

FOGLIO INFORMATIVO

3r - Servizi Telematici CRVONLINE BUSINESS offerto ai non consumatori

Servizio offerto a chi desidera un canale Internet per l'esecuzione di operazioni a carattere informativo e dispositivo sui rapporti abilitati, compresa la negoziazione di valori.

INFORMAZIONI SULLA BANCA

CASSA DI RISPARMIO DI VOLTERRA S.p.A.

Sede Legale: Piazza dei Priori, 16/18 – 56048 Volterra (PI)

Tel.: 0588 91111- Fax: 0588 86940

Indirizzo e-mail: info@crvolterra.it

Sito internet: www.crvolterra.it

Codice ABI: 06370

Cap. Sociale € 72.304.400,00

C.F., P.IVA e numero iscrizione Registro Imprese di Pisa: 01225610508

Numero di iscrizione all'albo delle banche presso la Banca d'Italia: 5176.30

Aderente al Fondo Interbancario di Tutela dei Depositi e al Fondo Nazionale di Garanzia

COSA SONO I SERVIZI TELEMATICI

Struttura e funzione economica

Il servizio consente alla clientela, tramite l'utilizzo di un computer collegato alla rete internet, di visualizzare ed operare sui rapporti intrattenuti con la Cassa, impartire disposizioni di incasso e pagamento, negoziare valori mobiliari ed ottenere informazioni di natura finanziaria, effettuare ricariche di telefoni cellulari, effettuare l'allineamento degli archivi dei debitori e creditori.

Il riconoscimento dell'utente viene effettuato tramite codici di accesso univoci, composti da un Codice Postazione, da una PASSWORD.

Per l'Accesso al servizio, il Cliente deve utilizzare il codice OTP semplice generato, in modo casuale e randomico, dal Token.

Per l'Autorizzazione delle operazioni a carattere dispositivo, il Cliente deve utilizzare, ove previsto, il codice OTP dinamico generato, in modo casuale e randomico, dal Token.

Principali rischi

Tra i principali rischi, vanno tenuti presenti:

- lo specifico rischio connesso ad eventuali mal funzionamenti e ritardi delle reti telematiche bancarie e/o interbancarie;
- l'utilizzo fraudolento, da parte di terzi, dei codici personali di accesso del cliente nel caso di smarrimento e/o sottrazione, con conseguente possibilità di utilizzo da parte di soggetti non legittimati. Pertanto il cliente dovrà osservare la massima attenzione nella custodia degli stessi, nonché la massima riservatezza nell'uso; nei casi di smarrimento e/o sottrazione, il cliente è tenuto a richiedere immediatamente il blocco dei servizi secondo le modalità contrattualmente previste.

PRINCIPALI CONDIZIONI ECONOMICHE**SPESE****CRVONLINE BUSINESS BASE**

Applicativo riservato a clientela business capo gruppo ad operare anche per le proprie imprese controllate. Consente, sui rapporti intrattenuti esclusivamente con la Cassa, l'esecuzione di operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in differita.

Canone: € 10,00 mensile

CRVONLINE BUSINESS BASE Proxi

Applicativo riservato a clientela business delegata di una capo gruppo. Consente, sui rapporti intrattenuti esclusivamente con la Cassa, l'esecuzione di operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in differita.

Canone: € 7,00 mensile

CRVONLINE Business ALL

Applicativo riservato a clientela business capo gruppo ad operare anche per le proprie imprese controllate. Consente, sui rapporti intrattenuti con la Cassa che con altri Istituti, l'esecuzione di operazioni a carattere informativo e dispositivo secondo gli standard CBI. In aggiunta consente, sui rapporti intrattenuti esclusivamente con la Cassa, specifiche operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in differita.

Canone: € 15,00 mensile

CRVONLINE BUSINESS ALL Proxi

Applicativo riservato a clientela business delegata di una capo gruppo. Consente, sui rapporti intrattenuti con la Cassa che con altri Istituti, l'esecuzione di operazioni a carattere informativo e dispositivo secondo gli standard CBI. In aggiunta consente, sui rapporti intrattenuti esclusivamente con la Cassa, specifiche operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in differita.

