



# GUIDA AI SERVIZI ONLINE DEL BANCO DESIO

DWeb Banking  
DMobile Banking

Documentazione destinata all'uso  
da parte dei clienti DWeb e DMobile.

Riproduzione ed uso riservati.

Tutte le immagini sono inserite a scopo  
illustrativo, i prodotti possono subire variazioni.

## Indice

INDICE.....	3
PRESENTAZIONE DEI SERVIZI .....	3
DWeb: più servizi on line, più tempo per te. ....	3
Prodotti e servizi offerti. ....	4
DWeb Banking Light. ....	4
DWeb Banking. ....	4
DWeb Trade. ....	4
DMobile Banking. ....	5
Riepilogo delle funzionalità dei prodotti DWeb .....	5
Sistemi di sicurezza .....	7
Requisiti minimi di sistema .....	8
Requisiti dispositivi Mobile .....	8
Consigli per la tua sicurezza .....	9
APP DMOBILE .....	11
SCARICARE L'APP DALLO STORE .....	11
ATTIVAZIONE DELLO SMARTOTP .....	12
ACCESSO AL SISTEMA DWEB .....	14
Mediante SmartOTP dal portale Web.....	14
ACCESSO AL SISTEMA DMOBILE .....	17
Mediante Smart OTP da App .....	17
CONVALIDA DELLE OPERAZIONI ESEGUITE IN DWEB.....	17
Mediante SmartOTP da portale web .....	17
CONVALIDA DELLE OPERAZIONI DA ESEGUITE DA DMOBILE .....	18
Autorizzazione delle disposizioni mediante Smart OTP da App .....	18
ASSISTENZA CLIENTI.....	19
Accesso al servizio.....	19

## Presentazione dei servizi

### DWeb: più servizi on line, più tempo per te.

Consentirti di accedere ad una vasta gamma di servizi nel modo più semplice, in ogni momento e ovunque ti trovi: questo è l'obiettivo di DWeb, la nuova offerta di servizi online che il Gruppo Banco Desio mette a tua disposizione.

Con DWeb avrai la possibilità di effettuare un'ampia serie di operazioni bancarie, informative e dispositive, in modo semplice e sicuro, utilizzando i seguenti canali:

1. PC (DWeb);
2. Smartphone (DMobile);

Scegli tu come: il tuo computer, il tuo smartphone. In ogni caso, i servizi DWeb ti consentiranno di avere sempre a “portata di mano” la tua banca.

## **Prodotti e servizi offerti.**

### ***DWeb Banking Light.***

Se desideri avere la possibilità di controllare on line, in ogni momento, i tuoi rapporti bancari e la tua documentazione, puoi richiedere DWeb Light. Attraverso questo servizio potrai essere sempre aggiornato in tempo reale sui tuoi principali rapporti in assoluta sicurezza.

Consulta la tabella sottostante per verificare le funzionalità disponibili in DWeb Light.

### ***DWeb Banking.***

Se desideri un servizio online che ti consenta di monitorare i tuoi rapporti con Banco Desio e che ti offra la possibilità di effettuare una vasta gamma di pagamenti tramite pc e smartphone, in qualunque momento ed ovunque ti trovi, il servizio DWeb è esattamente quello che stai cercando.

Con la garanzia dei più alti standard di sicurezza sul mercato garantiti dalla SCA<sup>1</sup>, potrai effettuare le principali funzioni informative e dispositive con la massima comodità e sicurezza.

Consulta la tabella sottostante per verificare le funzionalità disponibili in DWeb.

### ***DWeb Trade.***

Vuoi un servizio della banca online che ti permetta la massima operatività sui tuoi rapporti presso Banco Desio? I servizi DWeb Trade sono quel che fa per te. Tramite questi servizi e grazie all'elevatissimo standard di sicurezza fornito dalla SCA, potrai effettuare con la massima comodità e sicurezza le principali funzioni informative e dispositive ed essere sempre aggiornato sui principali mercati finanziari ed effettuare il trading on-line sui principali mercati disponibili in totale autonomia.

