

# ING Web Pay

## Ghidul Serviciilor E-commerce

Documentație pentru Comercianți

### Cuprins

<b>Capitolul I - Ghidul comerțului electronic.....</b>	<b>2</b>
1.1.Definiții.....	2
1.2.Considerații generale privind comerțul electronic.....	2
1.3.Cod de bune practici în comerțul electronic .....	4
1.4.Riscul în comerțul electronic.....	5
1.5.Politica de securitate privind utilizarea și procesarea Datelor de card .....	10
<b>Capitolul II - Manual de utilizare a interfeței Aplicației E-commerce .....</b>	<b>13</b>
2.1.Cerințe tehnice necesare utilizării ING WebPay – Interfața de Administrare.....	13
2.2.COT (Procedura de Închidere de Zi/„Batch Settlement”) .....	14
2.3.Identificare și Deconectare .....	14
2.4.Vizualizarea tranzacțiilor .....	15
2.5.Schimbarea parolei .....	22
2.6.Asistență tehnică și operațională .....	22
<b>Capitolul III - Manualul Utilizatorului API (Api for ING WebPay) .....</b>	<b>23</b>
<b>Capitolul IV – Date de test pentru simularea tranzacțiilor și testarea funcționalităților aplicației ING WebPay – mediu de test.....</b>	<b>38</b>

## Capitolul 1

### Ghidul comerțului electronic

#### 1.1. Definiții

**Comerțul electronic** (e-commerce) reprezintă cumpărarea sau vânzarea de bunuri și servicii prin intermediul tehnologiilor oferite de internet. Pentru scopul prezentului document termenul de comerț electronic va fi restrâns numai la cumpărarea/vânzarea pentru care plata s-a efectuat cu cardul pe internet.

**Aplicația ING WebPay/Aplicația E-commerce** – platforma software pusă la dispoziție de către ING Bank pentru a fi accesată prin internet de către Comerciant în scopul utilizării Serviciilor e-commerce. Aceasta include interfața de efectuare a Tranzacțiilor pentru Titularii de Card (MPI), conexiunile ce pot fi accesate de Comerciant pentru a facilita Tranzacțiile, precum și interfața de administrare oferită Comerciantului cu scopul de a obține informații detaliate asupra Tranzacțiilor.

**Procedura de Inchidere de Zi („Batch Settlement”)/Cut of Time/COT** - procedura prin care Comerciantul transmite către ING Bank toate Tranzacțiile efectuate în intervalul de timp ce decurge de la ultima astfel de procesare până la procesarea prezentă. Această procedură determină Decontarea;

**Disputa/Chargeback/Refuz la Plată:** o contestație inițiată de Banca Emitentă la cererea Titularului de Card pentru o Tranzacție pe care acesta o contestă, din diferite motive în temeiul regulilor Organizațiilor de Carduri sau al legii (cum ar fi, dar fără a se limita la, debitare dublă, plata prin alte mijloace, tranzacții efectuate fără consimțământul Titularului de Card, livrare neefectuată, bunuri ce nu corespund cu descrierea Magazinului sau bunuri rambursate conform prevederilor legale). Suma de bani reprezentând valoarea Tranzacției contestate va fi debitată de către Organizația de Carduri din conturile Comerciantului, prin intermediul ING Bank, în favoarea Băncii Emitente conform solicitării Titularului de Card.

#### 1.2. Considerații generale privind comerțul electronic

Pași esențiali în procesarea unei tranzacții de comerț electronic:

- **Autorizarea tranzacției:** Procesul prin care banca emitentă a cardului acceptă sau refuză tranzacția. Autorizarea are loc în momentul efectuării tranzacției.
- **Autentificarea Titularului de Card:** Procesul prin care se certifica faptul că persoana care efectuează tranzacția este Titularul (de drept al) Cardului ale cărui date sunt utilizate în tranzacție.
- **Decontarea:** Procesul prin care suma aferentă tranzacțiilor este creditată în contul Comerciantului de către banca acceptantă, în urma livrării bunului/serviciului care face obiectul tranzacției.

Participanții într-o tranzacție de comerț electronic sunt:

- **Banca Emitentă** – instituția de credit care a emis cardul și a pus la dispoziția Titularului de Card un instrument de plată electronică – Cardul – pe baza unui contract încheiat cu acesta;
- **Titularul de Card** – persoana fizică al cărei nume este înscris pe un Card utilizat în efectuarea plății;
- **Banca Acceptantă** – instituția de credit care pune la dispoziția Comerciantului serviciul de acceptare la plată a cardurilor prin internet și procesează tranzacțiile efectuate în Magazinul virtual al Comerciantului de Titularii de Card;
- **Comerciantul** – persoana juridică sau altă entitate care a solicitat ING Bank furnizarea Serviciului e-commerce;
- **Organizația de Carduri** – o organizație națională sau internațională de servicii (precum Visa sau MasterCard) care reglementează modalitatea de distribuire și utilizare a Cardurilor emise sub licența sa, mărcile disponibile și modul de utilizare a acestora, inclusiv normele și reglementările menite să asigure utilizarea organizată a Cardurilor pe piață;

### Prezentare schematică a unei tranzacții de e-commerce:



### Ce ar trebui să știe orice Comerciant despre comerțul electronic:

- Toate tranzacțiile cu cardul trebuie autorizate (se evită astfel utilizarea unor carduri declarate pierdute/furate sau care nu au fonduri disponibile)
- Comercianții sunt responsabili pentru tranzacțiile frauduloase efectuate pe website-ul lor, indiferent de faptul că au primit sau nu autorizare pentru respectiva tranzacție
- În cazul în care operează direct cu date de card (spre ex. tranzacții introduse manual la Terminalul Virtual) trebuie să își adapteze sistemele în conformitate cu regulile PCI DSS (Payment Card Industry – Data Security Standards, standarde obligatorii de stocare și vizualizare a informațiilor sensibile privind cardurile)
- Nu trebuie să stocheze vreodată codurile CVV2 sau CVC2 pentru utilizări ulterioare
- Comercianții intermediari în sistemele de plăți sau în sistemele comerciale sunt solidari în responsabilitate privind tranzacțiile cu comerciantul final (ex. agențiile de turism cu hotelul)

- Trebuie să accepte la plată toate cardurile VISA sau MasterCard, în conformitate cu regulile cadrului contractual al Serviciului e-commerce; Să afișeze logo-urile VISA, MC, VbV, MSC și toate celelalte logo-uri privind tipurile de carduri și tipurile de servicii acceptate în plată cu cardul
- Toate taxele adiționale (accize, TVA etc.) trebuie evidențiate separat, dar incluse în suma totală a unei tranzacții
- Să deruleze tranzacții comerciale doar în nume și interes propriu sau în baze contractuale
- În mediul electronic, data tranzacției este considerată data livrării produsului (nu data în care s-a efectuat comanda)
- Titularul de card trebuie informat cu privire la modalitatea de livrare, perioada livrării și taxele aferente acestora
- Politica de rambursare și anulare trebuie să fie clar expusă și agreată de client înainte de efectuarea tranzacției
- Tranzacțiile pentru care livrarea serviciului sau produsului se derulează în viitor trebuie desfășurate prin procesul de preautorizare/autorizare
- NU trebuie să aplice niciodată taxe suplimentare pentru utilizarea cardului la plată
- NU trebuie să utilizeze cardul decât strict în relație cu tranzacția consimțită de client (nu pentru alte încasări sau verificări care nu sunt necesare)
- Termenul în care o tranzacție poate fi disputată (comerciantul poate primi un refuz la plată) este de maxim 120 de zile de la data tranzacției

### **1.3. Cod de bune practici în comerțul electronic – Informații esențiale care trebuie să apară pe website**

#### Politica de confidențialitate

- informați clientul despre datele colectate și modul în care vor fi folosite;
- informați clientul cu privire la accesul la aceste date;
- oferiți clientului posibilitatea de a nu i se prelucra datele;

#### Securitatea informațiilor

- afișați toate mijloacele prin care datele clienților sunt securizate și nivelul la care sunt securizate;
- creați o pagină cu întrebări & răspunsuri frecvente despre cum se poate proteja clientul când cumpără online;
- afișați toate logourile sistemelor de securitate pe care le folosiți: de ex. Verified by VISA sau Mastercard SecureCode;

#### Metode de plată

- afișați metodele de plată agreate de site-ul dvs. și menționați foarte clar opțiunile: debit card, credit card etc.

#### Descrierea bunurilor/serviciilor

- asigurați-vă că bunurile sau serviciile oferite sunt descrise cât mai clar și complet (caracteristici tehnice, funcționalități, dacă fac sau nu obiectul unei promoții/discount, țara de origine, service dacă este cazul, prezentați o imagine fidelă a produsului unde este posibil etc.)

