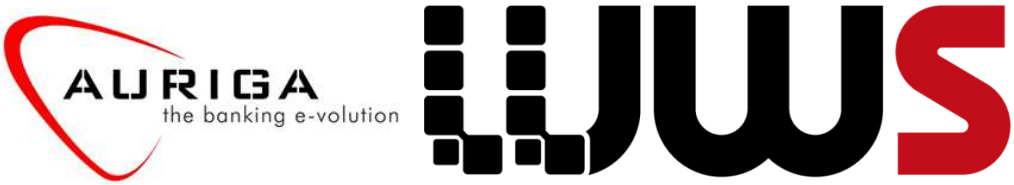


Guida ai servizi Home Banking

Novembre 2016

SOMMARIO

INTRODUZIONE

L'Home Banking è il servizio di banca on-line in tempo reale che permette ai clienti (privati e aziende) della Banca di accedere e gestire i propri conti mediante una vasta gamma di **funzioni informative, dispositive e finanziarie** conformi ai requisiti previsti dal Consorzio CBI, dalle normative SEPA e dall'orientamento EBA.

Il servizio viene erogato mediante un sistema multicanale evoluto che permette al cliente, ovunque si trovi e a qualunque ora del giorno, di accedere ed effettuare operazioni informative e dispositive in modo semplice, sicuro, diretto, integrato con la banca usando il canale (Internet e Mobile) che ritiene più adatto in quel momento.

Il sistema multicanale infatti permette la gestione dei conti su:

- **Internet** : consente ai clienti, che utilizzano qualsiasi browser da un qualsiasi desktop-pc o computer portatile con un semplice collegamento web, di collegarsi on-line in tempo reale alla propria area riservata sul portale della banca;
- **Mobile** : consente ai clienti, che utilizzano un dispositivo mobile con sistema operativo iOS, Android, BlackBerry e WindowsPhone con un semplice collegamento di rete, di collegarsi on-line in tempo reale alla propria banca mediante un'APP nativa disponibile sui market.
- **SMS/Telefono** : consente ai clienti, che utilizzano un telefono cellulare (anche non smartphone) in grado di inviare/ricevere SMS ed effettuare chiamate telefoniche, di essere in comunicazione con la propria Banca attraverso l'invio e la ricezione di SMS e chiamate telefoniche.

ATTIVAZIONE E DISATTIVAZIONE DEL SERVIZIO

ATTIVAZIONE DEL SERVIZIO

Per l'attivazione del servizio di Home Banking (Internet e Mobile) è necessario recarsi presso la filiale della propria Banca e sottoscrivere l'apposito contratto.
Per abilitare/disabilitare nuovi rapporti, modificare il livello di abilitazione sui rapporti abilitati (ad esempio passare da dispositivo a rendicontativo e viceversa) o attivare/disattivare nuovi servizi è necessario recarsi in filiale.
Per i contratti intestati a persone giuridiche e per i titolari minorenni, l'abilitazione dei rapporti ai servizi può essere richiesta esclusivamente in Banca solo dal legale rappresentante o dal tutore (per il minorenne).
Sottoscritto il contratto, la Banca consegna al titolare le credenziali per effettuare il primo accesso all'Home Banking (vedi il paragrafo *PRIMO ACCESSO AL SERVIZIO*).

DISATTIVAZIONE DEL SERVIZIO

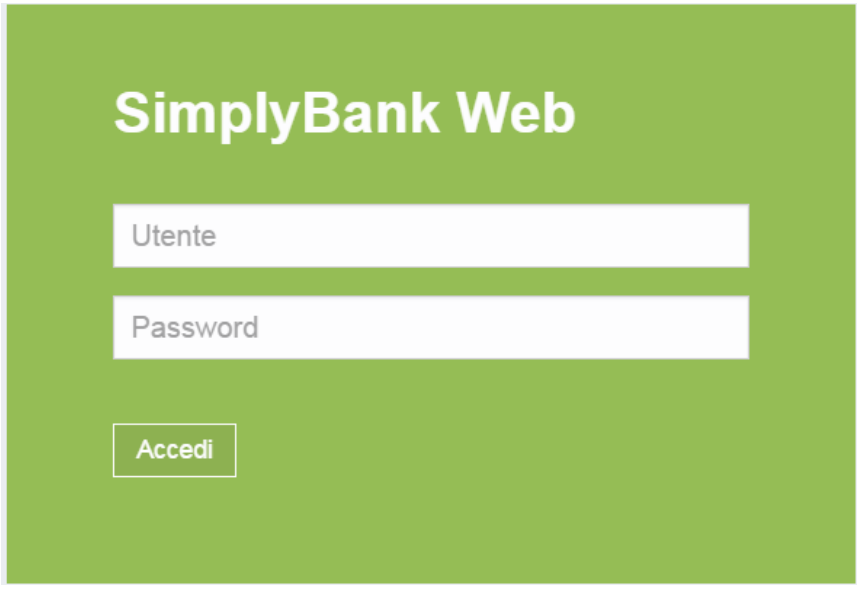
Per disattivare il servizio di Home Banking (Internet e Mobile) nel suo complesso, il cliente deve necessariamente recarsi presso la filiale della propria Banca.
L'estinzione del contratto comporta la revoca di tutti i servizi a cui hai aderito/attivato.
Per i contratti intestati a persone giuridiche e per i titolari minorenni, l'estinzione del contratto può essere richiesta esclusivamente in Banca solo dal legale rappresentante o dal tutore (per il minorenne).

PRIMO ACCESSO AL SERVIZIO, RESET E BLOCCO/SBLOCCO

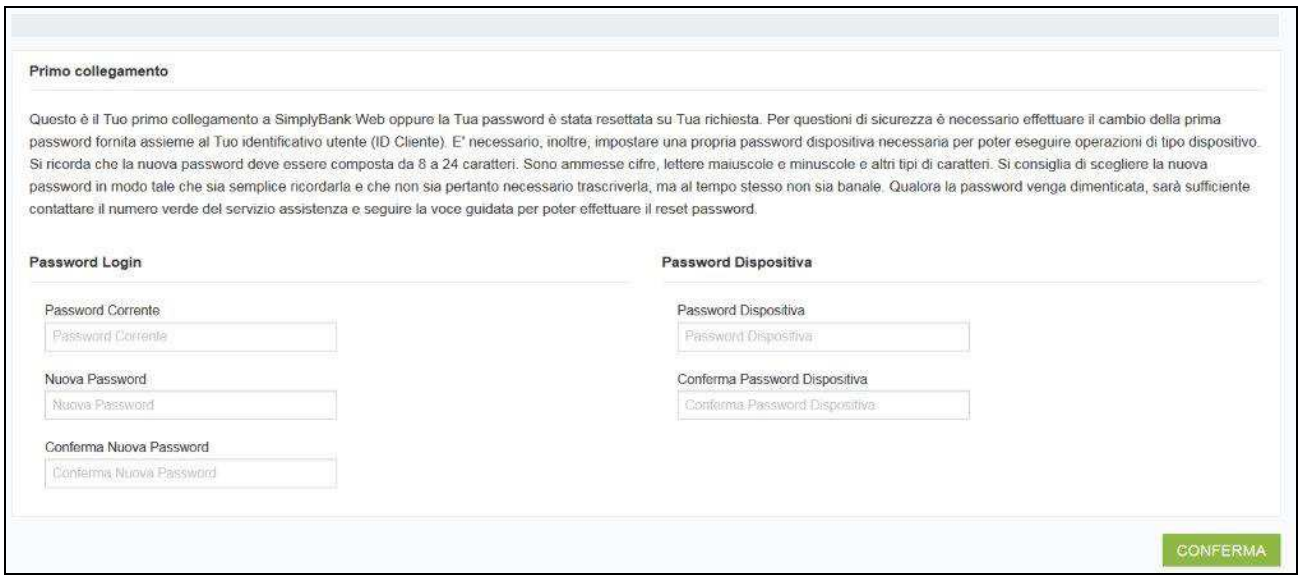
PRIMO ACCESSO AL SERVIZIO

Per operare in modalità multicanale (cioè da Internet o Mobile) è necessario effettuare il primo accesso dal canale Internet allo scopo di definire la nuova password di accesso al servizio e configurare le sicurezze da utilizzare nella gestione dispositiva dei conti.