Inoltre, a seconda delle tue esigenze, potrai scegliere il servizio che più si adatta a te:

- DWeb Trade Base (trading on-line + quotazioni in differita);
- DWeb Trade Avanzato (trading on-line + quotazioni in tempo reale);
- DWeb Trade Plus (trading on-line + quotazioni in tempo reale + book a 5 livelli).

---

<sup>1</sup> Strong Customer Authentication

## **DMobile Banking.**

Se vuoi monitorare i tuoi conti ed ottenere informazioni ed aggiornamenti in tempo reale con la massima comodità, scarica DMobile, la nostra nuova App che ti permetterà di operare in completa autonomia, in ogni momento e da qualunque luogo.

L'app è disponibile per i dispositivi IOS e ANDROID (no tablet).

## **Riepilogo delle funzionalità dei prodotti DWeb**

<b>Funzione</b>	<b>DWeb Light</b>	<b>DWeb</b>	<b>DWeb Trade Base</b>	<b>DWeb Trade avanzato</b>	<b>DWeb Trade plus</b>	<b>DMobile</b>
<i>Dati Personali</i>	x	x	x	x	x	x
<i>Elenco Rapporti</i>	x	x	x	x	x	x
<i>Elenco Rapporti di Default</i>	x	x	x	x	x	x
<i>Limiti Operativi</i>		x	x	x	x	
<i>Attivazione/Modifica Alert SMS</i>		x	x	x	x	
<i>Gestione Credenziali</i>	x	x	x	x	x	x
<i>Help</i>	x	x	x	x	x	x
<i>Messaggi</i>	x	x	x	x	x	x
<i>Elenco Movimenti</i>	x	x	x	x	x	x
<i>Bilancio Sintetico</i>	x	x	x	x	x	x
<i>Estratto Conto Estero</i>		x	x	x	x	x
<i>Assegni</i>	x	x	x	x	x	x
<i>Assegni Estero</i>	x	x	x	x	x	x
<i>Elenco Utenze</i>	x	x	x	x	x	x
<i>Posizione Globale Cliente</i>	x	x	x	x	x	x
<i>Elenco Mandati SDD</i>		x	x	x	x	x
<i>Time Deposit</i>		x	x	x	x	x
<i>Comunicazioni</i>	x	x	x	x	x	x
<i>Documenti Firmati Elettronicamente in Filiale</i>	x	x	x	x	x	
<i>Attivazione E-Commerce</i>		x	x	x	x	x
<i>Posizione Sintetica Titoli</i>		x	x	x	x	x
<i>Situazione Titoli</i>	x	x	x	x	x	x
<i>Titoli In Scadenza</i>	x	x	x	x	x	x
<i>Riepilogo Saldi</i>	x	x	x	x	x	x
<i>Canone Rai (Inquiry Storico)</i>		x	x	x	x	
<i>Finanziamenti</i>	x	x	x	x	x	x
<i>Bonifico Sepa (Italia/Europa)</i>		x	x	x	x	x

<i>Bonifico Urgente</i>		x	x	x	x	
<i>Bonifico Estero (bonifici in divisa e in euro verso paesi extra UE)</i>		x	x	x	x	
<i>Bonifico Ripetitivo</i>		x	x	x	x	x
<i>Acceleratore One Click</i>		x	x	x	x	x
<i>Pagamento F24</i>		x	x	x	x	X°
<i>Ricarica Cellulare</i>		x	x	x	x	x
<i>Ricarica Carta prepagata Nexi Prepaid</i>		x	x	x	x	x
<i>Pagamento Bollettino Postale</i>		x	x	x	x	x
<i>Pagamento MAV</i>		x	x	x	x	x
<i>Pagamento RAV</i>		x	x	x	x	x
<i>Pagamento Bollo Auto (tramite E- Billing/C-Bill/PagoPA)</i>		x	x	x	x	x
<i>Pagamento Bollettini Freccia</i>		x	x	x	x	x
<i>Domiciliazione</i>		x	x	x	x	
<i>E-Billing/C- Bill/PagoPA</i>		x	x	x	x	x
<i>Ri.Ba In Scadenza</i>		x	x	x	x	
<i>Anagrafica</i>		x	x	x	x	x
<i>Valorizzazione Portafoglio in tempo differito</i>			x			x*
<i>Valorizzazione Portafoglio in tempo reale</i>				x	x	x*
<i>Negoziazioni titoli azionari, warrant e covered warrant sui mercati MTA, Euronext, Xetra.Negoziazioni titoli di Stato e obbligazionari Italiani ed esteri sul mercato MOT</i>			x	x	x	x*
<i>Quotazioni mercato azionario Italia in tempo differito</i>			x			x*
<i>Quotazioni mercato azionario Estero in tempo differito</i>			x	x	x	x*
<i>Quotazioni mercato azionario Italia in tempo reale</i>				x	x	x*
<i>Quotazioni mercato obbligazionario MOT</i>			x	x	x	x*