Canone: € 7,00 mensile

Il canone mensile decorre:

- - per l'attivazione - dal mese successivo a quello di attivazione con cadenza trimestrale posticipata
- - per la disattivazione - dal mese di disattivazione con cadenza mensile posticipata.

Commissione Ricarica Carta Prepagata da canale Home Banking	€ 1,00
Commissione per ricariche telefoniche	€ 0,00
Commissione per Riproduzione e mancata restituzione Token	€ 15,00
Commissione bonifici per emolumenti canale Home Banking	€ 0,00
Commissione giroconto canale Home Banking	€ 0,25
Commissione bonifici verso Italia e Ue su Filiali CRV canale Home Banking	€ 0,50
Commissione bonifici verso Italia e Ue su Filiali altre Banche canale Home Banking	€ 1,50
Commissione per pagamento delega F24 canale Home Banking	€ 0,00

Commissione per pagamento bollettino bancario freccia canale Home Banking	€ 0,00
Commissione per pagamento bollettino postale canale Home Banking	€ 0,40 (più il rimborso delle commissioni richieste da Poste Italiane)
Commissione per pagamento CBILL/PAGOPA	€ 1,50
Commissione per pagamento MAV	€ 0,00
Commissione per pagamento RAV	€ 1,03
Per le ulteriori condizioni vedi relativo foglio informativo Conti Correnti, Servizi di incasso e pagamento, Titoli.	

VALUTE

Canone	13° gg lav del mese successivo al trimestre di competenza
Ricariche Carta Prepagata	Data esecuzione
Ricariche telefoniche	Data esecuzione
Commissione per Riproduzione e mancata restituzione Token	Data esecuzione
Giroconto disposto canale CRVONLINE	Data esecuzione
Bonifici disposti canale Home Banking	Data esecuzione 1 giorno lavorativo antecedente la Valuta Fissa Beneficiario, se indicata. In ogni caso la data valuta addebito non può precedere la data esecuzione
Pagamento delega F24 canale Home Banking	Data esecuzione
Pagamento bollettino bancario freccia canale Home Banking	Data esecuzione
Pagamento bollettino postale canale Home Banking	Data esecuzione
Pagamento CBILL/PAGOPA	Data esecuzione
Pagamento MAV	Data esecuzione
Pagamento RAV	Data esecuzione

RECESSO E RECLAMI

Recesso dal contratto

Si può recedere dal contratto in qualsiasi momento, senza penalità e senza spese di chiusura.

Recesso in caso di modifica unilaterale delle condizioni contrattuali

Fatto salvo quanto diversamente specificato con riferimento alla modifica dei tassi nella prestazione dei Servizi di Pagamento, qualsiasi modifica unilaterale delle condizioni contrattuali (ivi incluse del Documento di Sintesi) è comunicata dalla Banca al Cliente mediante comunicazione scritta, su supporto cartaceo o su altro Supporto Durevole, contenente la formula "Proposta di modifica unilaterale del contratto", con preavviso minimo di due mesi dalla data prevista per l'applicazione delle modifiche. In caso di modifica del tasso di interesse collegata a modifica del tasso di riferimento, le relative informazioni saranno fornite al

Cliente mediante resoconto periodico, essendo rese pubbliche presso le dipendenze le variazioni dei tassi di riferimento.

Il Cliente che non intende accettare le modifiche proposte dalla Banca:

(a) deve comunicare espressamente alla Banca il proprio rifiuto entro la data prevista per l'applicazione delle modifiche, e

(b) ha il diritto di recedere dal contratto a cui sono state apportate le modifiche, senza spese prima della data prevista per l'applicazione delle modifiche stesse.

In tale caso, in sede di liquidazione del rapporto, il Cliente ha diritto all'applicazione delle condizioni precedentemente praticate.

