

Come attivare il Mobile Token

Il **Mobile Token** è un sistema di sicurezza che consente di accedere e autorizzare le operazioni in modo semplice, veloce e sicuro, direttamente dal proprio smartphone.

Nel caso in cui fosse interessato ad attivare tale sistema di sicurezza **prima del 13/01/2026**. La invitiamo a contattare la Sua filiale di riferimento che Le darà tutte le indicazioni del caso.

In ogni caso dal 13/01/2026 il sistema di sicurezza **Mobile Token** sarà automaticamente attivato e a Sua disposizione e per renderlo operativo sarà sufficiente seguire i seguenti pochi passaggi:

1. **Scaricare (se non già fatto) l'APP della Banca** dallo store del Suo smartphone (es.: Google Play o App-Store).
2. **Accedere all'APP** con le proprie credenziali dell'Internet Banking e avviare la procedura guidata di attivazione (*enrollment*).
3. Seguire le indicazioni sullo schermo:
 - o selezionare il numero di telefono da associare,
 - o impostare un codice personale **MPIN** di 6 cifre,
 - o inserire il codice di sicurezza (OTP) ricevuto via SMS.
4. Se si desidera è anche possibile attivare il **riconoscimento biometrico** (impronta digitale o Face ID), così da autorizzare le operazioni ancora più rapidamente.

Una volta completata l'attivazione, potrà accedere al Suo Internet Banking e confermare le operazioni dispositive direttamente dal proprio smartphone, tramite **notifica push** con codice MPIN o riconoscimento biometrico.

Tutorial passo-passo: per vedere nel dettaglio la procedura di attivazione può consultare i video e le guide disponibili sul nostro sito www.bancodilucca.it – sezione Privati – Internet Banking – Mobile Token ([Mobile Token - Banco di Lucca](#))

Supporto dedicato: se ha dubbi o difficoltà, puoi contattare il **numero verde** 800.321.036 attivo 24 ore su 24 ore 365 giorni anno dove troverà assistenza per l'attivazione e l'utilizzo del Mobile Token. In caso di richieste di supporto dal estero: + 39-051.4992.138 con costo della chiamata a Suo carico in linea con la normale prassi telefonica internazionale).

Lucca, 30 settembre 2025

Oggetto: Proposta di modifica Unilaterale del Contratto di Internet Banking – Dispositivi di sicurezza del servizio di Internet Banking

Gentile Cliente,

in un contesto in continua evoluzione, la crescente digitalizzazione dei servizi pagamento sta trasformando profondamente le modalità con cui operiamo ogni giorno, offrendo vantaggi in termini di efficienza e rapidità. L'evoluzione digitale rende inoltre necessario adeguare costantemente i presidi di sicurezza adottati per fronteggiare tentativi di frode sempre più complessi ed insidiosi.

Queste ragioni sono alla base dell'impegno costante della Banca nella ricerca di soluzioni che possano rafforzare la sicurezza delle operazioni effettuate in modalità elettronica.

In tale contesto, con la presente comunicazione, la Banca Le propone di modificare il contratto di Internet Banking da Lei sottoscritto (di seguito, il "**Contratto**"), con riguardo ai dispositivi di sicurezza collegati al servizio di Internet Banking per allineare talune previsioni del Suo Contratto ai presidi di sicurezza implementati.

Al riguardo, Le ricordiamo che attualmente per usufruire delle funzioni informative e dispositive tramite il servizio di Internet Banking oltre alla digitazione delle credenziali personali (codice utente e chiave di accesso), è necessario confermare la propria identità attraverso l'autenticazione forte del cliente (cd. SCA)

Con l'obiettivo di garantire un costante allineamento con il progresso tecnologico, la Banca ha adottato un sistema di autenticazione forte denominato *Mobile Token* che rappresenta una soluzione più evoluta e progettata per garantire un accesso agevole e protetto ai servizi informativi e dispositivi della Banca tramite Internet Banking.

Attraverso il *Mobile Token*, è possibile autorizzare le Sue operazioni tramite la conferma di una "*Notifica Push*", ricevuta sull'APP MOBILE della Banca e non sarà più necessario confermare le operazioni tramite chiamata al numero verde (*Secure Call*).

Per tale motivo, nel caso in cui il Suo metodo di autenticazione forte consista nell'utilizzo del *Secure Call*, La informiamo che, a decorrere dal mese di febbraio 2026, varieremo le Sue modalità di accesso al servizio di Internet Banking dal *Secure Call* al *Mobile Token*.

Tali variazioni non comporteranno alcuno costo e/o modifica peggiorativa alle Sue attuali condizioni economiche e parimenti il Suo Contratto sarà integrato come meglio specificato a seguire, per introdurre il *Mobile Token* quale sistema di autenticazione.

Per maggiori dettagli operativi su tale nuova funzionalità, La invitiamo a visionare le istruzioni operative di seguito riportate.

Qualora, invece, il Suo metodo di autenticazione forte consistesse già nell'utilizzo del *Mobile Token*, la presente comunicazione ha il solo scopo di informarLa delle modifiche contrattuali che la Banca ha apportato e che non comportano variazioni alla Sua attuale operatività, inoltre non saranno più dovuti (se presenti) costi a Suo carico per l'utilizzo del *Mobile Token*.

Le comunichiamo infine che, in un'ottica di continuo adeguamento all'evoluzione tecnologica e con l'obiettivo di rafforzare costantemente la sicurezza nelle operazioni di pagamento, la Banca si riserva la facoltà di introdurre, nuovi e diversi dispositivi di sicurezza in funzione dell'evoluzione normativa e delle innovazioni tecnologiche rese disponibili tempo per tempo. Sarà in ogni caso cura della Banca comunicarLe eventuali aggiornamenti secondo le modalità previste nel Suo Contratto.

Per assicurarLe una completa chiarezza e comprensione delle modifiche apportate dalla Banca al Suo Contratto, si riportano di seguito evidenziate in carattere grassetto le parti di testo aggiunte e in barrato le parti eliminate. Conformemente alla normativa vigente, resta salva la Sua facoltà di comunicare alla Banca, prima della data suindicata, che non intende accettare dette modifiche e di esercitare il diritto di



recesso, senza spese, dal Contratto. Nel caso in cui non esercitasse il diritto di recesso nei termini previsti, le modifiche proposte si intenderanno approvate.