Valorizzazione Watch List in tempo reale				x	x	x*
News			x	x	x	x*
Analisi				x	x	
Book 5 Livelli					x	x*

Figura 1- Riepilogo delle funzionalità dei prodotti DWeb

° Solo per modello F24 Semplificato

\* Funzioni disponibile se il prodotto sottoscritto è DWeb Trade

## **Sistemi di sicurezza**

La sicurezza ed in particolare i presidi atti a garantire la confidenzialità e l'integrità delle comunicazioni è implementata a più livelli come richiesto dalle normative delle autorità bancarie (così detta: "sicurezza in profondità" o "deep security").

In questa sede ci limitiamo a considerare i seguenti livelli:

- di protocollo di rete mediante tecnologie di autenticazione e cifratura delle comunicazioni;
- di applicazione mediante credenziale protetta da schema di autenticazione che si avvale della tecnologia di "Smart OTP" basata su librerie di sicurezza incluse nell'applicazione mobile.

Consideriamo ad un livello di maggior dettaglio questi livelli.

I protocolli di rete imposti dai nostri web server (i server utilizzati come interfaccia per i servizi di home / remote banking) sono i protocolli di tipo Transport Layer Security (TLS) di ultima generazione (TLS v1.1 e TLS v1.2) e sono quindi esclusi dai sistemi i protocolli precedenti in quanto affetti da vulnerabilità conclamate. Occorre aggiungere che, all'interno di questi, sono utilizzati protocolli di scambio chiavi, cifratura simmetrica (tecnologie utilizzate per la confidenzialità), autenticazione (tecnologia per accreditare il web server), hashing (tecnologia utilizzata per assicurare l'integrità) di ultima generazione con chiavi da 256 bit per la cifratura simmetrica e algoritmo SHA1 da 256 bit per l'hashing.

A livello applicativo l'utente accede mediante credenziali autenticate validate successivamente con tecnologia di OTP software incluso nell'applicazione per la conferma dell'operazione di accesso o dispositiva.

In particolare, relativamente ai presidi presenti per la protezione dell'accesso occorre sottolineare che ad ogni utente:

- è associato un codice utente univoco e una password;
- è associato un univoco numero di telefono in modo da attivare il dispositivo utilizzato quale strumento dove poter confermare le operazioni di accesso e autorizzazione delle disposizioni di pagamento; questo schema di autenticazione recepisce tutte le previsioni indicate dalla Direttiva PSD<sup>2</sup>.

Questo schema è definito come autenticazione forte (strong authentication schema) in quanto prevede due elementi per l'autenticazione: un elemento conosciuto dall'utente (la password) ed un elemento in suo possesso (lo smartphone da cui effettua le operazioni di accesso e le dispositive). Inoltre, lo schema recepisce le indicazioni della Direttiva europea sopraindicata in quanto il codice è collegato alla specifica transazione - così detto *dynamic linking* - che si sta autorizzando (i.e. il codice è parte del codice IBAN del destinatario, del numero telefonico per cui si effettua la ricarica, etc.).

Al primo collegamento, per ragioni di sicurezza, il programma richiede all'utente obbligatoriamente di cambiare la password assegnata in occasione dell'attivazione del servizio; queste informazioni sono memorizzate negli archivi del sistema di gestione in forma criptata, e sono quindi note solo all'utente. Ogni utente può cambiare la propria password d'accesso in ogni momento e senza limiti di quantità di variazioni. In ogni caso, per ragioni di sicurezza, dopo 180 giorni ne viene richiesta obbligatoriamente la variazione. Infine, ad ogni accesso al servizio, l'utente viene informato in merito al suo ultimo collegamento (precedente a quello in corso) ed al numero totale di collegamenti effettuati.