Collegandosi all'indirizzo web (vedi il paragrafo *Indirizzi Web*) verrà richiesto l'inserimento delle credenziali (userid e password iniziale) ricevute dalla Banca in sede di sottoscrizione del contratto:

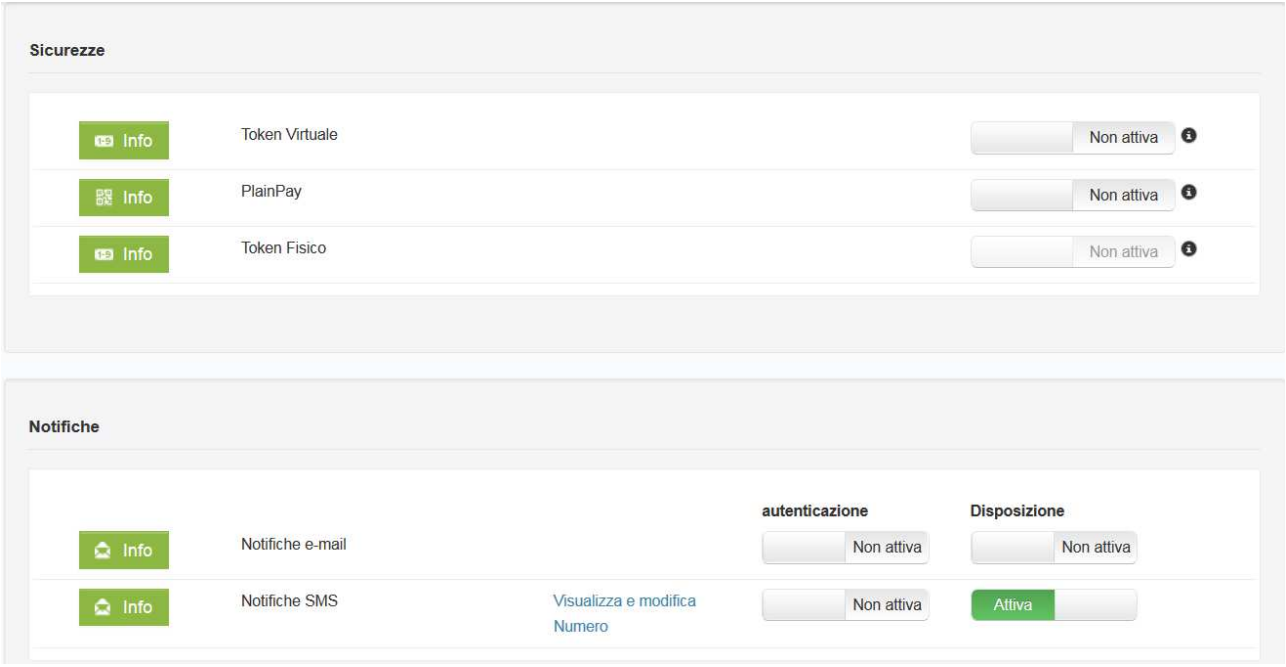


Il sistema, riconoscendo il cliente, mostra la seguente pagina per effettuare il **cambio password** e definire così la nuova password di accesso da usare nei prossimi collegamenti:



Completata la procedura del **cambio password**, il sistema (a seconda che la Banca abbia consegnato o meno il Token Fisico all'utente) può richiedere al cliente una delle seguenti due ulteriori informazioni:

a. Se la Banca non ha consegnato al cliente il Token Fisico: è necessaria la configurazione delle sicurezze da utilizzare nella gestione dispositiva dei conti (vedi il paragrafo *PROFILO DI SICUREZZA*).



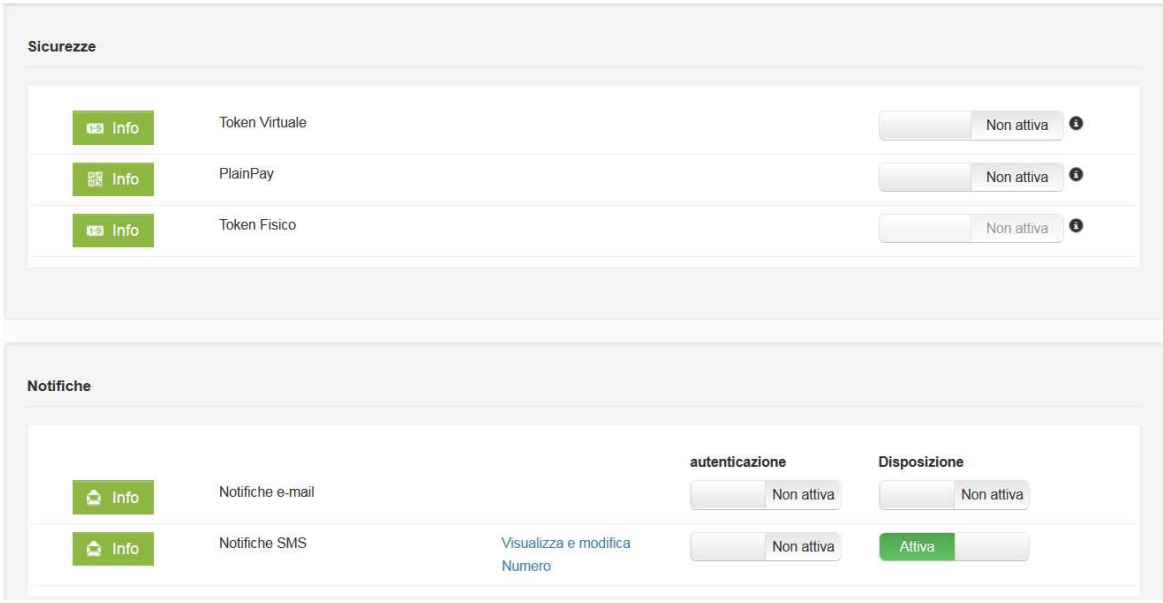
b. Se la Banca ha consegnato al cliente il Token Fisico: è necessario l'inserimento, nell'apposito campo richiesto dalla pagina, del codice OTP (One Time Password) per autenticare l'accesso.

Nel caso in cui il cliente abbia difficoltà ad eseguire il primo accesso può contattare al numero verde il Servizio Clienti per ricevere supporto e informazioni.

PROFILO DI SICUREZZA

La pagina, mostrata dal sistema in fase di primo accesso se la Banca non ha consegnato al cliente il Token Fisico, permette al cliente di configurare in qualsiasi momento gli strumenti di sicurezza (conformi all'orientamento EBA) utilizzati per accedere al servizio e inviare disposizioni (es. bonifici).

Per visualizzare la pagina basta cliccare la voce di menù *Profilo Sicurezza* disponibile nel menù disponibile nella pagina di benvenuto:



L'attivazione/disattivazione di ogni strumento avviene cliccando sul toggle button 'Non attiva'  o 'Attiva'  .

La pagina mostra due sezioni : *Sicurezze* e *Notifiche*.