SEZIONE CLIENTI CON CONTRATTO SOTTOSCRITTO DOPO 25.02.2022
CONTRATTO DI INTERNET BANKING

DOCUMENTO DI SINTESI

Testo attuale		Proposta di modifica	
Costo rilascio primo Digipass	0,00 EUR	Costo rilascio primo Digipass	0,00 EUR
Costo rilascio altri Digipass	0,00 EUR	Costo rilascio altri Digipass	0,00 EUR
Costo unitario per avvisi tramite SMS op. disposte da Internet Banking e invio SMS con OTP	0,15 EUR	Costo unitario per avvisi tramite SMS op. disposte da Internet Banking e invio SMS con OTP	0,15 EUR

SEZIONE CONTRATTUALE

Testo attuale	Proposta di modifica
II/I Sottoscritto/i (di seguito indicato/i come il 'Cliente' o 'Titolare') chiede/chiedono a LA CASSA DI RAVENNA S.P.A. (di seguito indicata come la 'Banca') ➤ l'attivazione del servizio di INTERNET BANKING / GSM BANKING: [...] ➤ Il Cliente prende atto che i servizi sopra elencati sono regolati dalle Condizioni Economiche indicate nel Documento di Sintesi, frontespizio e parte integrante del Contratto nonché dalle seguenti norme: • Condizioni Generali relative al rapporto Banca-Cliente; • Norme che regolano il Servizio di Internet Banking e Norme che regolano il Servizio di Gsm Banking comprensive delle sottosezioni relative ai servizi Digipass, Secure Call e Corrispondenza OnLine; tutte allegate alla presente richiesta, che il Cliente firma per accettazione e benestare, nonché, per quanto non espressamente previsto dalle stesse, dalle Norme relative al Conto Corrente Bancario e Servizi Connessi, che	II/I Sottoscritto/i (di seguito indicato/i come il 'Cliente' o 'Titolare') chiede/chiedono a LA CASSA DI RAVENNA S.P.A. (di seguito indicata come la 'Banca') ➤ l'attivazione del servizio di INTERNET BANKING / GSM BANKING: [...] ➤ Il Cliente prende atto che i servizi sopra elencati sono regolati dalle Condizioni Economiche indicate nel Documento di Sintesi, frontespizio e parte integrante del Contratto nonché dalle seguenti norme: • Condizioni Generali relative al rapporto Banca-Cliente; • Norme che regolano il Servizio di Internet Banking e Norme che regolano il Servizio di Gsm Banking comprensive delle sottosezioni relative ai servizi Digipass, Secure Call e di Corrispondenza OnLine; tutte allegate alla presente richiesta, che il Cliente firma per accettazione e benestare, nonché, per quanto non espressamente previsto dalle stesse, dalle Norme relative al Conto Corrente Bancario e Servizi Connessi, che qui si

Testo attuale	Proposta di modifica
qui si intendono integralmente richiamate. [...]	intendono integralmente richiamate. [...]

Testo attuale	<u>Proposta di modifica</u>
Il Cliente dichiara di approvare specificamente le seguenti norme, ai sensi dell'art. 1341 comma 2 del codice civile: [...] Servizio Internet Banking (Sottosezione A) Servizio Digipass Art. 5 – Custodia e corretto funzionamento Art. 6 – Restituzione Servizio Internet Banking (Sottosezione B) Servizio Secure Call Art. 3 – Utilizzo Art. 5 - Accesso Servizio Internet Banking (Sottosezione C) Servizio di Corrispondenza OnLine: Art. 6 - Presunzione di avvenuta ricezione	Il Cliente dichiara di approvare specificamente le seguenti norme, ai sensi dell'art. 1341 comma 2 del codice civile: [...] Servizio Internet Banking (Sottosezione A) Servizio Digipass Art. 5 – Custodia e corretto funzionamento Art. 6 – Restituzione Servizio Internet Banking (Sottosezione B) Servizio Secure Call Art. 3 – Utilizzo Art. 5 – Accesso Servizio Internet Banking (Sottosezione AG) Servizio di Corrispondenza OnLine: Art. 6 - Presunzione di avvenuta ricezione

NORME CHE REGOLANO IL SERVIZIO DI INTERNET BANKING

Testo attuale	Proposta di modifica
Art. 4 - Codici 1. L'Utente, dopo aver attivato il servizio, potrà utilizzare i seguenti codici: - codice utente; - chiave di accesso (password); ulteriore password dispositiva (Digipass o Secure Call) Questi codici sono necessari per utilizzare il servizio e per attivare il sistema di sicurezza. Il Cliente prende inoltre atto che per accedere al sito internet della Banca, per	Art. 4 - Codici 1. L'Utente, dopo aver attivato il servizio, potrà utilizzare i seguenti codici: - codice utente; - chiave di accesso (password); ulteriore password dispositiva (Digipass o Secure Call) Questi codici sono necessari per utilizzare il servizio e per attivare il sistema di sicurezza. Il Cliente prende inoltre atto che per accedere al sito internet della Banca, per effettuare

Testo attuale	Proposta di modifica
effettuare operazioni dispositive tramite la rete internet o effettuare qualsiasi altra azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi, la Banca si riserva la facoltà, in conformità con la normativa vigente, di richiedere una forma di autenticazione forte. Per "autenticazione forte del cliente" si intende 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. Le modalità tecniche per usufruire di questi ulteriori criteri di sicurezza sono esplicitate nella "Scheda dispositivi di sicurezza" allegata al presente contratto e sempre disponibile nella versione aggiornata sul sito internet della Banca. [...]	operazioni dispositive tramite la rete internet o effettuare qualsiasi altra azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi, la Banca si riserva la facoltà, in conformità con la normativa vigente, di richiedere una forma di autenticazione forte. Per "autenticazione forte del cliente" si intende 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. Le Banca si riserva, in ogni caso, la possibilità di modificare e/o aggiornare le modalità tecniche di utilizzo dei criteri di sicurezza in funzione dell'evoluzione normativa e delle innovazioni tecnologiche rese disponibili tempo per tempo. Le eventuali variazioni saranno comunicate al Cliente secondo le modalità previste dall'art. 5 ("Invio della corrispondenza alla clientela") delle Condizioni Generali relative al rapporto banca-cliente. Resta inteso che tali variazioni non incideranno sulla modalità di prestazione del consenso alle operazioni dispositive o ad altre attività effettuate tramite canali a distanza, per le quali resterà sempre necessaria l'autenticazione forte del cliente, in conformità alla normativa di volta in volta vigente. [...]