Ad ogni collegamento viene poi richiesto, oltre al codice utente ed alla password, l'autenticazione tramite lo schema di conferma definito sia per l'accesso che per le disposizioni di pagamento.

Infine, se è stata precedentemente attivata la funzione "Acceleratori One Click", è possibile, per alcuni beneficiari preventivamente impostati dall'utente, escludere l'inserimento della credenziale dispositiva.

## **Requisiti minimi di sistema**

Per utilizzare i servizi DWeb è necessario rispettare i seguenti requisiti minimi:

- connessione analogica o digitale attiva;
- personal computer con processore 800 Mhz o superiore;
- 512Mbyte di memoria RAM disponibile e capacità HDD 20Gb;
- sistema operativo *Windows®* (Windows 7, Windows Server 2008 e Windows 10);
- browser:
  - Mozilla Firefox 42 o superiore;
  - Internet Explorer 9 o superiore;
  - Google Chrome 48 o superiore;
  - Safari 9.1 o superiore;
- risoluzione video: 1024 \* 768 o superiore.

## **Requisiti dispositivi Mobile**

DMobile è fruibile con qualunque tipologia di terminale, come ad esempio:

- Iphone;
- Android (smartphone).



I requisiti sono i seguenti:

- iOS:
  - iPhone versione iOS 9.0 o successive;
- Android:
  - smartphone di qualsiasi dimensione versione 5.0 o successive.

## **Consigli per la tua sicurezza**

Di seguito riportiamo in nostri consigli per la sicurezza dei tuoi dispositivi e di tutti i tuoi dati sensibili<sup>3</sup>.

Se hai un PC o uno smartphone:

- installa e mantieni sempre aggiornato il software di protezione antivirus<sup>4</sup> e antispyware;
- installa sempre gli aggiornamenti ufficiali del sistema operativo e dei principali programmi che usi appena vengono rilasciati;
- installa gli aggiornamenti e le patch di sicurezza del browser e delle applicazioni;
- installa/attiva un firewall<sup>5</sup>;
- effettua regolarmente scansioni complete con l'antivirus;
- non aprire messaggi di posta elettronica di cui non conosci il mittente o con allegati sospetti;
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro;
- se lo stesso PC/smartphone è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole;
- proteggi i tuoi dispositivi con PIN, password o altri codici di protezione.

Per la generazione delle tue password ti suggeriamo di non creare codici facilmente intuibili da altre persone avendo l'accortezza di:

- definire una password sicura - deve essere obbligatoriamente composta da un minimo di 8 e massimo di 20 caratteri alfanumerici – contenente almeno una lettera maiuscola, almeno una minuscola ed almeno un numero. Utilizza ad esempio le iniziali di una frase che possa ricordare soltanto tu e non associabile ai tuoi dati anagrafici. Ad esempio: Cmdqeb2609 (*Come mi divertivo quando ero bambino*);
- non utilizzare dati anagrafici per comporre la tua credenziale (es. non inserire la tua data di nascita o quella di un tuo caro);
- non utilizzare password condivise con altri servizi online;
- definire una password che sia completamente diversa dalle ultime generate;
- evitare di utilizzare parole di senso comune;

---

<sup>3</sup> Il Gruppo Banco Desio non fornisce supporto tecnico su antivirus, firewall e altre soluzioni di sicurezza installati sui dispositivi personali del cliente, né può essere ritenuta responsabile per la configurazione degli stessi.

<sup>4</sup> Il software antivirus permette di tenere il proprio dispositivo al riparo da software indesiderati ("malware") che potrebbero essere installati senza il consenso dell'utente, e carpire i dati di pagamento e altri dati sensibili del cliente a scopo fraudolento.

<sup>5</sup> Il firewall ha lo scopo di controllare e filtrare tutti i dati in entrata e in uscita del proprio dispositivo, aumentando il livello di sicurezza del dispositivo su cui è installato.

