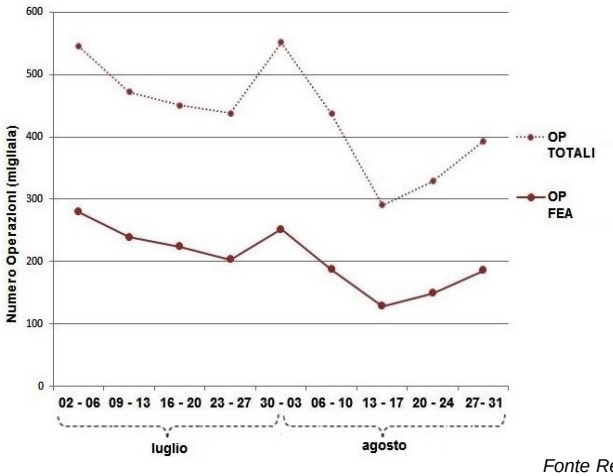
Andamentale Adesioni FEA Clienti Target *



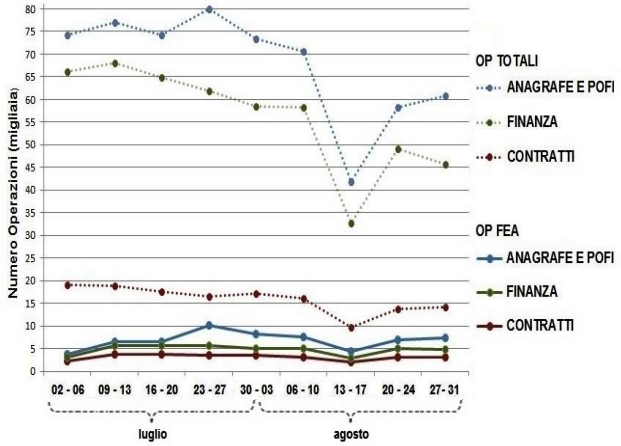
	2013	2014	2015	2016	2017	08/2018
Adesioni FEA	6.103	35.301	930.372	1.489.336	2.059.496	2.391.738
Clienti Target	3.811.408	3.819.751	3.845.677	3.732.706	3.586.559	3.565.994

Fonte Report Cognos

Andamentale Operatività FEA Operazioni di Sportello**



Andamentale Operatività FEA Altre Operazioni**



Fonte Report Cognos

(*) *Clienti Target: NGR relativo ad una Singola Persona Fisica (SPF), MDS Retail, presenza di poteri di firma pieni e disgiunti su rapporti CC/TI con esclusione dei rapporti tecnici (es. CC FANT)*

(**) *Operatività relativa a tutta la clientela BMPS*

2 Attività svolta: *Adesione FEA (1/5)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Verificare il grado di diffusione del Servizio di Firma Elettronica Avanzata, accertando che l'erogazione del Servizio avvenga nel rispetto di quanto previsto dalla normativa vigente in materia (rif. DPCM del 22/02/2013).

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi campionaria dei dati

RISCHI IMPATTATI

51846 - Rischio di non conformità del contenuto dei contratti alle prescrizioni della normativa di riferimento.

878120 - La rilevazione di documenti e/o allegati mancanti rispetto a quanto presente su Pardo, può portare a perdite economiche e reputazionali in caso di reclami/vertenze con la clientela per la mancata ottemperanza del disposto civilistico in materia di formalizzazione e custodia dei contratti / disposizioni della clientela.

108040 - rischio di errori, negligenze, ritardi in sede di Gestione contratto per servizio di Firma Elettronica Avanzata e Dematerializzazione Documenti.

55875 - perdita di documentazione e/o errata archiviazione della stessa.

VERIFICHE SVOLTE

Verifica che il template della Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA (e quello della Nota Informativa sul Servizio) in vigore sia stato validato dalla Funzione Legale/Compliance di BMPS.

Accertare che venga fornita adeguata informativa alla clientela in merito alle caratteristiche (ivi comprese quelle tecnologiche) della Soluzione FEA implementata.

ESITI

Ottenuto dal Settore Digital Center il parere legale dello Studio "TOSI & PARTNERS HIGH TECH LEGAL®" dell'11/05/2015 che la Banca ha richiesto in merito agli effetti giuridici della Firma Elettronica Avanzata (di seguito, per brevità, "FEA") - in relazione alle diverse soluzioni tecniche e operative adottate in Filiale e online. Relativamente alla conformità legale dei documenti informativi e contrattuali FEA elaborati da BMPS, il legale giudica tale materiale «adeguato allo scopo sia dal punto di vista contenutistico e di trasparenza bancaria sia per quanto riguarda le modalità di consegna e formalizzazione» raccomandando «in via prudenziale, di procedere all'attivazione del Servizio di FEA previa sottoscrizione di modulo cartaceo di attivazione con firma autografa». Non sono emerse variazioni di contenuto nella documentazione in vigore rispetto quella esaminata dal legale.

2 Attività svolta: *Adesione FEA (2/5)*

VERIFICHE SVOLTE	ESITI
Verifica della correttezza/completezza dei documenti di «Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA» su modulo cartaceo con firma autografa del cliente archiviati presso il Centro Documentale Esterno (CDE) (a campione).	La presenza di un rapporto «DE» nell'elenco rapporti di un cliente in Anagrafe Generale Banca lo identifica come titolare del Servizio di FEA. I clienti che hanno aderito al servizio nel periodo di rilevazione gennaio 2015 – aprile 2018, il cui contratto è stato validato e conferito al Centro Documentale Esterno (CDE) dalle Filiali/Centri Specialistici della Banca per l'archiviazione cartacea tramite «Procedura Archiviazione e Ricerca Documenti – PARDO», sono risultati 1.350.437. La verifica è stata condotta su un campione di n. 30 clienti per accertare la correttezza e completezza della documentazione archiviata presso il CDE. Test effettuati: ▪ che i riferimenti anagrafici del cliente riportati sul documento (nome, cognome e NDC) fossero esattamente quelli del cliente ricercato; ▪ che il contratto fosse completo (template composto da n. 5 pagine); ▪ la presenza delle 2 firme grafiche del cliente previste a pagina n. 4 del documento. Tutti i test sono stati superati.
Analisi dei sospesi PARDO relativi alla Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA.	E' responsabilità delle Filiali/Centri Specialistici assicurare, per gli ambiti di competenza, l'appropriata gestione della documentazione da rimettere al CDE, evitando il formarsi di sospesi oltre i tempi strettamente necessari all'esecuzione degli adempimenti, ed attivando tutte le iniziative necessarie alla rimozione di eventuali situazioni di criticità. I sospesi del Servizio di FEA nel periodo gennaio 2015 – aprile 2018 sono risultati 10.260, pari allo 0,75% dei documenti prodotti in Pardo, cioè n.1.360.697*. Sempre da un punto di vista quantitativo l'indagine, ristretta all'andamento del 1Q 2018, ha mostrato una percentuale di sospesi pari al 3,26% dei documenti da conferire (3.882 contro 118.942), inferiore rispetto a quella del rapporto tra tutti documenti PARDO sospesi a livello Banca e quelli prodotti: 5,53% (148.805 contro 2.692.310). In termini assoluti il fenomeno dei sospesi del Servizio FEA ha mostrato una incidenza molto bassa sul totale dei sospesi a livello Banca: 2% (3.882 contro 148.805). In termini tendenziali il fenomeno registra però numeri in crescita: a luglio 2018 erano presenti infatti 11.892 sospesi contro gli 10.260 di aprile (+ 1.632 documenti)**. L'analisi quantitativa è stata integrata con una qualitativa sui sospesi in essere, al netto di quelli il cui stato lavorazione PARDO «da validare» li pone ancora come da assoggettare al controllo del service esterno che precede l'effettiva archiviazione, riducendo il numero a 9.671 casi.

* Rilevazione del 30/05/2018.
** Rilevazione del 30/08/2018.
Fonte dati Servizio Audit Rete

2 Attività svolta: *Adesione FEA (3/5)*

VERIFICHE SVOLTE

ESITI

Gli esiti dell'analisi hanno prodotto le seguenti considerazioni:

- il delinearsi di un trend di crescita nell'accumulo dei sospesi, con 142 ante 2016, 2.819 originati nel 2016, 3.149 originati nel 2017 e 3.561 originati nel solo 1Q 2018;
- l'esposizione ad un rischio di natura legale/compliance, ad oggi però mai concretizzato, ma confermato dai pareri forniti dalle Funzioni Legale e Compliance della Banca, sottostante la mancata firma del cliente sulla Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA, potenzialmente riferibile a tutti i sospesi;
- l'evidenza di una negligenza operativa/ritardi in sede di gestione del contratto diffusa su tutta la Rete commerciale della Banca, con sospesi datati (60% originato ante 2018) e giustificativi per la sospensione in gran parte vaghi, assenti o che confermano la mancata firma del cliente.

Più in dettaglio, sul rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente senza preventiva adesione al servizio, la Funzione Legale, pur in mancanza di una posizione consolidata della dottrina giurisprudenziale indica: "*che una FEA non preceduta dalla sottoscrizione delle condizioni di adesione sia assimilabile ad una firma elettronica semplice, la stessa non sarebbe sufficiente a supportare efficacemente la sottoscrizione di un contratto bancario*" e ancora "*tale firma sarebbe in ogni caso liberamente valutabile sotto il profilo probatorio dal giudice, quindi, esporrebbe la banca a valutazione giudiziale, aleatoria per definizione, caso per caso*".

