Policy di Sicurezza IT per i Servizi di Pagamento Via Mobile

Consiglio di Amministrazione di Flowe S.p.A. del 26/07/2023

1. PREMESSA

Lo scopo di questa policy è quello di fornire una descrizione dei principi e delle regole, ad alto livello, adottati da Flowe S.p.A. (di seguito anche la "Società"), circa la sicurezza informatica dei sistemi informativi abilitanti i servizi di pagamento.

1.1. Contesto di riferimento

La policy in conformità con la Direttiva (Ue) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (cosiddetta PSD2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

1.2. Ambito del documento

Sono esclusi dall'ambito di applicazione:

- i sistemi e i servizi che supportano l'operatività generale della Società, come, ad esempio, quelli per la gestione della compensazione delle transazioni.

Entro tale ambito, la policy si applica a tutti i soggetti (personale interno, personale esterno, outsourcer, ecc.) coinvolti nelle attività di progettazione, erogazione e utilizzo del sistema informativo della Società, ivi comprese le attività affidate in outsourcing, per quanto all'interno del perimetro definito.

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente:

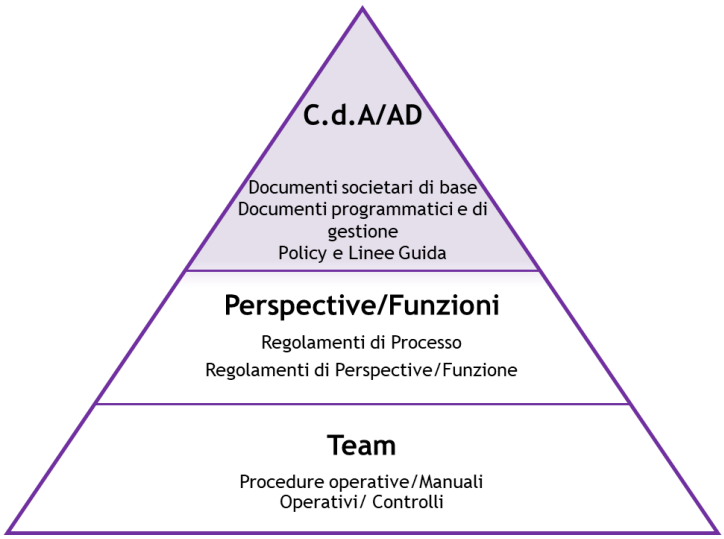

Figura 1. Modello della normativa aziendale

2. APPLICABILITÀ

2.1. Destinatari del documento

Il presente documento è approvato dal Consiglio di Amministrazione di Flowe S.p.A. e trova diretta applicazione all'interno della Società. I principi definiti si applicano a tutte le unità organizzative di Flowe S.p.A. incluse nel perimetro di intervento.

2.2. Responsabilità del documento

L'aggiornamento e la revisione del presente documento sono di responsabilità della funzione IT Operation Security and Governance, che opera all'interno della Perspective Augmented Intelligence.

3. DEFINIZIONI

2FA: autenticazione a due fattori; viene utilizzata per proteggere l'account dagli accessi non autorizzati chiedendo di inserire un codice aggiuntivo all'accesso.

Autenticazione forte del cliente: un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.

Certificati SSL con validazione estesa: Certificati di chiave pubblica per i protocolli SSL/TLS, per i quali le verifiche fatte dalla Certification Authority sull'identità del soggetto richiedente, e quindi anche sulla legittimità della richiesta, risponde a requisiti più stringenti di quelli previsti per i normali certificati SSL/TLS. Le verifiche soddisfano in particolare i requisiti posti dalle "Extended Validation SSL Certificate Guidelines" emesse dal CA/Browser Forum.

Firewall: dispositivo di rete (c.d. gateway) che filtra la comunicazione tra due o più reti, coerentemente con regole di sicurezza definite localmente.

Four-eyes principle: principio di sicurezza che richiede che un'azione sia approvata da almeno due individui distinti prima di essere eseguita.

Dispositivo con *root* o *jailbreak*: il rooting è l'operazione che permette all'utente di ottenere i privilegi di amministratore di sistema (diventare "*root*" appunto) e quindi di poter eseguire operazioni sullo smartphone, normalmente impossibili. Anche il jailbreaking, come il rooting esegue una "privilege escalation" per i dispositivi iOS.

Incidenti di sicurezza: relativamente alla definizione di Incidente di sicurezza informatica, Grave Incidente di Sicurezza si fa riferimento a quanto riportato nella Policy di Incident Management.

Near Real-Time: indica che l'operazione è effettuata in real-time, al netto dei tempi di elaborazione ed eventuale presentazione dei risultati dell'operazione stessa. Indica in sostanza che l'operazione viene svolta senza ritardi aggiuntivi, salvo quelli tecnici per l'elaborazione automatica.

Network Segmentation: la segmentazione della rete consiste nella suddivisione di una rete in più sottoreti, ognuna con policy di sicurezza informatica e protocolli specifici, nel tentativo di prevenire il movimento laterale di potenziali attacchi informatici. Rappresenta uno degli strumenti più utilizzati per ridurre la superficie di attacco di una rete e combattere gli attacchi informatici.

Sensitive Payment Data (Dati di pagamento sensibili): dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate. Per l'attività dei prestatori di servizi di disposizione di ordini di pagamento e dei prestatori di servizi di

informazione sui conti, il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti.

Servizi di pagamento: sono considerati servizi di pagamento tutti quelli definiti nell'ambito dell'allegato 1 della Direttiva PSD2.

ASPSP (Account Servicing Payment Service Provider): prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore, con le seguenti caratteristiche:

- è depositario dei conti degli utenti;
- espone l'interfaccia per la comunicazione con le terze parti.