#### Modalități de completare a comenzii:

- descrieți/exemplificați modalitatea de completare a comenzii;
- actualizați informațiile despre stocurile disponibile;

#### Expedierea

- menționați obligatoriu modalitățile de livrare;
- clientul trebuie să opteze pentru o singură modalitate de livrare, în cazul în care există mai multe;
- explicați opțiunile de expediție (durata și costurile);
- oferiți serviciul de urmărire a expedițiilor dacă aveți posibilitatea, informați clientul dacă există întârzieri în livrarea bunului/serviciului comandat;
- informați clientul cu privire la modalitățile de returnare a bunurilor comandate și cine suportă costurile returnării;
- menționați responsabilitatea cu privire la deteriorarea bunurilor pe durata transportului sau a celor blocate în vamă;

#### Facturarea

- detaliați modalitatea de facturare, perioada de timp în care suma va apărea pe extrasul de cont, datele de identificare ale comerciantului/ale tranzacției care vor apărea pe extras. Prin aceste detalii eliminați posibilele confuzii;
- încurajați clientul să păstreze datele cu privire la facturare;
- afișați explicit suma totală a tranzacției, taxele și comisioanele incluse (TVA) și valuta în care este emisă factura;
- menționați posibilitatea ca la momentul debitării contului să apară diferențe de curs valutar;

#### Anularea comenzii și returnarea banilor

- asigurați-vă că aveți o politică clară și transparentă de anulare și returnare a banilor;
- oferiți clienților de fiecare dată posibilitatea de a accepta sau respinge politica site-ului;
- în cazul tranzacțiilor de tip abonament, asigurați-vă că taxarea clientului încetează după anularea abonamentului și informați clientul de acest lucru;

#### Adresa de contact

- oferiți clientului toate datele dvs. de contact: e-mail, telefon, adresa sau chestionar spre completare pe site precum și programul de lucru al serviciului de asistență;
- dezvoltați o politică internă de răspuns la mesajele clienților și transmiteți această politică clienților, indicând în măsura în care este posibil timpul estimativ de răspuns;

#### Politicile restrictive

- afișați pe site excepțiile privind acceptarea comenzilor, livrarea bunurilor, produselor, țara de origine a titularului cardului (de ex dacă nu livrați în afara UE);

### 1.4. Riscul în comerțul electronic

#### 1.4.1. Cunoașterea riscului și instruirea angajaților

Este important să cunoașteți cât mai multe metode de prevenire a fraudei pe internet, să le faceți cunoscute persoanelor din firmă care sunt implicate în activitatea de acceptare și să instruiți personalul implicat direct în gestionarea acestor riscuri. Includeți aceste riscuri în politicile de afaceri, practicile operaționale, procedurile de prevenire a fraudelor și în sistemele de monitorizare. Înțelegerea riscurilor reduce cheltuielile ocazionate de refuzurile la plată.

Solicitați Băncii informații cu privire la motivele pentru care s-au primit refuzuri la plată, în special cele pe motiv de :

- probleme legate de autorizare și expirarea perioadei de autorizare;

- probleme legate de nelivrarea bunurilor și serviciilor;
- probleme legate de calitatea bunurilor și serviciilor;
- probleme legate de fraudă;

În calitate de comerciant, sunteți responsabil financiar pentru refuzurile de plată inițiate de titularii de card astfel încât trebuie să vă asigurați că folosiți mijloacele necesare pentru prevenirea lor. Monitorizați personalul implicat direct în preluarea comenzilor clienților și expedierea bunurilor/serviciilor solicitate.

Riscuri tipice pentru comerțul electronic:

a. Frauda

- datele cardurilor furate sunt utilizate pentru achiziționarea de bunuri sau servicii;
- membri ai familiei utilizează datele cardurilor fără consimțământului titularului;
- clienți care reclamă în mod fals neprimirea bunurilor sau serviciilor;
- hackeri și alte tipuri de persoane care fură informații din baza dvs de date pentru a le utiliza în mod organizat;

b. Alte tipuri de refuz la plată care pot rezulta ca urmare a faptului că:

- bunurile și serviciile nu sunt corect descrise pe site;
- există erori tehnice de comandă;
- nu se respectă politica de anulare și returnare de produse a firmei;
- bunurile sau serviciile nu s-au primit sau s-au primit cu întârziere;
- au existat neînțelegeri cu privire la preț, comisioane, taxe;
- au existat erori tehnice de genul dublărilor de facturare;
- există confuzii legate de denumirea comerciantului care apare pe extrasul de cont;

### 1.4.2. Abordarea riscului

Din perspectiva riscului este util că fiecare comerciant, pentru protecția sa și a clienților săi, să-și implementeze mijloace proprii de monitorizare și prevenirea a riscului.

Una din principalele sarcini care intră în atribuțiile unui comerciant este, și în cazul tranzacțiilor pe internet ca și în cazul celor cu prezența cardului, autentificarea, adică identificarea celui care plasează comanda și oferă la plata un card.

Principalele mijloace de identificare a clientului, titular de card, în cursul unei operațiuni de tip e-commerce sunt:

- CVV2 sau CVC2 – codurile VISA și Mastercard, din trei cifre, aflate pe spatele cardurilor și utilizate special pentru autentificare.
- VbV și MSC – „Verified by VISA” și „Mastercard Secure Code” sunt denumirile celor două sisteme de securitate, identificare a titularului cardului, oferite de VISA și Mastercard. Acestea presupun verificarea unei parole alocate titularului cardului și înlătură în cea mai mare măsură responsabilitatea comerciantului privind tranzacțiile pe net.

Aceste servicii de identificare a titularului de card sunt oferite și implementate de banca dumneavoastră și este foarte important să fie folosite conform specificațiilor.

Mijloace suplimentare de verificare:

- este recomandată o evidență, la nivel de comerciant, a tranzacțiilor frauduloase sau suspecte (de ex.: numele celui care face comanda care trebuie să fie același cu numele titularului de card, adrese de mail, adrese de livrare, codul de utilizator și parola de înregistrare pe site, numere de telefon, numere de card etc.).
- contorizarea frecvenței comenzilor; dacă un client depășește un număr normal de comenzi efectuate pe site, într-o perioadă restrânsă de timp, poate exista o suspiciune de fraudă. Este recomandat să se țină evidența pe clienți, iar la apariția suspiciunii să se facă verificări suplimentare.
- este bine să se stabilească un profil al clientului (care sunt sumele cheltuite de obicei, cumpărăturile efectuate de obicei, dacă un client face comenzi cu livrare la mai multe adrese sau dacă mai mulți clienți au aceeași adresă de livrare sau alte date comune etc.)
- o evidență a comenzilor returnate și gestionarea motivelor pentru care au fost returnate
- monitorizarea operațiunilor în funcție de IP-urile de unde provin comenzile (atenție la comenzile provenind de la același IP cu carduri diferite; același card de la mai multe IP-uri; etc)

Gestionarea tranzacțiilor cu risc mare de fraudă:

- utilizați mijloacele de prevenție a fraudelor pentru identificarea tranzacțiilor care prezintă risc: verificați lista internă de clienți, verificați depășirea limitelor setate, etc;
- IP-urile internaționale trebuie privite ca fiind cu risc mare; astfel pentru acestea trebuie luate măsuri suplimentare, adică este necesară verificarea a cât mai multor elemente de siguranță: CVV2, validarea printr-un link trimis la adresa de e-mail, verificarea telefonică, solicitarea unor documente suplimentare de identificare: pașaport, factura de utilități, etc.
- Tratați cu atenție cazurile în care adresa de livrare nu este aceeași cu cea de facturare;
- Verificați tipul adresei de livrare; atenție sporită la locații cu risc mare ca: închisori, cutii poștale, spitale, adrese publice în general;

### **1.4.3. Refuzuri de plată (chargeback)**

#### **1.4.3.1. Ce sunt, cum le evităm și cum recuperăm sumele contestate (eventualele pierderi)**

O dispută între un client titular de card și un comerciant înseamnă timp de procesare și costuri, un profit scăzut în ceea ce privește vânzările și o posibilă scădere a veniturilor pentru majoritatea comercianților.

Este important să urmăriți cu atenție și să înregistrați/administrați refuzurile de plată pe care le primiți, să luați măsuri pentru evitarea acestora și să vă cunoașteți drepturile de a reprezenta/respinge un refuz de plată.

O cerere de documente (copy request) reprezintă o solicitare, făcută înaintea unui refuz la plată, din partea unui titular de card privind o tranzacție regăsită pe extrasul său de cont. Acesta face solicitarea la banca sa, iar banca emitentă transmite solicitarea către banca acceptatoare (a comerciantului). Banca comerciantului trebuie să răspundă acestei solicitări în maxim 30 de zile de la inițierea acesteia de către banca titularului de card. Banca acceptatoare solicită



documentele justificative/detaliile privind tranzacția în cauza comerciantului., iar acesta trebuie să trimită către banca sa toate documentele aferente tranzacției și trebuie să se încadreze în limita de timp acordată. Lipsa unui răspuns sau un răspuns incomplet/ilizibil poate conduce la primirea unui refuz de plată și ulterior la anularea încasării de către comerciant.