La Funzione Compliance ha invece indicato che "*se non è stato firmato il modulo di adesione, il trattamento del dato biometrico non è autorizzato*" e che "*il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica e ha validità, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere*". Le sanzioni amministrative relative al trattamento di dati biometrici non autorizzato (violazioni relative al consenso) vanno da 10.000€ a 120.000€.

Il rischio di natura legale/compliance va potenzialmente esteso anche a tutte le rimesse di documenti cancellate, stato lavorazione PARDO «annullato», cioè i casi in cui le Filiali/Centri Specialistici rinunciano a conferire la documentazione cartacea al Centro Documentale Esterno (16.839 casi nel periodo di rilevazione gennaio 2015 – aprile 2018)*, come conferma l'esito della verifica condotta su un campione di 30 unità.

Test effettuato:

- che all'annullamento del sospeso corrispondesse anche una equivalente chiusura del rapporto «DE» nell'elenco rapporti del cliente in Anagrafe Generale Banca e che nel contempo non vi fossero altri documenti PARDO collegati

Il test è fallito per tutti i casi campionati.

Occorre altresì evidenziare che gli annullamenti di sospesi PARDO a livello generale sono assoggettati ad una serie di controlli operativi che, a vari livelli, Titolare Filiale/Responsabile Centro Specialistico prima, settori del Servizio Controlli, Conformità e Operations della Capogruppo poi, ne indagano le motivazioni a supporto. Questi ultimi tuttavia sono attivi solo su 5 tipologie di documenti, tra i quali non rientra la Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA.

*Alla rilevazione del 30/08/18, riferimento luglio il fenomeno risultava in crescita: 17.593 (+ 754 casi). Fonte dati Servizio Audit Rete

2 Attività svolta: *Adesione FEA (4/5)*

VERIFICHE SVOLTE	ESITI
Verifica dello stato di avanzamento dell'azione di recupero delle Dichiarazione di Accettazione delle condizioni di utilizzo del Servizio di FEA sottoscritte ante 21/12/2015 e giacenti in Rete	Il conferimento delle Dichiarazioni di Accettazione delle condizioni di utilizzo del Servizio di FEA sottoscritte dai clienti tramite procedura PARDO per l'archiviazione cartacea è disposizione in vigore dal 21/12/2015. In precedenza il documento normativo di processo Banca 1030D1747 – "Definizione rapporto/contratto con il cliente: gestione contratto per servizio di Firma Elettronica Avanzata e Dematerializzazione Documenti" prevedeva la conservazione presso gli archivi delle Filiali/Centri Specialistici che avevano raccolto le adesioni. Per il recupero di quanto giacente in Rete (circa 1,3M di contratti sottoscritti dalla clientela dal 2013 al 20 dicembre 2015) la Funzione Organizzazione ha previsto nel 2017 un programma di lavoro destinato al personale di Filiale/Centro Specialistico, distinto in 4 sessioni della durata di 60/90 giorni con termine atteso entro il 1H 2018, per la generazione massiva di lavorazioni PARDO. Al momento della revisione di audit l'esecuzione di tale piano di lavoro si è conclusa producendo solo 12.102 lavorazioni PARDO validate. La mancata concretizzazione del piano è stata imputata a sopravvenute esigenze della Rete ritenute maggiormente prioritarie, con conseguente accantonamento di qualsiasi ulteriore iniziativa. L'esito lascia pressoché inalterata l'esposizione al rischio di natura legale/compliance precedentemente descritto, tenendo conto che circa 996K clienti con contratti non ancora accentrati hanno eseguito almeno una operazione con firma grafometrica a novembre 2018. Nell'intento di fornire una dimensione meramente indicativa del grado di rispetto assicurato dalla gestione documentale conservata in Rete (documento di adesione presente e completo di firme), in data 20/09/2018 il team di audit ha condotto una ricognizione su 2 agenzie della piazza di Siena: ▪ codice filiale 5802: 65% di documentazione verificata non firmata*; ▪ codice filiale 5806: 99% di documentazione verificata non firmata**.
Verifica nell'archivio della Filiale della presenza del modulo di revoca dal servizio firmato dal cliente (a campione).	La normativa di processo Banca 1030D1747 – "Definizione rapporto/contratto con il cliente: gestione contratto per servizio di Firma Elettronica Avanzata e Dematerializzazione Documenti" stabilisce che l'adesione da parte del cliente al Servizio di FEA possa essere da questi revocata. In tale caso il personale di Filiale/Centro Specialistico procede ad annullare il rapporto «DE» nell'elenco rapporti del cliente in Anagrafe Generale Banca ed a fargli sottoscrivere il documento di revoca (mod. 24381) che deve essere custodito nell'archivio della succursale per 20 anni. La ricognizione dell'Anagrafe Generale Banca al 26/06/2018 ha identificato 11.399 clienti cessati dal servizio sui quali è stata compiuta una verifica su base campionaria mirata su un campione di 30 unità (cfr. Allegato 3 «Criteri di Selezione» per il dettaglio delle scelte abbracciate dal team di audit). La verifica ha avuto il seguente esito: n.10 filiali hanno fornito il documento, le restanti n. 20 non sono riuscite a reperirlo. Sebbene di minor rilevanza intrinseca rispetto al contratto di adesione, l'elevato numero di documenti irreperibili costituisce un indicatore del rischio di smarrimento che la Banca corre nel mantenere la documentazione presso gli stabilimenti di Rete.

* Verificati 149 doc. su 1.414, 11% del campione.
** Verificati 437 doc. su 1.086, 40% del campione.

2 Attività svolta: *Adesione FEA (5/5)*

VERIFICHE SVOLTE	ESITI
Verifica che siano state rispettate le disposizioni normative in merito agli obblighi a carico dei soggetti che erogano soluzioni di Firma Elettronica Avanzata, con particolare riferimento alla dotazione di adeguata copertura assicurativa e alla sua pubblicazione sul sito Internet.	La prescrizione presente nel DPCM 22/02/2013 art 57 comma 2 recita: «Al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti di cui all'art. 55, comma 2, lettera a), si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila». La Banca ha ottemperato al suddetto comma con il rinnovo fino al 31/12/2018 della polizza n. 370531506 stipulata con Generali il 31/12/2017. L'esistenza di tale polizza è pubblicizzata sul sito Internet della Banca.
Verifica che la Banca si sia dotata di idoneo supporto legale per la procedura di escrow.	Il processo di recupero di un documento informatico originale archiviato in conservazione sostitutiva, corredato dei dati grafometrici cifrati relativi alla firma apposta dal cliente sul documento stesso, con annessa decrittazione dei dati grafometrici, si attiva solo a fronte di specifica richiesta dell'autorità giudiziaria. Il processo predetto (detto di "escrow") è risultato normato dal documento normativo D 1523 v.12 del 22/03/2018. Il pubblico ufficiale incaricato di conservare le chiavi che consentono di decrittare i dati grafometrici è stato individuato nel Notaio Martino Valmasoni del distretto notarile di Padova. La procedura di generazione delle chiavi si è tenuta il giorno 6/11/2014 come risulta da atto Repertorio n. 5663/Raccolta n. 3393. La funzionalità processuale è stata simulata con il test di escrow effettuato presso i locali del fornitore InfoCert (certificatore accreditato ai sensi dell'articolo 29 del Codice Amministrazione Digitale) in data 14/07/2015. Il processo non è mai stato attivato per un caso reale di contenzioso.

2 Attività svolta: *Firma Grafometrica (1/8)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Analizzare l'implementazione della soluzione di Firma Elettronica Avanzata (FEA), accertando il rispetto dei requisiti funzionali previsti, nell'ambito del processo ARIS *Vendita e Contrattualizzazione prodotti e servizi,* per l'Operatività con Firma Elettronica.

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati.

RISCHI IMPATTATI

878100 - L'archiviazione di contratti / disposizioni non correttamente formalizzate può portare a perdite economiche e reputazionali in caso di reclami / vertenze con la clientela per la mancata ottemperanza del disposto civilistico in materia di formalizzazione e custodia dei contratti / disposizioni della clientela

VERIFICHE SVOLTE

Verifica che la soluzione di Firma Elettronica Avanzata implementata rispetti i requisiti di processo previsti nell'ambito della sottoscrizione delle Operazioni di Sportello con specifico riferimento alla produzione delle relative distinte.

La verifica è stata condotta su un campione di operazioni di sportello del 18/06/2018 estratte dal Log Unico.

ESITI

In generale, l'esecuzione di un'operazione di sportello è subordinata alla sottoscrizione di una distinta da parte del cliente (es. distinta di versamento) che ne comprovi la richiesta. Nell'ambito dell'operatività con FEA, l'esecuzione è subordinata dunque alla produzione di una distinta elettronica ovvero di un documento digitale contenente gli estremi dell'operazione richiesta, il segno grafico e i dati biometrici del cliente acquisiti al momento della sottoscrizione sul tablet.

Le verifiche condotte hanno tuttavia evidenziato la presenza di operazioni di sportello che da Log Unico risultano sottoscritte grafometricamente a fronte delle quali, negli archivi informatici, non sono presenti le corrispondenti distinte elettroniche.

Nello specifico, sul totale di n. 45.696 operazioni di sportello esaminate per le quali la modalità di sottoscrizione registrata nel Log Unico risulta quella grafometrica è stato rilevato che:

- n.163 distinte elettroniche non sono mai entrate nel sistema di trattamento documentale e quindi, ad oggi, non sono presenti negli archivi informatici.

  Di queste:

  - n. 143 relative ad operazioni di cambio a/b (tot. 878);
  - n. 5 relative a bonifici bancari (tot. 3.780);
  - n. 15 relative a versamenti in cc (tot 21.845).

