NORME TECNICHE E SICUREZZA DEI PAGAMENTI
Versione del 19/03/2025

CAPO I – NORME TECNICHE PER L'UTILIZZO DEL CONTO DI PAGAMENTO E DELLA CARTA

1. Introduzione

I termini e le espressioni utilizzati in maiuscolo nel presente documento, ove non altrimenti definiti all'interno del medesimo, hanno il medesimo significato indicato nel Contratto di Conto di Pagamento.
Il presente documento identifica le regole che il Cliente è chiamato a rispettare nell'utilizzo del Conto di Pagamento (di seguito, per brevità, il "**Conto**"), tramite l'APP e nell'esecuzione di Operazioni di pagamento con il Conto e/o con la Carta di debito internazionale. Il documento viene messo a disposizione del Cliente e, di volta in volta aggiornato, sul Sito Internet di BKN301 S.p.A., sulla base di quanto previsto dal Contratto sottoscritto dal Cliente.
Le norme contenuto nel presente documento si ispirano ai più alti standard di sicurezza dei dati del settore delle carte di pagamento.
L'avvio dell'operatività del Conto può essere effettuata mediante le apposite procedure informatiche rese disponibili e fruibili (tempo per tempo) nell'APP di BKN301 S.p.A. previa la sottoscrizione dei documenti necessari per l'apertura del Conto.

2. Dotazione informatica del Cliente

Il Cliente, per accedere al Conto, è tenuto a dotarsi autonomamente di accesso alla rete Internet e di idonee apparecchiature informatiche e programmi/applicazioni che devono costantemente rispondere alle specifiche di sicurezza riconosciute. Il Cliente è altresì tenuto a custodire con ogni cura l'apparecchiatura informatica di cui si avvale per accedere all'APP.

3. APP

Le procedure informatiche per operare sul Conto sono rese disponibili e fruibile (tempo per tempo) a seguito di un primo versamento da parte del Cliente dell'importo determinato nel "Documento di Condizioni economiche BKN301 S.p.A." e come previsto dalle disposizioni del "Regolamento Conto di Pagamento Consumer BKN301 S.p.A." per le Persone Fisiche (di seguito congiuntamente anche **"Regolamenti contrattuali"**).
BKN301 S.p.A. mette a disposizione del Cliente un'APP, che consente al Cliente di accedere al Conto e alla Carta di debito internazionale, e di gestirli, consultare la posizione e disporre Operazioni di Pagamento.

3.1 Tempi di disponibilità dell'APP

L'App è pienamente disponibile senza limitazioni di giorni e/o orario compatibilmente con la disponibilità dei sistemi informatici di cui si avvale BKN301 S.p.A. e della disponibilità dei servizi di connettività di cui si avvale il cliente..
Tuttavia, BKN301 S.p.A. si riserva la facoltà di limitare o sospendere l'accesso all'APP e di conseguenza di limitare o sospendere tutti o parte dei servizi attivi e fruibili (a titolo esemplificativo, la facoltà del Cliente di impartire Ordini di Pagamento per ragioni connesse alla manutenzione dei propri sistemi informatica) anche per ragioni di 'efficienza e sicurezza del servizio, qualora riscontri tentativi di accesso non autorizzato, ovvero un utilizzo del Conto, della Carta, dell'APP in modo anomalo o difforme da quanto previsto nei Regolamenti contrattuali o da quanto disciplinato nel presente documento, informando preventivamente il Cliente laddove possibile.
BKN301 S.p.A., non appena possibile, comunica al Cliente le eventuali interruzioni non programmate dell'accesso all'APP.

3.2 Mancato o difettoso funzionamento dell'APP

Il Cliente, in caso di mancato o difettoso funzionamento dell'APP, è tenuto a contattare tempestivamente BKN301, ai recapiti riportati nella sezione Contatti del Sito Internet di BKN301 S.p.A. e rinvenibili anche nel foglio informativo.
BKN301 S.p.A. non risponde delle conseguenze derivanti dal malfunzionamento dell'APP, dovute a cause di forza maggiore o comunque a eventi non imputabili all'Istituto di pagamento stesso.
In particolare, BKN301 S.p.A. non può essere considerata responsabile:

- del malfunzionamento dell'infrastruttura di sicurezza e dell'APP in genere, conseguenti al non corretto funzionamento delle apparecchiature del Cliente;
- dell'eventuale perdita, alterazione o diffusione dei dati trasmessi attraverso l'APP, se dovuta a circostanze non imputabili all'Istituto di pagamento stesso.