Testo attuale	Proposta di modifica
SERVIZIO INTERNET BANKING (SOTTOSEZIONE A) SERVIZIO DIGIPASS Art. 1 – Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con	SERVIZIO INTERNET BANKING (SOTTOSEZIONE A) SERVIZIO DIGIPASS Art. 1 – Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con

Testo attuale	Proposta di modifica
cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Art. 2 - Il Digipass dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà sempre effettuato utilizzando User-Id e Password già in uso. Art. 3 - Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi. Art. 4 - Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Art. 5 - Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: - il dispositivo non deve essere aperto, smontato a manomesso in alcun modo;	cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Art. 2 - Il Digipass dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà sempre effettuato utilizzando User-Id e Password già in uso. Art. 3 - Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi. Art. 4 - Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Art. 5 - Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: — il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; — deve essere tenuto lontano da fonti di calore;

Testo attuale	Proposta di modifica
- deve essere tenuto lontano da fonti di calore; - non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Art. 6 - Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anomalo rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Art. 7 - Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene	- non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Art. 6 - Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anomalo rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Art. 7 - Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa

Testo attuale	Proposta di modifica
restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa password, l'autenticazione avrà esito negativo a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte	password, l'autenticazione avrà esito negativo a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte

Testo attuale	Proposta di modifica
SERVIZIO INTERNET BANKING (SOTTOSEZIONE B) SERVIZIO SECURE CALL Art. 1 - Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. Art. 2 - L'attivazione del Secure Call è subordinato al possesso di un numero cellulare italiano. Il numero di cellulare collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite sul servizio di Internet Banking. Art. 3 - Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per l'utilizzo del servizio. L'accesso al servizio verrà effettuato utilizzando User-Id e Password già in uso dal Cliente e Servizio Secure Call. Art. 4 - Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. Art. 5 - In fase di accesso al servizio e di conferma di una disposizione il Cliente ha a disposizione 60 secondi per comporre il numero verde visualizzato a video, dal numero di cellulare associato al servizio di Internet Banking da cui sta effettuando l'accesso al servizio/la disposizione. Quando richiesto il Cliente deve inserire il codice PIN di 4 cifre riportato sul monitor. Inserito il codice corretto l'accesso al servizio/la disposizione viene autorizzata.	SERVIZIO INTERNET BANKING (SOTTOSEZIONE B) SERVIZIO SECURE CALL Art. 1 - Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. Art. 2 - L'attivazione del Secure Call è subordinato al possesso di un numero cellulare italiano. Il numero di cellulare collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite sul servizio di Internet Banking. Art. 3 - Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per l'utilizzo del servizio. L'accesso al servizio verrà effettuato utilizzando User-Id e Password già in uso dal Cliente e Servizio Secure Call. Art. 4 - Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. Art. 5 - In fase di accesso al servizio e di conferma di una disposizione il Cliente ha a disposizione 60 secondi per comporre il numero verde visualizzato a video, dal numero di cellulare associato al servizio di Internet Banking da cui sta effettuando l'accesso al servizio/la disposizione. Quando richiesto il Cliente deve inserire il codice PIN di 4 cifre riportato sul monitor. Inserito il codice corretto l'accesso al servizio/la disposizione viene autorizzata. Art. 6 - Il Cliente ha a disposizione tre tentativi

Testo attuale	Proposta di modifica
Art. 6 - Il Cliente ha a disposizione tre tentativi per l'inserimento del codice PIN di 4 cifre in fase di autorizzazione di una disposizione. Superata tale soglia di tentativi il Cliente non può più confermare le disposizioni dal servizio di Internet Banking, deve richiedere lo sblocco del numero di cellulare alla propria filiale di competenza.	per l'inserimento del codice PIN di 4 cifre in fase di autorizzazione di una disposizione. Superata tale soglia di tentativi il Cliente non può più confermare le disposizioni dal servizio di Internet Banking, deve richiedere lo sblocco del numero di cellulare alla propria filiale di competenza.

SCHEDA DISPOSITIVI DI SICUREZZA DEL SERVIZIO INTERNET BANKING

Testo attuale	Proposta di modifica
DIGIPASS Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Il Digipass dovrà essere utilizzato personalmente dal Cliente: ☐ per l'accesso al servizio dopo aver digitato User-Id e Password già in uso; ☐ per l'attività dispositiva, previa comunicazione alla Banca di un dispositivo mobile su cui ricevere via SMS una parte di codice di sicurezza da utilizzare accoppiata alla OTP generata dal Digipass. Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. Il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi.	DIGIPASS Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Il Digipass dovrà essere utilizzato personalmente dal Cliente: ☐ per l'accesso al servizio dopo aver digitato User-Id e Password già in uso; ☐ per l'attività dispositiva, previa comunicazione alla Banca di un dispositivo mobile su cui ricevere via SMS una parte di codice di sicurezza da utilizzare accoppiata alla OTP generata dal Digipass. Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. Il Cliente potrà richiedere, qualora disponga dei necessari

Testo attuale	Proposta di modifica
Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: ☐ il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; ☐ deve essere tenuto lontano da fonti di calore; ☐ non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anormale rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul	requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi. Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: ☐ il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; ☐ deve essere tenuto lontano da fonti di calore; ☐ non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anormale rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente

Testo attuale	<u>Proposta di modifica</u>
Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa password, l'autenticazione avrà esito negativo a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte.	dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa password, l'autenticazione avrà esito negativo a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte.