PISP (Payment Initiation Service Provider): prestatore di servizi di disposizione di ordine di pagamento che esercita l'attività di disposizione di ordini di pagamento, che, previo consenso utente, esegue le seguenti funzioni:

- avvia una nuova disposizione di pagamento per conto dell'utente;
- richiede lo stato di una disposizione di pagamento precedentemente effettuata.

AISP (Account Information Service Provider): prestatore di servizi di informazione sui conti, che, previo consenso utente, svolge le seguenti funzionalità:

- richiede alla Banca saldo, movimenti e informazioni generali sul conto di un utente;
- aggrega le informazioni sopra ottenute e le rende fruibili all'utente.

PIISP (Payment Instrument Issuing Service Provider): prestatore di servizi di pagamento che emette strumenti di pagamento basati su carta di debito (anche detti Card Issuer Service Provider, CISP), che, previo consenso utente, può interrogare la Banca circa la presenza di sufficienti fondi sul conto di un utente.

PSU (Payment Service User): utilizzatore dei servizi di pagamento che possiede almeno un conto presso un ASPSP.

PSP (Payment Service Provider): un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore.

4. RUOLI E RESPONSABILITÀ

4.1. Consiglio di Amministrazione

Il Consiglio di Amministrazione assume la responsabilità generale di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali. Nell'ambito della presente policy, approva la relazione sui "Servizi di pagamento: risultanze dell'analisi dei rischi operativi e di sicurezza" richiesta da Banca d'Italia (Circolare n. 285 di Banca d'Italia del 17 dicembre 2013).

4.2. IT Operation Security and Governance

Il team IT Operation Security and Governance della Perspective Augmented Intelligence ha il compito di presidiare il governo della sicurezza informatica della Società e in particolare ha il compito di:

- definire il quadro di riferimento metodologico e di controllo di primo livello per il presidio e per il governo della sicurezza informatica, condividendolo con la Società;
- presidiare il recepimento delle evoluzioni normative in materia di sicurezza informatica, coordinandosi con la funzione Compliance Flowe;
- curare la redazione e l'aggiornamento delle politiche di sicurezza informatica, valutando periodicamente l'effettiva applicabilità delle normative di sicurezza e le necessità di aggiornamento, raccordandosi con quanto disciplinato dalla Capogruppo Banca Mediolanum;
- presidiare la coerenza delle misure di sicurezza informatica disciplinate nell'ambito della Policy di Sicurezza Informatica e garantirne l'applicazione nello sviluppo delle soluzioni IT;
- definire modelli, requisiti e linee guida in materia di sicurezza informatica per la realizzazione di nuovi servizi ICT (Security by Design e Privacy by Design) e per le esternalizzazioni, con il supporto del Settore IT Security di Banca Mediolanum;
- presidiare l'attività di valutazione d'impatto dei gravi incidenti cyber;
- presidiare l'implementazione ed il funzionamento dei presidi di sicurezza, nell'ambito della realizzazione di nuovi servizi ICT (Security by Design e Privacy by Design) e per le esternalizzazioni, valutandone i rischi di sicurezza informatica, anche al fine di identificare le misure di sicurezza da implementare e/o richiedere nell'ambito dell'affidamento di servizi a terze parti;
- effettuare il monitoraggio nel continuo delle minacce di sicurezza informatica applicabili alle risorse informatiche e servizi IT in uso e dei relativi programmi di mitigazione, al fine di progettare, sviluppare e mantenere la strategia della sicurezza informatica costantemente aggiornata avvalendosi anche di attività di scouting per le evoluzioni dei prodotti e dei servizi specifici.

Infine, può ingaggiare il team opportuno della Perspective Business Acceleration nei casi per i quali si rende necessario dare comunicazioni di sicurezza verso i clienti.

4.3. Account Monitoring & Fraud MNG

Il team Accounting Monitoring & Fraud MNG della Unità Controls & Regulatory Reporting si occupa dei controlli a presidio della sicurezza dell'operatività dei clienti, in merito alle credenziali di accesso, della gestione dei casi di disconoscimento di operazioni (anche per frodi informatiche) e delle attività di rafforzamento delle procedure di sicurezza. Effettua la revisione dei parametri di configurazione dei tool automatici a supporto delle attività di analisi sulle operazioni di disconoscimento dei clienti. Infine, può ingaggiare il team opportuno della Perspective Business Acceleration nei casi per i quali si rende necessario dare comunicazioni di sicurezza verso i clienti.

4.4. Business Acceleration

La Perspective attiva i meccanismi di comunicazione verso il cliente nei casi di campagne di phishing verso i clienti.

4.5. Organization and Business Continuity

La Perspective collabora con il team IT Operation Security and Governance per:

- definire gli scenari di crisi afferenti il piano di Business Continuity, cui consegue l'identificazione delle soluzioni di Disaster Recovery
- approvare l'attribuzione di profili infrastrutturali privilegiati attraverso un'approvazione di secondo livello ed effettuare verifiche periodiche circa il rispetto dei principi di *segregation of duties* nell'utilizzo degli stessi;

4.6. Funzione Risk Management di Banca Mediolanum

La funzione Risk Management, esternalizzata per Flowe in Banca Mediolanum, è responsabile del processo di valutazione e gestione del rischio ICT e di sicurezza. In particolare:

- definisce e manutiene il framework di controllo e gestione del rischio ICT e di sicurezza;
- svolge campagne periodiche di analisi del rischio ICT e di sicurezza, al fine di identificare, analizzare e valutare il rischio residuo ICT e di sicurezza connesso alle risorse informatiche utilizzate da Flowe S.p.A., identificando eventuali misure compensative/presidi ICT da integrare nei piani di trattamento del rischio ICT e di sicurezza;
- redige e aggiorna la Policy di Gestione del Rischio ICT e di sicurezza di Flowe S.p.A.
- redige, per conto di Flowe S.p.A., la Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento

- nell'ambito del processo di classificazione e segnalazione dei gravi incidenti Operativi o di Sicurezza, effettua nella fase di analisi di gravità dell'incidente, una prima valutazione circa l'impatto derivante dall'incidente rilevato secondo quanto disciplinato nell'ambito del *Regolamento del processo di classificazione e segnalazione dei gravi incidenti operativi o di sicurezza*;
- nell'ambito dei processi di esternalizzazione, ricopre il ruolo di Funzione di Esternalizzazione ed esprime la propria valutazione dei rischi in merito agli accordi in ambito e in linea con quanto disciplinato nella Policy in materia di Esternalizzazioni.