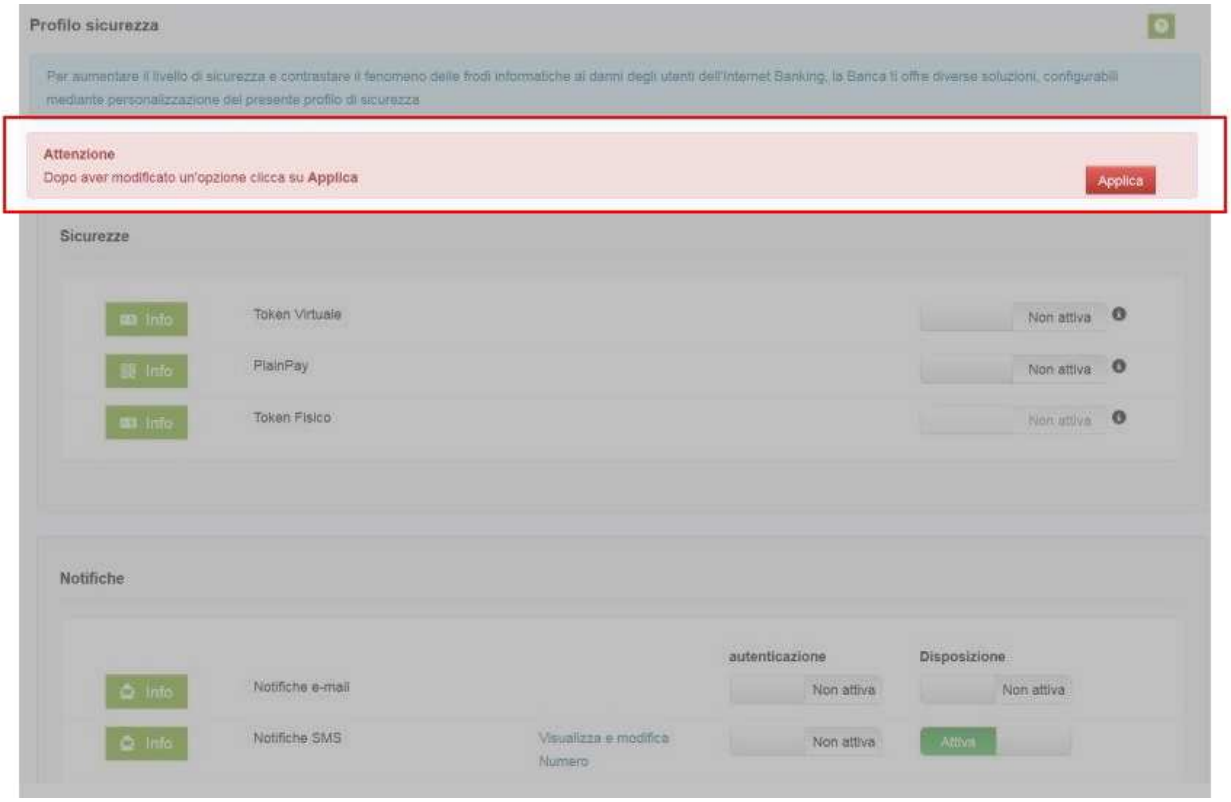
Nella sezione *Sicurezze* sono disponibili le seguenti opzioni:

- **PlainPay**: permette di utilizzare un'APP da scaricare sullo smartphone (iPhone o Android) come strumento di autenticazione in fase di accesso e autorizzazione l'invio delle disposizioni.
  Per attivare il PlainPay basta seguire la procedura guidata disponibile dal tasto "Info" che fornisce informazioni su come effettuare il download dell'APP sullo smartphone e attivare l'APP.
  Attivato questo strumento di sicurezza, tutti gli eventuali altri strumenti di sicurezza saranno sostituiti dal PlainPay.
  Per i dettagli si vedi il paragrafo *PLAINPAY*.
- **Token Virtuale:** permette di utilizzare un'APP da scaricare sullo smartphone (iPhone o Android) e generare un codice OTP (One Time Password) da utilizzare per autenticare l'accesso e autorizzazione l'invio delle disposizioni.
  Per attivare il Token Virtuale basta seguire la procedura guidata disponibile dal tasto "Info" che fornisce informazioni su come effettuare il download dell'APP sullo smartphone e attivare l'APP.
  Attivato questo strumento di sicurezza, tutti gli eventuali altri strumenti di sicurezza saranno sostituiti dal Token Virtuale.
  Per i dettagli si vedi il paragrafo TOKEN *VIRTUALE*.
- **Token Fisico**: permette di autenticare l'accesso e autorizzare l'invio delle disposizioni tramite un dispositivo di generazione di codici chiamato 'token' o 'chiave elettronica'. Per attivare il Token Fisico è necessario contattare la propria filiale della Banca.

Per i dettagli si vedi il paragrafo TOKEN *FISICO*.

Nella sezione *Notifiche*, sono disponibili le seguenti opzioni:

- **Notifiche e-mail**: consente, mediante la ricezione di e-mail all'indirizzo configurato, di monitorare le disposizioni inviate e/o gli accessi effettuati.
  Attivato questo strumento di sicurezza, è sempre possibile per il cliente visualizzare e modificare l'indirizzo e-mail sul quale ricevere le mail.
  Per i dettagli si vedi il paragrafo NOTIFICHE E-MAIL.
- **Notifiche SMS**: consente, mediante la ricezione di SMS al numero configurato, di monitorare le disposizioni inviate e/o gli accessi effettuati.
  Attivato questo strumento di sicurezza, è sempre possibile per il cliente visualizzare e modificare il numero del cellulare sul quale ricevere gli SMS.
  Per i dettagli si vedi il paragrafo NOTIFICHE SMS.



Nel caso di primo accesso al servizio, al completamento della configurazione del Profilo, il sistema effettuerà un logout automatico per fare ricollegare il cliente.

RESET PASSWORD

Il cliente può effettuare il reset della password di accesso in qualunque momento, anche nei giorni festivi ed in orari non lavorativi, contattando il numero verde.

I prerequisiti per effettuare il reset password in autonomia contattando il numero verde sono :

1. aver già comunicato in banca il numero del cellulare sul quale ricevere via SMS il nuovo codice di accesso;
2. contattare il numero verde da una utenza telefonica che non abbia la numerazione nascosta, cioè non sia anonimo.

Se i sopra elencati prerequisiti non sono soddisfatti, il cliente può contattare la filiale della propria Banca e richiedere il reset della password.

Se invece i sopra elencati prerequisiti sono soddisfatti, i passi che il cliente dovrà eseguire sono:

a. comporre il numero verde
b. seguire le indicazioni della voce guida che invita a :
    a. inserire la userid per cui richiede il reset password
    b. digitare il numero **0** (zero) per richiedere il reset password.
    c. digitare il numero **1** (uno) per confermare il reset password o il numero **2** (due) per annullare l'operazione.

Se il cliente effettua più volte consecutive il reset password, deve sempre usare l'ultima password ricevuta via SMS per effettuare l'accesso.

RESET DEL PIN DI PLAINPAY E DEL TOKEN VIRTUALE

Il cliente può richiedere il reset del PIN di PlainPay e del Token Virtuale contattando la filiale della propria Banca.

BLOCCO DELL'ACCESSO

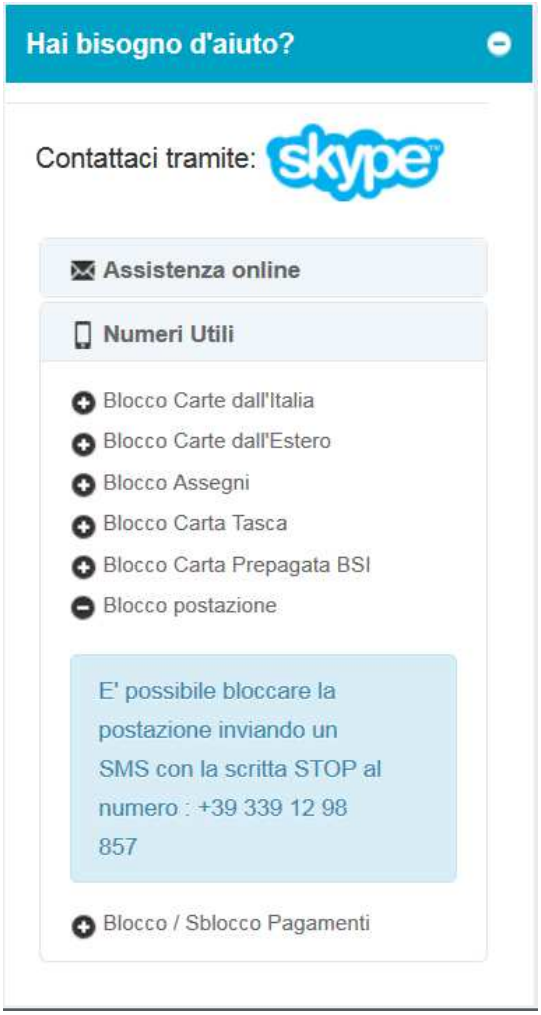
Per rendere più sicuri i servizi a distanza sono previste due modalità di blocco:

- blocco volontario
- blocco automatico

In entrambi i casi lo sblocco potrà essere effettuato, per ragioni di sicurezza, rivolgendosi alla filiale della propria Banca o eseguendo il reset password.