Un refuz de plată (chargeback) înseamnă transferarea responsabilității financiare, totală sau parțială, a valorii unei tranzacții, de la emitentul de carduri către acceptatorul de carduri și de la aceasta către comerciant.

În anumite condiții, impuse de Regulamentele Organizațiilor de Carduri, un refuz de plată poate fi contestat de către comerciant (representment); în astfel de situații comerciantul se va consulta cu banca sa acceptatoare.

Pentru a minimiza pierderile aveți nevoie de un sistem adecvat de urmărire/monitorizare a cererilor de documente și a refuzurilor de plată și o înțelegere amănunțită a drepturilor de representment (reprezentarea/respingerea refuzurilor).

Urmați cele mai bune practici:

- Nu finalizați o tranzacție dacă cererea de autorizare a fost respinsă (declined) și nu cereți o nouă autorizare. Solicitați o altă formă de plată.
- Acționați prompt atunci când clienților cu dispute justificate li se cuvin returnarea banilor (creditate pe card/refund). Când titularii de card vă contactează direct pentru a soluționa o dispută, inițiați creditarea cardului în timp util în așa fel încât să evitați disputele inutile și costurile de procesare aferente acestora. Trimiteți clienților un e-mail pentru a-i înștiința imediat de inițierea creditării sumei contestate.
- Furnizați răspunsuri amănunțite la solicitările de documente

Răspundeți la solicitările băncii cu toate informațiile privind tranzacțiile și fiți siguri că ați inclus în răspuns următoarele elemente (obligatorii):

- numărul de card;
- data expirării cardului;
- numele titularului de card;
- data tranzacției;
- suma tranzacției;
- codul de autorizare;
- numele comerciantului;
- adresa online/site-ul comerciantului;
- o descriere generală a bunurilor sau serviciilor furnizate;
- adresa de livrare – dacă este cazul;

Puteți furniza în plus și informații suplimentare care pot ajuta la rezolvarea solicitării și pot reduce astfel riscul de a primi refuz de plată, cum ar fi:

- ora tranzacției;
- adresa de e-mail a clientului;
- numere de telefon ale clientului;
- IP-ul calculatorului
- adresa de facturare a clientului;
- descriere detaliată a bunurilor sau serviciilor furnizate;



- dacă este disponibilă o semnătură de primire obținută la livrarea bunurilor sau serviciilor;

Toate documentele trebuie să fie lizibile, complete și corecte. Un astfel de răspuns conduce în general la lămurirea situației și preîntâmpină un refuz de plată.

Este recomandat să aveți un șablon pentru astfel de solicitări și doar să îl completați atunci când este necesar.

Furnizați răspunsurile la timp pentru solicitările de documente:

- Colaborați cu banca dumneavoastră pentru a implementa o procedură prin care să răspundeți complet și la timp la solicitările de documente venite de la clienți.
- Verificați solicitarea primită de la banca acceptatoare – dacă este potrivită cu bunurile sau serviciile pe care le furnizați.

#### **1.4.3.2. Monitorizarea refuzurilor**

Cele mai bune practici de monitorizarea refuzurilor de plată pot fi:

- Urmărirea/înregistrarea refuzurilor de plată și a contestațiilor acestora după motivul/codul pentru care au fost inițiate. Fiecare motiv de refuz de plată implică metode specifice de a fi remediate și strategii ca acestea să fie diminuate.
- Dacă activitatea dumneavoastră combină vânzările tradiționale cu tranzacțiile pe Internet, urmăriți/înregistrați refuzurile de plată separat pentru aceste tipuri de activități.
- Organizațiile de carduri monitorizează activitatea tuturor comercianților în ceea ce privește numărul de refuzuri de plată și tipul acestora și alertează băncile acceptatoare atunci când unii dintre comercianții lor au primit refuzuri de plată în exces.

#### **1.4.4. Comercianți în turism**

Dacă desfășurați activități conexe turismului, cum ar fi: linii aeriene, hoteluri, agenții de turism, linii de croazieră și închirieri de mașini, condițiile în care puteți accepta la plată carduri, ca și condițiile în care oferiți servicii, prezintă anumite particularități.

În mod deosebit, pentru acești comercianți, există obligații, dar și drepturi suplimentare.

Dintre obligații:

- afișarea, cât mai clară, a termenilor și condițiilor, în special condițiile de anulare și rambursare, cu evitarea clauzelor abuzive
- de a oferi serviciul pentru care s-au obligat sau ceva superior în situația indisponibilității serviciului contractat
- de a transmite o confirmare a rezervărilor imediat ce acestea sunt acceptate
- în cazul anulării rezervărilor este obligatoriu să se transmită o confirmare a acesteia în care să apară clar legătura dintre anulare și confirmarea inițială
- de a-și asuma responsabilitatea solidar cu partenerul de afaceri, dacă oferă servicii prin intermediari

- este esențial să se stabilească o legătură de comunicare cu clientul, de aceea o adresă validă de e-mail este obligatorie
- afișați cât mai clar obligațiile clientului la momentul la care se prezintă să utilizeze serviciul contractat (să se prezinte cu un anumit tip de card sau cu cardul cu care a făcut rezervarea, să se prezinte cu acte de identitate, să se asigure că are banii pentru garanții etc.)
- menționați costurile adiacente (taxe de aeroport, bagaje suplimentare, acces la centre SPA, transport de la aeroport etc.)
- reversați operațiunile cu cardul nefinalizate, anulate. În acest mod veți pune banii la dispoziția titularului cardului.
- este important să capturați și să rețineți IP-ul calculatorului de pe care s-a efectuat comanda

Printre drepturi:

- aveți posibilitatea să opriți garanții de pe card și să obțineți preautorizări înainte de a presta serviciile contractate
- puteți dispune de condiții speciale în cazul refuzurilor la plată, în funcție de motivul pentru care un titular de card refuză tranzacția, detalii pe care le puteți solicita băncii la momentul respectiv

## 1.5. Politica de securitate privind utilizarea și procesarea Datelor de card în conformitate cu PCI DSS

### 1.5.1. Date de card

Cardul bancar este cel mai flexibil instrument de plată. Diversitatea metodelor de plată urmăresc deopotrivă confortul clienților și siguranța tranzacției.

Pentru a participa la o plată, sunt necesare anumite informații despre card. Aceste informații se găsesc tipărite pe card sau stocate pe banda magnetică și în cipul electronic. Pentru banda magnetică și pentru cip se folosesc cititoarele de card din componenta terminalului POS.

Pentru tranzacțiile efectuate în lipsa fizică a cardului au fost stabilite o serie de date de card la care clientul/comerciantul poate avea acces direct, fără intervenția unui cititor electronic. Acestea sunt: **Numele utilizatorului** așa cum a fost inscripționat pe card, **Numărul de card**, **Data expirării**, precum și **Codul de verificare card** (CVV2 la cardurile VISA sau CVC2 la cardurile MasterCard). Aceste date de card sunt numite generic Cardholder Data ("Datele Cardului") respectiv Sensitive Authorization Data ("Date Sensitive de Autorizare") și sunt folosite în tranzacțiile cu card absent. Datorită vulnerabilității lor sunt subiectul unei politici de protejare din partea organizațiilor de carduri.

Un aspect important de reținut este că NU este permisă comerciantului stocarea Codului de verificare card sub nicio formă ulterior autorizării. Banca acceptatoare poate pune la dispoziție comerciantului sistemele necesare pentru procesarea tranzacțiilor de card fără manipularea sau stocarea Datelor Cardului sau ale Datelor Sensitive de Autorizare.

O definiție mai completă și mai exactă a Datelor de Card este dată de PCI Consiliul Standardelor de Securitate din industria cardurilor de plată (PCI Security Standards Council) [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

### 1.5.2. Cadrul comercial

Operațiunea de rezervare, pas premergător plății serviciilor prestate, reprezintă o modalitate de plată oferită clienților lor de către comercianții din industria turistică. Această modalitate de contractare a serviciilor oferă siguranță clienților deținători de card în ceea ce privește programarea sejururilor. În acest sens, ING Bank v-a pus la dispoziție un terminal POS care permite încărcarea de la tastatura a Datelor Sensibile cât și o serie de alte operațiuni care să vă permită un acces util la aplicația de plată cu cardul (pre-autorizare, completare, late charge).

**Canale de recepție** Contactarea clienților și recepționarea datelor de card în vederea pre-autorizării se poate realiza în cele mai felurite moduri de la discuția telefonică la aplicațiile securizate pe internet. Iată câteva exemple de transmitere a Datelor Sensibile:

- a) Date de Card pe suport hârtie obținute prin:
  - poștă,
  - fax,
  - la recepție prin intermediul unui formular intern completat de client,
  - la telefon ;
- b) În format electronic, se pot obține Datele de Card prin:
  - e-mail,
  - formular intern electronic completat de către comerciant în cadrul unei convorbiri telefonice cu deținătorul de card,
  - formular electronic completat de client pe site-ul comerciantului sau pe site-ul unui colaborator de tip booking.com.