Tempi massimi di chiusura del rapporto contrattuale

N. 30 giorni.

Reclami

Per eventuali contestazioni inerenti il presente rapporto contrattuale, il Cliente può presentare reclamo, inviando comunicazione scritta all'Ufficio Reclami della Cassa all'indirizzo Cassa di Risparmio di Volterra SpA - Ufficio Reclami - Piazza dei Priori, 16/18 56048 Volterra (PI) – o per via telematica tramite il sito web della Cassa www.crvolterra.it, sezione "Reclami". L'Ufficio Reclami risconterà il reclamo così ricevuto, inviando comunicazione scritta al Cliente, entro 30 giorni dalla data di ricezione.

Se il reclamo è ritenuto fondato, la Cassa comunica al Cliente le iniziative che si impegna ad assumere ed i tempi entro i quali verranno realizzate.

Risoluzione stragiudiziale di controversie e Mediazione

In mancanza di risposta scritta entro i termini stabiliti da parte dell'Ufficio Reclami ai sensi del precedente articolo, ovvero nel caso in cui la risposta ottenuta sia ritenuta insoddisfacente, il Cliente, ove ne ricorrano i presupposti, prima di ricorrere al giudice può rivolgersi all'ABF – Arbitro Bancario Finanziario di cui all'art. 128-bis del Testo Unico delle leggi bancarie e creditizie -. Per conoscere le modalità e la relativa disciplina attuativa emanata dalla Banca d'Italia consultare il sito www.arbitrobancariofinanziario.it. È sempre possibile ottenere ulteriori indicazioni rivolgendosi direttamente alla Cassa, che mette a disposizione dei clienti presso i propri locali e sul proprio sito internet le guide relative all'accesso all'ABF, ovvero chiedendo informazioni presso le sedi della Banca d'Italia aperte al pubblico.

Per qualunque contestazione inerente il presente rapporto contrattuale, in alternativa all'ABF o per le questioni che esulano la sua competenza, il Cliente, anche in assenza di preventivo reclamo alla Cassa e prima di ricorrere all'autorità giudiziaria, può attivare - singolarmente o in forma congiunta con la Cassa - una procedura di conciliazione finalizzata al tentativo di trovare un accordo. A tal fine le parti concordano di rivolgersi in via esclusiva all'Organismo istituito presso la Camera di Commercio della Provincia della Filiale nella quale è intrattenuto il rapporto oggetto di contestazione. Nel caso in cui tale Organismo non sia presente presso la Camera di Commercio della Provincia così determinata, il tentativo dovrà essere esperito davanti all'Organismo istituito presso la Camera di Commercio di Pisa.

In ogni caso, l'istanza di soluzione stragiudiziale delle controversie ai sensi di una delle procedure descritte ai precedenti paragrafi costituisce condizione di procedibilità della eventuale domanda giudiziale.

INFORMATIVA SULLA SICUREZZA CORPORATE BANKING E MOBILE BANKING

Credenziali di Sicurezza Personalizzate previste per Corporate e Mobile Banking destinati ai clienti "Business"

Per accedere al Corporate e Mobile Banking vengono richieste le seguenti Credenziali di Sicurezza Personalizzate:

- il Codice Postazione che è quello indicato nel contratto e inviato tramite email all'indirizzo riportato nel contratto stesso;
- la Password scelta dall'Utente dopo l'accesso iniziale (al primo accesso è richiesta la password fornita dalla Banca e ricevuta tramite SMS). La Password non deve essere di semplice intuizione evitando riferimenti personali o familiari. E' inoltre necessario modificare periodicamente la password a tutela dell'Utente nonché per evitare il blocco del dispositivo trascorsi 180 giorni dall'ultima modifica,
- il codice OTP (One Time Password) semplice generato dal Token assegnato dalla Banca all'Utente per l'accesso ai servizi;
- il codice OTP (One Time Password) dinamico generato dal Token assegnato dalla Banca all'Utente per autorizzare la disposizione, legando in maniera univoca il beneficiario e l'importo della disposizione (incluso quella di pagamento).

L'Utente deve conservare le Credenziali di Sicurezza Personalizzate con cura, evitando di comunicarle o consegnarle a terzi.