Testo attuale	<u>Proposta di modifica</u>
TOKEN T806 (con TASTIERINO NUMERICO) – Servizio Comodo Banking Viene concesso in comodato un dispositivo token denominato "T806 - Token Challenge Response", token fisici ultraleggeri con "display LCD" e "tastierino" integrato, che consentono di generare:	TOKEN T806 (con TASTIERINO NUMERICO) – Servizio Comodo Banking Viene concesso in comodato un dispositivo token denominato "T806 - Token Challenge Response", token fisici ultraleggeri con "display LCD" e "tastierino" integrato, che consentono di

Testo attuale	Proposta di modifica
☐ OTP (one time password) "usa e getta" Time based con cadenza regolare di circa 30 (trenta) secondi; ☐ OTP Transaction based, ovvero collegate all'operazione da validare. Il Token è contrassegnato da un codice numerico e viene consegnato ai Clienti per l'accesso al servizio e per autorizzare le funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Il Token T806 dovrà essere utilizzato personalmente dal Cliente. Il "tastierino" integrato sugli apparati permette di effettuare: ☐ l'accesso al servizio tramite la scelta innescata dal "pulsante 1" con la conseguente generazione di una OTP "semplice"; ☐ l'attività dispositiva tramite la scelta innescata dal "pulsante 3" che attiva il display con indicazione di inserire un dato numerico variabile ritornato dai sistemi di on-line banking, in base al quale sarà possibile generare – tramite il tasto OK - la OTP da utilizzare per autorizzare l'operazione. Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Token dovrà essere restituito alla filiale di riferimento della Banca. Il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Token. Il Token: ☐ viene attivato dalla Banca contestualmente all'attivazione del servizio ☐ viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Il Cliente ha l'obbligo di custodire e conservare il dispositivo con diligenza,	<u>generare:</u> ☐ OTP (one time password) "usa e getta" Time based con cadenza regolare di circa 30 (trenta) secondi; ☐ OTP Transaction based, ovvero collegate all'operazione da validare. Il Token è contrassegnato da un codice numerico e viene consegnato ai Clienti per l'accesso al servizio e per autorizzare le funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Il Token T806 dovrà essere utilizzato personalmente dal Cliente. Il "tastierino" integrato sugli apparati permette di effettuare: ☐ l'accesso al servizio tramite la scelta innescata dal "pulsante 1" con la conseguente generazione di una OTP "semplice"; ☐ l'attività dispositiva tramite la scelta innescata dal "pulsante 3" che attiva il display con indicazione di inserire un dato numerico variabile ritornato dai sistemi di on-line banking, in base al quale sarà possibile generare – tramite il tasto OK - la OTP da utilizzare per autorizzare l'operazione. Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Token dovrà essere restituito alla filiale di riferimento della Banca. Il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Token. Il Token: ☐ viene attivato dalla Banca contestualmente all'attivazione del servizio ☐ viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Il Cliente ha l'obbligo di custodire e conservare il dispositivo con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo

Testo attuale	Proposta di modifica
separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Token dovranno in ogni caso essere adottati i seguenti accorgimenti: ☐ il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; ☐ deve essere tenuto lontano da fonti di calore; ☐ non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Le One Time Password generate dai Token T806 e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Le password "time based" generate dal dispositivo variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Token nell'ambito di tale intervallo temporale, viene restituita la stessa password.	stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Token dovranno in ogni caso essere adottati i seguenti accorgimenti: ☐ il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; ☐ deve essere tenuto lontano da fonti di calore; ☐ non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Le One Time Password generate dai Token T806 e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Le password "time based" generate dal dispositivo variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Token nell'ambito di tale intervallo temporale, viene restituita la stessa password. Le One Time Password generate dai dispositivi Token T806, a seguito di digitazione sul tastierino numerico da parte del cliente del codice riveniente dal sistema, vengono calcolate univocamente e derivano dall'importo e dalle coordinate dell'operazione (OTP transaction based). La OTP da inserire sul

Testo attuale	Proposta di modifica
Le One Time Password generate dai dispositivi Token T806, a seguito di digitazione sul tastierino numerico da parte del cliente del codice riveniente dal sistema, vengono calcolate univocamente e derivano dall'importo e dalle coordinate dell'operazione (OTP transaction based). La OTP da inserire sul sistema per autorizzare l'operazione è pertanto calcolata dinamicamente sull'importo, sull'iban e sull'orario dell'operazione (dynamic linking).	sistema per autorizzare l'operazione è pertanto calcolata dinamicamente sull'importo, sull'iban e sull'orario dell'operazione (dynamic linking).

Testo attuale	Proposta di modifica
SECURE CALL Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. L'attivazione del Secure Call è subordinata al possesso di un dispositivo mobile contrattualizzato con un operatore mobile che operi in Italia. Il numero del dispositivo mobile collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite su tale servizio. Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per l'utilizzo del servizio. Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. In fase di accesso al servizio, il Cliente ha a disposizione 60 secondi per: ☐ comporre il numero verde visualizzato a video, dal dispositivo mobile associato al servizio di Internet Banking da cui sta effettuando l'accesso; ☐ inserire, quando richiesto, il codice PIN di 4 cifre riportato sul monitor. Dopo aver inserito il codice corretto, l'accesso al servizio viene autorizzato. In fase di autorizzazione di una disposizione il Cliente ha a disposizione 60 secondi per: ☐ comporre il numero verde visualizzato a video, dal dispositivo mobile associato al	SECURE CALL Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. L'attivazione del Secure Call è subordinata al possesso di un dispositivo mobile contrattualizzato con un operatore mobile che operi in Italia. Il numero del dispositivo mobile collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite su tale servizio. Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per l'utilizzo del servizio. Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. In fase di accesso al servizio, il Cliente ha a disposizione 60 secondi per: ☐ comporre il numero verde visualizzato a video, dal dispositivo mobile associato al servizio di Internet Banking da cui sta effettuando l'accesso; ☐ inserire, quando richiesto, il codice PIN di 4 cifre riportato sul monitor. Dopo aver inserito il codice corretto, l'accesso al servizio viene autorizzato. In fase di autorizzazione di una disposizione il Cliente ha a disposizione 60 secondi per: ☐ comporre il numero verde visualizzato a video, dal dispositivo mobile associato al servizio di Internet Banking da cui sta

Testo attuale	Proposta di modifica
servizio di Internet Banking da cui sta effettuando l'accesso; ☐ inserire quando richiesto il codice PIN di 4 cifre riportato sul monitor; ☐ seguire la voce guida e, quando richiesto, inserire il secondo PIN di 4 cifre. Dopo aver inserito i codici corretti, viene autorizzata la disposizione inserita. Il Cliente ha a disposizione cinque tentativi per l'inserimento del codice PIN di 4 cifre in fase di accesso o di autorizzazione di una disposizione. Superata tale soglia di tentativi, il Cliente non può più confermare le disposizioni dal servizio di Internet Banking e deve richiedere lo sblocco del numero di cellulare alla propria filiale di competenza.	effettuando l'accesso; ☐ inserire quando richiesto il codice PIN di 4 cifre riportato sul monitor; ☐ seguire la voce guida e, quando richiesto, inserire il secondo PIN di 4 cifre. Dopo aver inserito i codici corretti, viene autorizzata la disposizione inserita. Il Cliente ha a disposizione cinque tentativi per l'inserimento del codice PIN di 4 cifre in fase di accesso o di autorizzazione di una disposizione. Superata tale soglia di tentativi, il Cliente non può più confermare le disposizioni dal servizio di Internet Banking e deve richiedere lo sblocco del numero di cellulare alla propria filiale di competenza.