Inoltre, per un campione discrezionale di 3 operazioni grafometriche (una per tipologia) per le quali non risultano archiviate le corrispondenti distinte elettroniche, è stata verificata la presenza di eventuali distinte cartacee, archiviate tra i documenti di cassa delle filiali disponenti. A tal proposito è stato rilevato che:

- relativamente a n. 2 operazioni è stata riscontrata la presenza di cedolini cartacei precompilati;
- relativamente a n. 1 operazione non è stata riscontrata alcuna distinta cartacea.

(segue)

2 Attività svolta: *Firma Grafometrica (2/8)*

VERIFICHE SVOLTE	ESITI
	Stante quanto sopra, ad oggi, non risulta assicurata la coerenza tra la modalità di sottoscrizione (grafometrica/cartacea) delle operazioni di sportello registrata nel Log Unico ed il contenuto degli archivi documentali (gap 6).
Verifica volta ad accertare che la soluzione di Firma Elettronica Avanzata implementata rispetti i requisiti funzionali previsti per la modalità di firma grafometrica. La verifica è stata condotta su un campione discrezionale di operazioni in conto corrente sottoscritte in modalità grafometrica in data 18/06/2018.	Nell'ambito del processo *Vendita e Contrattualizzazione prodotti e servizi*, sono declinati i criteri in base ai quali un'operazione di sportello può essere sottoscritta grafometricamente in relazione, ad esempio, ai poteri di firma definiti sul rapporto oggetto della disposizione (rif. D01747 - *Vendita/contrattualizzazione Prodotti e Servizi - Gestione del servizio di "Firma Elettronica Avanzata e Dematerializzazione Documenti" e operatività digitale in filiale– par. 5.1.1).* Allo scopo di accertare che la soluzione FEA implementata rispetti tali criteri, è stata condotta una verifica su un campione di 18 operazioni in cc (2 per tipologia) sottoscritte grafometricamente. L'analisi comparata delle informazioni riportate sulle distinte grafometriche rinvenute all'interno dei dossier digitali dei clienti (es. nominativo del firmatario) e dei poteri di firma definiti sui rapporti oggetto delle operazioni ha confermato, su tutto il campione, la coerenza della modalità di firma con i criteri stabiliti.

(*) DPCM del 22 febbraio 2013 «*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*».

2 Attività svolta: *Firma Grafometrica (3/8)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Analizzare la soluzione di Firma Grafometrica erogata dalla Banca e verificare che soddisfi i requisiti di processo, tecnici e di sicurezza stabiliti per la Firma Elettronica Avanzata regolamentati nel 'DPCM del 22/02/2013 - Regole tecniche in materia di generazione, Apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali'.

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati.

RISCHI IMPATTATI

60067 - Rischi collegati alla mancanza di conformità con specifica normativa esterna (organismi di vigilanza, bankit, leggi dello stato, ...)

VERIFICHE SVOLTE

Verifica del sistema di identificazione del firmatario del documento nell'ambito della soluzione FEA implementata.

ESITI

La soluzione FEA realizzata dalla Banca lascia la responsabilità dell'identificazione del firmatario del documento in carico all'operatore di sportello, così come nel caso di operatività su cartaceo. Il processo implementato non prevede infatti una fase di *enrollment* per la raccolta dei campioni biometrici eventualmente utilizzabili ai fini dell'identificazione cliente.

Verifica volta ad accertare il rispetto dei requisiti per la Firma Elettronica Avanzata inerenti:

- *«l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati»;*
- *«la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma»*.

Allo scopo di rispettare i requisiti espressi nel DPCM del 22/02/2013, la soluzione FEA implementata dalla Banca prevede l'adozione del formato PDF/A* per i documenti elettronici a firma grafometrica.

Le analisi condotte sulla soluzione implementata hanno tuttavia evidenziato l'assenza di controlli (gap 3):

- in ingresso al sistema di acquisizione della firma, atti a garantire che i documenti prodotti dalle diverse applicazioni bancarie e sottoposti alla firma del cliente siano conformi al formato PDF/A;
- in uscita dal sistema di acquisizione della firma, atti a garantire la produzione e archiviazione di documenti sottoscritti, conformi al suddetto formato.

Si osserva a tal proposito che nel corso della revisione sono stati rilasciati in produzione modelli, per la sottoscrizione di operazioni su Fondi Anima, non conformi al formato PDF/A perché contenenti collegamenti a font esterni ai documenti. Tale circostanza ha determinato la produzione e archiviazione di documenti illeggibili.

Nello specifico, è stato rilevato quanto segue:

- in data 12/06 sono stati rilasciati in produzione n. 5 modelli non conformi che hanno determinato l'archiviazione di n. 165 documenti illeggibili su un totale di n. 429 sottoscritti;
- in data 28/06 sono stati rilasciati in produzione n. 2 modelli non conformi che hanno determinato l'archiviazione di n. 18 documenti illeggibili su un totale di n. 41 sottoscritti.

(*) Standard ISO 19005-1:2005, Document management -- Electronic document file format for long-term preservation, https://www.iso.org/standard/38920.html

2 Attività svolta: *Firma Grafometrica (4/8)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Verificare che la soluzione di Firma Grafometrica erogata dalla Banca rispetti le limitazioni e le prescrizioni espresse dal Garante con riferimento alla sottoscrizione di documenti informatici (rif. 'GPDP 513 del 12/11/2014 - Provvedimento generale prescrittivo in tema di biometria').	Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati e accesso diretto ai sistemi.	60067 - Rischi collegati alla mancanza di conformità con specifica normativa esterna (organismi di vigilanza, bankit, leggi dello stato, ...)

VERIFICHE SVOLTE	ESITI
Verifica che l'inibizione della sottoscrizione in modalità cartacea delle operazioni di sportello sia conforme ai requisiti espressi dal Garante (rif. GPDP n. 513, punto 4.4. lettera a)).	Con riferimento alla sottoscrizione di documenti informatici il GPDP n. 513, punto 4.4. lettera a), prescrive che siano *resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici*. Se tali strumenti non sono messi gratuitamente a disposizione del cliente è necessario che la Banca, in qualità di Titolare del trattamento, presenti istanza di verifica preliminare al Garante per la Protezione dei dati personali. A tal proposito si osserva che, in data 11/06/2018, è stato avviato il processo di inibizione della sottoscrizione di operazioni di sportello in modalità cartacea, per tutti qui clienti che abbiano aderito ad uno dei Servizi di Firma Elettronica, FEA e/o FDR*. Si rileva altresì che attualmente il servizio FDR non è commercializzabile *stand alone* ma unicamente in abbinamento al servizio - a pagamento - Digital Banking. In assenza di istanza di verifica preliminare è stato pertanto ritenuto opportuno richiedere un parere specialistico in merito al Servizio ICT Compliance di Capogruppo, responsabile dei controlli di conformità sul servizio di Firma Elettronica Avanzata.. La Funzione di Compliance ha confermato la conformità della soluzione ai requisiti espressi dal Garante, a tal proposito ha specificato che «*l'obbligo di porre a disposizione del cliente modalità di firma alternative alla FEA è da intendersi applicabile ove il cliente non abbia già sottoscritto il contratto di adesione alla FEA ovvero non si può obbligare un cliente che intenda acquisire un prodotto /servizio a sottoscriverlo solo con la FEA e quindi obbligarlo ad aderire anche a quest'ultimo servizio*». Ove un cliente abbia aderito al servizio FEA, nel caso non desideri utilizzarla per la sottoscrizione di un contratto, può esercitare la propria facoltà di scelta, recedendo dall'adesione alla FEA e apponendo la propria firma con altre modalità che non prevedano l'uso di dati biometrici (es. su carta). Ciò detto la Funzione di Compliance ritiene quindi lecito prevedere per i clienti che abbiano aderito alla FEA l'utilizzo di quest'ultima come unica modalità di sottoscrizione dei contratti e/o operazioni di sportello.

(*) FDR – Firma Digitale Remota

2 Attività svolta: *Firma Grafometrica (5/8)*

VERIFICHE SVOLTE	ESITI
Verifica del sistema dii Firma Elettronica Avanzata implementato volta ad accertare l'archiviazione dei documenti contenenti i dati biometrici dei clienti all'interno del sistema informativo della Banca.	La soluzione FEA adottata dalla Banca non prevede l'archiviazione a sé stante dei dati biometrici dei clienti (blocco biometrico) che vengono invece criptati e incapsulati nel documento oggetto della sottoscrizione. Le verifiche condotte sul sistema implementato hanno rilevato che i documenti contenenti i dati biometrici sono archiviati all'interno di specifiche cartelle di rete condivise nelle quali vengono salvati tutti i documenti prodotti/acceduti dalle diverse applicazioni coinvolte nel processo. Le cartelle in oggetto sono peraltro sottoposte alle seguenti politiche di backup: *\\nasfi1.local\vpt* - backup di tipo incrementale a nastro con retention di 60 gg; *\\nasfi3.sum.local\stampecentralizzate\stampe* - backup on line (a disposizione sulla share) con retention di 30 gg; - dopo 30 gg backup su nastro con retention 5 anni. Si evidenzia a tal proposito che se da una parte la conservazione dei documenti contenenti i dati biometrici della clientela all'interno del sistema informativo della Banca introduce un rischio di accesso non autorizzato, dall'altra non porta alcun beneficio dal momento che i documenti archiviati al di fuori della Conservazione a norma (i.e. Conservazione Sostitutiva) non sono opponibili in giudizio (gap 11). Nell'ambito delle stesse verifiche è altresì emersa un'anomalia sui documenti prodotti a fronte dell'annullamento di operazioni di versamento in cc sottoscritte grafometricamente. Nello specifico è emerso che la procedura di annullamento prevede la clonazione della distinta grafometrica sottoscritta al momento del versamento originale e l'apposizione sul nuovo documento di un marcatura (watermark) di annullamento. Il documento così prodotto viene quindi intercettato dal sistema di trattamento documentale che provvede all'apposizione della firma digitale della banca e al successivo invio in conservazione sostitutiva. A tal proposito si osserva che la distinta clone (gap 10): - non è un documento realmente sottoscritto dal cliente; - è priva di qualsiasi valore legale perché alterata dalla marcatura di annullamento; - contiene lo stesso blocco biometrico di un altro documento (la distinta di versamento originale), in contrasto ai requisiti regolamentari. Si osserva inoltre che l'archiviazione di documenti della specie, prodotti e alterati dalla stessa procedura informatica, evidenzia l'assenza di un controllo volto ad assicurare l'integrità del documento elettronico prima dell'apposizione della firma digitale della Banca (gap 8).