Inoltre, la funzione Risk Management si occupa di:

- contribuire alla definizione dei principi e delle regole ad alto livello relativi alla Sicurezza Informatica dei sistemi informativi abilitanti i servizi (operazioni) di pagamento via Internet e Mobile;
- coinvolgere il team IT Operation Security and Governance nell'ambito delle analisi relative al rischio ICT e di sicurezza previste dal framework di controllo e gestione del rischio ICT e di sicurezza;
- interagire con il team IT Operation Security and Governance nella valutazione delle perdite operative derivanti da incidenti gravi o rilevanti;
- ricevere i dati per il calcolo degli indicatori di rischio ICT, previsti dal framework di controllo e gestione del rischio ICT e di sicurezza.

FUNZIONE COMPLIANCE

La Funzione Compliance è responsabile del processo di verifica della conformità alle norme e presiede la gestione dei rischi di non conformità alle norme, secondo un approccio risk based. Oltre al presidio del quadro normativo di riferimento, alla Funzione competono attività di consulenza specialistica, alert normativo e gap analysis, verifiche di adeguatezza di assetti e processi aziendali rispetto al quadro normativo vigente e identificazione di azioni di mitigazione dei rischi di non conformità.

5. PRINCIPI IN TEMA DI CONTROLLO GENERALE E SICUREZZA DEI SERVIZI DI PAGAMENTO

Di seguito sono raccolti i principi e le regole ad alto livello relativi alla gestione della sicurezza dei pagamenti via *Mobile*. Si precisa che nell'ambito di tale policy non sono richiamati i principi e le regole in ambito alla complessiva gestione della sicurezza dei sistemi informativi.

5.1. Governo della Policy

La Società è responsabile della revisione della presente policy almeno a cadenza annuale oltre che a fronte di cambiamento rilevante alle sue infrastrutture, ai suoi processi o alle

procedure tali da pregiudicare la sicurezza dei servizi di pagamento oppure a fronte di gravi incidenti di sicurezza.

5.2. Approccio Risk-Based

In linea con quanto previsto dagli orientamenti EBA sulla gestione dei rischi informatici e con le direttive di Capogruppo, la Società adotta un approccio risk-based per l'erogazione dei servizi di pagamento.

A tal riguardo, la Società fa riferimento alle attività svolte dalla funzione Risk Management, esternalizzata in Banca Mediolanum. Le attività prevedono:

- il disegno, l'implementazione e l'aggiornamento periodico di un framework per la gestione dei rischi operativi nel cui ambito sono ricompresi anche quelli rivenienti dai servizi di pagamento in perimetro alla policy, comprensivo di un modello strutturato per la gestione del rischio ICT e di sicurezza[1];
- la valutazione, almeno annuale, del rischio IT associato ai servizi di pagamento via App[2]. La valutazione deve comunque essere riconsiderata:
    - in fase di introduzione di un nuovo servizio;
    - dopo incidenti di sicurezza informatica, classificati come "gravi" dalla Società[3];
    - in caso di iniziative in grado di impattare significativamente il livello di rischio ICT e di sicurezza dei sistemi informativi (e.g. sviluppo di nuovi progetti, accordi di esternalizzazione e modifiche rilevanti del sistema informativo);
    - se il monitoraggio degli indicatori di rischio evidenzia un rischio residuo superiore alla valutazione degli utenti

Inoltre, in accordo alla normativa vigente in ambito:

- deve essere definito e aggiornato periodicamente un inventario delle risorse informatiche, per poter gestire le risorse che supportano le funzioni e i processi aziendali critici[4];

---

[1] Per maggiori dettagli si rimanda agli orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza, requisito 1.3.3. Classificazione e valutazione dei rischi.

[2] Nella determinazione del rischio specificatamente per i servizi di pagamento via Mobile, devono essere considerati i rischi associati a:

- le soluzioni tecnologiche utilizzate;
- i servizi affidati in outsourcing a fornitori esterni. In tal senso, i PSP sono tenuti a definire SLA e a verificare l'adeguatezza e a mantenere i presidi di Sicurezza Informatica per i servizi esternalizzati;
- il contesto gli strumenti e le modalità di utilizzo del servizio tipiche della clientela, che ne costituiscono l'ambiente tecnologico;
- l'individuazione e la protezione dei dati sensibili di pagamento.

[3] Flowe adotta i criteri di classificazione in "grave incidente operativo o di sicurezza" definiti per le banche classificate 'significant', in linea con l'approccio della Capogruppo.

[4] Per maggiori dettagli si rimanda agli orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione e di sicurezza, requisito 1.5. Gestione delle operazioni ICT.

- deve essere svolto il monitoraggio continuo delle minacce e delle vulnerabilità, nonché la revisione periodica degli scenari di rischio che impattano le risorse IT.

La Società collabora con la Funzione di Risk Management nella produzione dei seguenti documenti, richiesti da Banca d'Italia e richiamati altresì dalla normativa bancaria italiana (Circ.285[5]) e comunitaria (Direttiva PSD2[6]):

- questionario "Servizi di pagamento: risultanze dell'analisi dei rischi operativi e di sicurezza", recepito nell'ambito della successiva "Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento" e inviato annualmente a Banca d'Italia;
- relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento"; che recepisce il questionario di cui al punto precedente e rappresenta il documento riepilogativo delle verifiche svolte da parte della suddetta Funzione sui presidi in essere sui servizi di pagamento via Internet e Mobile. La relazione viene portata a conoscenza dell'organo con funzione di supervisione strategica e successivamente inviata a Banca d'Italia.