BKN301 S.p.A., non appena possibile, comunica al Cliente l'eventuale malfunzionamento dell'APP.

3.3 Accesso all' APP

BKN301 S.p.A. protegge la sicurezza dei dati del Cliente e delle operazioni dispositive effettuate tramite il Conto e/o la carta di debito (se richiesta, rilasciata ed attivata), attraverso l'utilizzo di "Autenticazione Forte del Cliente" (o Strong Customer Authentication e, di seguito, per brevità, "**SCA**") che il Cliente deve seguire per avvalersi del citato servizio e per le operazioni disposte.

4. Credenziali

4.1 Rilascio della OTP

Al momento della sottoscrizione del Contratto, il Cliente fornisce un numero di cellulare che verrà utilizzato da BKN301 S.p.A. per inviare via sms la OTP. La OTP è un codice numerico, di lunghezza di 6 caratteri ed ha una validità di durata pari a 2 minuti.
La OTP, unitamente alla Password abilitativa, permette di accedere all'APP e disporre le Operazioni di Pagamento.
BKN301 non richiede mai di comunicare via mail, telefono o altri canali di comunicazione la OTP ricevuta dal Cliente che pertanto non deve comunicarla a soggetti terzi.

4.2 Modifica della password iniziale

La password abilitativa è la Credenziale, impostata dal Cliente, che unitamente alla OTP, permette di accedere all'APP.
Tale password abilitativa deve essere alfanumerica, di lunghezza di almeno 8 caratteri e deve avere le seguenti caratteristiche:

- contenere almeno una cifra, una lettera maiuscola e una lettera minuscola;
- essere diversa dallo User ID e non deve contenerlo;
- non può essere uguale alle ultime tre password utilizzate;

Al Cliente è fatto divieto di comunicare a terzi le Credenziali impostate e ha l'obbligo di utilizzarle secondo una condotta diligente.

4.3 Aggiornamento delle password

Il Cliente deve modificare le password qualora sussistano opportune motivazioni e, in ogni caso, se ed ogni qualvolta lo stesso abbia il minimo dubbio che la sicurezza delle password sia stata compromessa e/o che qualcuno, anche in modo fraudolento, possa esserne venuto a conoscenza. Tuttavia è consigliabile che periodicamente il cliente provveda al cambio delle password.
Per modificare le password, il Cliente è tenuto a seguire la procedura guidata disponibile nell'APP.
BKN301 S.p.A. riporta di seguito alcuni suggerimenti per creare – e custodire – una password sicura e facilmente memorizzabile dal

Cliente, ma non facilmente intuibile da altri:

- la password può venire creata utilizzando combinazioni di caratteri come riportato al precedente Paragrafo 4.2: nella definizione della password il Cliente può utilizzare ad esempio le iniziali di una frase che può ricordare solamente lui e non associabile ai suoi dati anagrafici. Per contro, la data di nascita del Cliente o quella di una persona vicina al Cliente stesso sono password facilmente intuibili da truffatori che possono conoscere il nome o la situazione anagrafica del Cliente;
- la password non deve essere condivisa con altri servizi online;
- la password non deve contenere parole di senso comune o riferite alla propria vita privata o aziendale (e.g. nomi propri, codice fiscale, date di nascita, targa dell'auto, numero del badge personale, etc.).