SCHEDA RAPPORTI INTERNET BANKING

Testo attuale	Proposta di modifica
[...] Nota bene: possono essere collegati al servizio sia i rapporti intestati al cliente che i rapporti di cui il cliente sia cointestatario a firme disgiunte con funzionalità sia informativa che dispositiva. Per le persone giuridiche il contratto viene sottoscritto dal legale rappresentante in veste di Utente. Successivamente all'apertura del contratto il presente modulo può essere utilizzato anche per modificare il tipo di abilitazione sui rapporti (profilo) nonché per abilitare nuovi rapporti, con le stesse modalità richieste per l'abilitazione iniziale. Per accedere ai servizi l'Utente si collega con il sito Internet della Banca: www.lacassa.com. Nella maschera di accesso digita il codice "Identificativo Utente". Immette al primo accesso la "Password" contenuta nel preimbustato avendo cura per ragioni di sicurezza di variare successivamente tale "password" con una propria personalizzata (massimo 20 caratteri). Successivamente, verrà richiesto di immettere un codice generato dal dispositivo di sicurezza utilizzato dal Cliente:	[...] Nota bene: possono essere collegati al servizio sia i rapporti intestati al cliente che i rapporti di cui il cliente sia cointestatario a firme disgiunte con funzionalità sia informativa che dispositiva. Per le persone giuridiche il contratto viene sottoscritto dal legale rappresentante in veste di Utente. Successivamente all'apertura del contratto il presente modulo può essere utilizzato anche per modificare il tipo di abilitazione sui rapporti (profilo) nonché per abilitare nuovi rapporti, con le stesse modalità richieste per l'abilitazione iniziale. Per accedere ai servizi l'Utente si collega con il sito Internet della Banca: www.lacassa.com. Nella maschera di accesso digita il codice "Identificativo Utente". Immette al primo accesso la "Password" contenuta nel preimbustato avendo cura per ragioni di sicurezza di variare successivamente tale "password" con una propria personalizzata (massimo 20 caratteri). Successivamente, verrà richiesto di immettere un codice generato dal dispositivo di sicurezza utilizzato dal Cliente: Digipass o Secure Call Notifica Push (Mobile)



Testo attuale	<u>Proposta di modifica</u>
Digipass o Secure Call, che servirà anche per effettuare disposizioni (acquisto/vendita titoli, bonifico, giroconto, pagamento effetti, ricariche telefoniche, etc.). Si ricorda che l'utilizzo del profilo "Trading" può indurre a moltiplicare il numero delle proprie transazioni operando in una prospettiva "intraday" (rif. Comunicazione CONSOB n. 30396 del 21 Aprile 2000). [...]	Token), che servirà anche per effettuare disposizioni (acquisto/vendita titoli, bonifico, giroconto, pagamento effetti, ricariche telefoniche, etc.). Si ricorda che l'utilizzo del profilo "Trading" può indurre a moltiplicare il numero delle proprie transazioni operando in una prospettiva "intraday" (rif. Comunicazione CONSOB n. 30396 del 21 Aprile 2000). [...]

SEZIONE CLIENTI CON CONTRATTO SOTTOSCRITTO PRIMA DEL 25.02.2022
CONTRATTO DI INTERNET BANKING

DOCUMENTO DI SINTESI

Testo attuale		Proposta di modifica	
Canone mensile MOBILE TOKEN	0,25 EUR	Canone mensile MOBILE TOKEN	0,25 EUR
Costo rilascio primo Digipass	0,00 EUR	Costo rilascio primo Digipass	0,00 EUR
Costo rilascio altri Digipass	0,00 EUR	Costo rilascio altri Digipass	0,00 EUR

SEZIONE CONTRATTUALE

Testo attuale	Proposta di modifica
Il/la Sottoscritto/i (di seguito indicato/i come il 'Cliente' o 'Titolare') chiede/chiedono alla CASSA DI RISPARMIO DI RAVENNA S.P.A. (di seguito indicata come la 'Banca') ➤ l'attivazione del servizio di INTERNET BANKING / GSM BANKING: [...] ➤ Il Cliente prende atto che i servizi sopra elencati sono regolati dalle seguenti norme: • Condizioni Generali relative al rapporto Banca-Cliente; • Norme che regolano il Servizio di Gsm Banking comprensive delle sottosezioni relative ai servizi Digipass, Secure Call e Corrispondenza OnLine; tutte allegare alla presente richiesta, che il Cliente firma per accettazione e benestare, nonché, per quanto non espressamente previsto dalle stesse, dalle Norme relative al Conto Corrente Bancario e Servizi Connessi, che qui si intendono integralmente richiamate. [...]	Il/la Sottoscritto/i (di seguito indicato/i come il 'Cliente' o 'Titolare') chiede/chiedono alla CASSA DI RISPARMIO DI RAVENNA S.P.A. (di seguito indicata come la 'Banca') ➤ l'attivazione del servizio di INTERNET BANKING / GSM BANKING: [...] ➤ Il Cliente prende atto che i servizi sopra elencati sono regolati dalle seguenti norme: • Condizioni Generali relative al rapporto Banca-Cliente; • Norme che regolano il Servizio di Gsm Banking comprensive delle sottosezioni relative al servizio Digipass, Secure Call e di Corrispondenza OnLine; tutte allegare alla presente richiesta, che il Cliente firma per accettazione e benestare, nonché, per quanto non espressamente previsto dalle stesse, dalle Norme relative al Conto Corrente Bancario e Servizi Connessi, che qui si intendono integralmente richiamate. [...]