Tali valutazioni di rischio guidano la definizione o l'aggiornamento di contromisure atte a proteggere i dati sensibili di pagamento e a mitigare il rischio di frodi, incidenti di sicurezza informatica e disservizi.

5.3. Approccio della defence-in-depth

La Società deve implementare misure di sicurezza a presidio della riservatezza, integrità e disponibilità dei dati e dei sistemi utili all'erogazione dei servizi di pagamento, adottando un approccio di tipo 'defence-in-depth' che prevede l'implementazione di misure di sicurezza fisica[7] (e.g., CCTV, accesso controllato ai locali critici), sicurezza logica (identity and access management, four-eyes principle, segregation of duties), sicurezza delle reti (network segmentation, firewall), sicurezza degli asset IT (antimalware, antivirus, strumenti di 'advanced threat protection') e sicurezza dei dati (strumenti di data loss prevention). In particolare, la Società deve:

- limitare la diffusione, l'elaborazione, la memorizzazione, l'archiviazione e la visualizzazione dei dati sensibili, in conformità con quanto disposto dal Regolamento EU 2016/678 (GDPR) con particolare riguardo ai dati sensibili di pagamento dei clienti e predisporre specifiche misure di sicurezza informatica volte a proteggere i dati sensibili di pagamento dei clienti nonché i sistemi informativi utilizzati per l'erogazione dei servizi di pagamento.

[5] Per maggiori dettagli si veda: Titolo IV – Governo societario, controlli interni e gestione dei rischi Capitolo 4 – Il sistema informativo; Sezione VII – Principi organizzativi relativi a specifiche attività o profili di rischio.
[6] Per maggiori dettagli si rimanda all'art. Articolo 95 Gestione dei rischi operativi e di sicurezza.
[7] Flowe eredita le misure di sicurezza fisica implementate da Banca Mediolanum

- segregare gli ambienti tecnologici;
- verificare gli aggiornamenti, l'autenticità e l'integrità del software e delle informazioni;
- applicare il principio del privilegio minimo (least privilege) e della segregation of duties;
- monitorare l'operato del personale che dispone per l'esercizio della propria operatività, di ruoli abilitativi privilegiati o amministrativi.

La Società deve predisporre registri degli accessi applicativi e all'infrastruttura cloud per i servizi di pagamento, da conservare in conformità agli obblighi di conservazione previsti dalla normativa applicata. La Società dovrà utilizzare tali registri per facilitare l'individuazione di attività anomale per la prestazione dei servizi di pagamento e per lo svolgimento delle eventuali indagini relative.

5.4. Business Continuity e Disaster Recovery Management

Il processo di Business Continuity & Disaster Recovery Management, ha lo scopo di presidiare l'adeguatezza delle strutture organizzative preposte a gestire situazioni di crisi e a contenere gli impatti derivanti da eventi eccezionali (es. indisponibilità dei centri di elaborazione dati, indisponibilità del sito, ecc.).

Tali soluzioni che rappresentano un presidio fondamentale di sicurezza informatica prevedono la predisposizione di linee guida specifiche che sono state definite nel Piano di Continuità Operativa del Conglomerato Finanziario Mediolanum e, per quanto riguarda la Società, nella Policy di Continuità Operativa di Banca Mediolanum di responsabilità dell'Unità Business Continuity Office & Digital Process Automation di Banca Mediolanum, cui si rimanda per maggiori dettagli.

5.5. Monitoraggio e report degli incidenti

La Società deve attuare processi e procedure per monitorare e rilevare nel minor tempo possibile le attività anomale considerando i fattori interni ed esterni, disponendo di specifiche funzionalità per rilevare attività fraudolente, implementando soluzioni per individuare le eventuali perdite di informazioni, accessi non autorizzati, la presenza di codice malevolo e le vulnerabilità hardware e software[8].

Devono essere definite soglie e indicatori per classificare un evento come incidente operativo o di sicurezza nonché indicatori di preallerta (early warnings) che consentano di identificare un incidente in tempi ridotti.

[8] Per maggiori dettagli si rimanda agli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza, requisito 1.3.3. Classificazione e valutazione dei rischi.

La gestione e il monitoraggio degli incidenti relativi ai sistemi di pagamento via Mobile rientrano nell'ambito del più ampio processo di gestione degli incidenti IT il cui perimetro identifica processi e strutture organizzative dedicati, a presidio del monitoraggio, della gestione e del follow-up degli incidenti operativi o di sicurezza informatica. In particolare, i gravi incidenti operativi e di sicurezza che interessano i servizi di pagamento via applicazione mobile rappresentano, in tale processo, un caso particolare di grave incidente IT.

Il modello organizzativo per la gestione degli incidenti operativi e di sicurezza, nonché le modalità di analisi, raccolta informativa e segnalazione dei gravi incidenti alle Autorità di Vigilanza di volta in volta preposte, deve essere adottato secondo quanto definito nel *Regolamento del processo di classificazione e segnalazione dei gravi incidenti operativi o di sicurezza*, redatto in conformità ai relativi requisiti normativi.

5.6. Controllo dei rischi e mitigazione

La Società deve definire e supervisionare l'implementazione di misure di sicurezza coerentemente con le politiche di sicurezza definite per il sistema informativo nel suo complesso. Nell'ambito di tali politiche sono da definire:

- le modalità di protezione dei servizi e dei dati sensibili di pagamento;
- le modalità di test dei servizi offerti, anche in relazione all'evoluzione delle minacce;
- la pianificazione e le modalità di verifica interna, anche in relazione all'entità dei rischi individuati;
- i criteri per l'outsourcing di servizi di pagamento via Mobile, o di componenti o funzioni specifiche;
- la modalità di gestione e l'analisi dei log delle transazioni e degli accessi ai dati sensibili di pagamento.