Requisiti Hardware e Software del PC dell'Utente

I requisiti minimi per gli applicativi di Corporate e Mobile Banking sono i seguenti:

Corporate Banking

- Hardware: non previsti requisiti minimi
- Software: previsti i seguenti requisiti minimi
 - ✓ MICROSOFT INTERNET EXPLORER versione IE7 e superiori
 - ✓ CHROME versione 5 e superiori
 - ✓ FIREFOX versione 5 e superiori
 - ✓ OPERA versione 11 e superiori
 - ✓ SAFARI versione 4 e superiori

Mobile Banking

- Hardware Smartphone e Tablet: non previsti requisiti minimi
- Software Smartphone e Tablet Software: previsti i seguenti requisiti minimi
 - ✓ APPLE IOS SAFARI MOBILE versione 5 e superiori
 - ✓ ANDROID MOBILE GOOGLE CHROME versione 3 e superiori

Protocollo di sicurezza

Tutti i dati e le informazioni, su PC e App della Banca, sono protetti con il sistema più avanzato di crittografia SSL a 128 bit.

Per entrare nel sito della Banca deve essere sempre:

- verificato che la trasmissione dei dati sia protetta (presenza di un lucchetto chiuso sulla finestra del browser);
- verificato che sia presente il prefisso https://
- effettuato l'accesso dal sito istituzionale della Banca www.crvolterra.it evitando l'accesso da link diversi;
- verificato di non aver memorizzato la password sul sistema di navigazione.

Tentativi di accesso

Per la sicurezza e tutela dell'Utente, sono a disposizione tre tentativi consecutivi per la corretta digitazione della password.

Al terzo tentativo errato l'applicativo viene bloccato dal sistema.

Il blocco del dispositivo può essere resettato dalla Banca.

Durata della sessione inattiva

Per la sicurezza e tutela dell'Utente, trascorsi 20 minuti di inattività, la connessione con la Banca decade ed apparirà un avviso di sessione scaduta.

Per rientrare deve essere nuovamente eseguito l'accesso.

Procedura di pagamento via Internet

Le disposizioni di pagamento disposte prevedono un'operatività progressiva:

- *inoltro*: operazione tramite la quale l'Utente predispone ed inserisce - con valorizzazione di tutti i campi obbligatori previsti - una disposizione;
- *salvataggio*: operazione – facoltativa – che permette di salvare la disposizione inserita prima dell'autorizzazione;
- *autorizzazione*: operazione che - tramite digitazione del codice OTP dinamico prodotto dal Token - permette l'autorizzazione della disposizione. Con tale azione la disposizione viene trasmessa al servizio di riferimento della disposizione per la registrazione sul conto corrente e l'inoltro alla controparte;
- *esito*: la conferma dell'esecuzione della disposizione autorizzata viene comunicata all'Utente tramite email nonché resa visibile sul conto corrente con registrazione contabile.

Orientamenti per la sicurezza dei dispositivi

i propri dispositivi (PC, tablet, smartphone) con programmi Antivirus efficienti (per proteggerlo da virus, malware, browser o man in the middle, spyware, app non sicure e altre minacce) e Firewall (per proteggerlo da intrusioni indesiderate), non rispondere ad email sospette quali cd. "phishing" e mantenere aggiornata la sicurezza di questi programmi.

Analoga cura deve essere seguita nella custodia dei dispositivi.

I comportamenti, per limitare la possibilità di subire attacchi, debbono essere orientati alla conservazione con cura ed in luogo separato delle Credenziali di Sicurezza Personalizzate, nonché nell'evitare di aprire o rispondere ad email sospette o ricevute da nominativi sconosciuti (nella quale vengono richieste TUTTE le informazioni personali).

Procedura in caso di abuso riscontrato o sospetto

Nel caso di abuso riscontrato o sospetto, per evitare possibili ricadute negative in termini di sicurezza, l'Utente deve:

- eseguire in autonomia senza indugio il blocco del servizio digitando tre volte consecutive in maniera errata la password di accesso o, qualora impossibilitati, comunicare l'evento alla Banca od al soggetto terzo designato per l'esecuzione del blocco
- inviare senza indugio alla Banca segnalazione su (presunti) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via Internet accedendo al sito istituzionale della Banca alla sezione "Contatti" e compilando il form predisposto sotto la voce "Sicurezza pagamenti via Internet" o contattando la Banca.