2 Attività svolta: *Firma Grafometrica (6/8)*

VERIFICHE SVOLTE	ESITI
Verifica della presenza della relazione tecnica aggiornata delle misure messe in atto dalla Banca allo scopo di ottemperare alle prescrizioni inerenti la sottoscrizione dei documenti informatici di cui al GPDP n. 513, punto 4.4.	Il GPDP n. 513, punto 4.4. lettera k), richiede la predisposizione e l'aggiornamento nel continuo di «...*una relazione che descriva gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità*...». Tale relazione non è necessaria qualora la Banca sia dotata della certificazione SGSI secondo la norma tecnica ISO/IEC 27001 «...*potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico*». Le verifiche condotte rilevano, tuttavia, l'assenza di una relazione tecnica aggiornata sul sistema attualmente in esercizio pur non essendo la Banca in possesso della certificazione SGSI secondo la norma ISO/IEC 27001 (gap 9).

2 Attività svolta: *Firma Grafometrica (7/8)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Accertare l'effettivo impiego del Servizio FEA nell'operatività corrente e il relativo monitoraggio	Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati.	55591 - Non corretta gestione del magazzino (carichi, scarichi, assegnazioni).

VERIFICHE SVOLTE

Verificare la numerosità delle tavolette grafometriche in esercizio in relazione al ciclo di vita documentato.

ESITI

La statistica delle tavolette grafometriche in esercizio è curata dalla Funzione di Fleet Management del Consorzio e rientra nell'ambito più ampio della gestione delle apparecchiature in dotazione al Gruppo.
La rilevazione del 26/06/2018 ha registrato 7.906 tavolette collegate alla Rete Informatica della Banca. Il numero è stato posto a confronto:

- con quello delle tavolette che risultano in esercizio secondo le informazioni ricavate dallo strumento di Enterprise Asset Management (Maximo di IBM) utilizzato dalla Funzione (13.725 tavolette in stato "operating"), con il quale si riscontra un gap di 5.819 dispositivi (42% del totale), non giustificabile con possibili eccezioni legate alla singolarità del giorno di rilevazione o la sua vicinanza a periodi di ferie;

- con quello delle risorse in servizio destinatarie dello strumento (12.159 unità, rilevazione al 16/07/2018 delle Funzioni Organizzazione e Risorse Umane), con il quale si palesa un gap di 4.523 dispositivi (37% del totale).

L'anomalia ha condotto ad approfondimenti sulla qualità dell'informazione fornita dallo strumento "Maximo" relativa alle tavolette grafometriche.

Test effettuati:
- verificata la presenza di filiali chiuse con ancora tavolette grafometriche assegnate (campione di 30 filiali cessate) e nel caso, se i dispositivi fossero risultati comunque collegati alla Rete Informatica della Banca (rintracciamento attraverso numero seriale);
- verificato che il numero di tavolette grafometriche collegate da una filiale non fosse superiore a quello di tavolette assegnate presso lo stesso stabilimento operativo (campione di 30 filiali con almeno 1 tavoletta collegata alla Rete Informatica della Banca alla rilevazione del 26/06/2017).

Nel primo caso per 23 filiali chiuse (76% del totale) sono risultate allocate le tavolette, per un totale di 73; di queste 13 sono risultate collegate alla Rete Informatica della Banca da altri stabilimenti (18% del totale).

Attività svolta: *Firma Grafometrica (8/8)*

VERIFICHE SVOLTE	ESITI
	Il risultato del secondo test invece è stato di 4 filiali in cui sono risultate più tavolette collegate di quelle assegnate (13% del totale), 5 filiali con un numero perfettamente corrispondente e 21 con un numero inferiore (dato quest'ultimo che può essere influenzato in maniera non quantificabile per esempio da assenze di personale/operatori che omettono di collegare il dispositivo). Le anomalie emerse configurano una inadeguatezza nell'attuale gestione del parco delle tavolette rappresentata da mancati aggiornamenti che attengono lo spostamento dei dispositivi a seguito di eventi che interessano la Rete Commerciale (spin off/incorporazioni per chiusura di sportelli,ecc.). L'inattendibilità della base informativa: ▪ condiziona negativamente qualsiasi iniziativa la Funzione Organizzazione voglia intraprendere per monitorare l'effettivo impiego delle tavolette da parte degli operatori di Filiale/Centro Specialistico; ▪ rende impossibile quantificare l'effettiva dispersione di un bene così facilmente trasportabile .

2 Attività svolta: *Archiviazione Documenti Digitali (1/4)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Accertare la corretta archiviazione e fruibilità dei documenti digitali. Verificare altresì l'adeguata conservazione secondo i limiti temporali previsti dalla legge.	Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati.	51445 - Mancata/ inadeguata archiviazione della documentazione

VERIFICHE SVOLTE

Verifica di consistenza tra le operazioni sottoscritte con Firma Grafometrica e i corrispondenti documenti archiviati nel sistema informativo aziendale e in Conservazione Sostitutiva.

La verifica è stata condotta su un campione di n.45.533 operazioni di sportello grafometriche disposte il 18/06/2018, tramite:

- accesso alagli archivi del Trattamento Documentale e analisi dei dati;
- richiesta estrazione dati al fornitore In.Te.S.A. S.p.A e successiva quadratura.

ESITI

Le verifiche condotte sulle tabelle operative del Trattamento Documentale, all'interno delle quali viene tracciato lo stato di avanzamento delle operazioni effettuate sui documenti elettronici sottoscritti con FEA, hanno confermato su tutto il campione analizzato il completamento delle operazioni di:

- invio e archiviazione in Conservazione Sostitutiva (CS);
- salvataggio nel Content Manager (CM).

Allo scopo di accertare l'avvenuta archiviazione presso il Conservatore dei documenti della Banca è stata altresì effettuata una quadratura tra le distinte che nelle tabelle del Trattamento Documentale risultavano correttamente inviate e archiviate (tutto il campione) e quelle effettivamente presenti nel Sistema di Conservazione, sulla base dei dati forniti di In.Te.S.A. S.p.A. La verifica svolta ha avuto esito positivo sul 100% del campione.

Verifica del ciclo di vita dei documenti elettronici.
L'attività è stata condotta, su un campione di 31 distinte grafometriche prodotte a fronte di operazioni di sportello del 18/06/2018, attraverso:

- accesso agli archivi documentali tramite
  - Portale Documenti* (CS);
  - Dossier Digitale PaschiFace (CM);
- raccolta e analisi delle evidenze.

Allo scopo di attestare il ciclo di vita dei documenti elettronici prodotti a fronte di una generica operazione bancaria sottoscritta grafometricamente, è stata accertata la presenza negli archivi informatici delle distinte (con e senza blocco biometrico) relative ad un campione di disposizioni di sportello.

Sul campione osservato, nel 100% dei casi:

- la distinta contenente il blocco biometrico è risultata correttamente archiviata in Conservazione Sostituiva;
- la distinta contenente il solo segno grafico è risultata correttamente archiviata nel Content Manager.

(*) Portale Documenti: applicazione web di In.Te.S.A. s.p.a messa a disposizione di BMPS per la consultazione on line dei documenti in Conservazione Sostitutiva - https://mps.tdocgold.intesa.it/

2 Attività svolta: *Archiviazione Documenti Digitali (2/4)*

VERIFICHE SVOLTE

Verifica delle attività di monitoraggio condotte sul Sistema di Trattamento Documentale, a presidio dell'effettiva archiviazione dei documenti elettronici prodotti nell'ambito della FEA.

ESITI

Il monitoraggio del Sistema di Trattamento Documentale, ovvero delle operazioni che vengono effettate sui documenti elettronici a valle della sottoscrizione cliente (es. firma digitale Banca, inoltro in CS), si fonda allo stato attuale sull'inoltro automatico, a tre risorse del Settore Portali Interni, di due email contenenti le seguenti informazioni:

- numero di operazioni di invio in CS e/o CM non andate a buon fine per più di 4 volte nell'arco della giornata (email infragiornaliera);
- numero delle operazioni non ancora terminate, con una profondità temporale di 10 giorni (email giornaliera).

Le evidenze raccolte nel corso della revisione hanno tuttavia evidenziato che, a fronte della ricezione delle email, non venivano svolte attività di verifica sistematiche e riproducibili, volte ad accertare e rimuovere le cause delle anomalie segnalate nonché ad assicurare l'effettiva archiviazione dei documenti.