### 1.5.3. Stocarea Datelor de card

În vederea efectuării și validării rezervării, Datele Sensibile de Autorizare sunt stocate până la completarea tranzacției. Mediul de stocare și accesul la informație trebuie să respecte normele PCI DSS.

**Atenție!** După autorizare, codul de verificare card CVV2/CVC2 trebuie șters sau făcut ilizibil. Această informație de card nu mai este necesară pentru operațiunile ulterioare (completare, late charge) și nici în procesul unui eventual refuz la plată.

#### 1.5.3.1. Mediul de stocare

Pentru documentele pe suport hârtie, se recomandă scanarea acestora și stocarea copiei electronice într-un calculator securizat cu parolă.

După stocare, suportul hârtie trebuie distrus!

Dacă nu se poate stoca electronic, se recomandă păstrarea acestor documente în incinte securizate, sub controlul persoanei/persoanelor cu atribuții în efectuarea tranzacțiilor cu card.

Pentru accesul la Datele Sensitive de Autorizare stocate electronic este obligatoriu să se folosească controale specifice. Minimul acceptat este folosirea parolei de acces.

#### **1.5.3.2. Iată câteva recomandări pentru stabilirea și administrarea parolelor:**

- i. Lungime: Minim 8 caractere  
Componența: Cel puțin o literă mare, cel puțin o cifră și cel puțin un caracter special: !@#\$%^&\*  
Nu folosiți date personale cunoscute și de alte persoane, nu notați, nu faceți publică parola.
- ii. Accesul va fi limitat strict la persoana/persoanele cu atribuții de serviciu în efectuarea plăților cu cardul. Se recomandă urmărirea atribuirii parolelor către angajații noi (prin instruire) și anularea accesului pentru persoanele care încetează relația de muncă sau primesc atribuțiuni în altă activitate.
- iii. Sistemul de management a parolelor trebuie să permită:
  - a. Schimbare periodică la intervale de maximum 90 zile. Să nu permită folosirea aceleiași parole la reînnoire. Schimbarea parolei ori de câte ori aveți vreo suspiciune cu privire la cunoașterea ei de către alte persoane.
  - b. După acordarea unei parole noi să se ceară obligatoriu modificarea acesteia astfel încât utilizatorul să folosească o parola știută numai de el.
  - c. Blocarea contului după introducerea greșită a parolei de trei ori consecutiv.

Mai multe detalii se pot obține pe site-ul <https://www.pcisecuritystandards.org>. ING Bank vă stă la dispoziție cu informații suplimentare sau lămuriri la adresa [rsm-mcse@ing.ro](mailto:rsm-mcse@ing.ro) subiect: **PCI – DSS**.

## Capitolul 2

### Manual de utilizare a interfeței

### aplicației E-commerce

Serviciului e-commerce (Serviciul **ING WebPay**) reprezintă serviciul ce vă permite acceptarea cardurilor la plată prin internet.

**Interfața de administrare ING WebPay** (Aplicația E-commerce) permite vizualizarea ordinelor de plată inițiate de clienți, selectarea / descărcarea rapoartelor cu tranzacții, precum și anularea ordinelor (în cazul în care nu se mai dorește livrarea bunurilor).

Pentru orice informații sau sesizări, vă rugăm să apelați la numărul de telefon **021 403 83 04** sau să scrieți la adresa de e-mail [contact@ing.ro](mailto:contact@ing.ro).

#### 2.1. Cerințe tehnice necesare utilizării ING WebPay – Interfața de Administrare

Serviciul **ING WebPay – Interfața de Administrare** este disponibil din orice locație din lume atâta timp cât există o conexiune la Internet:

- un calculator cu conexiune la Internet
- sistem de operare Windows 2k, XP, Vista, Mac OSx sau mai recent
- un browser (Microsoft Internet Explorer, Mozilla Firefox, Safari)
- rezoluție de cel puțin 800\*600 SVGA

**!Atenție.** Vă rugăm să vă asigurați că site-ul dumneavoastră corespunde cerințelor standard de securitate prin actualizarea periodică a platformelor folosite.

##### 2.1.1. Codul de utilizator și parola

Utilizatorii Aplicației E-commerce vor primi parola inițială de activare a serviciului și adresa web prin email, la adresa de email declarată către ING Bank la momentul solicitării serviciului. Pentru a obține User-ul (codul de utilizator) este necesar ca reprezentantul legal/mandatar al firmei în relația cu banca să apeleze numărul de telefon **021 403 83 04**.

Utilizatorii Aplicației E-commerce pot beneficia de următoarele drepturi acordate de Comerciant:

1. Utilizatorul API – angajatul are dreptul de a iniția tranzacții prin intermediul Aplicației E-commerce
2. Utilizatorul Raportare – angajatul are dreptul de a vizualiza tranzacțiile efectuate prin intermediul Aplicației E-commerce și a întocmi rapoarte în privința acestora
3. Utilizatorul Administrare – angajatul are, în plus pe lângă drepturile Utilizatorului Raportare, dreptul de a anula sau modifica o tranzacție în aceeași zi în care a fost efectuată, dacă acest lucru

este efectuat înainte de închiderea de zi. Utilizatorul Raportare sau/și Utilizatorul Administrare nu poate/pot fi același/aceeași cu Persoana de Contact Tehnic.

### 2.1.2. Resetarea parolei

În situația în care Utilizatorii au uitat parola sau au contul blocat, reprezentantul legal/mandatar al firmei în relația cu banca trebuie să apeleze pentru deblocare numărul de telefon 021 403 83 04. Utilizatorii vor primi codul de deblocare pe email, în perioada imediat următoare după finalizarea apelului.

## 2.2. COT (Procedura de Închidere de Zi/„Batch Settlement”)

Închiderea de zi se efectuează zilnic, automat.

Momentul limită pentru efectuarea tranzacțiilor înainte de închiderea de zi este COT 22:00. Toate tranzacțiile efectuate înainte de această limită vor fi decontate în perioada de decontare menționată în contract, iar cele efectuate după COT vor intra în următorul ciclu de decontare.

## 2.3. Identificare și Deconectare

### 2.3.1. Cum se accesează aplicația ING WebPay

Interfața de administrare este disponibilă la pagina de internet:

<https://securepay.ing.ro/consola/index.html>

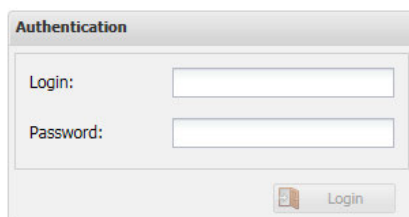


Figura 1

Autentificarea se realizează prin introducerea codului de utilizator alocat de ING Bank și a parolei aferente (Fig 1).

**!Atenție.** Câmpurile sunt „case sensitive”, vă rugăm să respectați formatul userilor și al parolelor transmise de ING Bank.

### 2.3.2. Posibile erori de autentificare si mesaje de eroare

Dacă se introduce un cod de utilizator invalid sau un cod incorect următorul mesaj de eroare va fi afișat pe ecran: *"Form has errors. Bad credentials"*.

După 3 introduceri consecutive greșite contul va fi blocat. Pentru a debloca contul trebuie ca reprezentantul legal/mandatar al firmei în relația cu banca să contacteze ING Bank la numărul de telefon 021 403 83 04.

### 2.3.3. Deconectare

Pentru a închide sesiunea, se selectează butonul Logout din partea dreapta sus a ecranului.

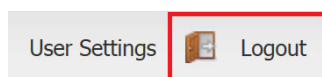


Figura 2

## 2.4. Vizualizarea tranzacțiilor

Prin selectarea opțiunii Orders din meniul principal (Fig. 3). Meniul se încarcă automat în câteva secunde de la logare.

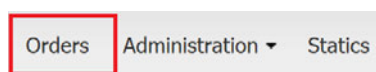


Figura 3

Platforma permite vizualizarea tranzacțiilor în funcție de anumite criterii de selecție disponibile în meniul Filter (în partea stângă a ecranului). Tranzacțiile vor fi afișate în ordinea efectuării lor: **cele mai recente în perioada de timp selectată.**

Se poate actualiza în orice moment lista cu tranzacții (spre ex. pentru a include pe cele noi) prin selectarea butonului Search.