NORME CHE REGOLANO IL SERVIZIO DI INTERNET BANKING

Testo attuale	Proposta di modifica
Art. 4 - Codici 1. L'Utente, dopo aver attivato il servizio, potrà utilizzare i seguenti codici: - codice utente; - chiave di accesso (password); ulteriore password dispositiva (Digipass o Secure Call) Questi codici sono necessari per utilizzare il servizio e per attivare il sistema di sicurezza. Il Cliente prende inoltre atto che per accedere al sito internet della Banca, per effettuare operazioni dispositive tramite la rete internet o effettuare qualsiasi altra azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi, la Banca si riserva la facoltà, in conformità con la normativa vigente, di richiedere una forma di autenticazione forte. Per "autenticazione forte del cliente" si intende 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. [...]	Art. 4 - Codici 1. L'Utente, dopo aver attivato il servizio, potrà utilizzare i seguenti codici: - codice utente; - chiave di accesso (password); ulteriore password dispositiva (Digipass o Secure Call) Questi codici sono necessari per utilizzare il servizio e per attivare il sistema di sicurezza. Il Cliente prende inoltre atto che per accedere al sito internet della Banca, per effettuare operazioni dispositive tramite la rete internet o effettuare qualsiasi altra azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi, la Banca si riserva la facoltà, in conformità con la normativa vigente, di richiedere una forma di autenticazione forte. Per "autenticazione forte del cliente" si intende 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. Le modalità tecniche per usufruire di questi ulteriori criteri di sicurezza sono esplicitate nella "Scheda dispositivi di sicurezza" allegata al presente contratto e sempre disponibile nella versione aggiornata sul sito internet della Banca. Le Banca si riserva, in ogni caso, la possibilità di modificare e/o aggiornare le modalità tecniche di utilizzo dei criteri di sicurezza in funzione dell'evoluzione normativa e delle innovazioni tecnologiche rese disponibili tempo per tempo. Le eventuali variazioni saranno comunicate al

Testo attuale	Proposta di modifica
	Cliente secondo le modalità previste dall'art. 5 ("Invio della corrispondenza alla clientela") delle Condizioni Generali relative al rapporto banca-cliente. Resta inteso che tali variazioni non incideranno sulla modalità di prestazione del consenso alle operazioni dispositive o ad altre attività effettuate tramite canali a distanza, per le quali resterà sempre necessaria l'autenticazione forte del cliente, in conformità alla normativa di volta in volta vigente. [...]
Art. 15 - Servizio digipass e secure call Al momento dell'apertura del contratto, sulla base delle preferenze espresse dall'Utente in relazione ai due servizi resi disponibili: A. viene rilasciato un dispositivo 'Digipass', che consente di generare delle password 'dinamiche' utilizzabili una sola volta, che garantiscono un elevato livello di sicurezza dell'attività dispositiva. Il servizio è disciplinato dalle norme di cui alla sottosezione A del presente contratto; oppure, B. viene attivato il servizio 'Secure Call', che consiste nell'autenticazione dispositiva in grado di incrementare la sicurezza delle operazioni del cliente. Il servizio è disciplinato dalle norme di cui alla sottosezione B del presente contratto.	Art. 15 - Servizio digipass e secure call Al momento dell'apertura del contratto, sulla base delle preferenze espresse dall'Utente in relazione ai due servizi resi disponibili: A. viene rilasciato un dispositivo 'Digipass', che consente di generare delle password 'dinamiche' utilizzabili una sola volta, che garantiscono un elevato livello di sicurezza dell'attività dispositiva. Il servizio è disciplinato dalle norme di cui alla sottosezione A del presente contratto; oppure, B. viene attivato il servizio 'Secure Call', che consiste nell'autenticazione dispositiva in grado di incrementare la sicurezza delle operazioni del cliente. Il servizio è disciplinato dalle norme di cui alla sottosezione B del presente contratto

Testo attuale	Proposta di modifica
SERVIZIO INTENET BANKING (SOTTOSEZIONE A) SERVIZIO DIGIPASS Art. 1 – Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è	SERVIZIO INTENET BANKING (SOTTOSEZIONE A) SERVIZIO DIGIPASS Art. 1 – Viene concesso in comodato un dispositivo denominato Hardware Digipass, dotato di display in grado di generare con cadenza regolare di circa 30 (trenta) secondi codici numerici monouso. Il Digipass è

Testo attuale	Proposta di modifica
contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Art. 2 - Il Digipass dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà sempre effettuato utilizzando User-Id e Password già in uso. Art. 3 - Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi. Art. 4 - Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Art. 5 - Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: - il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; - deve essere tenuto lontano da fonti di calore;	contrassegnato da un codice numerico. Il Digipass viene consegnato ai Clienti abilitati alle funzioni dispositive. La sicurezza dell'apparecchio è certificata dall'azienda produttrice. Art. 2 - Il Digipass dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà sempre effettuato utilizzando User-Id e Password già in uso. Art. 3 - Il comodato avrà durata dalla data di consegna fino a quando cesserà il funzionamento del dispositivo (la batteria è garantita per una durata di almeno 5 anni). Alla scadenza il Digipass dovrà essere restituito alla filiale di riferimento della Banca. il Cliente potrà richiedere, qualora disponga dei necessari requisiti, il rilascio di un nuovo Digipass previa sottoscrizione di un nuovo contratto di servizi. Art. 4 - Il Digipass viene attivato dalla Banca contestualmente all'attivazione del servizio. Il Digipass viene consegnato nello stato di conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente. Art. 5 - Il Cliente ha l'obbligo di custodire e conservare il Digipass con diligenza, separatamente dagli altri Codici Identificativi e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualunque intervento sullo stesso. In caso di smarrimento / sottrazione il Cliente dovrà effettuare regolare denuncia di smarrimento alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvederà al blocco immediato dell'operatività' effettuando la relativa sostituzione se richiesta. Per garantire un corretto funzionamento del Digipass dovranno in ogni caso essere adottati i seguenti accorgimenti: _____ il dispositivo non deve essere aperto, smontato a manomesso in alcun modo; _____ deve essere tenuto lontano da fonti di calore; _____ non deve essere bagnato o comunque