La criticità, rappresentata in sede di exit meeting, è stata sanata prima della pubblicazione del presente rapporto. Nello specifico è stato implementato un sistema di monitoraggio giornaliero delle operazioni non terminate correttamente, nell'ambito del quale vengono registrate le attività di controllo puntuali effettuate.

2 Attività svolta: *Archiviazione Documenti Digitali (3/4)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Accertare la corretta archiviazione e fruibilità dei documenti digitali. Verificare altresì l'adeguata conservazione secondo i limiti temporali previsti dalla legge.

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati

RISCHI IMPATTATI

878100 - L'archiviazione di contratti / disposizioni non correttamente formalizzate può portare a perdite economiche e reputazionali in caso di reclami / vertenze con la clientela per la mancata ottemperanza del disposto civilistico in materia di formalizzazione e custodia dei contratti / disposizioni della clientela.

VERIFICHE SVOLTE

Verifica che i periodi di conservazione previsti dalla normativa di riferimento siano effettivamente in essere, sia per la conservazione cartacea che per quella sostitutiva.

ESITI

I termini per la conservazione cartacea sono fissati dalla normativa Banca 1030D1748 che a sua volta declina le disposizioni dall'art. 2220 del Codice Civile, che stabilisce in 10 anni il tempo di conservazione dei documenti relativi ai rapporti con la clientela. In particolare:

- per i documenti che esauriscono l' efficacia temporale al momento della stessa creazione (es.: ordini dispositivi), i 10 anni decorrono dalla creazione della stessa;
- per i documenti che mantengono inalterata la validità nel tempo e rimangono in essere finché non giungono a naturale conclusione –ovvero non vengono revocati da una delle parti (es.: contratti) –, i 10 anni decorrono dal momento della conclusione del rapporto in essere.

Al momento della redazione del report le lavorazioni cartacee PARDO relative a conferimenti verso il Centro Documentale Esterno prevedono 99 anni di mantenimento, indipendentemente dalla tipologia di documenti che viene inviata. Le prassi agite non richiedono alle Filiali/Centri Specialistici di predisporre pacchi differenziati e la promiscuità del contenuto di ciò che viene inviato, unita all'indeterminabilità a priori della data di conclusione di un contratto, impone di assegnare al pacco la maggior durata di conservazione possibile.

Il principio base per la conservazione sostitutiva è che valgono le stesse regole previste per la conservazione cartacea. Per ragioni prudenziali tuttavia in data 29/06/18 la Funzione Legale ha indicato alla Funzione Organizzazione di uniformare le durate dei periodi di conservazione, e quindi conservare per 10 anni dalla data di chiusura del rapporto anche la documentazione relativa alle singole disposizioni a valere sui vari rapporti (siano di cc, che di deposito titoli, ecc.).

2 Attività svolta: *Archiviazione Documenti Digitali (4/4)*

VERIFICHE SVOLTE	ESITI
	In termini contrattuali con il fornitore In.Te.S.A. S.p.A. ciò si traduce nell'esigenza di modificare la condizione dell'accordo di servizio attualmente in vigore che, con i suoi 10 anni di periodo massimo di conservazione, indipendentemente dalla vita del documento, risultava già insufficiente. Tra le modifiche da introdurre è emersa anche quella di prevedere un congruo periodo di preavviso che consenta alla Banca di prolungare la conservazione di documenti giunti a scadenza, qualora lo ritenesse necessario. La Funzione Organizzazione ha pertanto previsto un termine di 6 mesi come periodo di preavviso prima della distruzione documentale e individuato in 20 anni il nuovo periodo massimo di conservazione sostitutiva per tutte le classi documentali che contengono documenti di natura contrattuale. Quest'ultima misura è frutto di una valutazione costi/benefici che tiene conto: ▪ della durata minima della marca temporale apposta sul documento dal certificatore accreditato ai sensi dell'articolo 29 del Codice Amministrazione Digitale (per BMPS il fornitore InfoCert); ▪ l'opportunità di non impegnarsi per 99 anni da subito (come avviene per la conservazione cartacea) ed attendere i probabili sviluppi della normativa in materia di documenti digitali di recente genesi; Tali modifiche, in fase di revisione, sono state riportate nell'addendum contrattuale con In.Te.S.A. S.p.A. firmato in data 01/10/2018.

2 Attività svolta: *Sicurezza Logica (1/6)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Accertare che l'accesso alle informazioni sia correttamente presidiato - secondo quanto previsto dalla Normativa di Vigilanza* e dalla policy di Gruppo** in materia - allo scopo di garantirne la riservatezza, l'integrità e disponibilità.

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati ed accesso diretto ai sistemi.

RISCHI IMPATTATI

897840 - Lo scambio di dati sensibili su percorsi inaffidabili o ambienti incontrollati, generato da un processo di gestione della sicurezza dei sistemi inadeguato, può comportare una mancata integrità delle informazioni e delle infrastrutture, vulnerabilità di sicurezza e incidenti. Ciò può comportare perdite economiche e impatti reputazionali.

VERIFICHE SVOLTE

Verifica dei permessi di accesso alle cartelle di rete condivise, nelle quali vengono salvati tutti i documenti prodotti/acceduti dalle diverse applicazioni coinvolte nel processo FEA.

ESITI

L'analisi dei permessi di accesso alle cartelle di rete condivise – utenze e relativi permessi sono stati forniti, in data 21/06/2018, dal Settore Sistemi Dipartimentali del COG - ha rilevato la presenza di utenze nominative con abilitazioni eccedenti alle reali necessità operative.
In particolare è stata evidenziata la presenza di utenze con permessi in modifica come di seguito indicato:

- 15 utenze (su 19 definite) con accesso alla cartella *nasfi1.local**vpt*;
- 4 utenze (su 6 definite) con accesso alla cartella *nasfi3.sum.local**stampecentralizzate**stampe*.

Sono state altresì rilevate utenze con permessi in lettura associate a personale, sia interno che esterno, afferente a strutture consortili eterogenee.

La criticità, rappresentata in sede di exit meeting, è stata sanata prima della pubblicazione del presente rapporto. A far data dal 28/08/2018 sono state rimosse tutte le utenze nominative con permessi in scrittura e il permesso in lettura è stato riservato a 6 utenze associate a dipendenti del Servizio Assisted Banking.

(*) Circ.Bankit n 285 del 17/12/2013 e successivi aggiornamenti
(**) D02026 *Regole in materia di Gestione e Controllo Accessi: Accesso ad Applicazioni e Sistemi ICT*
D00389 *Sistema Informativo Unitario (S.I.U.) - Accesso e Abilitazioni* (recepito dal Consorzio nel documento D00150 *Processo Gestione Accessi Logici*)

Attività svolta: *Sicurezza Logica (2/6)*

VERIFICHE SVOLTE	ESITI
Verifica delle utenze per l'accesso agli archivi del Trattamento Documentale.	L'analisi delle evidenze – utenze e relativi profili abilitativi – fornite dalla Funzione Gestione Utenti del Settore BCM del Consorzio ha rilevato che negli archivi del Trattamento Documentale (database DB2 *DD0002BU* e *SC0001BM*): - in scrittura risultano definite esclusivamente utenze applicative, di cui • 6 riconducibili al servizio tecnico DD (utenze APPDD*); • 1 associata al servizio tecnico HR (utenza APPHRTAB), utilizzata dall'applicativo «Gestione Tabellare», in carico al Servizio Credito del Consorzio; - in lettura è definito un utente applicativo del servizio tecnico DD (APPDDQLS) e 18 utenze nominative appartenenti a strutture consortili eterogenee (oltre a 4 utenze richieste dal Settore ICT Audit per lo svolgimento della presente attività di revisione). Nel periodo 01/01/2018 - 31/05/2018 sono state concesse, tramite applicativo GADIS, 8 abilitazioni temporanee in scrittura nessuna delle quali, alla data della verifica, è risultata attiva. Gli esiti delle analisi condotte hanno confermato la conformità alle policy aziendali in materia delle prassi agite nell'assegnazione delle abilitazioni agli utenti personali. Nel corso delle verifiche è emerso tuttavia un limite strutturale dell'attuale soluzione tecnica utilizzata per la gestione dei privilegi di accesso, in lettura o scrittura, ai database host (vsam e/o DB2) che sarà oggetto di uno specifico approfondimento.
Verifica delle operazioni di accesso diretto ai dati: analisi del log. L'attività è stata condotta tramite analizzando i dati estratti tramite esecuzione della query di monitoraggio degli accessi diretti ai dati «*Audit DML DB2\ Log Interventi DB2 GADIS*» disponibile su *SID Navigator* (periodo di riferimento 01/01/2018 - 31/05/2018).	L'analisi del log degli accessi diretti al database *DD0002BU* ha evidenziato l'esecuzione di sole istruzioni di lettura. L'analisi del log degli accessi diretti al database *SC0001BM* ha evidenziato, nelle date 16/03/2018 e 05/04/2018, l'esecuzione di operazioni di scrittura. Approfondimenti successivi, svolti con il Settore Sistemi Centrali del COG, hanno permesso di ricondurre tali operazioni ad attività automatiche interne al database collegate alla compilazione di programmi software modificati secondo il regolare processo di Change Management (RFC n.151470 del 16/03, RFC C37884 del 05/04). A fronte della segnalazione del Team di Audit, il Settore Sistemi Centrali ha provveduto a modificare l'interrogazione «*Audit DML DB2\ Log Interventi DB2 GADIS*» al fine di restituire esclusivamente la tracciatura di operazioni riconducibili ad operatività manuale.