Devono essere adottate configurazioni che prevedono la cifratura end-to-end tra i dispositivi usati dai clienti e i sistemi della Società. Questa cifratura deve essere basata su:

- algoritmi riconosciuti dagli standard internazionali di settore, ampiamente diffusi e validati;
- lunghezze di chiavi definite sulla base degli standard internazionali di sicurezza del settore; la lunghezza delle chiavi è validata nel corso delle attività di valutazione del rischio, rispetto all'evoluzione dei rischi e delle minacce specifiche.

La Società durante la progettazione, lo sviluppo e la prestazione dei servizi, deve disporre che le attività di raccolta, instradamento, trattamento, memorizzazione e/o archiviazione nonché di visualizzazione dei dati sensibili per i servizi di pagamento degli utenti siano limitate a quanto strettamente necessario per la prestazione dei servizi stessi.

5.7. Verifica delle misure di sicurezza

Il team IT Operation Security & Governance effettua vulnerability assessment e test di sicurezza per la verifica delle misure di sicurezza in essere, implementate nell'applicazione mobile, guidando l'aggiornamento, ove necessario, delle soluzioni già esistenti alla luce dei risultati ottenuti.

Inoltre, con il supporto del Settore IT Security di Banca Mediolanum, vengono svolti periodici assessment per la valutazione delle misure di sicurezza. Tali verifiche di sicurezza sui sistemi di pagamento devono avvenire:

- considerando nell'ambito oggetto di verifica periodica dei servizi di pagamento (app mobile): i presidi attuati in materia di autenticazione forte dei Clienti, i canali adottati nell'interazione con le Terze Parti per l'erogazione dei servizi di pagamento;
- coinvolgendo terze parti indipendenti con specifiche competenze nella verifica delle misure di sicurezza per servizi di pagamento[9];
- prevedendo almeno annualmente, assessment di sicurezza specifici volti a verificare l'adeguatezza e la conformità ai requisiti di sicurezza informatica per i servizi di pagamento in ambito erogati dalla Banca, di cui alla Direttiva PSD2 e ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (in particolare in merito alle misure di sicurezza per l'applicazione dell'autenticazione forte del Cliente e alla riservatezza e integrità delle credenziali di sicurezza personali degli utenti dei servizi di pagamento).

Sono inoltre considerate, anche per il tramite della Capogruppo, informazioni di contesto ricavate da autorevoli report nazionali ed internazionali che evidenziano i trend di attacco per il settore finanziario, quali il "Rapporto Clusit annuale sulla sicurezza ICT in Italia" e le comunicazioni scambiate e condivise con il CERTFIN italiano e a livello associativo da ABI.

[9] Come previsto dall'art.3 dei Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). L'attuazione delle misure di sicurezza di cui all'articolo 1 è documentata, sottoposta a prove periodiche, valutata e controllata in conformità con il quadro giuridico applicabile del prestatore di servizi di pagamento da revisori con competenze in materia di sicurezza informatica e pagamenti e indipendenti dal punto di vista operativo nell'ambito o nei confronti del prestatore di servizi di pagamento.

5.8. Tracciabilità

La Società ed i fornitori di cui si avvale per l'erogazione dei servizi di pagamento devono tracciare le operazioni di pagamento via Mobile. In particolare, le registrazioni:

- devono comprendere le informazioni rilevanti delle transazioni, compresi i numeri di sequenza e gli orari esatti delle operazioni;
- devono essere gestite nell'ambito della più complessiva gestione dei log delle operazioni bancarie;
- devono essere protette dalla manomissione e devono essere rese accessibili solo al personale che ne ha necessità, nell'ambito del proprio incarico.

Il team Account Monitoring & Fraud MNG della Perspective Happiness and Services, effettua nel continuo l'analisi delle transazioni.

6. I PRINCIPI IN TEMA DI MISURE DI CONTROLLO E DI SICUREZZA SPECIFICI PER I PAGAMENTI VIA APPLICAZIONE MOBILE

6.1. Autenticazione forte del cliente

La Società deve proteggere l'accesso ai servizi di pagamento via Mobile adottando misure di autenticazione forte del cliente[10], sia per quanto attiene l'accesso a dati sensibili di pagamento, sia con riferimento ad operazioni dispositive. Queste ultime devono essere documentate e comunicate ai clienti.

Per l'autenticazione forte del cliente, la Società prevede l'uso di:

- un cellulare come fattore di possesso del cliente su cui sarà installata l'applicazione mobile (con *enrollment* del cellulare e generazione interna delle cifre del token software);
- un codice segreto come fattore di conoscenza o un dato biometrico (impronta digitale o riconoscimento del volto) come fattore di inerenza.

La Società deve altresì prevedere regole di configurazione relative alla lunghezza, alla complessità, alle modalità e alla frequenza di cambiamento dei codici segreti (in possesso esclusivo del cliente).

La Società deve valutare in fase di progettazione o di manutenzione evolutiva che abbia impatto sui servizi di pagamento, se le modifiche informatiche introdotte richiedano, a presidio della sicurezza del cliente, la necessità di una nuova autenticazione forte.

Le operazioni che devono essere protette da autenticazione forte del cliente sono:

[10] Flowe non prevede l'autenticazione forte del cliente per avere un accesso di fall-back in caso di problemi con la stessa.

- L’accesso al conto di pagamento via applicazione mobile;
- La disposizione di operazioni di pagamento elettronico da parte del cliente. Relativamente alle operazioni dispositive online (effettuate con la carta di pagamento), esse sono messe in sicurezza prevedendo un codice di autenticazione legato alla specifica coppia importo-beneficiario (dynamic link);
- Qualsiasi operazione effettuata tramite l’applicazione Mobile che possa comportare un rischio di frode nei pagamenti o altri abusi, tra cui anche le modifiche ad alcuni parametri da parte del cliente (e.g. limiti operativi massimi e minimi, whitelist, etc…).