Blocco volontario: il cliente può bloccare volontariamente l'accesso al servizio :

- inviando un SMS (al numero e con la sintassi indicati nella sezione Numeri Utili):

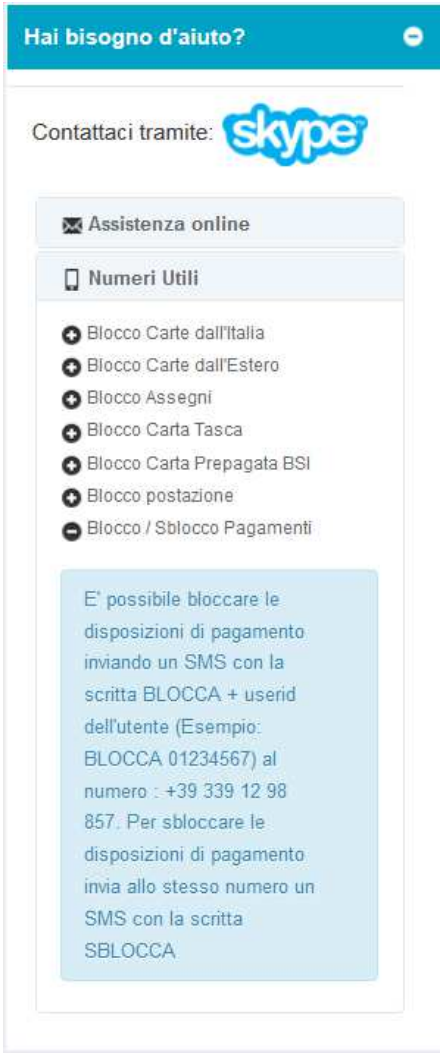


- effettuando 5 accessi consecutivi errati, cioè inserendo volontariamente la corretta userid ma una password di accesso errata;
- contattando la filiale della propria Banca.

Blocco automatico: nel caso in cui per 5 volte consecutive vengano effettuati accessi errati, cioè inserendo la userid corretta ma la errata password di accesso, il sistema bloccherà automaticamente il servizio.

BLOCCO/SBLOCCO DELL'INVIO DELLE DISPOSIZIONI

Per rendere più sicuri i servizi a distanza il cliente può effettuare in piena autonomia il blocco dell'invio delle disposizioni e lo sblocco inviando un SMS (al numero e con la sintassi indicati nella sezione Numeri Utili):



FURTO/SMARRIMENTO DELLE SICUREZZE E DEI CODICI DI ACCESSO

Nel caso in cui il cliente **non ricordi la userid**, che insieme alla password di accesso costituiscono le credenziali preliminari di accesso al servizio, tale codice può essere recuperato sul contratto o, se non fosse possibile, recandosi presso la filiale della propria Banca.

Nel caso in cui il cliente **non ricordi la password di accesso**, che insieme alla userid di accesso costituiscono le credenziali preliminari di accesso al servizio, tale codice può essere recuperato effettuand un reset password o, se non fosse possibile, recandosi presso la filiale della propria Banca.

Nel caso di **furto o smarrimento dello smartphone** (sul quale è installata l'APP PlainPay o il Token virtuale) **o del Token Fisico** al cliente si consiglia di effettuare il blocco dell'acceso al servizio e di rivolgersi alla filiale della propria Banca.
La Banca, a seconda dei casi e dopo le opportune verifiche, potrà effettuare:

- la disattivazione del Token Fisico rubato/smarrito fornendo al cliente un nuovo Token Fisico;
- reset/disattivazione del PlainPay. In questo caso si vorrà mantenere questa sicurezza il cliente dovrà eseguire la procedura di attivazione (scaricare l'APP, configurarla, ecc…);

- reset/disattivazione del Token virtuale. In questo caso si vorrà mantenere questa sicurezza il cliente dovrà eseguire la procedura di attivazione (scaricare l'APP, configurarla, ecc…);

Nel caso in cui la chiavetta token non dovesse più funzionare rivolgersi in filiale, la quale provvederà ad assegnarti una nuova chiavetta; sarà necessario in seguito eseguire nuovamente il primo accesso tramite Internet o telefono e creare un nuovo codice PIN.

TECNOLOGIA E SICUREZZA

REQUISITI E TECNOLOGIE

Per poter usufruire del servizio via Internet è sufficiente disporre di un normale collegamento telefonico ADSL, di un personal computer corredato di modem e di un collegamento a Internet tramite un Internet Service Provider a scelta (con spese di collegamento telefonico a carico del chiamante).

I **requisiti di navigazione** sono:
- Internet Explorer 10.0 su sistemi operativi Windows 7 o superiori;
- Firefox 35 e superiori su sistemi operativi Windows 7 o superiori;
- Chrome 39 e superiori su sistemi operativi Windows 7 o superiori;
- Safari 8 o superiori s sistema operativo Macintosh OS X vers. 10.10 o superiore;
- Chrome 18 o superiori per sistemi Android 4.4+;
- Safari 8 e superiori per sistemi iOS 7 o superiori.

Gli **applicativi necessari** sono:
- Acrobat Reader 9.0 (o versioni superiori);
- WinZip;
- Flash Player 9.0 o superiori.

Risoluzione:
Sito ottimizzato per la risoluzione 1366x768 ma realizzato nella sua quasi totalità in tecnologia full responsive e, quindi, in grado di essere fruito dalla più diverse risoluzioni (ad esempio quelle tipiche di dispositivi smartphone e tablet).

Connessione Internet:
ADSL, UMTS o superiori, in condizioni di connessione minima garantita dal singolo operatore.

Per poter usufruire del servizio via Mobile è sufficiente disporre di un dispositivo mobile (smartphone o tablet) con sistema operativo iOS, Android, BlackBerry e WindowsPhone con un semplice collegamento di rete (rete dati o WiFi).

Le **versioni minime dei sistemi operativi mobile** sono:
- iOS 8.3 e successivi per iPhone;
- Android 4.1 e successivi;
- Windows Phone 8.1 e successivi.

SICUREZZA IN FASE DI ACCESSO ED INVIO DELLE DISPOSIZIONI

Oltre alla *password di accesso*, definitiva dal cliente in fase di primo collegamento (vedi il paragrafo *PRIMO ACCESSO AL SERVIZIO*), ognuno dei seguenti strumenti di sicurezza, che ad eccezione del Token Fisico sono attivabili dal cliente attraverso il Profilo di Sicurezza (vedi il paragrafo *PROFILO DI SICUREZZA*), è una strong-authentication conforme all'orientamento EBA usato dal cliente sia per autenticare l'accesso sia per autorizzare l'invio delle disposizioni:

- *PlainPay*
- *Token Virtuale*
- *Token Fisico*

In aggiunta ai sopra elencati strumenti di strong-authentication, il cliente può configurare in autonomia (vedi il paragrafo *PROFILO DI SICUREZZA*) anche i seguenti strumenti di notifica:

- Notifiche via SMS e/o via e-mail degli accessi effettuati
- Notifiche via SMS e/o via e-mail delle disposizioni inviate

Il paniere di tali strumenti di sicurezza e le relative obbligatorietà sono definite dalla Banca, quindi in caso di necessità di informazioni il cliente deve rivolgersi alla filiale della propria Banca.

PASSWORD DI ACCESSO

La password di accesso è un codice utilizzato esclusivamente per la validazione dell'accesso al servizio (Internet e Mobile) che viene definito dal cliente in fase di primo collegamento (la *password iniziale* usata nel primo collegamento viene invece generata dalla Banca e consegnata direttamente al cliente al completamento della sottoscrizione del contratto).

Le caratteristiche della password di accesso sono:

- viene definita dal cliente in fase di primo collegamento
- può essere composta da cifre, numeri e un set di caratteri speciali
- può avere una lunghezza compresa tra 8 e 24 caratteri

La Banca, per questioni normative, attribuisce alla password di accesso una scadenza di validità. Superato il periodo di validità, al primo collegamento con password di accesso scaduta, il cliente dovrà cambiare la password ridefinendone una nuova che non può essere uguale alle ultime cinque password utilizzate.

Il cliente può in qualunque momento ridefinire la password di accesso usando l'apposita funzione disponibile nell'Home Banking (Internet e Mobile).