4.4 Credenziali - Doveri dell'Istituto di Pagamento

BKN301 S.p.A. ha l'obbligo di:

- assicurare la riservatezza e l'integrità delle Credenziali durante tutte le fasi del processo di autenticazione;
- assicurare che la creazione delle Credenziali avvenga in un ambiente protetto;
- assicurare che solo il Cliente sia associato, in modo sicuro, alle Credenziali;
- assicurare che le Credenziali non siano accessibili a soggetti non legittimati ad utilizzarle, fatti salvi gli obblighi posti in capo al Cliente;
- assicurare che siano sempre disponibili per il Cliente gli strumenti previsti per eseguire la comunicazione di smarrimento e/o furto delle Credenziali, conformemente a quanto previsto nei Regolamenti contrattuali.
- impedire qualsiasi utilizzo delle Credenziali successivo alla comunicazione di smarrimento e/o furto delle stesse, conformemente a quanto previsto nei Regolamenti contrattuali.

4.5 Credenziali - Doveri del Cliente

Il Cliente è pienamente responsabile della custodia e del corretto utilizzo delle Credenziali che devono restare personali e quindi non cedibili a terzi. Dunque il Cliente è tenuto a:

- mantenere segrete le Credenziali e a custodirle con la massima cura e in luoghi tra di loro separati;
- adottare tempestivamente tutte le misure necessarie per impedire l'utilizzo delle Credenziali;
- adempiere con scrupolosa diligenza agli altri obblighi previsti dalle presenti norme tecniche.

4.6 Smarrimento, furto, sottrazione, distruzione e uso non autorizzato delle Credenziali

In caso di smarrimento, furto, sottrazione, distruzione delle Credenziali e qualunque uso non autorizzato di queste ultime, il Cliente oltre a quanto previsto al precedente Paragrafo 4.5, deve darne immediata comunicazione a BKN301 S.p.A..
In caso di smarrimento, furto, sottrazione, distruzione delle apparecchiature informatiche utilizzate per accedere all'APP, e qualunque uso non autorizzato, il Cliente deve adempiere agli obblighi specificamente indicati nel paragrafo che precede, agendo tempestivamente.
In entrambi i casi, il Cliente deve contattare immediatamente il Servizio Clienti ai recapiti e attivo negli orari riportati nella sezione Contatti del Sito Internet di BKN301 S.p.A e rinvenibili anche nel foglio informativo, per

- bloccare immediatamente il Conto;
- bloccare immediatamente la Carta;
- verificare immediatamente eventuali pagamenti sospetti.

In caso di furto o smarrimento della Carta è comunque necessario rivolgersi alle Forze dell'Ordine per sporgere denuncia. La Carta può venire bloccata istantaneamente con un blocco temporaneo anche dall'APP BKN301 S.p.A.

4.7 Custodire il PIN della Carta in modo sicuro e mantenere alto il livello di attenzione

In modo analogo a quanto previsto per le Credenziali, il Titolare della Carta non deve mai comunicare a terzi il PIN (Personal Identification Number) della propria Carta. **Il Titolare della Carta è tenuto a conservare il PIN in un luogo sicuro e lontano dalla propria Carta e deve ricordare che BKN301 S.p.A. non chiede mai questa informazione, né telefonicamente né via Internet né per posta, anche se sicura.**
Il PIN deve essere conosciuto solo dal Titolare della Carta che è l'unico soggetto con la facoltà di inserire tale codice: nessun altro soggetto può inserire tale codice, neppure alla presenza del Titolare della Carta. Il Titolare della Carta è tenuto a mantenere alto il livello di attenzione anche durante gli acquisti più sicuri. Il Titolare della Carta deve ritirare sempre le ricevute ai self service, controllare sempre l'importo prima di inserire il PIN, conservare le ricevute d'acquisto fino alla ricezione o pubblicazione dell'estratto conto.
Per garantire la sicurezza della Carta, le Carte BKN301 utilizzano esclusivamente la tecnologia Chip&PIN con i seguenti vantaggi:

- la tecnologia Chip&PIN rende più difficile la duplicazione e l'accesso ai dati memorizzati sulla Carta;
- le Carte Chip&PIN rafforzano la protezione antifrode in caso di smarrimento, furto o contraffazione delle Carte;
- questo implica una riduzione del rischio che la Carta venga usata illecitamente da persone diverse dal Titolare.