Le operazioni per le quali la Società si avvale dell’esenzione all’applicazione dell’autenticazione forte del cliente, sono:

- le operazioni di pagamento al punto vendita senza contatto fisico, come previsto dalla normativa vigente (articolo 11 della normativa “Regulatory Technical Standards on strong customer authentication and secure communication under PSD2”);
- le operazioni di pagamento per modeste entità (articolo 16 della normativa “Regulatory Technical Standards on strong customer authentication and secure communication under PSD2”).

6.2. Enrollment e distribuzione di strumenti di autenticazione e/o software fornito al cliente

La registrazione di nuovi clienti deve avvenire attraverso l’utilizzo dell’applicazione Mobile messa a disposizione da parte della Società e, coerentemente con le valutazioni di rischio IT effettuate all’atto della realizzazione delle soluzioni informatiche, in linea con i principi di *Security By Design* ed alla normativa vigente.

La Società per l’accesso e la gestione dei canali fruiti dai propri clienti deve:

- attuare presidi di sicurezza mediante cifratura dei canali di interazione a garanzia anche della consegna sicura delle credenziali di autenticazione;
- definire profili di accesso che supportino i ruoli definiti e utilizzare meccanismi di autenticazione e controllo accessi coerenti con la criticità del servizio;
- realizzare e aggiornare i propri strumenti utilizzati per l’*enrollment* in linea con quanto previsto dalle best practices di settore in tema di sviluppo sicuro del software;

Nell’ambito del processo di gestione degli incidenti IT, e anche a supporto dell’analisi del rischio IT, vanno analizzati anche gli incidenti occorsi nelle attività di *enrollment* e distribuzione di strumenti di autenticazione forte, al fine di migliorare il processo e mitigarne i rischi.

Con riferimento alla distribuzione dell’applicazione per lo smartphone:

- deve avvenire tramite gli store ufficiali dei *vendor* in quanto considerati sicuri (in particolare App Store di Apple e Google Store per Android);
- non è consentito l’utilizzo di dispositivi caratterizzati da *root* o *jailbreak*;

- l’utilizzo dell’applicazione da parte del medesimo cliente è consentito per un massimo di due dispositivi.

6.3. Tentativi di accesso, sessioni scadute, validità dell’autenticazione

Il numero di tentativi falliti di log-in ai servizi di pagamento via Mobile deve essere limitato, coerentemente con le disposizioni normative e le valutazioni di rischio effettuate. In caso di superamento del numero massimo di tentativi di accesso[11], l'accesso deve essere bloccato (temporaneamente o permanentemente)[12] e il cliente deve essere informato della necessità di contattare gli operatori del team Customer Interaction per la riattivazione dei codici di accesso, o in alternativa lo sblocco dei codici deve essere disponibile anche in modalità *self-service* secondo procedure definite e comunicate sempre alla clientela.

Analogamente viene limitato il periodo di tempo per le sessioni inattive[13] prima della disconnessione delle stesse.

I valori dei diversi limiti (time-out per le sessioni scadute, numero massimo di login falliti, etc...) associati ai sistemi di pagamento via Mobile devono essere rivalutati a fronte dell’evoluzione dei fenomeni frodatori occorsi, al fine di valutarne l’adeguatezza.

6.4. Monitoraggio transazioni

Nel caso di un’operazione di pagamento non autorizzata (disconoscimento da parte del PSU), il prestatore di servizi di pagamento del pagatore, sia tenuto a rimborsare l’importo dell’operazione di pagamento non autorizzata a meno che il prestatore di servizi di pagamento del pagatore abbia ragionevoli motivi per sospettare una frode e comunichi tali motivi per iscritto all’Autorità di Vigilanza di riferimento (Banca d’Italia). Pertanto, in conformità a quanto richiamato, la Società:

- definisce il proprio modello di monitoraggio degli accessi, delle transazioni o dei tentativi di transazioni o di accessi effettuati tramite il canale Mobile, al fine di individuare e prevenire quelli potenzialmente fraudolenti;
- utilizza strumenti automatici a supporto delle attività di analisi, configurandoli in modo tale da consentire di individuare le attività fraudolente, comprese quelle eventualmente effettuate attraverso sistemi compromessi da malware;

[11] A seguito di 3 tentativi falliti di login, viene impostato un blocco temporaneo di 15 minuti. Il blocco risulta permanente qualora i tentativi falliti di login siano pari a 5.
[12] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) articolo 4 Authentication code.
[13] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) articolo 4 Authentication code: la durata massima delle sessioni inattive è pari a 5 minuti dopo i quali il sistema effettua il logout automatico.

- predispone specifici report sull'attività svolta e sui controlli effettuati, mantenendoli a disposizione delle Funzioni Aziendali di Controllo;
- raccoglie, classifica e invia i dati relativi alle operazioni di pagamento fraudolente individuate, riepilogati nella reportistica dedicata, secondo le tempistiche previste dall'Autorità di Vigilanza di riferimento in conformità a quanto disposto normativamente[14].

7. PRINCIPI IN TEMA DI GESTIONE COLLOQUIO TERZE PARTI

7.1. Requisiti generali

Le misure di sicurezza informatica presentate nel precedente capitolo si estendono altresì alla comunicazione con le Terze Parti (di seguito anche "TPP") ai sensi della normativa PSD2.