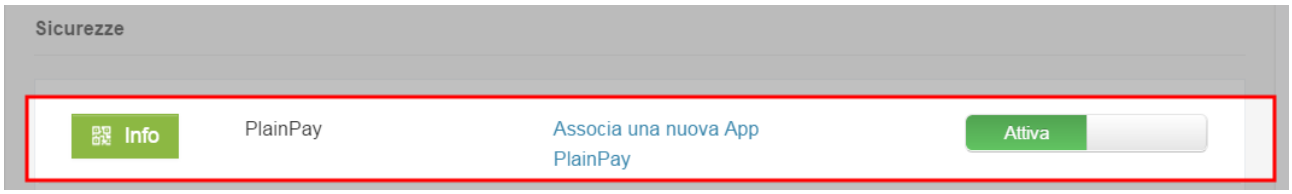
PLAINPAY

PlainPay è l'APP nativa sviluppata da Auriga S.p.A. che il cliente può scaricare sul proprio smartphone (https://secure.plainpay.it/verifica) e configurare come strumento di strong authentication per autenticare l'accesso al servizio (Internet e Mobile) ed autorizzare l'invio delle disposizioni.

Progettata per funzionare sui principali sistemi operativi utilizzati dagli smartphone, PlainPay è disponibile per i dispositivi iPhone e Android ed è uno strumento in grado di sostituire o affiancare gli altri sistemi di sicurezza attualmente presenti sul mercato (es. token), garantendo maggiore economicità, praticità e sicurezza.

Sfruttando la tecnologia QR Code, che usa la fotocamera dello smartphone per acquisire e trasferire informazioni senza inserire dati sulla tastiera, e la capacità di colloquiare con l'Home Banking, PlainPay rende l'autenticazione ancora più forte fornendo al cliente informazioni aggiuntive non disponibili con gli strumenti di sicurezza attualmente presenti sul mercato.
In questo caso ai punti di forza sopra esposti si aggiunge il vantaggio di contrastare gli attacchi di tipo Man-In-The-Browser (MITB). Infatti, i dati sensibili della disposizione sono riepilogati nell'App PlainPay in modo che l'utente possa averne evidenza prima che la stessa venga spedita, inoltre la validazione dei dati sensibili della disposizione è sottoposta ad ulteriore autorizzazione da parte del cliente che inserendo il PIN PlainPay (definito in fase di attivazione) ne conferma l'autenticità.

Il cliente che desidera attivare PlainPay quale strumento di strong-authentication dovrà scaricare l'APP dal relativo market (AppStore per gli utenti iPhone, Google Play per gli utenti Android), attivarla sullo smartphone seguendo una semplice procedura guidata e associarla alla postazione Home Banking utilizzando una specifica funzione disponibile sul Profilo di Sicurezza.



Completato il processo di attivazione e associazione, ogni volta che il cliente effettuerà l'accesso dovrà semplicemente lanciare l'APP Plainpay sul proprio smartphone e catturare (schermo dello smartphone) il QR Code - one shot che gli verrà presentato, quindi confermare l'operazione inserendo sull'APP il PIN PlainPay.

Analogamente, ogni volta che il cliente autorizzerà l'invio di una disposizione, dopo aver confermato i dati della disposizione dovrà semplicemente lanciare l'APP PlainPay sul proprio smartphone e catturare il QR Code - one shot che gli verrà presentato, controllare che le informazioni relative alla disposizione da autorizzare presentate sul display dell'app siano corrispondenti ai dati inseriti sull'Home banking, quindi confermare l'invio della disposizione inserendo sull'APP il PIN PlainPay.

PlainPay (nella modalità "QR Code") è una funzionalità alternativa all'utilizzo del Token Fisico e del Token Virtuale.

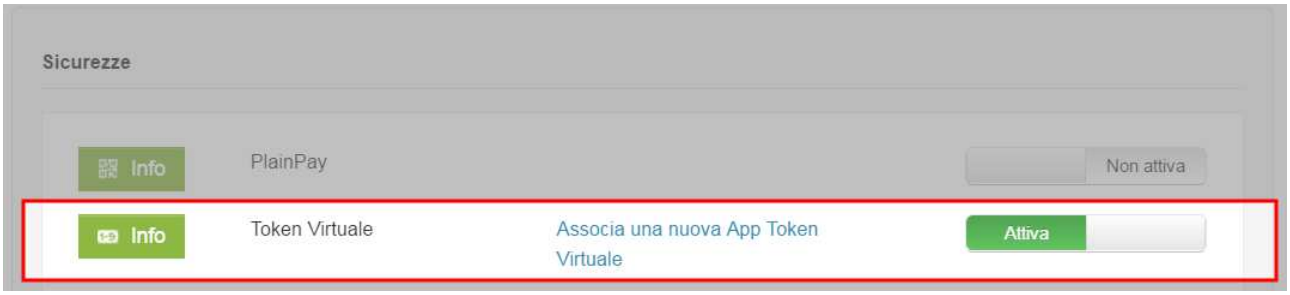
TOKEN VIRTUALE

Il Token Virtuale è uno strumento di strong-authenticaton che ha lo scopo di utilizzare l'APP PlainPay come generatore di password temporanee (OTP – One Time Password) della durata di 30 secondi, utili a validare l'accesso al servizio ed autorizzare l'invio delle disposizioni.

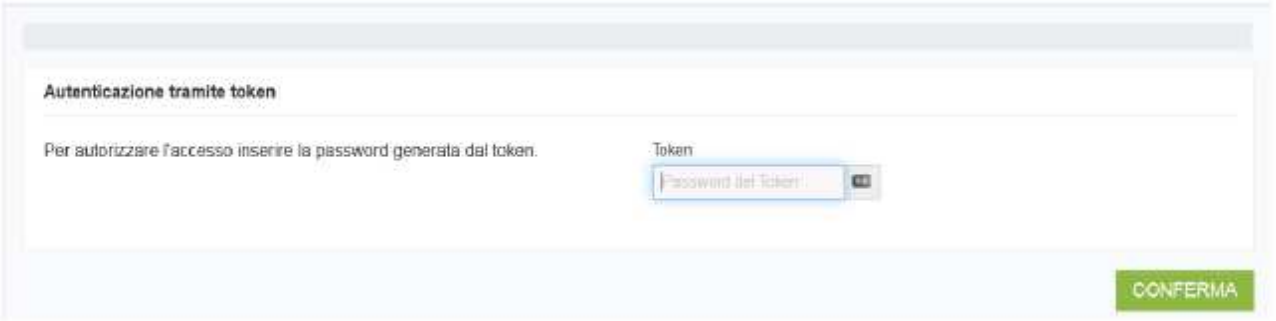
Il cliente, dopo aver scaricato, attivato e associato l'APP PlainPay, potrà così utilizzare l'APP PlainPay per generare password temporanee sia in modalità on-line sia in modalità off-line (assenza di connessione dati o wi-fi), come se utilizzasse un dispositivo token fisico tradizionale.

La funzionalità di Token Virtuale è alternativa all'utilizzo del Token Fisico e del PlainPay (nella modalità "QrCode").

Il cliente che desidera attivare il Token Virtuale quale strumento di strong-authentication dovrà scaricare l'APP PlainPay dal relativo market (AppStore per gli utenti iPhone, Google Play per gli utenti Android), attivarla sullo smartphone seguendo una semplice procedura guidata e associarla alla postazione Home Banking utilizzando una specifica funzione disponibile sul Profilo di Sicurezza.



Completato il processo di attivazione e associazione (quest'ultimo necessita una connessione dati o wi-fi dello smartphone in quanto richiede di inquadrare un QR Code e trasmettere dati), ogni volta che il cliente effettuerà l'accesso dovrà semplicemente lanciare l'APP Plainpay sul proprio smartphone ed inserire nell'Home Banking la password temporanea one-shot generata dall'APP.



I clienti abilitati al servizio via Mobile utilizzeranno la modalità standard della sicurezza PlainPay (con inserimento del PIN PlainPay) sia per l'autenticazione dell'accesso sia per l'autorizzazione dell'invio delle disposizioni.

TOKEN FISICO

Il Token Fisico è uno strumento di strong-authenticaton attivato dalla Banca che, mediante un dispositivo hardware (token) delle dimensioni di un portachiavi, genera password temporanee (OTP – One Time Password) numeriche univoche per ogni sessione/matricola di token, utili a validare l'accesso al servizio ed autorizzare l'invio delle disposizioni.