---

- non salvare la password nel browser e evitare per quanto possibile di annotare la password per ricordarla;
- non comunicare la password ad amici, conoscenti, operatori del Servizio Clienti<sup>6</sup>.

Nel caso in cui ti vengano sottratti i codici di accesso e gli strumenti di identificazione (o in caso di smarrimento), ti consigliamo di:

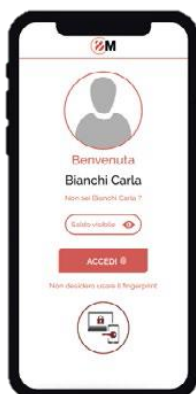
- segnalare immediatamente alla tua filiale di riferimento (o in alternativa al Servizio Clienti (numero verde 800.382.511) l'accaduto. La banca provvederà al blocco cautelativo dell'account al fine di evitare accessi indesiderati al tuo account;
- verificare con la tua filiale di riferimento la presenza di eventuali pagamenti/transazioni sospette;
- richiedere l'emissione di nuove credenziali per l'accesso al tuo account.

In caso di operazioni fraudolente contatta immediatamente la tua filiale di riferimento ed effettua quanto prima la denuncia alle autorità competenti.

---

<sup>6</sup> Gli operatori della Banca non chiedono mai di comunicare o inviare le credenziali di accesso.

## APP DMobile



DMobile è il servizio che ti permette di avere le funzionalità di DWeb, servizio del portale di home banking del Banco Desio, sul tuo smartphone mediante l'App DMobile, scaricabile dallo store di riferimento e disponibile per tutti i dispositivi dotati dei seguenti sistemi operativi:

- Android versione 5.0 e successive;
- IOS versione 7.0 e successive.

## Scaricare l'app dallo store

Per poter utilizzare il servizio in mobilità è necessario scaricare l'applicazione tramite il proprio store di riferimento.

L'app è possibile cercarla tramite il consueto campo di ricerca disponibile nella pagina dello store oppure inquadrando uno dei due QRCode riportati di seguito. Fai attenzione a scaricare il l'applicazione riferita al tuo sistema operativo.



## Attivazione dello SmartOTP

L'attivazione dello Smart OTP è semplice e veloce: dovrai solo seguire i pochi passaggi che ti verranno proposti sul tuo smartphone. Per maggior chiarezza, di seguito vengono descritti, in elenco, i passaggi che dovrai eseguire per completare l'attivazione dello Smart OTP:

1. Accedi all'app appena scaricata e inserisci negli appositi spazi le credenziali di accesso al servizio (username e password<sup>7</sup>);



2. Inventa un codice PIN personale di 5 (cinque) cifre che dovrai ricordare. Il pin ti servirà per autorizzare l'accesso al sistema e convalidare le tue operazioni dispositive;



---

<sup>7</sup> Per i nuovi clienti, in fase di primo accesso dovrà essere inserita la password originale fornita dalla Banca.

3. Riceverai sul tuo cellulare un SMS con un codice numerico “usa e getta”<sup>8</sup>. Recupera il codice e inseriscilo nel campo proposto nell’applicazione. Fai attenzione: per sicurezza il codice ha una durata limitata<sup>9</sup> e quindi, una volta scaduto il tempo limite, il codice viene automaticamente invalidato; sarà pertanto necessario chiedere l’invio di un nuovo codice usa e getta<sup>10</sup>. Una volta trascritto il codice clicca su “CONFERMA” per proseguire;



4. Dopo aver confermato il codice, ti verrà chiesta l’abilitazione all’invio delle notifiche e all’utilizzo della biometria (se il tuo dispositivo lo prevede). Le due funzionalità servono a:
- Notifiche:** consente al sistema di inviarti sul tuo dispositivo una notifica push che dovrà essere aperta per completare l’operazione che stai eseguendo;
  - Biometria:** Per garantirti una migliore user experience e facilitarti le operazioni di accesso e convalida delle operazioni. La biometria ti permetterà di avere un’alternativa all’utilizzo del PIN personale creato al punto 2.

Clicca sul tasto “PROCEDI” per passare allo step successivo:



<sup>8</sup> L’SMS viene spedito al numero di cellulare indicato sul contratto sottoscritto in filiale.