5. Tentativi di accesso, sessione scaduta, validità di autenticazione

Qualora il Cliente, tentando l'accesso all'APP, inserisca erroneamente le Credenziali per più di 3 (tre) volte consecutive, l'Istituto di Pagamento provvede a bloccare temporaneamente l'accesso all'APP del Cliente per motivi di sicurezza.
Per il recupero delle Credenziali di accesso si rimanda ai Paragrafi 6.1 e 6.2 del presente documento.
BKN301 S.p.A. ha definito un periodo massimo dopo il quale le sessioni inattive vengono automaticamente terminate, in particolare l'accesso all'APP rimane attivo per una durata pari a 30 minuti.

6. Recupero delle Credenziali

6.1 Recupero del codice cliente e della password

Nel caso in cui l'accesso all'APP risulti bloccato in via permanente, il Cliente per recuperare il codice cliente e/o la password è tenuto a rivolgersi all'assistenza telefonando **esclusivamente al numero** riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A., e rinvenibili anche nel foglio informativo, e fornire i propri dati personali (nome, cognome, codice fiscale, documento di identità, luogo e data di nascita) e/o altre informazioni al solo ed esclusivo scopo di consentire al Servizio Clienti di indentificare il Cliente.
Si ricorda che BKN301 S.p.A. non chiede mai ai propri Clienti di inviare per e-mail o comunicare telefonicamente o con altro mezzo dettagli e informazioni riservate relative al Conto e alla Carta, nemmeno nel contesto della procedura di recupero password. In ogni caso, BKN301 non contatta mai di propria iniziativa il Cliente per chiedere dettagli e/o informazioni riservate relative all'identità del Cliente stesso e/o al Conto e/o alla Carta.

6.2 Modifica del numero telefonico sul quale ricevere la OTP

Nel caso in cui il Cliente avesse necessità di modificare il proprio numero di cellulare su cui riceve la OTP, dovrà procedere secondo quanto riportato nei Regolamenti contrattuali.

CAPO II – SICUREZZA DEI PAGAMENTI

7. Introduzione

L'Istituto di pagamento si impegna, per quanto di propria competenza, a mettere in atto, con adeguata diligenza, interventi volti a tutelare la sicurezza e la riservatezza dei dati trasmessi e delle comunicazioni effettuate dal/al Cliente per via telematica. Inoltre, BKN301 S.p.A. è costantemente impegnata a tutelare i dati dei Cliente attraverso l'adozione dei più moderni sistemi di sicurezza. I sistemi garantiscono transazioni affidabili e sicure; le interazioni on-line con i Clienti avvengono con il protocollo HTTPS; inoltre, BKN301 S.p.A. garantisce il corretto trattamento dei dati personali dei Clienti.

Al fine di supportare il Cliente, l'Istituto di pagamento ha delineato alcune regole che il Cliente è tenuto a seguire per aumentare la sicurezza nell'utilizzo dei dati sia personali sia relativi al Conto ed alla Carta:

- conservare con la massima cura il nome utente, la password abilitativa e la password dispositiva;
- non rendere note ad altri le proprie Credenziali;
- non inserire le proprie Credenziali in siti Internet raggiunti cliccando su un link presente nelle comunicazioni ricevute via mail o altri servizi di messaggistica o in qualsiasi altro sito che non sia dell'Istituto di pagamento;
- non rispondere ai messaggi dalla dubbia autenticità;
- visitare i siti web digitando l'indirizzo Internet nella barra degli indirizzi;
- modificare periodicamente le Credenziali di accesso;
- installare sul proprio dispositivo software ricevuti da fonti affidabili.

BKN301 non contatta mai, di propria iniziativa, attraverso e-mail o telefono o qualsiasi altro mezzo il Cliente per chiedere dettagli e/o informazioni riservate relative all'identità del Cliente stesso e/o alle sue Credenziali né trasmette al Cliente link per richiedere informazioni e/o l'accesso all'APP né chiede al Cliente di contattare un numero di telefono specifico. In presenza di contatti di questo tipo, anche apparentemente provenienti da BKN301, il Cliente è tenuto ad informare immediatamente BKN301 S.p.A. chiamando il numero riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A. e rinvenibili anche nel foglio informativo**.**

7.1 Phishing

'Phish' significa andare in cerca di informazioni finanziarie riservate: i truffatori inviano false e-mail, creano siti web fasulli ed effettuano telefonate fingendosi funzionari di banca o di società di carte di credito. Lo scopo è quello di indurre con l'inganno i Clienti a rilasciare informazioni personali, finanziarie o bancarie.