### 2.4.1. Filtrarea și afișarea tranzacțiilor

Prin accesarea opțiunilor disponibile în submeniul Filter (Fig. 3.1) aveți posibilitatea de a căuta și de a vizualiza tranzacțiile în funcție de următoarele criterii de selecție:

- Perioada From – To
  - ✓ Tranzacțiile afișate vor fi cele efectuate în perioada selectată, pot fi aprobate sau respinse în funcție de “Situția plății” (Order Status), sau pot fi limitate de alte criterii de selecție
- Suma minimă, maximă: Maximum / Minimum amount
  - ✓ Tranzacțiile afișate vor fi cele cu suma de autorizare cuprinsă în intervalul selectat, pot fi aprobate sau respinse în funcție de “Situția plății” (Order Status), sau pot fi limitate de alte criterii de selecție.
  - Atenție!** Valoarea introdusă în ambele câmpuri trebuie să respecte formatul “0.00”, în caz contrar filtrarea nu se va efectua.
- Situația plății: Order Status – Creată (Created), Aprobata (Approved), Refuzată (Declined), Anulată (Reversed), Depusă (Deposited), Returnată (Refunded)
- Referința: Reference number
  - ✓ Permite identificarea unei singure tranzacții în funcție de referința internă “RRN” utilizată de regulă de către ING Bank; poate fi utilă în comunicarea cu Banca



- Număr ordine: **Order number**
  - ✓ Permite identificarea unei singure tranzacții în funcție de referința acordată la momentul plății de către ING Bank sau transmisă de către comerciant (vezi Capitolul 3.7.1 ), și afișată în pagina de plată; poate fi utilă în comunicarea cu plătitorul sau cu Banca
  - ✓ Order number este setat automat pentru a fi transmis de către ING. În cazul în care comerciantul transmite acest parametru, este foarte important să anunțe banca, pentru a modifica această setare. (vezi Capitolul 3.7.1)
- Alte criterii specifice.

The screenshot displays the 'Orders Administration Statics' interface. It features a 'Filter' section on the left with the following options:

- Period:** From: 2016-03-15 00:00, To: 2016-03-16 00:00. Search by: ☒ Order creation time, ☐ Time payment.
- Order parameters:**
  - Order Number:** [Text input]
  - Order Status:** [Dropdown menu with options: Approved, Created, Declined, Deposited, Refunded, Reversed]
  - Means of payment:** [Dropdown menu with options: Batch binding payment, Binding, Card, Card (MOTO), SMS binding payment]
  - Order ID:** [Text input]
  - Reference number:** [Text input]
  - Confirmation code:** [Text input]
  - Response code:** [Text input]
- Card Parameters:**
  - Card number:** [Text input]
  - Card holder:** [Text input]
  - IP address:** [Text input]
  - Issuing bank:** [Dropdown menu]
  - Country of the issuing Bank:** [Dropdown menu]
  - Country of the payer:** [Dropdown menu]

At the bottom of the filter section are 'Reset' and 'Search' buttons. The main area on the right shows a table header with columns: Order Number, Date, IP address, and Unique oi.

Figura 3.1

### ATENȚIE!

Criteriile de selecție rămân active pe toată durata sesiunii, ceea ce poate crea confuzii atunci când sunt selectate tranzacții fără să se țină cont de criteriile folosite anterior. De aceea, pentru actualizarea tranzacțiilor se accesează butonul **Reset**, după care se pot aplica alte criterii de selecție sau se pot modifica criteriile selecție și apoi se accesează butonul **Search** pentru actualizare.

### 2.4.2. Descărcare tranzacții

Pentru a descărca o tranzacție sau o listă de tranzacții pe stația locală în vederea procesării cu diverse programe informatice, se accesează opțiunea de „Export to Excel” sau a opțiunii „Export to CSV” disponibile în partea de jos stânga a ecranului (Fig. 3.2).

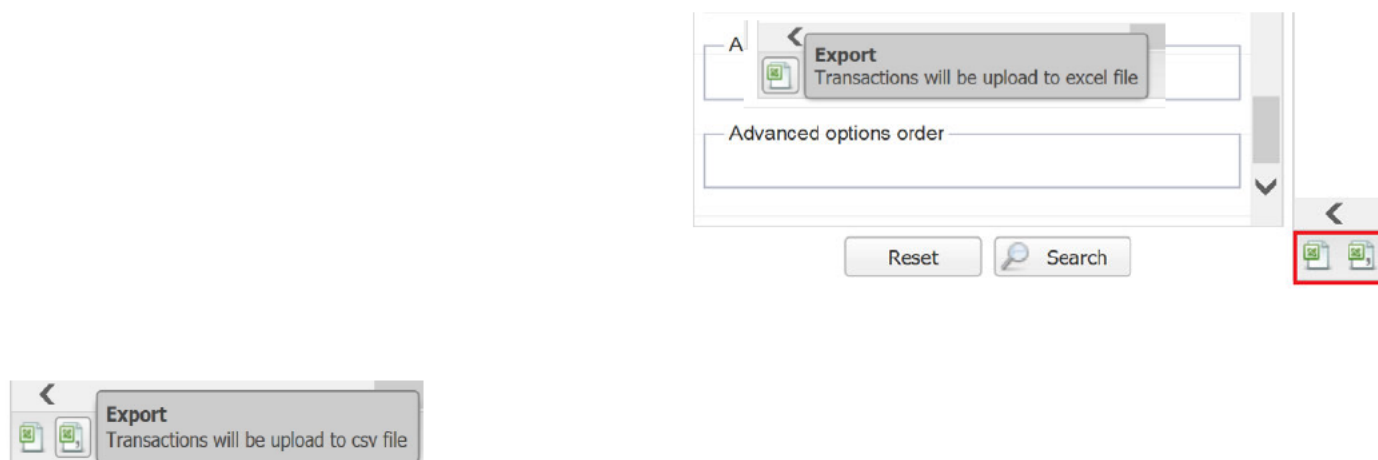


Figura 3.2

### 2.4.3. Selectarea unei tranzacții

Se pot accesa detaliile suplimentare ale unei tranzacții prin dublu-click pe tranzacție. Aceste detalii vor fi afișate într-un tab separat în browser-ul folosit. (Fig. 3.3):

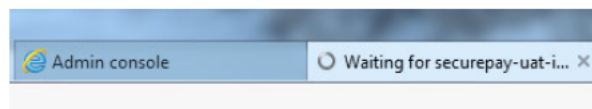
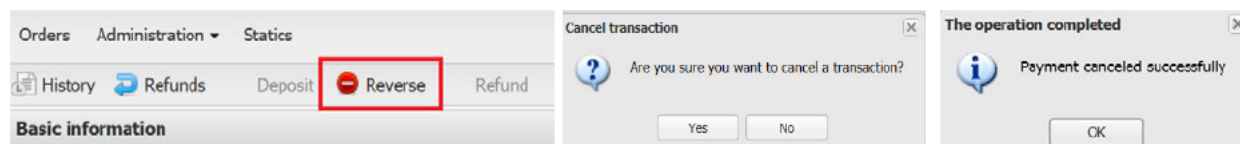


Figura 3.3

### 2.4.4. Anularea unei tranzacții

După selectarea tranzacției (vezi Capitolul Figura 3.2

2.4.3. *Selectarea unei* ), se poate anula o tranzacție până la COT (ora 22.00) prin accesarea opțiunii **Reverse** disponibilă în tab-ul nou deschis (Fig.3.4):



**Figura 3.4**

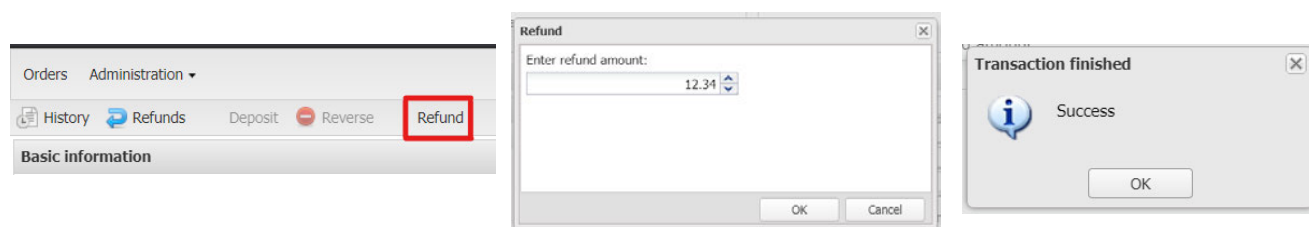
Statusul tranzacției se va modifica în “Reversed”. Actualizarea listei de tranzacții din meniul **Orders** se poate realiza prin selectarea butonul **Search**.

**Atenție!** Opțiunea de anulare a unei tranzacții este disponibilă atât pentru autorizări, cât și pentru preautorizări pe toata durata de valabilitate a acestora sau înainte de a fi completate.

#### 2.4.5. Returnarea unei tranzacții (refund)

După selectarea tranzacției (vezi Capitolul *Figura 3.2*

2.4.3. *Selectarea unei* ), se poate returna o tranzacție după COT (ora 22.00) prin accesarea opțiunii **Refund** disponibilă în tab-ul nou deschis (Fig.3.5). Se va deschide o nouă fereastră unde va trebui introdusă suma ce se dorește a fi returnată .



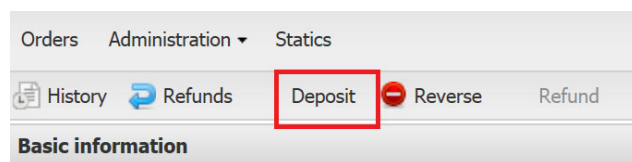
Ulterior, după apăsarea butonului „OK”, se va afișa o nouă fereastră care să confirme efectuarea cu succes a returnării, iar statusul tranzacției se va modifica în “Refunded”. Actualizarea listei de tranzacții din meniul **Orders** se poate realiza prin selectarea butonul **Search**.