Testo attuale	Proposta di modifica
- non deve essere bagnato o comunque pulito con solventi, acidi e liquidi in genere. Art. 6 - Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anomalo rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Art. 7 - Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante	pulito con solventi, acidi e liquidi in genere. Art. 6 - Il Cliente deve restituire il dispositivo alla Banca alla scadenza del contratto nonché qualora la Banca stessa lo richieda in relazione al mancato adempimento degli obblighi contrattuali o qualora vengano meno i presupposti di utilizzo. Qualora il dispositivo restituito risulti danneggiato ovvero lo stesso manifesti un deterioramento anomalo rispetto ad un uso normale o comunque conforme a quello stabilito nel contratto ovvero qualora il Digipass non possa essere restituito o in caso di smarrimento/sottrazione dello stesso il Cliente dovrà corrispondere alla Banca un'indennità nella misura prevista nel Documento di Sintesi. Art. 7 - Le One Time Password generate dai dispositivi Digipass e digitate dal cliente sul Front End del collegamento Internet sono calcolate in funzione di uno specifico algoritmo che considera, congiuntamente, come variabili il 'serial number' dell'apparecchio ed il 'clock' ovvero l'orario in cui è stata richiesta la One Time Password. Considerando che il 'Serial Number' è collegato in modo univoco al cliente, il software utilizzato è in grado di autenticare la One Time Password indicata dal cliente restituendo un esito positivo o negativo al menzionato processo di autenticazione. Si sottolinea, altresì, che il software utilizzato è predisposto per gestire, nel corso del tempo, eventuali progressivi disallineamenti del 'clock' dei dispositivi Digipass rispetto al 'clock' del Sistema Informativo utilizzato, grazie ad uno specifico meccanismo che consente di adattare, per singolo dispositivo, l'entità del disallineamento tollerato. Le password generate dai Digipass variano ogni circa 30 secondi; di conseguenza qualora si accenda e si spenga più volte il Digipass nell'ambito di tale intervallo temporale, viene restituita la stessa password. Qualora il cliente effettui più operazioni che necessitano di essere confermate mediante OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa password, l'autenticazione avrà esito negativo

Testo attuale	Proposta di modifica
OTP nel lasso temporale menzionato e digiti sul Front End di Internet Banking due o più volte consecutive la stessa password, l'autenticazione avrà esito negativo a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte.	a partire dalla seconda volta; di conseguenza non è possibile digitare la stessa password consecutivamente più volte.

Testo attuale	Proposta di modifica
SERVIZIO INTERNET BANKING (SOTTOSEZIONE B) SERVIZIO SECURE CALL Art. 1 - Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. Art. 2 - L'attivazione del Secure Call è subordinato al possesso di un numero cellulare italiano. Il numero di cellulare collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite sul servizio di Internet Banking. Art. 3 - Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà effettuato utilizzando User-Id e Password già in uso dal Cliente. Art. 4 - Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. Art. 5 - In fase di conferma di una disposizione il Cliente ha a disposizione 60 secondi per comporre il numero verde visualizzato a video, dal numero di cellulare associato al servizio di Internet Banking da cui sta effettuando la disposizione. Quando richiesto il Cliente deve inserire il codice PIN di 4 cifre riportato sul monitor. Inserito il codice corretto la disposizione viene autorizzata. Art. 6 - Il Cliente ha a disposizione tre tentativi per l'inserimento del codice PIN di 4 cifre in fase di autorizzazione di una disposizione. Superata tale soglia di tentativi il Cliente non può più confermare le disposizioni dal servizio di Internet Banking,	SERVIZIO INTERNET BANKING (SOTTOSEZIONE B) SERVIZIO SECURE CALL Art. 1 - Il Servizio Secure Call viene attivato contestualmente all'attivazione del servizio Internet Banking. Art. 2 - L'attivazione del Secure Call è subordinato al possesso di un numero cellulare italiano. Il numero di cellulare collegato al contratto di Internet Banking permette di autorizzare le disposizioni inserite sul servizio di Internet Banking. Art. 3 - Il Servizio di Secure Call dovrà essere utilizzato personalmente dal Cliente per la sola attività dispositiva. L'accesso al servizio verrà effettuato utilizzando User-Id e Password già in uso dal Cliente. Art. 4 - Il Servizio è attivo per le operazioni disposte dall'Italia e dall'estero. Art. 5 - In fase di conferma di una disposizione il Cliente ha a disposizione 60 secondi per comporre il numero verde visualizzato a video, dal numero di cellulare associato al servizio di Internet Banking da cui sta effettuando la disposizione. Quando richiesto il Cliente deve inserire il codice PIN di 4 cifre riportato sul monitor. Inserito il codice corretto la disposizione viene autorizzata. Art. 6 - Il Cliente ha a disposizione tre tentativi per l'inserimento del codice PIN di 4 cifre in fase di autorizzazione di una disposizione. Superata tale soglia di tentativi il Cliente non può più confermare le disposizioni dal servizio di Internet Banking, deve richiedere lo sblocco del numero di cellulare alla propria filiale di

Testo attuale	Proposta di modifica
deve richiedere lo sblocco del numero di cellulare alla propria filiale di competenza.	competenza.