BKN301 non contatta mai, di propria iniziativa, attraverso e-mail o telefono o qualsiasi altro mezzo il Cliente per chiedere dettagli e/o informazioni riservate relative all'identità del Cliente stesso e/o alle sue Credenziali né trasmette al Cliente link per richiedere informazioni e/o l'accesso all'APP né chiede al Cliente di contattare un numero di telefono specifico. In presenza di contatti di questo tipo, anche apparentemente provenienti da BKN301, il Cliente è tenuto ad informare immediatamente BKN301 S.p.A. chiamando il numero riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A. e rinvenibili anche nel foglio informativo**.**

7.2 Vishing

Il vishing è una forma di phishing basata sull'uso del telefono. Viene richiesto al Cliente, tramite e-mail o SMS, di chiamare un numero telefonico al quale comunicare le proprie Credenziali (Username/Email e password). In alternativa, viene effettuata una chiamata preregistrata, in cui viene chiesta l'immissione e conferma delle Credenziali.

BKN301 non contatta mai, di propria iniziativa, attraverso e-mail o telefono o qualsiasi altro mezzo il Cliente per chiedere dettagli e/o informazioni riservate relative all'identità del Cliente stesso e/o alle sue Credenziali né trasmette al Cliente link per richiedere informazioni e/o l'accesso all'APP né chiede al Cliente di contattare un numero di telefono specifico. In presenza di contatti di questo tipo, anche apparentemente provenienti da BKN301, il Cliente è tenuto ad informare immediatamente BKN301 S.p.A. chiamando il numero riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A..

7.3 Smishing

Lo Smishing consiste in un messaggio che spesso afferma di provenire da BKN301 S.p.A. chiedendo informazioni finanziarie o personali come il numero di Conto o di Carta al Cliente.

L'Istituto riporta di seguito alcuni consigli che il Cliente è tenuto a seguire per proteggersi da eventuali attacchi di Smishing:

- considerare gli avvisi urgenti sulla sicurezza e/o i messaggi urgenti di riscatto di coupon, offerte e affari, come campanelli d'allarme per un tentativo di attacco informatico;
- non cliccare un link e non contattare un numero di telefono presenti all'interno di messaggi ricevuti dal Cliente;
- non rispondere a messaggi ricevuti dal Cliente;
- non conservare i propri dati bancari o della Carta di pagamento sullo smartphone.

BKN301 non contatta mai, di propria iniziativa, attraverso e-mail o telefono o qualsiasi altro mezzo il Cliente per chiedere dettagli e/o informazioni riservate relative all'identità del Cliente stesso e/o alle sue Credenziali né trasmette al Cliente link per richiedere informazioni e/o l'accesso all'APP né chiede al Cliente di contattare un numero di telefono specifico. In presenza di contatti di questo tipo, anche apparentemente provenienti da BKN301, il Cliente è tenuto ad informare immediatamente BKN301 S.p.A. chiamando il numero riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A..

7.4 Utilizzo del servizio SMS e del servizio di notifiche nell'APP

BKN301 S.p.A., per assicurare la massima sicurezza possibile, mette a disposizione il servizio SMS e ove disponibile il servizio di notifiche push per avvisare il Cliente quando la Carta viene utilizzata. In questo modo il Cliente, oltre a controllare il corretto esito degli acquisti, può accorgersi in tempo reale di eventuali furti e bloccare immediatamente la Carta.

7.5 Protezione dalle frodi in Internet

In caso di acquisti tramite Internet, il Cliente è tenuto a verificare sempre l'attendibilità dell'esercente anche controllando che il sito riporti tutti i suoi dati, compreso l'indirizzo. Inoltre, il Cliente è tenuto ad inserire il numero ed i dati del proprio Conto e/o Carta solo all'atto dell'acquisto e per nessun altro motivo. Il Cliente deve evitare di utilizzare la propria Carta su siti non protetti o non sicuri.