**Atenție!** Suma returnată poate fi doar mai mică sau egală cu suma tranzacției inițiale.

#### 2.4.6. Completarea unei pre-autorizări

După selectarea unei tranzacții de pre-autorizare (valabil doar pentru comercianții cu opțiunea respectivă, (a se vedea *Figura 3.2*

2.4.3. *Selectarea unei* ), aceasta se poate completa prin accesarea opțiunii **Deposit** (Fig. 3.6):



și introducerea sumei în căsuța următoare:

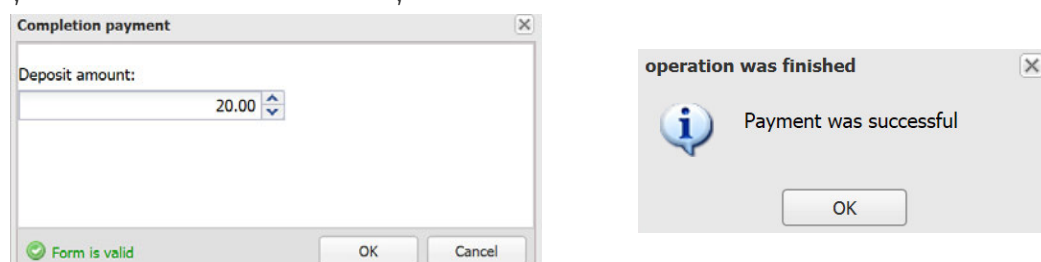


Figura 3.6

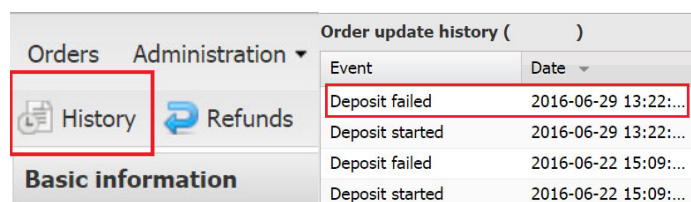
**Atenție! Suma se introduce cu două zecimale folosind separatorul punct „.” (de exemplu: 20.00).** O tranzacție poate fi completată doar pentru o sumă mai mică sau egală cu suma pre-autorizată.

După completarea tranzacției, butonul **Reverse** devine inactiv iar tranzacția va avea status “Deposited” (Figura 3.8). Actualizarea listei de tranzacții din meniul **Orders** se poate realiza prin selectarea butonul **Search**.

**ATENȚIE!**

Termenul de valabilitate al unei pre-autorizări este de 14 zile calendaristice pentru tranzacțiile efectuate cu carduri VISA/Mastercard și de 7 zile calendaristice pentru tranzacțiile efectuate cu carduri Maestro, de la data efectuării tranzacției de către plătitor. Dacă acest termen se depășește, pre-autorizarea expiră și banii nu vor putea fi încasați. În astfel de situații, plătitorul trebuie să efectueze o nouă tranzacție aprobată.

**! Dacă se completează o pre-autorizare după termenul menționat mai sus, vă rugăm să verificați în meniul **History** (Figura 3.7) rezultatul corect al acestei operațiuni, deoarece statusul tranzacției nu se va modifica în interfața (tranzacția va avea în continuare statusul **Approved**).**



Order update history ( )	
Event	Date
Deposit failed	2016-06-29 13:22:00
Deposit started	2016-06-29 13:22:00
Deposit failed	2016-06-22 15:09:00
Deposit started	2016-06-22 15:09:00

Figura 3.7

Completările nu pot fi anulate ulterior, dacă se dorește returnarea sumei completate este necesară contactarea departamentului de asistență la numărul de telefon **021 403 83 04** sau depunerea în sediul ING Bank a unei cereri specifice.

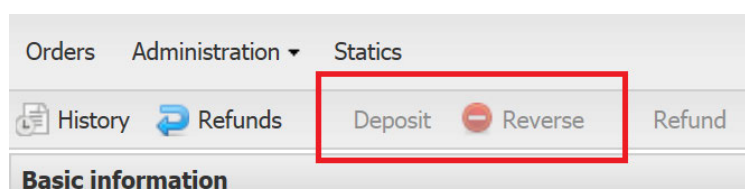


Figura 3.8

Completarea unei pre-autorizari se poate realiza inclusiv din interfața site-ului prin intermediul unui Webservice. Pentru mai multe detalii cu privire la această opțiune, vă rugăm să verificați Capitolul 3.7.3.5.

#### 2.4.7. Detalii comenzi (status, decontare, time-out, culori)

Tabelul de mai jos reprezintă toate statusurile posibile ale unei comenzi:

	State name in the console	Internal name	Description
1	CREATED	started	The order was created
2	APPROVED	payment_approved	The order amount was preauthorized successfully
3	DECLINED	payment_declined	Authorization / preauthorization was declined
4	REVERSED	payment_void	The order was reversed
5	DEPOSITED	payment_deposited	Money were deposited
6	REFUNDED	refunded	Money were refunded

Când un posesor de card începe să facă plata statusul este “Created” și trece în starea de **“Deposited”** după autorizarea tranzacției (atunci când s-a realizat cu succes). În cazul în care nu se finalizează cu succes trece în **“Declined”**, iar dacă e reversată ulterior, în **“Reversed”**.

**Status-ul** în care se poate considera tranzacția finalizată cu succes și se poate elibera bunul este **“Deposited”**. Pentru aflarea online (în timp real) a rezultatului tranzacției trebuie implementat protocolul de comunicare menționat în Capitolul III, punctul 5.3 (pentru detalii discutate cu persoana care va asigura asistența tehnică, cel care a implementat serviciul de plată cu cardul).

O **sesiune de plată** rămâne deschis timp de **10 minute**, după care tranzacția se încheie cu “time out”.

Durata de trecere de la o stare la alta depinde de durata acțiunilor care se fac între stări. De ex. dacă clientului magazinului (posesorul de card) îi ia mai mult timp să valideze parola 3D Secure, trecerea de la “Created” la “Deposited” va să fie mai lungă.

O **plată este deja încasată** în contul de comerciant dacă accesând detaliile acesteia (dublu-click pe plată), în meniul History, câmpul stateExplanation are starea finală “Day Ended”.

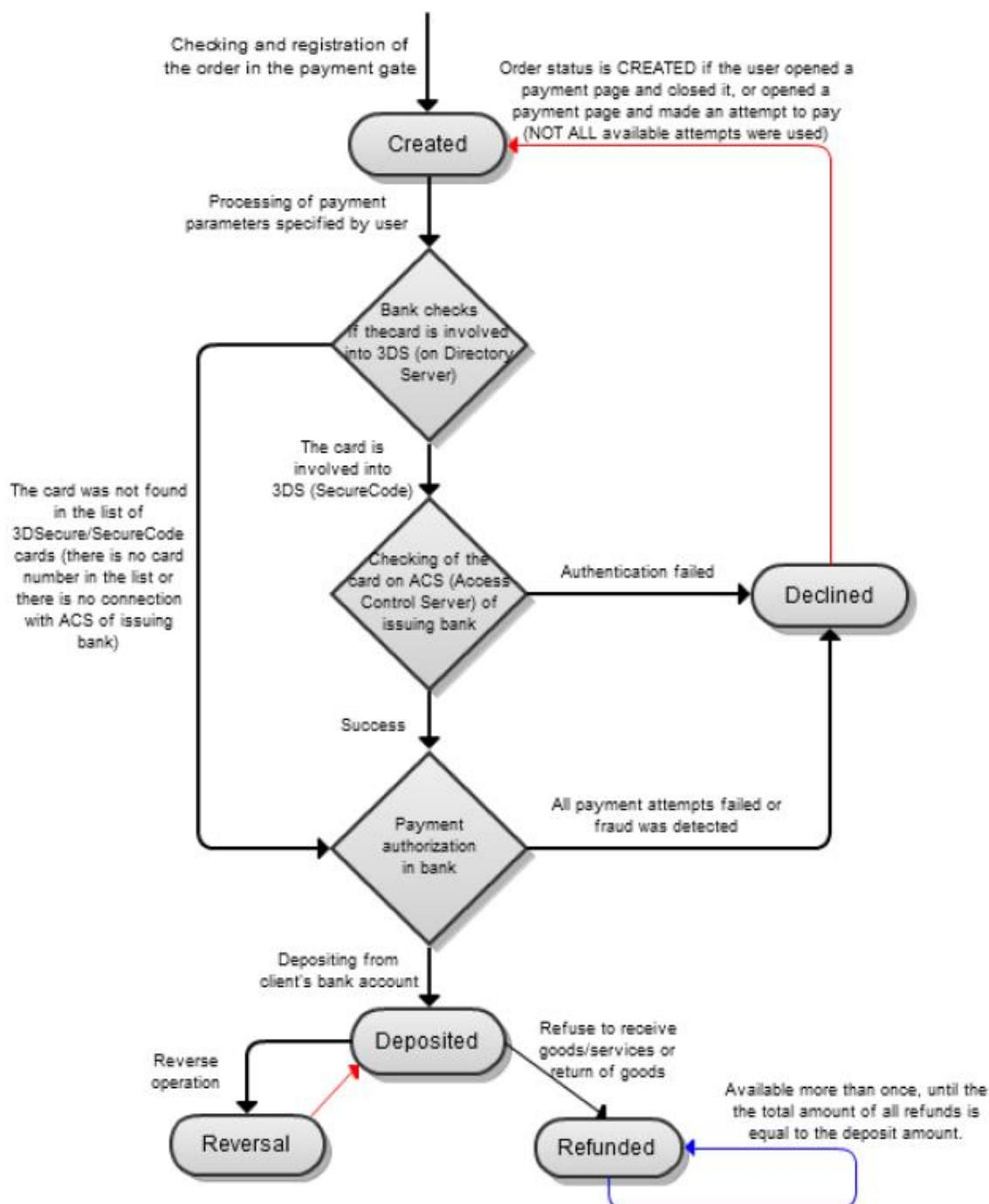
**Sumele decontate** se pot vedea în contul de e-commerce a doua zi de la data la care s-au efectuat plățile (autorizările) de către clienții magazinului (pentru tranzacțiile efectuate înainte de COT 22.00, când are loc settlementul automat).