(*) Circ.Bankit n 285 del 17/12/2013 e successivi aggiornamenti
(**) D02026 *Regole in materia di Gestione e Controllo Accessi: Accesso ad Applicazioni e Sistemi ICT*
D00389 *Sistema Informativo Unitario (S.I.U.) - Accesso e Abilitazioni* (recepito dal Consorzio nel documento D00150 *Processo Gestione Accessi Logici*)

Attività svolta: *Sicurezza Logica (3/6)*

VERIFICHE SVOLTE	ESITI
Verifica dell'operatività svolta tramite applicativo «Gestione Tabellare».	L'applicativo Gestione Tabellare, in gestione al Settore Crediti Bancari, nasce per la gestione delle tabelle di dominio. Di fatto, non essendo possibile distinguere le tabelle di dominio da quelle operative, l'applicazione consente di operare direttamente su generiche tabelle DB2 secondo le abilitazioni assegnate (gap 5). Si osserva a tal proposito che le politiche di sicurezza logica di Gruppo prevedono: - l'estemporaneità delle operazioni di accesso in modifica ai dati, riservate a situazioni limitate e di particolare urgenza; - la durata massima delle abilitazioni in modifica, stabilita a 2 giorni; - la gestione delle abilitazioni attraverso la transazione GADIS; - la tracciatura degli accessi diretti ai dati, consultabile attraverso un'apposita query disponibile in SIDNavigator. Le analisi condotte hanno tuttavia rilevato casi di accesso diretto ai dati in modifica attraverso l'applicativo Gestione Tabellare e quindi, in deroga a tutte le tutte le politiche di sicurezza logica di Gruppo Con riferimento a quanto sopra, si osserva peraltro che l'applicativo in oggetto presenta una serie di criticità tra cui: - assenza di meccanismi automatici di attribuzione/revoca delle abilitazioni che tengano conto, ad esempio, dell'effettiva assegnazione delle risorse alle strutture aziendali; - profili abilitativi, gestiti direttamente sull'applicativo, ad oggi assegnati senza scadenza; - accesso in lettura ai dati non tracciato; - modifiche ai dati storicizzate in una tabella applicativa; - accessi ai dati (lettura/scrittura) non intercettati dalla query SIDNavigator preposta al monitoraggio. L'analisi delle informazioni contenute nelle tabelle operative della Gestione Tabellare in cui sono storicizzati gli interventi in modifica sui dati ha rilevato, per il periodo compreso dal 01/01/2018 al 25/07/2018, quanto segue: *DD0002BU* 968 interventi di aggiornamento diretto sulle tabelle, eseguiti da Settore Portali Interni (n.839, 87%) e Settore Anagrafe (n.129, 13%) *SC0001BM* 25 interventi di aggiornamento diretto sulle tabelle, eseguiti da Settore Portali Interni (n.25, 100%) L'applicazione risulta inoltre utilizzata in modo diffuso all'interno del Consorzio, avendo il relativo utente applicativo (APPHRTAB) diritti di scrittura su 76 distinti servizi. Tenuto conto dell'ampia diffusione nell'utilizzo dello strumento all'interno del Consorzio, nonché della rilevanza dell'informazione relativa agli accessi in modifica anche ai fini della corretta valutazione del rischio informatico, è stata da subito avviata una specifica attività finalizzata a ricondurre l'accesso diretto ai dati nell'ambito delle corrette Policy di Gruppo.

Attività svolta: *Sicurezza Logica (5/6)*

VERIFICHE SVOLTE	ESITI
Verifica dei permessi di accesso alle cartelle di rete condivise, nelle quali vengono salvati tutti i documenti prodotti/acceduti dalle diverse applicazioni coinvolte nel processo FEA.	L'analisi dei permessi di accesso alle cartelle di rete condivise – utenze e relativi permessi sono stati forniti, in data 21/06/2018, dal Settore Sistemi Dipartimentali del COG - ha rilevato la presenza di utenze nominative con abilitazioni eccedenti alle reali necessità operative. In particolare è stata evidenziata la presenza di utenze con permessi in modifica come di seguito indicato: - 15 utenze (su 19 definite) con accesso alla cartella *nasfi1.local**vpt*; - 4 utenze (su 6 definite) con accesso alla cartella *nasfi3.sum.local**stampecentralizzate**stampe*. Sono state altresì rilevate utenze con permessi in lettura associate a personale, sia interno che esterno, afferente a strutture consortili eterogenee. La criticità, rappresentata in sede di exit meeting, è stata sanata prima della pubblicazione del presente rapporto. A far data dal 28/08/2018 sono state rimosse tutte le utenze nominative con permessi in scrittura e il permesso in lettura è stato riservato a 6 utenze associate a dipendenti del Servizio Assisted Banking.
Verifica dei presidi di sicurezza logica dell'archivio documentale della Banca, *IBM Content Manager* con particolare riferimento a a) utenze b) modalità accesso c) tracciatura dell'operatività	a) Il governo e la gestione delle utenze applicative per l'accesso al CM nonché dei relativi profili abilitativi vengono condotti difformemente dalle policy aziendali in materia. Le prassi agite per il censimento di nuove utenze non consentono, allo stato attuale, di ricostruire l'associazione delle utenze ai corrispondenti asset di riferimento e le Strutture responsabili dell'utilizzo. Al 09/07/2017, sul CM * risultano definite 7 utenze applicative di cui 3 con permessi di scrittura. b) Con riferimento alle modalità di accesso agli strumenti nativi per l'amministrazione e la navigazione dei contenuti*, è stato osservato che: • le applicazioni non sono integrate con il sistema di autenticazione Single Sign-On (SSO) e non risultano implementati i processi di gestione centralizzati delle credenziali e dei profili abilitativi; • la consolle di amministrazione, utilizzata anche per il censimento delle utenze, è accessibile esclusivamente tramite un'utenza generica (*icmadmin*) condivisa tra più risorse afferenti a strutture consortili diverse; • l'applicazione web per l'accesso diretto ai contenuti del CM è acceduta da risorse della Banca e del Consorzio utilizzando le utenze applicative. c) Gli strumenti nativi a supporto del CM non sono risultati auditabili non essendo disponibili né log degli accessi né delle operazioni effettuate. Allo stato attuale non è possibile ricostruire a posteriori l'operatività degli utenti e pertanto l'accountability dell'Archivio Documentale della Banca non risulta garantita. (gap 4)

(*) *BM System Administration Client*, consolle di amministrazione del CM; *IBM Content Navigator*, applicazione web per l'accesso diretto ai contenuti del CM

Attività svolta: *Sicurezza Logica (6/6)*

VERIFICHE SVOLTE

Verifica dei presidi di sicurezza logica del Sistema di Conservazione Sostitutiva.

L'attività, condotta sulla base delle evidenze fornite da In.Te.S.A. S.p.A., ha interessato:

a) gestione delle utenze di accesso al Portale Documenti;
b) tracciatura dell'operatività utente.

ESITI

a) La gestione delle utenze di autenticazione al Portale Documenti non viene condotta nel rispetto delle policy di Sicurezza Logica emanate dalla Capogruppo**. Nello specifico, è stato osservato che sino ad ora, le richieste di censimento di nuove utenze sono state sempre gestite direttamente dal Servizio Organization Partner COO e Digital Center, diversamente da quanto riportato nel Regolamento n.1 della Banca, che assegna al Servizio Cash Management, ATM e Logistica la responsabilità della gestione del servizio di archiviazione e della consultazione dei documenti. Peraltro l'analisi delle utenze censite al 03/08/2018, il cui dettaglio è stato fornito In.Te.S.A. S.p.A. ha rilevato, sul totale di 34 utenze, la presenza di:

   - 13 utenze generiche (di cui 2 hanno effettuato accessi nell'ultimo semestre);
   - 1 utenza relativa ad un nominativo non più dipendente del Gruppo MPS

   La criticità, rappresentata in sede di exit meeting, è stata sanata prima della pubblicazione del presente rapporto.

b) L'analisi del log, dal 01/01/2018 al 31/07/2018, del Portale Documenti fornito da In.Te.S.A. S.p.A., ha rilevato che il sistema di tracciatura registra:

   - l'utenza che ha effettuato l'accesso;
   - la classe documentale acceduta.

   Il sistema non tiene traccia né dei documenti acceduti né delle operazioni effettuate (visualizzazione e/o download).

   Stante quanto sopra, l'*accountability* del Sistema di Conservazione Sostitutiva non risulta garantita (gap 7).

(*) Circ.Bankit n 285 del 17/12/2013 e successivi aggiornamenti
(**) D02026 *Regole in materia di Gestione e Controllo Accessi: Accesso ad Applicazioni e Sistemi ICT*
D00389 *Sistema Informativo Unitario (S.I.U.) - Accesso e Abilitazioni* (recepito dal Consorzio nel documento D00150 *Processo Gestione Accessi Logici*)

2 Attività svolta: *Monitoraggio e Reporting*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Verificare il rispetto della normativa in materia di gestione dei progetti.	Perimetro : progetto «Digital Enabler», il cui modulo «C – Paperless» si occupa dei rilasci per integrazione della FEA nei processi di Rete (es. Anagrafe e Antiriciclaggio, Finanza, Sportello, Carte, Conti Correnti). Metodologia : interviste con referenti strutture auditate. ed analisi delle evidenze documentali raccolte.	51559 - Mancata o non tempestiva azione di monitoraggio sull'effettivo raggiungimento degli obiettivi definiti.