<sup>9</sup> Il codice usa e getta ha una validità di 10 minuti.

<sup>10</sup> Funzionalità disponibile nella pagina visualizzata dall’utente.

5. Conferma l'attivazione della biometria (FaceID/FingerPrint) e avrai concluso il processo di attivazione dello Smart OTP. Il sistema ti porterà direttamente alla home page dell'app.

Ricorda che:

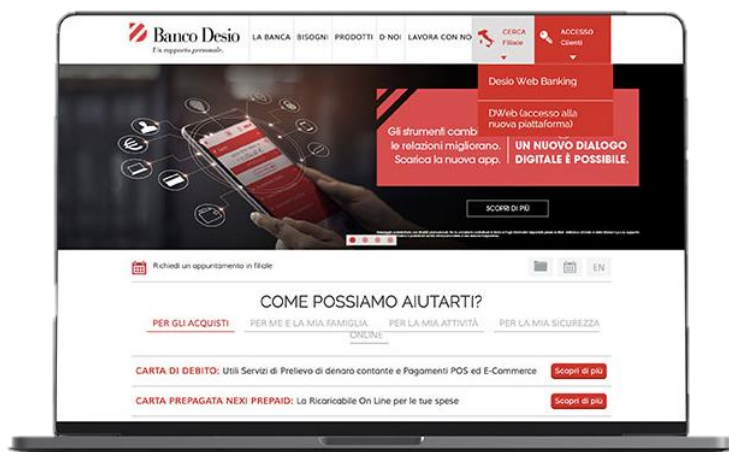
- a) Se stai effettuando il primo accesso ti sarà chiesta la modifica della password fornita dalla Banca. Il passaggio, per la tua sicurezza, è obbligatorio e sarà in aggiunta ai passaggi descritti sopra;
- b) Lo Smart OTP non può essere installato contemporaneamente su due o più dispositivi;
- c) Per i dispositivi:
  - a) *Android*: è possibile attivare/utilizzare esclusivamente il riconoscimento tramite FingerPrint (impronta digitale) anche se il dispositivo è abilitato al riconoscimento facciale;
  - b) *iOS*: se sul dispositivo è presente esclusivamente il riconoscimento tramite FingerPrint (impronta digitale) verrà attivata quest'ultima mentre se il dispositivo prevede anche il riconoscimento tramite FaceID (riconoscimento facciale) il sistema operativo privilegerà automaticamente quest'ultimo.
- d) Se il tuo smartphone non supporta il riconoscimento tramite biometria dovrai necessariamente utilizzare il PIN personale creato al punto 2 del processo di attivazione.

## Accesso al sistema DWeb

### Mediante SmartOTP dal portale Web

Per utilizzare lo Smart OTP in accesso è necessario preventivamente:

- a) aver sottoscritto un contratto di home banking che preveda come schema di sicurezza Smart OTP<sup>11</sup>;
- b) aver scaricato l'app sul proprio smartphone (cfr. paragrafo "Scaricare l'app dallo store";
- c) aver attivato Smart OTP sullo smartphone (cfr. paragrafo "Attivazione dello Smart OTP").



L'accesso al portale web tramite Smart OTP può avvenire in tre modalità:

#### 1. Tramite notifica push

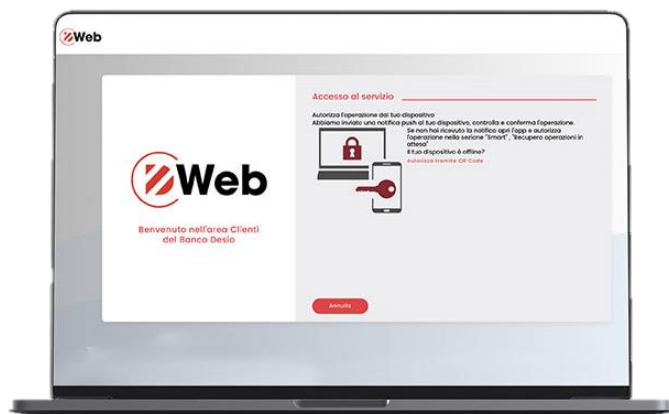
<sup>11</sup> Per i nuovi clienti/contratti, Smart OTP è attivato come default.