Per il dialogo con le TPP la Società adotta lo stesso modello tecnico utilizzato per erogare i servizi di pagamento verso i propri clienti, per le quali implementa le seguenti regole di sicurezza informatica:

- modalità di comunicazione sicura per:
  - lo scambio delle informazioni su uno o più conti e sulle operazioni di pagamento associate;
  - le disposizioni di un ordine di pagamento e la successiva ricezione delle informazioni su quanto disposto dal PSU;
- modalità di comunicazione che consente l'avvio dell'autenticazione sulla base del consenso del PSU;
- conformità agli standard di comunicazione richiamati dagli organismi di normazione internazionali o europei[15];
- integrità e riservatezza delle credenziali di sicurezza personalizzate e dei codici di autenticazione laddove trasmessi da o attraverso le TPP;
- autenticazione mediante le TPP con obbligo di *redirect* ai sistemi di autenticazione della Società;
- accesso che non richiede autorizzazioni o registrazioni aggiuntive rispetto a quanto già previsto attraverso il consenso fornito dal cliente ai TPP. In sede di registrazione del TPP (una tantum) viene richiesta una preregistrazione che è soggetta ad un

[14] Per maggiori dettagli si rimanda all'art. 96 comma 6 della PSD2 e agli Orientamenti in materia di obblighi di segnalazione per i dati sulle frodi, ai sensi dell'articolo 96, paragrafo 6, della PSD2.
[15] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) articolo 28.

processo di autorizzazione da parte della Società nei limiti di quanto disposto normativamente[16];

- interfaccia che offre lo stesso livello di disponibilità, di prestazione e di assistenza delle interfacce già a disposizione del PSU per l'accesso al proprio conto di pagamento online. Al fine di monitorare i livelli prestazionali dell'interfaccia dedicata vengono prodotti dei report trimestrali contenenti i dati delle API di Open Banking comparati con le API esposte per i servizi di online banking dalla Società.

7.2. Documentazione delle interfacce (perimetro e modalità di pubblicazione)

La Società predispone documentazione dedicata, riepilogativa delle specifiche tecniche delle interfacce di cui sopra, evidenziando aspetti relativi alle routine, ai protocolli e agli strumenti di cui le TPP necessitano, per consentire l'interoperabilità del loro software e delle loro applicazioni. La documentazione viene resa disponibile tramite il sito pubblico della Società.

7.3. Identificazione TPP

La Direttiva PSD2 richiede agli istituti di moneta elettronica di esporre interfacce per la comunicazione con TPP, permettendo a quest'ultime di accedere ai servizi di pagamento su richiesta del PSU, previa identificazione mediante certificati qualificati[17].

Nel dialogo con le TPP i PSP devono ricorrere all'uso di certificati qualificati, tra cui quelli resi disponibili da eIDAS[18].

[16] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), articolo 31 comma 5.

[17] Il RTS (cfr. par. 9, ID 8) definisce i requisiti di utilizzo dei certificati, i quali riportano, ad integrazioni delle informazioni tecniche (i.e. issuer certificato, possessore certificato, data inizio validità, data fine validità) i seguenti dati: Ruolo (o ruoli del PSP): ASPSP o TPP (AISP, PISP, CISP); Numero di autorizzazione del PSP; Nome dell'Autorità Competente nazionale di appartenenza.

[18] eIDAS rende disponibili le seguenti categorie di certificati, conformi alle normative vigenti:

- *Qualified website authentication certificate (QWAC)*: viene usato per proteggere la comunicazione da potenziali attacchi, stabilendo un canale TLS sicuro a presidio di confidenzialità, integrità e autenticità dei dati durante la trasmissione attraverso il canale. Tuttavia, i dati sono protetti solamente a livello di trasporto; a livello applicativo sono disponibili in chiaro a mittente e ricevente. Per tale motivo un QWAC non rappresenta una prova legale della transazione;
- *Qualified Certificate for electronic Seal (QSealC)*: viene usato per proteggere i dati da attacchi, durante e una volta terminata la comunicazione. La firma digitale dei dati trasmessi ne garantisce l'autenticità e l'integrità, ma non la confidenzialità. L'entità che riceve i dati può definire con certezza il mittente anche quando la trasmissione è terminata. Per questo motivo un certificato QSealC costituisce una prova legale della transazione.

7.4. Onboarding e gestione TPP

Le attività di onboarding delle TPP sono fondamentali per permettere la corretta operatività dei soli TPP autorizzati ad offrire servizi all'interno del mercato dei pagamenti.

Infatti, i TPP, prima di interagire con la Società, devono ottenere l'autorizzazione dall'Autorità Competente oltre che un certificato "qualified" rilasciato da un Qualified Trust Service Provider, contenente i ruoli per cui sono autorizzati a operare.

La Società definisce la propria modalità di onboarding dei TPP verificando:

- la presenza del TPP sul registro messo a disposizione da EBA;
- la validità dei certificati contenenti il ruolo;
- il rispetto delle specifiche dell'interfaccia in tutte le fasi della comunicazione.

Nella gestione dei TPP, la Società deve inoltre:

- supportarle qualora vi siano downtime (indisponibilità) degli ambienti di test o qualora sia necessario ripristinare le funzionalità o le utenze utilizzate dal TPP per l'accesso ai sistemi;
- in caso di dispute che coinvolgano il TPP, definire i processi e le procedure volte a individuare le responsabilità a livello organizzativo e le modalità di risoluzione delle controversie, verificando altresì il consenso prestato dal cliente nel caso di coinvolgimento di un TPP contattandolo in quanto coinvolto nell'operazione;
- monitorare i livelli di servizio offerti ai TPP al fine di garantire la stessa quality of service fornita al cliente nell'accesso diretto ai propri canali online. In caso di downtime dei sistemi avvisare i TPP impattati circa le misure di rientro attuate.

La Società può dialogare con le seguenti categoria di TPP:

- *AISP*: operativamente consentono ai clienti di accedere a diversi conti bancari online aperti presso diverse banche dalla medesima interfaccia. Se il conto di pagamento è infatti accessibile online, il pagatore ha il diritto di avvalersi di un prestatore di servizi di informazione sui conti, senza che sussista un rapporto contrattuale tra l'AISP e la Società.
- *PISP*: operativamente questi ultimi fungono da tramite tra il PSU e la Società e avviano la transazione per conto del PSU.