VERIFICHE SVOLTE	ESITI
Verifica che il Responsabile Proponente del progetto «Digital Enabler» abbia esaminato il SAL predisposto dal Responsabile di Progetto.	La Funzione Proponente il progetto è individuata nella Direzione Organizzazione ed Operation. Lo Sponsor è indicato nelle figure del responsabile dell'Area Organizzazione e del responsabile del Servizio Organization Partner COO e Digital Center. Dall'analisi della corrispondenza raccolta il Responsabile di Progetto ha coerentemente informato quest'ultimo in occasione: ▪ del monitoraggio quindicinale delle criticità riscontrate sul progetto, che si inserisce in quello più complessivo che riguarda tutti i principali progetti della Direzione (Strategici/Rilevanti), propedeutico alla discussione in Comitato di Direzione; ▪ dell'informativa sullo «stato avanzamento lavori/rifacimento del business case di progetto», resa alla Funzione Governo Progetti.
Verifica che il Responsabile di Progetto abbia inviato il SAL alla Funzione Governo Progetti. Verifica che la Funzione Governo Progetti abbia controllato la completezza della documentazione ricevuta. Verifica se la Funzione di Pianificazione Strategica abbia confrontato i dati su KPI e sui costi di progetto con i dati previsionali.	Dall'analisi delle comunicazioni intercorse nel primo quadrimestre 2018 è emersa la rispondenza alle richieste formulate dalla Funzione Governo Progetti preparatorie alla seduta del Comitato Operativo Progetti del 16/04 u.s.: predisposizione ed invio di SAL al 11/04/18 e del business case. La Funzione Pianificazione ha approvato il business case in data 23/04. La revisione dello stesso si era resa necessaria a seguito della riconduzione all'interno del progetto «Digital Enabler» dei costi e benefici relativi agli interventi iniziati nel progetto «Digitalizzazione Processi» (avviato nel 2016), secondo logiche di continuità progettuale.
Verifica che il Progetto «Digital Enabler» sia stato presentato/valutato dal Comitato Operativo Progetti. Verifica dell'archiviazione della documentazione dei SAL del Progetto nel corso del tempo.	Dall'esame del verbale relativo all'incontro del 16/04 u.s. lo stato di avanzamento del progetto «Digital Enabler» è stato discusso come primo punto all'ordine del giorno e, come elemento qualificante il modulo «C – Paperless», sono emersi dei ritardi motivati nella produzione dei delivery attesi, (causa principale indicata concorrenza con altre progettualità), cui ha fatto seguito la ripianificazione dei rilasci in produzione dal 1Q al 1H del corrente anno. In 2 casi su 5 le scadenze sono già slittate al prossimo mese di agosto. Il materiale esaminato fa parte della documentazione conservata dalla Funzione Governo Progetti in apposito team site, dal quale sono stati estratti, per verifica dell'archiviazione, anche i verbali delle riunioni di giugno e dicembre 2017.

2 Attività svolta: *Attività negoziale e contratti (1/3)*

ADESIONE FEA | FIRMA GRAFOMETRICA | ARCHIVIAZIONE DOCUMENTI DIGITALI

OBIETTIVO

Verificare:

- il rispetto delle prassi normative previste nelle trattative di acquisto al fine di ottenere forniture di beni o servizi al miglior rapporto qualità prezzo;
- la validità dei rapporti commerciali in vigore e valutare il monitoraggio dei Livelli di Servizio sulle prestazioni ricevute.

PERIMETRO/ METODOLOGIA

Perimetro : le attività negoziali riferite all'impianto della soluzione di firma grafometrica (anno 2014) ed a quelle per consentirne il funzionamento nel corrente anno. .

Metodologia : interviste con referenti strutture auditate. ed analisi delle evidenze documentali raccolte.

RISCHI IMPATTATI

51339 - Acquisti a condizioni non ottimali o in situazioni di conflitto con l'interesse aziendale.

51674 – Mancata identificazione dei migliori fornitori.

207440 – Rischio di controversie per mancato rispetto di accordi contrattuali.

VERIFICHE SVOLTE

Verifica che la modalità di negoziazione seguita sia stata quella prevista per la tipologia di bene/servizio da acquisire.

Verifica delle motivazioni che hanno condotto alla scelta del fornitore (anche in considerazione di eventuale esclusività/infungibilità).

** In forza dell'Accordo Bassilichi 2013 sui servizi innovativi (collaterale al Deal Fruendo)*

ESITI

Le evidenze raccolte hanno dimostrato che le negoziazioni delle spese sostenute sono avvenute nel rispetto delle regole previste dalla normativa che regola il ciclo passivo.

➢ **Impianto della soluzione per la creazione dei documenti digitali prodotti dalla Rete in occasione dell'interazione con la clientela (contabili, distinte, contratti, documenti post vendita)**

La selezione dei fornitori è avvenuta con Richiesta di Offerta tecnico-economica a fornitori nazionali che a seguito di gara, con relativo passaggio in Comitato Costi per il parere definitivo sull'esito, ha visto preferire:

- la soluzione tecnologica di firma grafometrica per la creazione di documenti digitali (acquisto signature-pad, software e hardware maintenance, servizi di consegna ed attivazione in filiale, system integration e supporto alla certificazione) del pool di aziende INFOCERT/Step/Euronovate, coordinate da Bassilichi in qualità di main contractor (*) della commessa dal valore di 5,04 Mln€ (gara anno 2014, accordo Consorzio-Bassilichi del 9/12/2014, durata triennale);
- la fornitura per il servizio di conservazione sostitutiva di documenti digitali del fornitore IN.TE.S.A. SpA (Gruppo IBM), commessa del valore € 514.250,00 (gara anno 2013, accordo BMPS-IN.TE.S.A. S.p.A. del 11/10/2013, scadenza 30/06/2017).

➢ **Scadenze e rinnovi**

Disintermediatosi Bassilichi, il Consorzio ha concluso accordi direttamente con il fornitore Step (distributore di Euronovate) in forza di vincolo di esclusività della fornitura, per assicurare la manutenzione software ed il presidio specialistico della soluzione tecnologica di firma grafometrica in essere.

Entrambe le commesse sono state gestite con richieste di acquisto negoziate dalla Funzione Acquisti di Gruppo e successive spese autorizzate dal Centro di Spesa consortile competente (Area Applicazioni Canali) nel rispetto dei limiti concessi dalle autonomie negoziali (Responsabile di Area Consorzio fino a €100k, come previsto dal 10D109 «Deleghe di Autonomia in materia di Ciclo Passivo delle Strutture del Consorzio»).

La prima, di € 76.860, durata 1/01-31/12 2018, firmata il 27/04/2018; la seconda, di € 61.000, firmata il 25/06/2018 e inserita come addendum al «Contratto di Servizio per la Manutenzione – Lotto F/E Interni - Portali» di IBM, durata 1/01/2016 – 31/12/2018.

Attività svolta: *Attività negoziale e contratti (2/3)*

VERIFICHE SVOLTE	ESITI
	In data 3/07/2018 la Funzione Acquisti di BMPS ha esteso l'accordo con il fornitore In.Te.S.A. S.p.A. fino al 31/12/2018, dopo averlo già prorogato in precedenza per il periodo 1/07/2017 – 30/06/2018, sempre alle stesse condizioni del 2013. E' intenzione della predetta Funzione impiegare la rimanente parte dell'anno per una analisi di mercato finalizzata a verificare l'effettiva competitività dell'offerta in essere. L'analisi delle modalità con cui è stata gestita la fornitura dalla Funzione Acquisti di Gruppo ha fatto emergere: ▪ che negli anni 2016-18 la commessa è stata spesata attraverso ordini di acquisto a "tacito rinnovo", nonostante gli accordi che si sono succeduti negassero esplicitamente tale condizione. La prassi ha comportato che la fase autorizzativa fosse considerata assolta con l'approvazione dell'apposito stanziamento di budget per l'esercizio di riferimento. Con l'obiettivo che ciò non si ripresenti in futuro, il team di audit ha segnalato l'incoerenza sia al Centro di Spesa titolare del merito della spesa (Funzione Logistica di BMPS), che alla Funzione Acquisti di Gruppo che gestisce l'elenco dei contratti a tacito rinnovo; ▪ la possibilità di ricondurre la fornitura In.Te.S.A. S.p.A. nel quadro del GSA (Global Service Agreement) di IBM, considerando il particolare timing in cui si trovano i due accordi, cogliendo vantaggi derivanti da standardizzazione e sconti se raggiunti determinati volumi di fatturato; ▪ la possibilità di armonizzare i livelli di servizio contrattualizzati (di seguito SLA – *Service Level Agreement*) relativi all'assistenza prestata da In.Te.S.A. S.p.A. (definizione e misurazione) agli standard di *help desk* che IBM già fornisce al Gruppo per il tramite del Consorzio.
Verifica dell'avvenuto monitoraggio della qualità della merce/servizi ricevuti e l'andamento del rapporto con il fornitore da parte del CdS.	Gli accordi in essere tra Consorzio e Step per assicurare la manutenzione software ed il presidio specialistico alla soluzione tecnologica di firma grafometrica non prevedono penali, ed impegnano il fornitore a garantire assistenza secondo SLA che sono ricompresi e puntualmente delineati già all'interno del «Contratto di Servizio per la Manutenzione – Lotto F/E Interni - Portali» di IBM. La formula consegue l'obiettivo di standardizzare il monitoraggio di medesime prestazioni da parte del Consorzio. Sebbene gli accordi predetti siano stati formalizzati a fine aprile ed a fine giugno c.a., erano formalmente operativi dall'inizio dell'anno e questo ha permesso di considerare rilevante, ai fini dell'attività di audit, sia i il verbale dell'incontro tra referenti del Consorzio (Servizio Assisted Banking) e di IBM del 23/04/2018 relativo all'analisi sull'andamento dei livelli di servizio del 1Q 2018, sia quello del 13 luglio 2018 relativo al 2Q 2018. Entrambi i report non segnalavano criticità in termini di azioni correttive, né indicavano necessità di modifiche dei valori target. La frequenza degli incontri è funzionale a consentire un'analisi andamentale per trimestre.

