SCHEDA DISPOSITIVI DI SICUREZZA DEL SERVIZIO INTERNET BANKING

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 dl 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 dl 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 dl conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente.

Il Cliente ha l'obbligo dl 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 dl 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 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 delle 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 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.

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:

- 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 dl 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 dl un nuovo Token.

Il Token:

- viene attivato dalla Banca contestualmente all'attivazione del servizio
- viene consegnato nello stato dl conservazione e nelle condizioni idonee all'uso determinato tra la Banca ed il Cliente.

Il Cliente ha l'obbligo dl 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 stesso. In caso dl 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 dl 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 sistema per autorizzare l'operazione è pertanto calcolata dinamicamente sull'importo, sull'iban e sull'orario dell'operazione (dynamic linking).

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 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.

NOTIFICA PUSH (Token Mobile) – 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 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 inziale 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 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 Token mobile 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 enrollandola nuovamente;
- abbia necessità di modificare il codice mpin, eseguire il reset tramite l'icona Token mobile disponibile nella pagina di accesso all'App bancaria ed enrollarla nuovamente;
- intenda sostituire il proprio smartphone su cui è attiva l'APP bancaria, è opportuno dis-enrollare il token dal vecchio dispositivo (va eliminata l'inscrizione) eseguendo il reset dall'icona "Token Mobile" nella pagina di accesso all'App. E successivamente installare l'app sul nuovo dispositivo ed enrollarla nuovamente

APP CON NOTIFICA PUSH – Servizio Comodo Banking

La soluzione "APP - PUSH notification" prevede la pubblicazione su "Play Store" e "Apple store" di una specifica APP della banca predisposta per:

- permettere l'accesso ai servizi telematici;
- gestire le fasi di autorizzazione delle disposizioni.

Tale dispositivo di sicurezza – attivato sul dispositivo mobile – permette la ricezione di specifiche notifiche:

- in fase di login all'area riservata
- in fase di autorizzazione di operazioni dispositive, ovvero qualora l'operatività posta in essere sull'on-line banking preveda di eseguire una autenticazione forte come da normativa.

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 inziale dell'app push notification, l'utente dovrà definire un PIN alfanumerico di 6 caratteri per gestire le autorizzazioni oppure potrà gestire l'autorizzazione con un fattore di inerenza (fingerprint o face ID)

In fase di accesso al servizio, il Cliente:

- alla ricezione della notifica push ha a disposizione 100 secondi per digitare il PIN dell'app 2 volte (una prima volta per accedere, la seconda per autorizzare l'accesso)
- nel caso di gestione accesso tramite QrCode (off-line) ha a disposizione 100 secondi per inquadrare il QrCode e digitare sul servizio il codice esposto sul dispositivo mobile

In fase di autorizzazione di una disposizione, il Cliente:

- alla ricezione della notifica push ha a disposizione 100 secondi per digitare il PIN dell'app 2 volte (una prima volta per accedere, la seconda per autorizzare la disposizione)
- nel caso di gestione accesso tramite QrCode (off-line) ha a disposizione 100 secondi per inquadrare il QrCode e digitare sul servizio il codice esposto sul dispositivo mobile