La Società per consentire il dialogo con le TPP deve:

- raccogliere il consenso esplicito del cliente; si precisa che nel caso dei PISP tale consenso deve essere richiesto per ogni singola operazione da disporre;
- consentire alle TPP di accedere alle informazioni afferenti conti di pagamento online dei PSU ed alle sole informazioni necessarie alla tipologia di servizio erogato;

- verificare che il consenso del PSU non sia "scaduto"[19];
- consentire ai TPP, di avere accesso ed esporre lo stesso livello di informazione erogato al PSU finale su canale online[20].

7.5. Approcci autenticazione forte

Nell'interazione con i TPP, la Società può adottare diversi approcci per consentire l'avvio e l'esecuzione della procedura di autenticazione forte del cliente al PSU.

Sul punto, le principali iniziative europee di standardizzazione del mercato delle API per la comunicazione tra IMEL e TPP, nell'ambito delle modalità di comunicazione sicura, avviene con SCA Decoupled con pre-step OAuth 2.0.

La Società adotta approcci in linea con la normativa e volti a non introdurre ostacoli alle TPP nell'interazione coi PSU.

8. I PRINCIPI IN TEMA DI CONSAPEVOLEZZA DEL CLIENTE, EDUCAZIONE E COMUNICAZIONE

Si premette che nella gestione del rapporto con gli utenti dei servizi di pagamento, la Società adotta i principi espressi nella sezione 1.8 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

8.1. Educazione del cliente e comunicazione

Nell'ambito delle attività di monitoraggio delle minacce e dell'evoluzione dei rischi IT, la Società tramite i team IT Operation Security and Governance a Account Monitoring & Fraud MNG, devono individuare eventuali informazioni utili ai clienti per contrastare possibili frodi nel contesto dei sistemi di pagamento via Mobile.

Tali comunicazioni devono essere previste periodicamente (derivandole anche dalle analisi svolte sulle fonti interne ed esterne alla base delle verifiche sulle misure di sicurezza indicate al paragrafo 5.7) e ad evento, ad esempio a seguito dell'analisi delle informazioni raccolte in occasione di accadimento di incidenti o da segnalazioni di reclami dei clienti. Tali informazioni sono utilizzate dai team IT Operation Security and Governance a Account Monitoring & Fraud MNG per proporre iniziative di educazione mirate alla clientela in merito ad esempio alle nuove modalità di attacco adottate dagli hacker, agli strumenti utilizzati dagli

[19] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), articolo 31 comma 5.
[20] Per maggiori dettagli si rimanda ai Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), articolo 31 comma 1.

stessi per perpetrare le frodi informatiche (es. dispositivi mobile, call center, mail..) e alle modalità esecutive, successivamente comunicate al team Business Acceleration, per definire il modello di comunicazione (template e contenuto) da utilizzare affinché possa rendere tali informazioni disponibili ai clienti (ad esempio tramite l'invio di e-mail, SMS, notifiche esposte nell'app mobile).

8.2. Programmi di formazione e di sensibilizzazione in tema di sicurezza

La Società definisce ed attua processi volti ad accrescere le conoscenze dei clienti dei servizi di pagamento sui rischi per la sicurezza connessi ai servizi stessi, fornendo agli stessi assistenza e orientamento, tramite pubblicazione delle informative sui canali digitali (e.g. blog pubblico sul sito della Società).

8.3. Notifiche e settaggio dei limiti

Nell'ambito dei sistemi di pagamento via Mobile, la Società consente ai clienti la possibilità di definire dei limiti di importo massimo per le diverse tipologie di operazione[21].

8.4. Accesso dei clienti alle informazioni sullo stato del pagamento, iniziazione ed esecuzione

I servizi offerti nell'ambito dei sistemi di pagamento via Mobile devono consentire al cliente di verificare lo stato del proprio conto corrente e delle operazioni in corso. Queste informazioni devono essere aggiornate in near-real time, e rese disponibili 24 ore su 24, 7 giorni su 7.

[21] In conformità a quanto disposto dalla PSD2 all'articolo 68 Limiti dell'utilizzo degli strumenti di pagamento e dell'accesso ai conti di pagamento da parte dei prestatori di servizi di pagamento.

9. CONTESTO NORMATIVO DI RIFERIMENTO

Nel presente capitolo si richiama il contesto normativo di riferimento per gli ambiti disciplinati. Riguardo alla Normativa Interna si fa riferimento alla versione del documento vigente all'atto della pubblicazione della presente policy. Si sottolinea che ai fini operativi sono da considerarsi in ambito anche i successivi aggiornamenti delle policy/procedure/regolamenti citati, cui si dovrà far riferimento.

9.1. Normativa esterna

- Circolare di Banca d'Italia n. 285/2013 "Disposizioni di vigilanza per le banche"
- Circolare di Banca d'Italia "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica;
- Direttiva (UE) 2015/2366 (PSD2);
- Circolare n. 272 del 30 luglio 2008 "Matrice dei conti";
- EBA/GL/2019/04 Final Report. "Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (ICT) e di sicurezza";
- Regolamento delegato (UE) 2018/389 della Commissione Europea (SCA Regulatory Technical Standards /RTS;
- Opinion della European Banking Authority (EBA) sugli ostacoli alla fornitura di servizi di fornitori terzi ai sensi della PSD2;
- Provvedimento del Garante per la protezione dei dati personali del 12/05/2011 - "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie";
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento Generale sulla protezione dei dati - GDPR).

9.2. Normativa interna

- Policy di Sicurezza Informatica;
- Policy di Incident Management;
- Procedura di Classificazione e Segnalazione degli Incidenti;
- Procedura operativa di Incident Management;
- Piano di Continuità Operativa Conglomerato Finanziario Mediolanum (vol.1 e vol. 2)
- Disaster Recovery Plan (versione 3.0);
- Regolamento di processo Log Management;
- Policy di Gestione del Rischio Informatico;
- Policy in materia di Esternalizzazioni;
- Regolamento del processo di Access Management.