Attività svolta: *Attività negoziale e contratti (3/3)*

VERIFICHE SVOLTE	ESITI
	Gli accordi che si sono succeduti per la fornitura per il servizio di conservazione sostitutiva di documenti digitali con il fornitore In.Te.S.A. prevedevano tutti penali a fronte del mancato rispetto dei livelli di servizio concordati. Gli SLA in questione sono risultati tesi a misurare la disponibilità del servizio (es. tempi impiegati per concludere il processo di conservazione, tempi di risposta del sistema di consultazione) e la reazione a segnalazioni di anomalie. Nel corso della revisione Il Servizio Cash Management e Logistica ha fornito un report riferito al periodo 2017/2018 relativo alla disponibilità del servizio di conservazione. Al contempo non sono stati riferiti fermi di produzione sul servizio ricevuto dalla Banca da parte dei referenti del Settore Digital Center della Capogruppo che governa il servizio di FEA.
Verifica dell'avvenuta iscrizione del fornitore/i nell'Albo di Gruppo.	Dall'esame dell'Albo Fornitori aggiornato al mese di giugno 2018: ▪ tutti i fornitori messi sotto contratto per il servizio di FEA sono risultati censiti, ad accezione di Euronovate; In corso di audit la Funzione Acquisti di Gruppo si è attivata per procurarsi il censimento di Euronovate (invito all'autocensimento sul portale di *e-procurement* di Gruppo inviato il 17/07 u.s.) e sollecitato In.Te.S.A. al completamento del profilo ai fini dell'acquisizione dello stato di «fornitore qualificato» (comunicazione del 25/06 u.s.), che di fatto, per quest'ultima, è avvenuto nel corso del mese di luglio (notizia del 25 luglio u.s.).
Verifica dell'avvenuto controllo e segnalazione di eventuale parte correlata o controllata.	Nessuna delle richieste di acquisto utilizzate per la gestione delle commesse relative alla FEA riportava segnalazioni particolari in merito alla presenza di fornitori identificabili come parte correlata o collegata (così come previsto dal documento di processo 1030D144 «Gestione della Spesa»). Anche il controllo di audit sugli elenchi in vigore nei diversi momenti delle negoziazioni (da novembre 2013 ad aprile 2018, versione in vigore al momento della redazione del report) ha confermato che nessuno dei fornitori contrattualizzati è o è stato parte correlata.
Verificare se è stato firmato ed archiviato il modello Mod 231 Vendor.	Con il modello in questione BMPS richiede ai fornitori o ai prestatori di servizi esterni di osservare una condotta in assoluta conformità e rispetto delle prescrizioni del D.lgs. 231/01 nonché in linea con i principi richiamati nel Modello Organizzativo della Banca, ovvero alle relative regole di condotta che vengono allegate alla firma dei contratti. Sono state pertanto richieste alla Funzione Acquisti di Gruppo ed acquisite le evidenze delle firme digitalmente apposte su tali moduli dai fornitori Step ed In.Te.S.A. in virtù delle forniture in corso.
Verifica dell'avvenuta effettuazione della Vendor Review/Questionario di Performance.	La Vendor Review è una iniziativa di monitoraggio periodica sull'andamento della fornitura che la Funzione Acquisti di Gruppo riserva a quei fornitori che per volume elevato di fatturato e/o strategicità della fornitura considera appunto strategici. Nessuno dei fornitori messi sotto contratto per il servizio di FEA rientra o è rientrato in questa classificazione.

Firme e destinatari del rapporto

Ruolo	Cognome e Nome	Firma
Responsabili Audit Team	Erbalisa Scarponi Giovanni Parigi	
Auditors	Andrea Bonci Silvia de Mauro Paolo Antonello Berlese	
V° Responsabile del Settore ICT Audit	Riccardo Salvini	
V° Responsabile del Settore Operational Audit	Elena Scarantino	
V° Responsabile del Servizio	Antonio Lombrano	
V° Responsabile dell'Area Revisione Specialistica	Andrea Furlani	
V° Responsabile della Direzione Chief Audit Executive	Pierfrancesco Cocco	

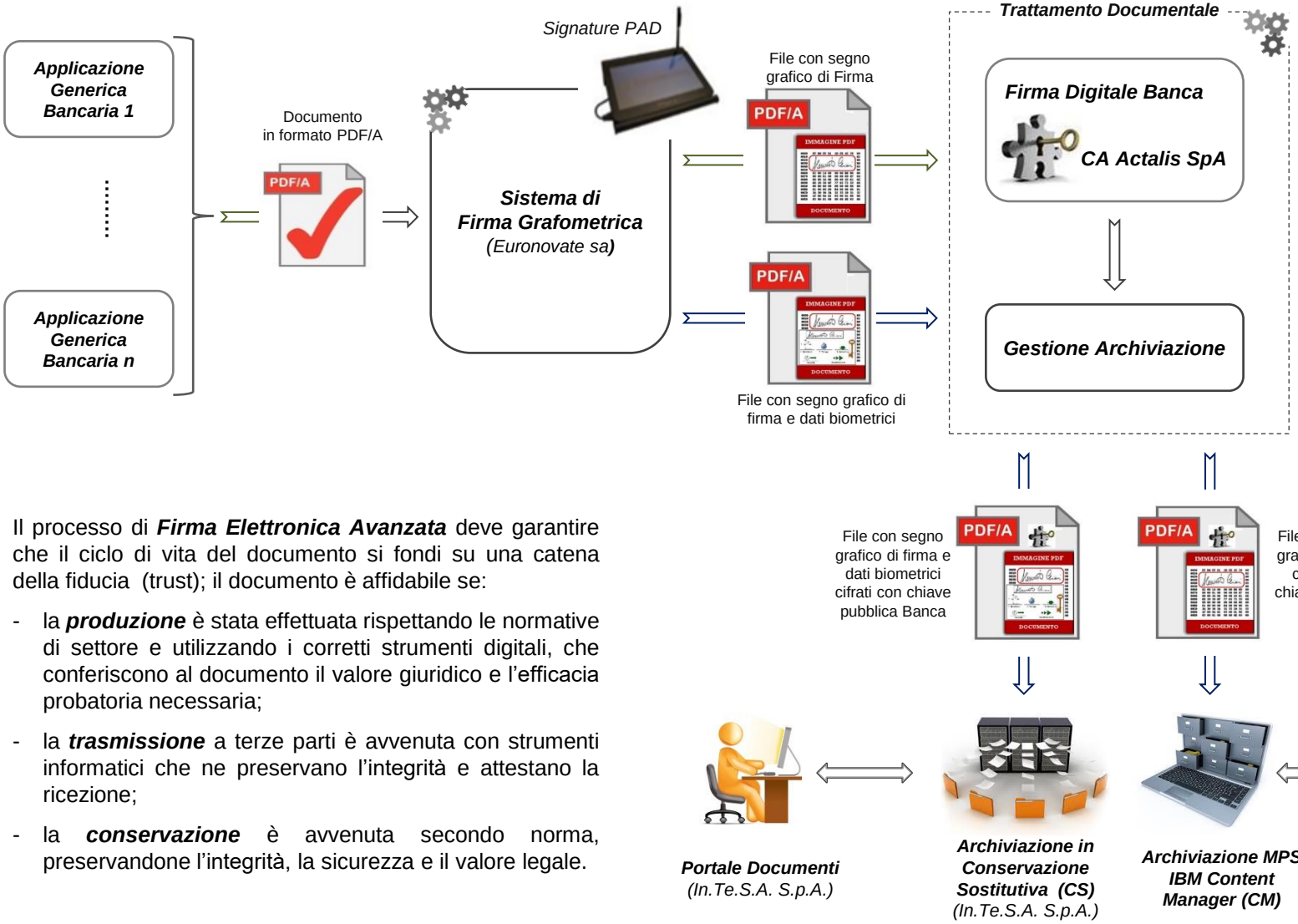
Organi destinatari di BMPS (invio tramite IAudit)	Selezione
Presidente del CdA	X
Amministratore Delegato	X
Collegio Sindacale	X
Comitato Rischi	X
OdV 231	

Altri organi destinatari	
Legal Entity	Organo destinatario
Consorzio Operativo Gruppo MPS	Presidente del CdA
Consorzio Operativo Gruppo MPS	Amministratore Delegato
Consorzio Operativo Gruppo MPS	Collegio Sindacale

Elenco allegati

» Allegato 1: Schema tecnico

Allegato 1: Schema soluzione di Firma Elettronica Avanzata



Il processo di ***Firma Elettronica Avanzata*** deve garantire che il ciclo di vita del documento si fondi su una catena della fiducia (trust); il documento è affidabile se:

- la ***produzione*** è stata effettuata rispettando le normative di settore e utilizzando i corretti strumenti digitali, che conferiscono al documento il valore giuridico e l'efficacia probatoria necessaria;
- la ***trasmissione*** a terze parti è avvenuta con strumenti informatici che ne preservano l'integrità e attestano la ricezione;
- la ***conservazione*** è avvenuta secondo norma, preservandone l'integrità, la sicurezza e il valore legale.