**Rapoartele** cu privire la plăți se pot obține din aplicație, atât prin utilizatorul raportare, cât și prin utilizatorul administrare. Se accesează Meniul Orders -> Filter -> Se aplică criteriile de filtrare

dorite -> Search-> Export to Excel/ Export to CSV (cele pentru care se vor încasa banii sunt cele cu statusul "Deposited").

**Culorile** din aplicație aferente câmpului "State" (galben, verde, roșu) nu au legătură cu sumele încasate în cont, tranzacțiile respinse sau acceptate, etc, ci sunt folosite strict pentru uzul intern al băncii.

## One-phase payments



## 2.5. Schimbarea parolei

Prin accesarea meniului **User Settings** – Change password (Fig. 4) se poate schimba parola unui Utilizator.

### ATENȚIE!

Parolele acceptate de ING Bank sunt parole complexe, formate din cel puțin 8 caractere, cel puțin un caracter special (e.g. \$, #, & etc...), cel puțin o cifră și cel puțin o literă mare. Fără spațiu.

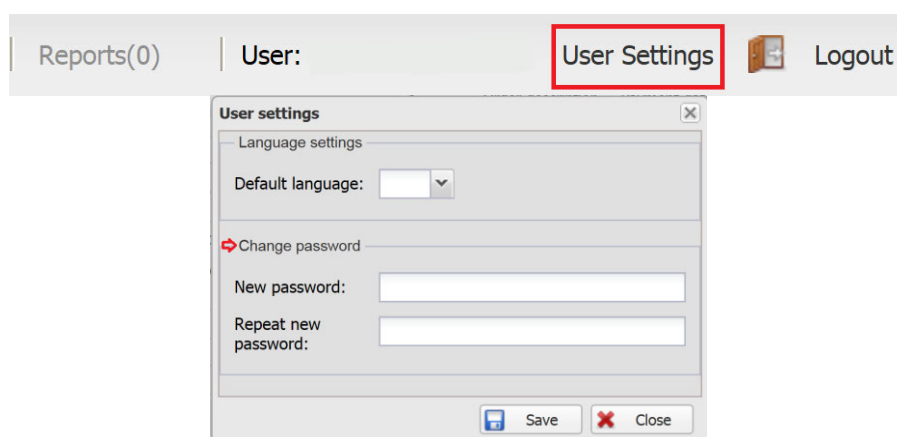


Figura 4

## 2.6. Asistența tehnică și operațională

Pentru orice informații sau sesizări, vă rugăm să ne contactați la numărul de telefon (021) 403 83 04 sau la adresa de e-mail [contact@ing.ro](mailto:contact@ing.ro).

Situațiile în care este necesar suport specializat pot fi următoarele:

- Imposibilitatea accesării paginii de administrare ING WebPay
- Probleme în vizualizarea tranzacțiilor sau descărcarea tranzacțiilor
- Imposibilitatea schimbării parolei
- Imposibilitatea efectuării tranzacțiilor de către titularii de card pe pagina de plată
- Întrebări cu privire la starea unei tranzacții
- Alte situații similare



## Capitolul 3

### Manualul Utilizatorului API

#### (Api for ING WebPay)

#### API pentru ING WebPay - Specificații tehnice

---

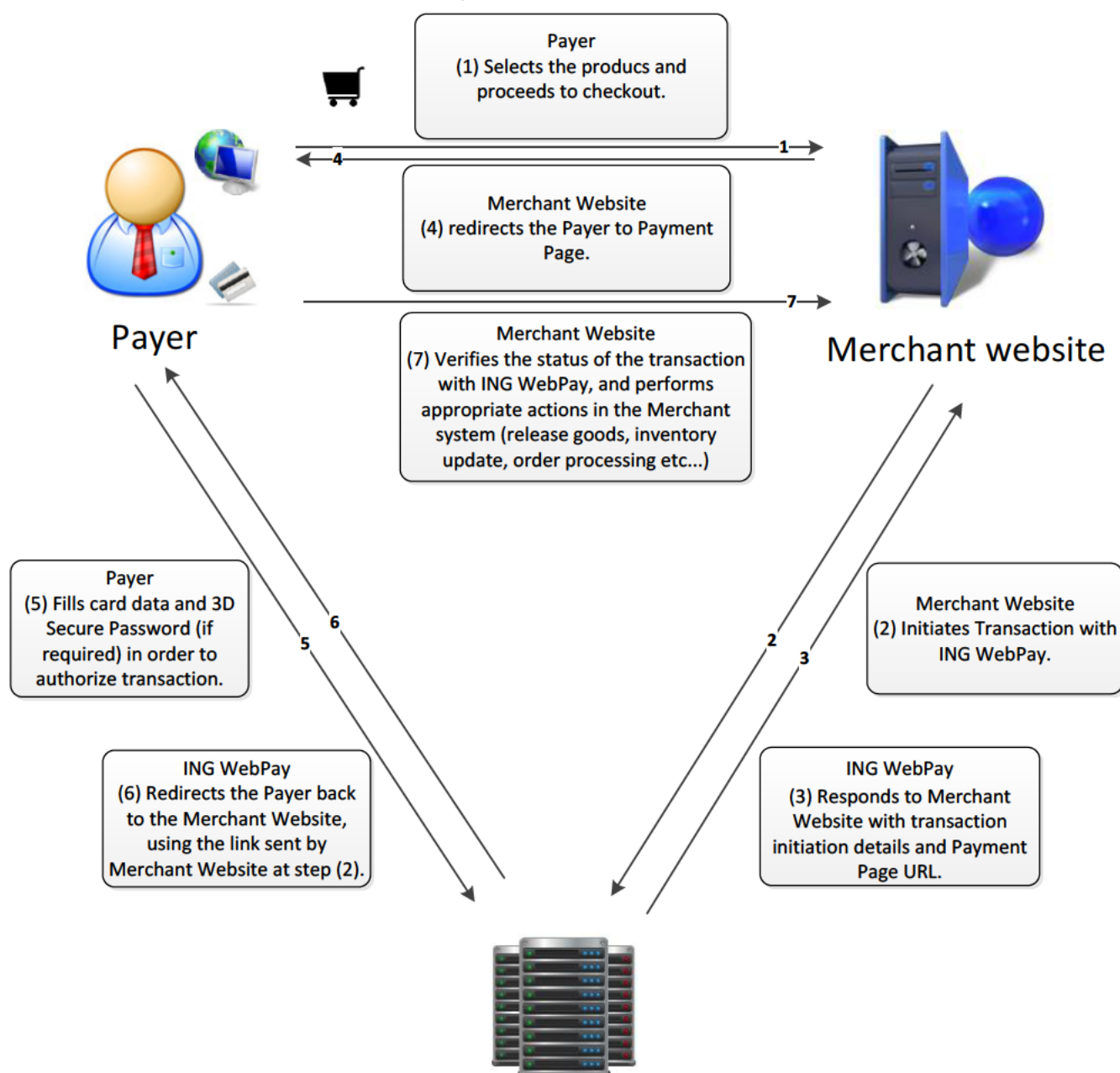
##### 3.1. Scopul documentației

Acest document descrie etapele tehnice care sunt necesare pentru a conecta site-ul comerciantului la serviciul ING WebPay, pentru a iniția tranzacții și a obține statusul autorizării pentru fiecare tranzacție. Documentația este destinată persoanei/persoanelor de contact tehnic desemnat/e de comerciant pentru a dezvolta aplicația.