Dopo aver digitato le proprie credenziali da accesso al servizio, utente e password, il sistema invierà una notifica push sul cellulare su cui è stato attivato SmartOTP.

E' necessario quindi aprire la notifica e confermare la propria identità tramite digitazione del PIN personale oppure, se abilitato, tramite riconoscimento biometrico.

Se il riconoscimento avviene con successo il servizio mostrerà la home page del servizio.

Per utilizzare questa soluzione è necessario che il proprio dispositivo sia collegato alla rete dati oppure sia collegato ad una rete Wi-Fi.



## 2. Tramite utilizzo della funzione Smart

La soluzione è utilizzabile nel caso in cui la notifica non sia stata ricevuta sul proprio smartphone.

Per accedere è quindi necessario convalidare l'operazione aprendo l'app e tappando sull'icona disponibile in home page (non è necessario effettuare il login).

Il sistema riconoscerà automaticamente che c'è un'azione in sospeso e proporrà il campo per l'inserimento del PIN personale.

Se la digitazione del codice avviene correttamente l'app confermerà l'avenuto accesso al portale web.



### 3. Tramite lettura del QRCode

La soluzione è utilizzabile nel caso in cui lo smartphone sia off-line<sup>12</sup>.

Dopo l'inserimento delle proprie credenziali all'utente verrà proposta la generazione di un QRCode.

L'utente è quindi obbligato ad aprire l'app della Banca dove verrà mostrata un'icona necessaria ad aprire la funzione di lettura del QRCode.

Inquadrato il codice l'app chiederà l'inserimento del PIN personale. Se l'inserimento avverrà correttamente verrà mostrato all'utente un codice numerico "usa e getta".

Il codice proposto dovrà quindi essere trascritto nell'apposito campo proposto sul web per completare l'accesso al servizio.

Si precisa che il QRCode è leggibile esclusivamente dall'app della Banca.



### Modifica della password di sistema

In occasione del primo accesso o dopo un reset della password, il sistema di sicurezza di DWeb richiede la sostituzione della password fornita dal Banco con una di propria creazione.

Per la sostituzione della password è sufficiente inserire la password originaria consegnata dal Banco nella casella situata vicino alla scritta *Password attualmente in uso*, quindi inserire la nuova password nella casella situata a fianco della scritta *Nuova password* e ripeterla nella casella relativa a *Conferma nuova password*; al termine, confermare l'inserimento della nuova password cliccando su *Modifica*.

La modifica della password verrà richiesta anche alla scadenza dei 180 giorni. Per la sostituzione inserire la *Password in uso* nella casella relativa, quindi inserire la nuova password nella casella posta a fianco della scritta *Nuova password* e ripeterla nella casella relativa a *Conferma nuova password*. Si suggerisce di effettuare il cambio password periodicamente (tramite il menu Modifica Profilo - Credenziali) per mantenere elevato il livello di sicurezza.

La password è *case sensitive*, cioè considera diverso il carattere maiuscolo dal carattere minuscolo: di conseguenza è necessario fare molta attenzione nell'inserimento del codice.

<sup>12</sup> Ovvero sia in assenza di connessione dati o in assenza di connessione Wi-Fi (es: modalità aereo).



La password creata dall'utente durante questa procedura non è conosciuta dagli operatori del Banco e non può essere in alcun modo recuperata: di conseguenza, si suggerisce di scrivere la password su un documento o un archivio elettronico prima di digitarla a video e conservarla in luogo sicuro e riservato.

Al termine delle operazioni di modifica, compare a video la pagina "Home".

## Accesso al sistema DMobile

### Mediante Smart OTP da App

Per accedere al servizio direttamente da app, è necessario inserire nella home page:

- nella casella "Codice utente" il *codice utente*;
- nella casella "Password" la *password*;

Inseriti i due dati richiesti è quindi necessario cliccare su *Accedi*.