Inoltre, il Cliente è tenuto a prestare attenzione anche alle condizioni di pagamento che sottoscrive. Un pagamento occasionale potrebbe corrispondere all'attivazione di ripetuti pagamenti a scadenza mensile o annuale. In quest'ultimo caso, BKN301 S.p.A. provvede a completare i pagamenti regolati da contratti autorizzati dal Titolare della Carta, senza nessuna responsabilità né autonomia di scelta nel blocco del pagamento. Il Contratto ed i termini di pagamento rimangono definiti solo tra il Cliente ed il soggetto che eroga il servizio in questione.

Per effettuare in sicurezza acquisti o prenotazioni tramite Internet il Cliente è tenuto a ricordare di:

- evitare di effettuare transazioni online da dispositivi condivisi o postazioni in luoghi che potrebbero essere poco sicuri, come ad esempio luoghi pubblici;
- effettuare il log out dal sito di e-commerce, al termine di ogni acquisto;
- utilizzare credenziali diverse per autenticarsi su siti diversi ed evitare il "salvataggio automatico" delle password sul browser;
- valutare sempre l'affidabilità del rivenditore e del sito di e-commerce a cui ci si sta rivolgendo. Leggere, se possibile, eventuali

commenti e recensioni lasciate da altri utenti per conoscere la controparte commerciale, qualora non nota;
- nel caso in cui il Cliente riceva richieste di acquisti/ prenotazioni tramite link, valutare se tale modalità di pagamento sia stata concordata con l'Esercente; una volta cliccato il link, verificare sempre che i dati inerenti l'operazione siano corretti.

7.6. Responsabilità di BKN301 e del Titolare della Carta per le operazioni tramite Internet

Sia BKN301 S.p.A. che il Cliente devono garantire, ciascuno per la propria parte, l'uso corretto e sicuro dei pagamenti tramite Internet. In particolare, il Cliente è responsabile della propria Carta (sia essa virtuale che fisica) e deve rispondere legalmente anche delle operazioni effettuate dai Titolari di Carte aggiuntive legate alla stessa.
In particolare il Cliente è tenuto a:

- custodire con cura la Carta (quando fisica), il PIN e gli eventuali altri i codici di sicurezza e le Credenziali;
- in caso di anomalie o problemi riscontrati durante le Operazioni di Pagamento tramite Internet, o in caso di abuso o utilizzo sospetto della Carta, immediatamente contattare il Servizio Clienti nelle modalità indicate in precedenza;
- controllare regolarmente le movimentazioni del Conto e l'Estratto Conto. Nel caso in cui il Cliente trovi un'operazione che ritiene di non aver eseguito o sulla quale vuole maggiori informazioni, questo è tenuto a contattare il Servizio Clienti che avvia eventuali verifiche. Il Cliente è tenuto a ricordare che dal momento in cui riceve l'Estratto Conto, ha a disposizione 60 giorni di tempo per inviare eventuali contestazioni relative alle operazioni addebitate. È possibile, comunque, contestare eventuali operazioni non autorizzate o non correttamente eseguite nei termini e alle condizioni previste dalle disposizioni vigenti.

BKN301 S.p.A. mette a disposizione dei Cliente un numero dedicato, riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A., e rinvenibili anche nel foglio informativ, disponibile 24 ore su 24, per bloccare la Carta.