La Banca, eseguiti i controlli del caso, fornirà risposta all'Utente direttamente nell'applicativo.

Procedura di segnalazioni di sicurezza

I dispositivi (PC, tablet, smartphone) e le Credenziali di Sicurezza Personalizzate sono elementi interfunzionali.

Il possibile abuso, perdita o furto necessita da parte dell'Utente di immediate azioni volte a impedire l'utilizzo fraudolento.

- *perdita e furto delle Credenziali di Sicurezza Personalizzate*: l'Utente deve comunicare senza indugio il furto, lo smarrimento o furto delle Credenziali di Sicurezza alla Banca od al soggetto terzo designato;
- *perdita e furto dei dispositivi e tentativi di intrusione*: l'Utente deve comunicare senza indugio il furto, lo smarrimento o l'indebita intrusione dei propri dispositivi (PC, tablet, smartphone, token) alla Banca od al soggetto terzo designato a tutela della riservatezza delle informazioni e sicurezza del servizio.

Responsabilità dell'Utente e della Banca

Nell'uso del servizio di pagamento, l'Utente assume responsabilità:

- in mancanza di rispetto dei termini e delle condizioni contrattuali;
- in mancanza dell'immediata adozione di tutte le misure idonee a garantire la sicurezza del servizio e delle Credenziali di Sicurezza Personalizzate;
- sulla perdita derivante dall'utilizzo indebito del servizio conseguente al furto o smarrimento o uso non autorizzato delle Credenziali di Sicurezza Personalizzate per un importo comunque non superiore complessivamente a 50 euro, salvo il caso in cui abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza delle Credenziali di Sicurezza Personalizzate;
- nella trasmissione dei dati tramite la rete Internet pubblica, per i quali assume piena e totale responsabilità, essendo a conoscenza dei rischi insiti nell'utilizzo dei dispositivi per usufruire del servizio.

Nell'uso del servizio di pagamento, la Banca assume responsabilità:

- affinché l'Utente abbia sempre a sua disposizione strumenti adeguati per effettuare in modo efficace la notifica in caso di furto, smarrimento, appropriazione indebita o uso non autorizzato delle Credenziali di Sicurezza Personalizzate per il blocco del servizio e richiedere lo sblocco del servizio;
- sull'impedimento di qualsiasi uso del servizio dopo il blocco del servizio;
- sui rischi derivanti dalla spedizione delle Credenziali di Sicurezza Personalizzate;
- sui rischi connessi alla continuità operativa del servizio;
- sui rischi connessi alla sicurezza informatica del servizio.

Difesa dai Rischi

AVVISO EMAIL OPERAZIONI INTERNET

Il servizio invia automaticamente, per ogni disposizione impartita, email al riferimento presente nel contratto, in modo tale che l'Utente possa avere immediata evidenza delle operazioni disposte ed autorizzate dal canale.

COMUNICAZIONI PERIODICA SULL'USO CORRETTO E SICURO DEL SERVIZIO

L'Utente sarà informato dalla Banca tramite avviso nel proprio applicativo internet sulle novità in materia di sicurezza del servizio.

CONTROLLO DELLA SITUAZIONE CONTABILE

E' necessario che l'Utente verifichi spesso – on line o tramite app – i movimenti del conto corrente per accorgersi di eventuali operazioni non conformi.

PROTEZIONE DEI DATI PERSONALI

Sulla rete Internet è meglio essere estremamente diffidenti nel consegnare i propri dati riservati senza essere certi dell'identità di chi li sta chiedendo.

Tentativi di "phishing", "social engineering" e "malware" sono sempre più diffusi.

Il "phishing" è una truffa informatica per carpire le Credenziali di Sicurezza Personalizzate attraverso false email, apparentemente provenienti dalla Banca, composte utilizzando logo, nome e il layout tipico dell'azienda imitata. Nella falsa email, ad esempio a causa di un imprecisato problema al sistema di "Corporate Banking", viene spesso richiesto di accedere all'home page del sito della Banca tramite un link da cliccare indicato nella email stessa. Procedendo e digitando le Credenziali di Sicurezza Personalizzate, qualcuno si impossesserà di tali dati.