Successivamente in fase di accesso ed in fase di autorizzazione delle operazioni dovrà essere inserito anche un PIN di autenticazione di 5 cifre, censito dall'utente durante il processo installazione dello Smart OTP (di seguito, fase di attivazione del dispositivo smartphone personale). Mediante specifica autorizzazione dell'utente, sui dispositivi dotati di riconoscimento biometrico il PIN potrà essere completamente sostituito dal riconoscimento dell'impronta o dal riconoscimento facciale.

## Convalida delle operazioni eseguite in DWeb

### Mediante SmartOTP da portale web

L'autorizzazione di una disposizione (ad esempio, un bonifico) inizializzata da web è possibile autorizzarla con Smart OTP nelle seguenti tre modalità:

#### 1. Tramite notifica push

Dopo aver compilato e verificato la correttezza dei dati del bonifico, è necessario convalidare la disposizione premendo il tasto "AUTORIZZA". Il sistema quindi invierà una notifica push sul cellulare su cui è stato attivato lo Smart OTP.

E' necessario aprire la notifica e confermare la propria identità tramite la digitazione del PIN personale oppure, tramite il riconoscimento biometrico.

Se il PIN o il riconoscimento avviene con successo il servizio convaliderà la disposizione mostrando un apposito messaggio di conferma.

Per utilizzare questa soluzione è necessario che il proprio dispositivo sia collegato alla rete dati oppure sia collegato ad una rete Wi-Fi.

#### 2. Tramite utilizzo della funzione Smart

La soluzione è utilizzabile nel caso in cui la notifica non sia stata ricevuta sul proprio smartphone oppure sia stata cancellata per errore dall'utente.

Per convalidare la disposizione è quindi necessario aprire l'app e tappare sull'icona disponibile in home page (non è necessario effettuare il login).

Il sistema riconoscerà automaticamente che c'è un'operazione in sospeso e proporrà il campo per l'inserimento del PIN personale oppure del riconoscimento biometrico.

Se la digitazione del codice o il riconoscimento della biometria avviene correttamente l'operazione verrà regolarmente autorizzata.

### 3. Tramite lettura del QRCode

La soluzione è utilizzabile nel caso in cui lo smartphone sia off-line<sup>13</sup>.

Per autorizzare una disposizione è necessario aprire l'app che riconoscerà automaticamente l'assenza di connessione e proporrà tramite apposita icona la scansione di un codice QRCode.

Il codice QRCode deve essere generato direttamente da web cliccando su "Genera QRCode".

Inquadrando il codice e dopo aver digitato il proprio PIN personale il sistema, tramite app, genererà un codice "usa e getta" che dovrà essere trascritto nell'apposito campo disponibile sulla pagina web.

Se il codice usa e getta viene riconosciuto valido il sistema autorizzerà l'accesso al servizio.

Si precisa che il QRCode è leggibile esclusivamente dall'app della Banca.

## Convalida delle operazioni da eseguite da DMobile

### Autorizzazione delle disposizioni mediante Smart OTP da App

Se stai provando ad effettuare la tua prima disposizione (ad esempio, un bonifico) mediante l'App DMobile, nel momento dell'autorizzazione attraverso lo SmartOTP dovrai inserire manualmente il PIN nell'apposito campo situato in fondo alla schermata riepilogativa; in corrispondenza di questo evento, ti verrà richiesto se vorrai autorizzare le successive operazioni tramite riconoscimento biometrico se previsto dallo smartphone in uso. In caso di consenso, le successive disposizioni potranno essere autorizzate con impronta/riconoscimento facciale.

---

<sup>13</sup> Ovvero sia in assenza di connessione dati o in assenza di connessione Wi-Fi (es: modalità aereo).

# Assistenza Clienti

## Accesso al servizio

L'accesso al servizio è possibile chiamando il numero verde **800.382.511**.

*In particolare, si segnala che:*

- il numero verde è gratuito (sia da rete fissa che da rete mobile);
- il servizio con operatore è attivo dalle 8.00 alle 22.00 dal lunedì alla domenica;

Il servizio può temporaneamente essere sospeso per motivi tecnici senza che ciò comporti responsabilità per la Banca (come da condizioni contrattuali).

Al termine del messaggio di benvenuto è sufficiente premere il tasto **1** del telefono per parlare con un operatore e richiedere assistenza circa il servizio di home banking / mobile banking.