Le OTP sono di tipo time-synchronized. Le nuove OTP generate dal token hanno validità temporale ristretta (dai 30 secondi a 1 minuto).

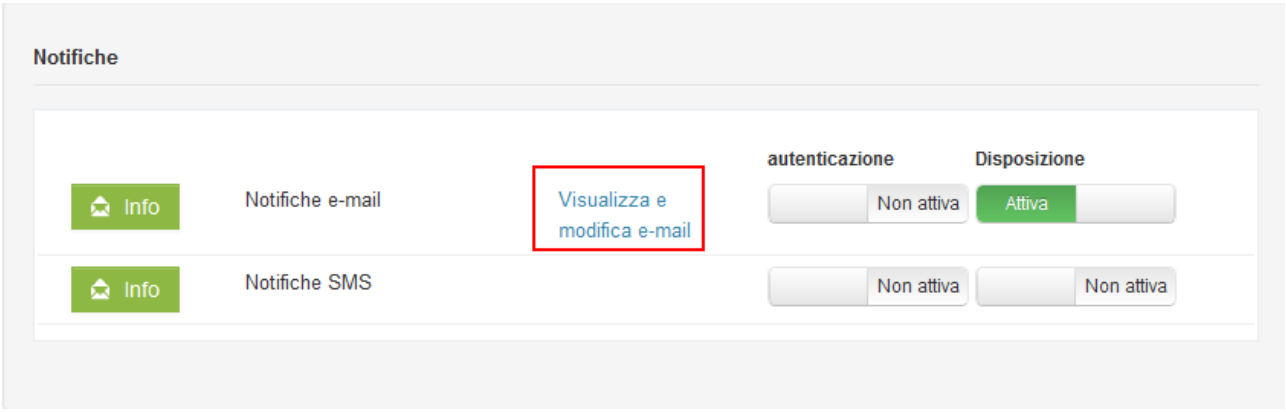
Il token è quindi sincronizzato a distanza con il server di autenticazione che, in quella data ora, genera una stringa numerica che sarà confrontata con quella digitata dal cliente e, solo se corrispondono, consentirà l'autenticazione. All'interno del token è presente un accurato orologio che è sincronizzato con l'orologio sul server di autenticazione. Su tali sistemi OTP, il tempo è una parte importante dell'algoritmo di generazione della password.

Il cliente può richiedere l'attivazione del Token Fisico solo recandosi presso la filiale della propria Banca.

Completato il processo di attivazione (in filale/Banca), ogni volta che il cliente effettuerà l'accesso dovrà semplicemente generare una OTP sul token ed inserire nell'Home Banking la password temporanea one-shot generata.

NOTIFICHE EMAIL

Tale strumento consente, mediante la ricezione di e-mail all'indirizzo mail configurato, di monitorare le disposizioni inviate e/o gli accessi effettuati.
Attivato questo strumento di sicurezza, è sempre possibile per il cliente visualizzare e modificare il l'indirizzo e-mail su cui ricevere le e-mail:



Attivando la notifica di tipo Autenticazione, il cliente riceverà una e-mail ad ogni:

- primo collegamento
- accesso andato a buon fine
- tentativo di accesso non andato a buon fine
- collegamento in seguito al reset password
- collegamento in seguito alla scadenza delle password
- blocco della postazione in seguito al raggiungimento del numero massimo dei login permessi
- attivazione, modifica o disattivazione di uno degli strumenti previsti nel profilo di sicurezza

Nell'e-mail sono riepilogate le seguenti informazioni (in base al tipo di notifica):

- la data e ora del collegamento
- il codice di accesso (mascherato) della postazione (userid)
- l'intestatario della postazione
- l'indirizzo ip della connessione e la corrispondente nazione di provenienza

Attivando la notifica di tipo Disposizione, il cliente riceverà una e-mail dopo aver autorizzato l'invio di una disposizione. Nell'e-mail sono riepilogate le informazioni principali relative alla disposizione:

- la data di spedizione della disposizione/distinta
- il codice di accesso (mascherato) della postazione (userid)
- l'intestatario della postazione
- la tipologia della disposizione/distinta
- il numero della disposizione/distinta
- per ogni disposizione della distinta:
  - il numero della disposizione
  - la tipologia della disposizione
  - l'importo e la divisa
  - il codice ABI del conto corrente dell'ordinante
  - il conto corrente (mascherato) di addebito
  - le IBAN del beneficiario
  - il nominativo del beneficiario

NOTIFICHE SMS

Tale strumento consente, mediante la ricezione di SMS al numero di cellulare configurato, di monitorare le disposizioni inviate e/o gli accessi effettuati.
Attivato questo strumento di sicurezza, è sempre possibile per il cliente visualizzare e modificare il numero di cellulare su cui ricevere l'SMS:

Attivando la notifica di tipo Autenticazione, il cliente riceverà un SMS ad ogni:

- primo collegamento
- accesso andato a buon fine
- tentativo di accesso non andato a buon fine
- collegamento in seguito al reset password
- collegamento in seguito alla scadenza delle password
- blocco della postazione in seguito al raggiungimento del numero massimo dei login permessi
- attivazione, modifica o disattivazione di uno degli strumenti previsti nel profilo di sicurezza

Nell'SMS viene riportata la data e ora dell'accesso o tentato accesso.

Attivando la notifica di tipo Disposizione, il cliente riceverà un SMS dopo aver autorizzato l'invio di una disposizione. Nell'SMS sono riepilogate le informazioni principali relative alla disposizione:

- la tipologia della disposizione

- la data di spedizione della disposizione
- il conto corrente (mascherato) di addebito
- l'importo della disposizione
- l'IBAN del beneficiario (solo nel caso di disposizione di bonifico singolo)
- il numero della distinta e il numero delle disposizioni della distinta (solo per distinte F24).

SERVIZI VIA INTERNET

INDIRIZZI WEB

L'accesso al servizio via Internet avviene dalla Homepage della Banca disponibile al seguente link https://bancaincasa.sba.bcc.it/XXXXX (dove XXXXX è il codice ABI della Banca).

PROFILATURA UTENTE

Il servizio di Internet Banking, a seconda della specifica esigenza operativa del cliente, viene profilato dalla Banca in sede di attivazione del servizio e può essere modificato dalla Banca su richiesta del cliente.
Ciascuno dei seguenti profili permette al cliente di operare, in termini di utilizzo di funzionalità informative e dispositive, sui rapporti di conto abilitati alla postazione:

- **Retail Informativo**: per clienti privati, permette l'utilizzo delle sole funzioni informative (es. Lista movimenti, ecc…);
- **Retail Dispositivo:** per clienti privati, permette l'utilizzo delle funzioni informative (es. Lista movimenti, ecc…) e dispositive (es. Bonifico, ecc..);
- **Business Informativo:** per clienti aziende, permette l'utilizzo delle sole funzioni informative (es. Lista movimenti, ecc…);
- **Business dispositivo senza portafoglio:** per clienti aziende, permette l'utilizzo delle funzioni informative (es. Lista movimenti, ecc…) e dispositive (es. Bonifico, ecc..), ma non delle funzioni dispositive di incasso (es. Presentazione RiBA, MAV, SDD, …) e l'F24 per commercialisti;
- **Business dispositivo:** per clienti aziende, permette l'utilizzo delle funzioni informative (es. Lista movimenti, ecc…) e dispositive (sia di pagamento es. Bonifico, sia di incasso es. Presentazione RiBA, MAV, SDD, …), ma non dell'F24 per commercialisti;
- **Business dispositivo full**: per clienti aziende, permette l'utilizzo delle funzioni informative (es. Lista movimenti, ecc…) e dispositive (sia di pagamento es. Bonifico, sia di incasso es. Presentazione RiBA, MAV, SDD, …), compreso l'F24 per commercialisti;
- ***Tesorerie*:** per i clienti enti locali, permette la gestione finanziaria dell'ente locale in termini di riscossione delle entrate, pagamento delle spese, custodia dei titoli e valori ed agli adempimenti connessi previsti dalla legge, dallo statuto e dai regolamenti dell'ente.