Se ricevuta una email sospetta come quella appena descritta, non deve essere risposto né deve essere cliccato sui link presenti nella email. La email non deve essere aperta ma cestinata subito !

Il "social engineering " è una truffa informatica usata da chi che conosce alcuni elementi personali dell'Utente ma non tutti. Nascondendo la propria identità, viene carpita la fiducia dell'interlocutore (tramite email o via telefono) fino a ricavare le informazioni necessarie.

Il "malware" è un truffa informatica che prevede l'installazione di virus tramite software creati per causare danni più o meno gravi al dispositivo su cui viene installato, quali ad esempio la cattura delle Credenziali di Sicurezza Personalizzate e per modificare le disposizioni impartite. Tali software possono venire installati tramite Internet oppure aprendo email sospette (ad esempio fatture o promozioni) o inviate da nominativi sconosciuti. La soluzione più efficace è quella di installare sui dispositivi Antivirus efficienti e certificati. Tra i vari software i più comuni sono:

- o *MITM (man-in-the-middle)* o *BITM (browser-in-the-middle)*: software usato per intercettare e per modificare i messaggi e la destinazione dei pagamenti tramite introduzione tra i server e le trasmissioni;
- o *Keylogger*: software in grado di registrare tutto ciò che l'Utente digita su una tastiera o incolla;
- o *Spyware*: software usato per raccogliere informazioni dal sistema dell'Utente e per trasmetterle ad un destinatario interessato;
- o *Trojan horse*: software che contiene istruzioni che vengono eseguite all'insaputa dell'Utente;
- o *Worm*: software che modifica il sistema operativo del sistema dell'Utente in modo da essere eseguito automaticamente.

La Banca non richiede mai, direttamente o tramite terzi, informazioni personali o le Credenziali di Sicurezza Personalizzate per i servizi di Corporate e Mobile Banking.

Ecco alcune semplici regole per evitare di cadere in questo tipo di truffe:

- diffidare di qualunque email che richieda l'inserimento di dati riservati riguardanti le Credenziali di Sicurezza Personalizzate o altre informazioni personali;
- è possibile riconoscere le truffe via email con qualche piccola attenzione; generalmente:
 - non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
 - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'Utente;
 - non riportano una data di scadenza per l'invio delle informazioni.
- nel caso in cui venga ricevuta una email contenente richieste di questo tipo, non deve essere risposto né aperti gli allegati od i file eseguibili. L'email deve essere cestinata subito !
- non deve essere cliccato su link presenti in email sospette dato che i collegamenti potrebbero proseguire su di un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, è bene non fidarsi: è possibile infatti visualizzare nella barra degli indirizzi del browser un indirizzo diverso da quello reale;
- diffidare inoltre di email con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @ o con errori grammaticali;
- inserire i dati riservati esclusivamente in una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella pagina è presente un lucchetto chiuso;

- diffidare del cambio di modalità con la quale viene chiesto l'inserimento delle Credenziali di Sicurezza Personalizzate se non provenienti dal sito istituzionale: tramite pop-up, con dimensioni diverse, in lingua diversa;
- diffidare da email o telefonate non richieste da persone che chiedono informazioni dettagliate o complete. Spesso oltre le Credenziali di Sicurezza Personalizzate vengono richiesti anche tutti i riferimenti anagrafici, personali e comportamentali.

LEGENDA

CRVONLINE	Applicativo che consente, tramite rete internet, l'esecuzione di operazioni a carattere dispositivo e informativo
CODICE POSTAZIONE	Codice personale di accesso stabilito dalla Cassa
CODICE OTP	Acronimo di One Time Password. Codice generato dal Token Hardware e calcolato in modo casuale e randomico
PASSWORD	Codice personale di accesso stabilito dal Cliente
PIN	Codice personale di accesso stabilito dal Cliente
CODICE OTP semplice	Acronimo di One Time Password. Codice semplice generato dal Token e calcolato in modo casuale e randomico
TOKEN	Dispositivo Hardware che genera l'OTP