7.7. Protezione dei dati e della privacy

- Il Cliente non deve dare la possibilità ad estranei di avvicinarsi a dati sensibili senza il proprio controllo e consenso, per esempio durante le operazioni di prelievo e di pagamento presso gli sportelli ATM. Il Cliente non deve permettere ad altri di avvicinarsi mentre digita il PIN, diffidando di luoghi affollati o non protetti. Inoltre, è consigliato usare una mano per digitare il PIN e l'altra per proteggerne la vista anche da potenziali telecamere.
- Durante operazioni di prelievo e di pagamento presso gli sportelli ATM, in caso di mancata restituzione della Carta, il Cliente è tenuto a chiamare subito ed esclusivamente il Servizio Clienti di BKN301 S.p.A. al numero riportato nella sezione Contatti del Sito Internet di BKN301 S.p.A. per ricevere le corrette indicazioni su come procedere.
- Il Cliente è tenuto a non perdere di vista la Carta nel momento in cui effettua un pagamento. Questo permette di evitare la possibilità di un evento di "skimming", cioè la memorizzazione dei dati contenuti sulle bande magnetiche delle carte di pagamento attraverso lo strisciamento della stessa in un apposito strumento chiamato skimmer.

7.8 Protezione Anti-frode 3D Secure/SCA

Il Servizio 3D Secure/SCA è il sistema di protezione degli acquisti online gratuito studiato dai Circuiti Internazionali Visa e Mastercard che consente di utilizzare la Carta in tutta tranquillità per le spese online. Il servizio permette di prevenire eventuali illeciti della Carta sul web, evitando che il numero di Carta venga usato per pagamenti online ad insaputa del Cliente.
Durante gli acquisti online, a seguito dell'inserimento dei dati richiesti dall'Esercente per il pagamento, verrà mostrata una finestra per completare l'acquisto tramite SCA, ove prevista dal sistema.
Al momento del pagamento, se previsto dal sistema:

1. il Cliente ricevere una notifica autorizzativa tramite APP per completare l'acquisto online:
   - tramite impronta digitale o riconoscimento facciale su device abilitati al riconoscimento biometrico, oppure
   - inserendo sull'apposita schermata di pagamento il codice OTP SMS, utilizzabile solo una volta e nella schermata successiva la password SCA.
2. in caso di indisponibilità temporanea dell'APP con impostazione della password SCA, completare l'acquisto online:
   - inserendo nell'apposita schermata di pagamento il codice OTP SMS, utilizzabile solo una volta e nella schermata successiva la password SCA.

7.9 Ulteriori consigli di sicurezza

Prima di allegare alle e-mail o inviare per altri canali immagini relative ai propri strumenti di pagamento è necessario valutare attentamente le motivazioni ed i destinatari.
Inoltre, è necessario verificare attentamente la provenienza di buoni acquisto ottenuti on-line e l'affidabilità della controparte, prima di fornire qualsiasi informazione personale.

8. Sicurezza delle password e delle credenziali

BKN301 S.p.A. riporta di seguito alcuni suggerimenti che il Cliente deve mettere in atto per proteggere le proprie Credenziali:

- impostare il blocco automatico del proprio dispositivo quando entra in stand-by per proteggere i dati e, quando possibile, attivare la crittografia del dispositivo e della memory card esterna;
- attivare, quando possibile, le funzionalità di "remote lock" e "remote wiping", che consentono al Cliente, in caso di furto, di bloccare e cancellare i dati contenuti sul dispositivo mobile da un altro PC;
- indipendentemente dal dispositivo utilizzato, ricordare di non aprire messaggi e-mail di cui non è conosciuto il mittente o con allegati sospetti. Applicare le stesse regole alle APP di messaggistica istantanea e non aprire allegati o link inviati da utenti sconosciuti.

BKN301 S.p.A. 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.

9. Protezione dei dispositivi personali

9Smartphone o tablet:

- installare sempre gli aggiornamenti ufficiali del sistema operativo appena vengono rilasciati;
- installare sempre gli aggiornamenti e le patch di sicurezza di browser e applicazioni;
- installare e mantenere aggiornato ove disponibile il software di protezione antivirus e ricorda di disattivare Wi-Fi, geolocalizzazione e bluetooth quando non in uso;
- utilizzare esclusivamente app ufficiali provenienti da app store affidabili e, in fase di installazione, fare attenzione ai permessi richiesti assicurandoti che siano strettamente connessi al servizio che si intende utilizzare;
- proteggere il proprio smartphone o tablet con password, PIN e se possibile con sistemi di riconoscimento biometrico (e.g. impronta digitale, riconoscimento del volto, etc.).