FUNZIONALITA' SPECIFICHE

Di seguito, per i principali 3 profili (Reatil, Business e Tesorerie) sono elencate le funzionalità (informative e dispositive) che il cliente potrà utilizzare per operare sui rapporti agganciati alla propria postazione.

FUNZIONI RETAIL

SALDI E MOVIMENTI
◦Movimenti in euro e in divisa
◦Posizione cliente
◦Saldi titoli con dettaglio movimenti, ordini e movimenti, nota informativa
◦Dossier titoli - Flussi finanziari
◦Dossier titoli - Storico ordini
◦Dossier titoli - Disponibilità C/C
◦Dossier titoli - Saldi e analisi
◦Situazione mutuo
◦Situazione assegni
◦Utenze domiciliate
◦Certificati di Deposito
◦Gestioni Patrimoniali
◦Situazione posizione estero
◦Movimenti posizione estero

COMUNICAZIONI
◦Comunicazioni con la banca (invio e ricezione messaggi)

PAGAMENTI
◦Bonifico singolo
◦Giroconto
◦Bollettino RAV
◦Bollettino MAV
◦Bollettino bancario Freccia
◦F24 (modello base, modello Accise, modello Elementi identificativi, modello semplificato)
◦Bonifico Sepa
◦Bonifico Assegno (SEPA)
◦Bonifico ristrutturazione
◦Bonifico urgente (SEPA)
◦Bollettino premarcato
◦Bollettino bianco
◦Bollettino ACI
◦Avvisi pagamento
◦Pagamento effetti
◦Bollettino CBILL

◦Bonifico estero

RICARICHE
◦Ricarica Cellulare
◦Ricarica Carta Tasca
◦Ricarica Mediaset Premium
◦Carta Ricarica

CORRISPONDENZA ON-LINE
◦Posta raccomandata
◦Posta prioritaria
◦Telegramma

ARCHIVIO
◦Bonifici
◦Bonifici ordinari (SEPA)
◦Giroconti
◦Ricariche cellulari
◦Ricariche Carta Tasca
◦Ricariche Mediaset Premium
◦Bollettino RAV
◦Bollettino MAV
◦Bollettino bancario Freccia
◦Bollettino premarcato
◦Bollettino bianco
◦Bollettino ACI
◦F24 (modello base, modello Accise, modello Elementi identificativi, modello semplificato)
◦Lista CRO
◦Avvisi pagamento
◦Pagamento effetti
◦Raccomandate
◦Posta prioritaria
◦Telegrammi
◦Bollettino CBILL
◦Beneficiari
◦Bonifico Estero
◦Quietanze F24

SICUREZZA
◦Profilo sicurezza
◦Cambio password
◦Attivazione notifiche

DOCUMENTI ON-LINE

◦Archivio documenti

SIMPLYSMS
◦Impostazioni
◦Alert
◦Nuovo alert

UTILITÀ
◦Ricerca ABI/CAB
◦Massimali
◦Coordinate IBAN
◦Listino cambi
◦Listino titoli
◦Variazioni anagrafiche
◦Simulazione mutuo
◦Altri servizi
◦Associazione Conti PlainPay
◦Controllo Assegni in PASS
◦Configurazione rapporti

CONTO DEPOSITO
◦Alimentazione
◦Trasferimento
◦Movimenti
◦Vincolo
◦Storico vincoli
◦Conto Predefinito

FUNZIONI BUSINESS

SALDI E MOVIMENTI
◦Movimenti in euro e in divisa
◦Posizione cliente
◦Saldi titoli - comprensiva di DT CBI, informative titoli e disponibilità c/c collegato, con possibilità di acquisto/vendita titoli
◦Situazione mutuo
◦Situazione assegni
◦Utenze domiciliate
◦Certificati di deposito - situazione attuale e operazioni scadute
◦Gestioni Patrimoniali
◦Saldi e analisi - comprensiva di grafico e disponibilità c/c collegato
◦Flussi finanziari - comprensiva di grafico e disponibilità c/c collegato
◦Situazione posizione estero
◦Movimenti posizione estero

COMUNICAZIONI
◦Comunicazioni con la banca (invio e ricezione messaggi)

PAGAMENTI
◦Bonifico singolo
◦Giroconto
◦Bollettino RAV
◦Bollettino MAV
◦Bollettino bancario Freccia
◦F24 (modello base, modello Accise, modello Elementi identificativi, modello semplificato)
◦Bonifico Sepa
◦Bonifico Assegno (SEPA)
◦Bonifico ristrutturazione
◦Bonifico urgente (SEPA)
◦Bollettino premarcato
◦Bollettino bianco
◦Bollettino ACI
◦Avvisi pagamento
◦Pagamento effetti
◦Bollettino CBILL
◦Bonifico estero
◦Distinta F24
◦Distinta bonifici SEPA
◦Distinta bonifici esteri
◦Movimenti POS
◦Girofondo
◦Distinta girofondi

RICARICHE
◦Ricarica Cellulare
◦Ricarica Carta Tasca
◦Ricarica Mediaset Premium
◦Carta Ricarica

CORRISPONDENZA ON-LINE
◦Posta raccomandata
◦Posta prioritaria
◦Telegramma

ARCHIVIO
◦Bonifici
◦Bonifici ordinari (SEPA)
◦Distinta bonifici SEPA

◦Giroconti
◦Ricariche cellulari
◦Ricariche Carta Tasca
◦Ricariche Mediaset Premium
◦Bollettino RAV
◦Bollettino MAV
◦Bollettino bancario Freccia
◦Bollettini Postali
◦Bollettino ACI
◦Deleghe F24
◦Lista CRO
◦Avvisi pagamento
◦Pagamento effetti
◦Bollettino CBILL
◦Raccomandate
◦Posta prioritaria
◦Telegrammi
◦Beneficiari
◦Ordini - comprensiva di disponibilità c/c collegato
◦Quietanze F24
◦Bonifici Esteri
◦Pronti contro termine
◦Utenze telefoniche
◦Utenze Carta Tasca
◦Utenze Mediaset Premium
◦Avvisatura bonifici - Avvisature ricevute
◦Storico istruzioni
◦Contribuenti
◦Disposizioni
◦RiBa
◦RID
◦MAV
◦Fatture
◦SDD
◦Debitori
◦Beneficiari esteri
◦Anticipo Fattura

SICUREZZA
◦Profilo sicurezza
◦Cambio password
◦Attivazione notifiche
◦Notifiche operative

DOCUMENTI ON-LINE
◦Archivio documenti
◦Lista documenti dei movimenti

SIMPLYSMS
◦Impostazioni
◦Alert
◦Nuovo alert
◦SMS inviati dalla Banca
◦SMS Ricevuti dalla banca

UTILITÀ
◦Ricerca ABI/CAB
◦Massimali
◦Coordinate IBAN
◦Listino cambi
◦Listino titoli
◦Variazioni anagrafiche
◦Simulazione mutuo
◦Altri servizi
◦Associazione Conti PlainPay
◦Controllo Assegni in PASS
◦Configurazione rapporti
◦Bilancio familiare
◦Export flussi CBI
◦Calendario con scadenziario
◦Impostazioni/Profilo utente
◦Funzioni preferite
◦Ricerca voce di menu

CONTO DEPOSITO
◦Alimentazione
◦Trasferimento
◦Movimenti
◦Vincolo
◦Storico vincoli
◦Conto Predefinito

TRADING
◦Ricerca titoli (con possibilità di acquisto/vendita)
◦Monitor ordini (con possibilità di revoca)
◦Compravendita titoli

PORTAFOGLIO
◦RIBA
◦Richiamo RiBa
◦Rendicontazione Portafoglio

◦Situazione effetti
◦Situazione Portafoglio
◦Esiti di portafoglio
◦RID
◦Richiamo Rid
◦Variazione coordinate RID
◦MAV
◦Richiamo Mav
◦Fatture
◦Rendicontazione conti anticipi
◦Esiti RAV/MAV
◦Mov. disposizioni portafoglio
◦Esiti bollettini
◦Allineamento archivi
◦SDD
◦Seda allineamento archivi

MULTIUTENZA
◦Code transazioni (Autorizzazione disposizioni)
◦Gestione sicurezza
◦Gestione utente secondario
◦Elenco utenti secondari