Testo attuale	Proposta di modifica
INFORMATIVA ANTITRUFFA [...] Per quanto concerne i propri servizi online, la Banca suggerisce di: 1.Custodire con cura: - i propri dati di accesso, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima; - il Digipass ed i codici di accesso generati. 2.Non fornire MAI le proprie password ed i codici di accesso elaborati dal Digipass ad alcuno. Si precisa che nessun dipendente è autorizzato a richiederle, pertanto è opportuno diffidare di qualsiasi richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, e-mail o altro mezzo. 3.Inserire il codice fornito dal Digipass solo ed esclusivamente in fase di autorizzazione e quindi alla fine dell'inserimento della disposizione. Ricordarsi di non dar corso ad alcuna operazione qualora il codice fornito dal Digipass venisse richiesto in un momento diverso. 4.Accedere sempre ai servizi online digitando il sito della Banca, evitando di 'cliccare' su eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute. 5.Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta, diffidando dei 'pop-up'. Per verificare che la pagina web sia protetta, controllare che l'indirizzo sia preceduto da 'https' e che sul browser sia presente l'icona  che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra.	INFORMATIVA ANTITRUFFA [...] Per quanto concerne i propri servizi online, la Banca suggerisce di: 1.Custodire con cura: - i propri dati di accesso, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima; - il Digipass ed i codici di accesso generati il codice impostato per autorizzare le operazioni tramite Mobile Token e/o tramite i dispositivi di sicurezza tempo per tempo messi a disposizione dalla Banca. 2.Non fornire MAI le proprie password ed i codici di accesso elaborati dal Digipass ad alcuno. Si precisa che nessun dipendente è autorizzato a richiederle, pertanto è opportuno diffidare di qualsiasi richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, e-mail o altro mezzo. 3.Inserire il codice fornito dal o i diversi elementi di autenticazione impostati per autorizzare le operazioni tramite Mobile Token o tramite i dispositivi di sicurezza tempo per tempo messi a disposizione dalla Banca Digipass solo ed esclusivamente in fase di autorizzazione e quindi alla fine dell'inserimento della disposizione. Ricordarsi di non dar corso ad alcuna operazione qualora il codice fornito dal Digipass l'autorizzazione a una operazione dispositiva o informativa (es. tramite conferma della Notifica Push o altri sistemi di sicurezza tempo per tempo messi a disposizione dalla Banca) ti venisse richiesto in un momento diverso. 4.Accedere sempre ai servizi online digitando il sito della Banca, evitando di 'cliccare' su

Testo attuale	Proposta di modifica
6. Controllare regolarmente gli estratti conto dei propri conti e depositi, per assicurarsi che le transazioni riportate siano quelle realmente effettuate. 7. Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza, in particolare: Sistema Operativo, Personal Firewall, Antivirus ed Anti-spyware. 8. Contattare immediatamente l'Help Desk nei seguenti casi: - Sono stati forniti a terzi i propri codici di accesso - E' stata dimenticata la propria password o persa la busta PIN per il primo accesso (prima di essersi collegati per la prima volta) - Si sono ricevute e-mail 'sospette' - Si notano transazioni sospette ed inattese nell'estratto conto	eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute. 5. Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta, diffidando dei 'pop-up'. Per verificare che la pagina web sia protetta, controllare che l'indirizzo sia preceduto da 'https' e che sul browser sia presente l'icona  che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra. 6. Controllare regolarmente gli estratti conto dei propri conti e depositi, per assicurarsi che le transazioni riportate siano quelle realmente effettuate. 7. Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza, in particolare: Sistema Operativo, Personal Firewall, Antivirus ed Anti-spyware. 8. Contattare immediatamente l'Help Desk nei seguenti casi: - Sono stati forniti a terzi i propri codici di accesso - E' stata dimenticata la propria password o persa la busta PIN per il primo accesso (prima di essersi collegati per la prima volta) - Si sono ricevute e-mail 'sospette' - Si notano transazioni sospette ed inattese nell'estratto conto

Testo attuale	Proposta di modifica
-	SCHEDA DISPOSITIVI DI SICUREZZA DEL SERVIZIO INTERNET BANKING NOTIFICA PUSH (Mobile Token) – Servizio Happy Banking La soluzione "NOTIFICA PUSH" prevede l'integrazione – tramite specifico enrollment autorizzato tramite SCA – della notifica dell'operazione direttamente sull'APP MOBILE della Banca. In questo caso la notifica gestita sull'app bancaria

Testo attuale	<u>Proposta di modifica</u>
	permette di gestire – entro 100 secondi (validità notifica) - tramite pin o tramite fattori di inerenza impostati sul dispositivo mobile: • l'accesso ai servizi telematici; • le fasi di autorizzazione delle disposizioni L'attivazione dell'App-Push notification è subordinata: • al possesso di un dispositivo mobile da parte del cliente; • al censimento del dispositivo nei recapiti del cliente depositati presso la banca: Nella fase di enrollment, ovvero nella fase di configurazione iniziale della push notification, l'utente dovrà definire un PIN alfanumerico di 6 caratteri per gestire le autorizzazioni (Mpin) oppure potrà gestire l'autorizzazione con un fattore di inerenza (fingerprint o face ID). La PUSH NOTIFICATION gestita sul dispositivo mobile a) nel caso di accesso od operatività da APP Bancaria permette di: • effettuare la fase di login tramite Mpin o fattore di inerenza; • autorizzare le operazioni dispositive gestendo l'autenticazione forte come da normativa utilizzando il secondo fattore di possesso (Mpin) o di inerenza (fingerprint) b) nel caso di accesso od operatività tramite sito (desktop) permette di: • generare una notifica sul dispositivo mobile - dopo aver inserito user e password - che va confermata tramite Mpin o fattore di inerenza e successivamente autorizzata; • autorizzare le operazioni dispositive gestendo l'autenticazione forte come da normativa utilizzando il secondo fattore di possesso (Mpin) o di inerenza (fingerprint) e successivamente

Testo attuale	Proposta di modifica
	autorizzata. Si ricorda che nel caso di operatività dal sito di internet banking della banca con dispositivo mobile off-line è possibile generare – al posto della notifica - un QRCode che permette di accedere o autorizzare la disposizione. In questo caso: • si accede all'icona Mobile Token disponibile nella pagina di accesso all'app bancaria; • si autorizza l'accesso con codice Mpin o tramite fattore di inerenza; • si seleziona l'icona operazioni offline e si inquadra il QRcode; • alla ricezione del codice questo va digitato sul sito di internet banking. Nel caso in cui il cliente: • "dimentichi" il codice mpin, sarà necessario disinstallare l'APP e reinstallarla, registrandola nuovamente; • abbia necessità di modificare il codice Mpin, eseguire il reset tramite l'icona Mobile Token disponibile nella pagina di accesso all'App bancaria e registrarla nuovamente; • intenda sostituire il proprio smartphone su cui è attiva l'APP bancaria, è opportuno disinstallare il token dal vecchio dispositivo eseguendo il reset dall'icona "Mobile Token" nella pagina di accesso all'App. E successivamente installare l'app sul nuovo dispositivo e registrarla nuovamente.

Cordiali saluti

BANCO DI LUCCA E DEL TIRRENO S.P.A.
Il Direttore Generale