FATTURAZIONE ELETTRONICA E FATTURA PER PUBBLICA AMMINISTRAZIONE
◦Fattura PA - Invio fatture ad iniziativa Azienda Fornitore
◦Fattura PA - Lista e dettaglio fatture PS (attivo)
◦Fattura PA - Esiti
◦Fattura PA - Ricezione fatture da parte della PA
◦Fattura PA - Lista e dettaglio fatture
◦Anticipo Fattura

DOCUMENTI NON STRUTTURATI
◦Perizie - invio con dettaglio
◦Perizie - storico perizie inviate (dettaglio, elimina, firma, scarica)
◦Perizie - storico perizie ricevute

FUNZIONI TESORERIE

TESORERIE
◦Mandati e reversali
◦Provvisori
◦Lista sospesi di pagamento
◦Lista incassi/pagamenti
◦Bilancio consuntivo

◦Situazione saldi Ente
◦Import Ordinativo Informatico
◦Storico mandati e reversali
◦Ricerca sub-beneficiari
◦Import bonifici per stipendi
◦Lista documenti
◦Verifica di cassa

ASSISTENZA

Il cliente può contattare il servizio di HelpDesk al numero verde riportato sul contratto, sulla Homepage di accesso e all'interno del Home Banking.

L'assistenza di tipo Help Desk viene comunque erogata anche attraverso i seguenti canali:

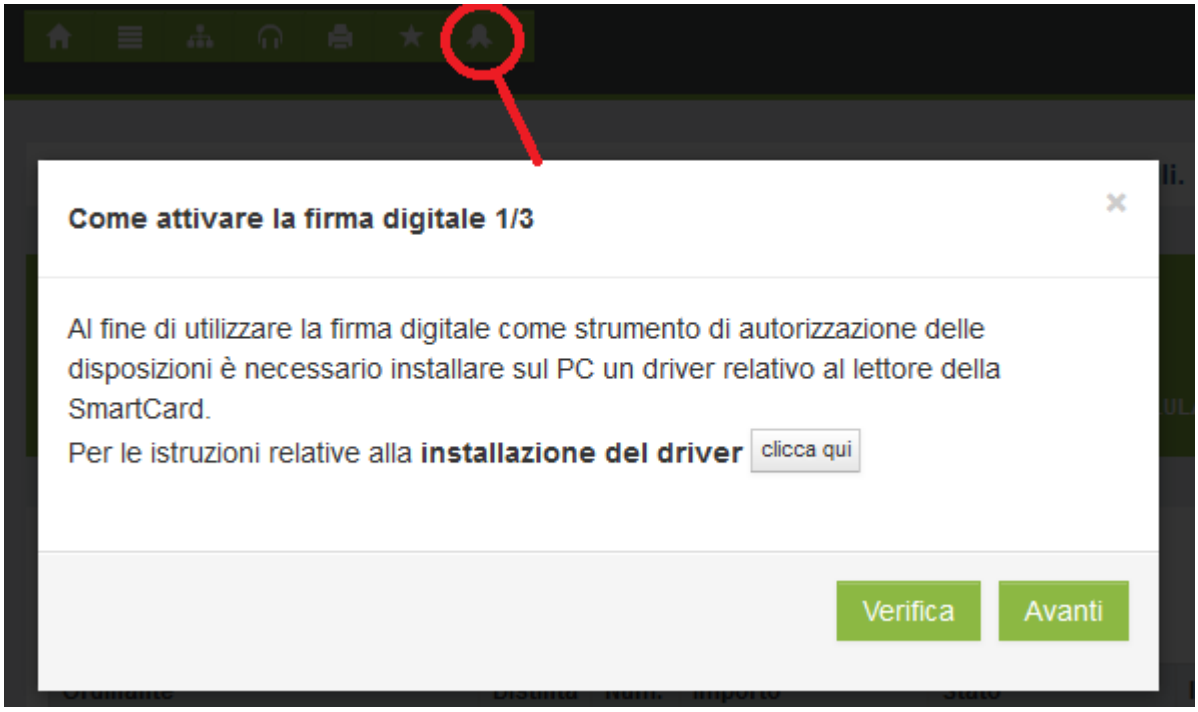
- **E-mail** : disponibile solo per il servizio via Internet, permette ai clienti che dispongono di un account di posta elettronica, di ricevere dall'operatore dell'HelpDesk le risposte alle richieste di informazioni inserite nell'apposita sezione "Assistenza online" disponibile nella pagina di benvenuto:

- **Skype** : permette ai clienti, che hanno installato e attivato Skype sul proprio desktop-pc, computer portatile e smartphone, di effettuare una chiamata telefonica via Internet all'operatore dell'Help Desk;
- **WhatsApp** : disponibile solo per il servizio via Mobile, permette ai clienti che hanno installato e attivato l'APP WhatsApp sul proprio smartphone, di inviare messaggi all'operatore dell'HelpDesk e ricevere risposte.

FIRMA DIGITALE

La firma digitale è uno strumento di autorizzazione dell'invio delle disposizioni attualmente disponibile nella versione Internet per la spedizione in banca delle disposizioni di tipo OI (Ordinativo Informatico) nell'ambito delle Tesorerie.

Per poter utilizzare la firma digitale è necessario innanzitutto che il cliente si rivolga alla propria Banca, che provvederà a profilare la postazione per l'utilizzo di tale strumento, e successivamente segua la procedura (in 3 step) descritta nell'apposita sezione accessibile dall'icona disponibile nella parte alta della pagina di benvenuto.



Cliccando su "cliacca qui" è possibile scaricare anche un documento.

Dopo aver installato e configurato la firma digitale e averne verificato il corretto funzionamento mediante l'apposita funzione disponibile dal tasto "Verifica", il cliente può autorizzare l'invio delle disposizioni di tipo OI (Ordinativo Informatico).

In fase di autorizzazione verrà richiesto al cliente di inserire la smartcard nel lettore e premere "Firma" dopo aver digitato il PIN della smartcard.

Inserite le corrette informazioni, la procedura provvederà in automatico all'estrazione dalla smartcard delle informazioni utili al firma della disposizione e all'invio in banca della disposizione firmata.

LIMITI ORARI (CUT-OFF) E LIMITI DI IMPORTO (MASSIMALI)

Nell'invio delle disposizioni in Banca sono previsti dei limiti sia orari che di importo.

I limiti orari (cut-off) sono impostati dalla propria Banca per poter elaborare le disposizioni entro i tempi previsti dalle procedure bancarie e CBI. Superati questi limiti, il cliente dovrà indicare come data di esecuzione della disposizione, una data successiva.

I limiti di importo (massimali) sono impostati dalla propria Banca e resi noti al momento della sottoscrizione del contratto. Tali limiti impongono un tetto massimo sull'importo delle disposizioni (di pagamento e ricarica) che il cliente può autorizzare dal canale Internet e Mobile. Tali limiti possono essere diversi per tipologia di disposizione. Per conoscere tali limiti, riportati comunque sul contratto sottoscritto in Banca, il cliente può usare l'apposita funzione "Massimali" disponibile tra le funzioni di utilità. Per modificare i limiti di importo il cliente deve rivolgersi alla propria Banca.

ANNULLO E STORNO DELLE DISPOSIZIONI

Le disposizioni di tipo Bonifico Italia, Stipendio, Giroconto, Girofondo, Bonifico estero, Deleghe F24, SDD e SEDA autorizzate dal canale Internet possono essere annullate dal cliente mediante l'apposita funzione resa disponibile nell'Archivio specifico delle disposizione, purchè tale annullo venga effettuato in brevissimo tempo, cioè prima che la fase automatica della procedura di contabilizzazione (che elabora e spedisce in Banca la disposizione) venga eseguita.

Nel caso in cui il cliente riesca ad annullare la disposizione prima che questa venga contabilizzata (cioè elaborata e spedita in Banca), la disposizione non verrà trasmessa in Banca.

Nel caso in cui invece non si riesca ad annullare la disposizione prima che questa venga contabilizzata, il cliente dovrà contattare la propria Banca per richiederne lo storno.

Per le Delega F24, oltre all'annullo, è prevista anche la funzione di storno che permette al cliente di revocare le disposizioni già spedite in Banca ed elaborate dalla Banca.