##### 3.2. Definiții

<b>Consola de administrare</b>	Interfața web pentru serviciul ING WebPay, utilizată de către comerciant pentru a vizualiza, a anula și a edita tranzacțiile
<b>ING WebPay</b>	serverul ING Bank care găzduiește Pagina de Plată și Consola de administrare a Comerciantului
<b>Emitent</b>	banca emitentă a cardului
<b>User-ul API</b>	utilizatorul tehnic atribuit de către ING Bank persoanei de contact tehnic al Comerciantului, cu scopul de a introduce și de a verifica plăți prin API-ul ING WebPay.
<b>Site-ul Comerciantului</b>	server aparținând Comerciantului, care include coșul de cumpărături și funcționalitățile de back-office
<b>Order ID</b>	ID unic asignat de ING WebPay unei tranzacții
<b>Plătitor</b>	persoana care intenționează să achiziționeze bunuri comerciale prin utilizarea cardului
<b>Pagina plății</b>	pagina web găzduită pe serverul ING WebPay care va fi utilizată pentru a colecta datele deținătorului de card

### 3.3. Procesul unei tranzacții E-commerce:



### 3.4. Primii pași înaintea implementării API:

- Înainte de a începe implementarea API, Utilizatorul API și persoana desemnată în relația cu Banca ("Persoana de contact tehnic" / Utilizatorul API), vor primi pe adresa de e-mail, menționată în Cererea de acordare ING WebPay, detaliile mediului de testare (Codul de utilizator API/ parola și codul de utilizator de Administrare/ parola pentru mediul de test)
- Urmați pașii menționați în e-mail și a celor de mai jos.
- După primirea codurilor de utilizator API și parolele aferente mediului de test, Support WebPay va solicita, prin e-mail, logo-ul companiei în format .jpeg,

dimensiune 160x60 px și informațiile subliniate mai jos, pentru personalizarea paginii de plată:

\* Tranzacția este procesată de ING Bank N.V. Amsterdam - Sucursala București în numele XXX (nume comerciant/firma/numele companiei care deține site-ul). Datele cardului dvs. nu sunt puse la dispoziția comerciantului.

\*\* În cazul în care banca emitentă a cardului dvs. și cardul dvs. sunt participante în sistemul 3DSecure, în ecranul următor veți fi invitat să introduceți datele de autentificare pentru 3DSecure.

Pentru detalii suplimentare despre procesare comenzii dvs. vă rugăm să contactați comerciantul XXX (nume comerciant/firma/numele companiei care deține site-ul) la numărul de telefon ZZZ sau la adresa de email xxx@yy.ro.

**Atenție!** La implementarea serviciului ING WebPay pe mai multe valute (RON/EUR), ING Bank va crea și va transmite prin e-mail coduri de utilizator și parole diferite pentru fiecare valută. De aceea, implementarea va fi efectuată de două ori, pentru ambele seturi de utilizatori.

### 3.5. Funcționalitatea “Pay By Link”

Comerciantul are posibilitatea de a implementa funcționalitatea “Pay by Link” în conformitate cu Condițiile Generale Atașate Contractului de Acceptare la Plată a Cardurilor prin Internet și prezentul Ghid.

Serviciul ING WebPay permite implementarea funcționalității “Pay by Link” de către comerciant folosind aceiași parametrii pentru inițierea tranzacției, procesul de plată fiind descris în Capitolele următoare.

Diferența intervine în cazul inițierii comenzii. În mod tradițional, comanda este creată de către client direct pe site-ul comerciantului, prin selectarea și adăugarea în coșul de cumpărături a produselor/serviciilor dorite. În cazul “Pay by Link” comanda este creată de către comerciant și transmisă pe e-mail clientului sub forma unui link administrat de site-ul declarat al comerciantului ce conține detaliile comenzii: pagina de « check-out ».

Pentru implementarea funcționalității “Pay by link” vă rugăm să respectați următoarele cerințe:

- Procesul de plată va fi descris clar și corect pe site-ul principal al comerciantului, alături de celelalte modalități de plată
- Pe site vor fi afișate următoarele informații: Termeni și condiții de livrare; Politica de returnare a produselor; Politica de rezolvare a reclamațiilor; Toate secțiunile impuse de Regulamentele Organizațiilor de Carduri sau Legislația națională tratate în documentele contractuale.
- Se va transmite pe e-mail către client link-ul paginii de « check-out » administrată de site-ul declarat al comerciantului (Atenție! nu pagina de plată ING Bank).
- Pentru accesarea paginii de « check-out » se va solicita clientului autentificarea

- (ex. user și parolă)
- Recomandăm ca pagina de « check-out » să fie de tip « https » sau în pagina de « check-out » să se menționeze faptul că plătitorul va fi direcționat către pagina de plată securizată de tip « https ». Aceste elemente trebuie verificate de către plătitor înainte de autorizarea tranzacției pentru a evita riscul de phishing.
- Pagina de « check-out » va conține următoarele informații: Datele companiei (CUI, denumire, țara de origine, sediul social și date de contact); Datele comenzii (descrierea produselor și prețul unitar și total); Modalitatea de livrare și costul aferent; Bifa pentru acceptarea Termenilor și Condițiilor, a Politicii de Retur și de Anulare ;
- În pagina de « check-out » se va menționa termenul de valabilitate al ofertei , pentru a evita situația în care clientul plătește ulterior și oferta nu mai poate fi respectată de către comerciant.
- Toți parametrii plății (vezi Cap. 3.7) vor fi transmiși de către serverul site-ului (declarat) al comerciantului și nu pot fi modificați de către plătitor.

### 3.6. Autentificarea API

Site-ul Comerciantului va iniția întotdeauna cereri către ING WebPay pentru accesarea serviciilor. Astfel, ING WebPay autentifică Site-ul Comerciantului pe baza codului de Utilizator API și a parolei atribuite responsabilului tehnic al comerciantului.



***Pentru a evita atacurile web, Site-ul Comerciantului trebuie să verifice certificatul ING WebPay, astfel se asigură că cererea este trimisă de un serviciu securizat. Site-ul Comerciantului ar trebui să utilizeze un mecanism care să permită certificatului să fie schimbat (în cazul în care ING Bank actualizează certificatul) și posibilitatea de a-i modifica configurația manual (în cazul în care ING Bank utilizează un certificat expirat). De asemenea, vă rugăm să consultați documentul "hosted\_payment\_page\_security\_visa.pdf" sau să verificați actualizările de securitate Visa Europe. Este necesar că Site-ul Comerciantului să îndeplinească standardele PCI DSS în materie de securitate și să fie actualizat constant. Nu folosiți browser-ul local pentru a apela API (ex: AJAX), pentru a evita divulgarea parolei comerciantului.***

### 3.7. Descriere câmpuri API

Pentru a implementa serviciul de E-commerce ING WebPay, vă rugăm să urmați pașii de mai jos. Dacă site-ul dumneavoastră folosește o platformă E-commerce "open source", vă rugăm să informați pe e-mail serviciul nostru de suport (SupportWebPay@ing.ro) pentru a verifica posibilitatea acordării unor Plug-in-uri pentru instalare.

#### 3.7.1. Inițierea tranzacției

Site-ul Comerciantului inițiază o tranzacție prin trimiterea unui mesaj HTTPS către <https://securepay.ing.ro/mpi/rest/register.do> pentru efectuarea vânzării (dacă nu sunteți sigur de tipul tranzacției pe care trebuie să o inițiați, vă rugăm să verificați cu reprezentantul ING Bank variantele posibile) sau <https://securepay.ing.ro/mpi/rest/registerPreAuth.do> pentru varianta de plată prin pre-autorizare cu specificațiile de mai jos. Pentru mai multe detalii privind pre-

autorizarile verificați capitolul 3.7.3.5. *Completarea sau reversarea tranzacțiilor Pre-autorizate.*

(Pentru mediul test, vă rugăm să verificați link-urile URL prezentate în cadrul capitolului 3.9. Pașii necesari pentru promovarea serviciului ING WebPay în producție)

### 3.7.1.1. Parametrii

Field	Type	Mandatory	Value/Comment
userName	AN..30	Yes	Codul de utilizator API al comerciantului așa cum este furnizat de către ING Bank
password	AN..30	Yes	Parola pentru codul de utilizator API al comerciantului, reprezentantul tehnic al comerciantului. Pentru mai multe detalii, verificați autentificarea API
currency	N3	Yes	Parametru obligatoriu 946 pentru tranzacții în RON. 978 pentru tranzacții în EUR.
orderNumber	AN..32	Yes/No	Element unic de identificare a unei tranzacții; poate fi stabilit de către comerciant sau poate fi atribuit automat de către ING WebPay. Parametrul orderNumber va fi atribuit în mod automat de către ING WebPay. Dacă este setat de către comerciant, ING trebuie să fie informat pentru a evita rejectarea tranzacției. Vă rugăm să verificați detaliile de mai jos*
description	AN..512	No	Descrierea tranzacției, poate fi transmisă de către comerciant și va fi afișată în platforma ING WebPay. Câmpul poate fi lăsat necompletat.
amount	N..20	Yes	Valoarea tranzacției fără separator de zecimale. De exemplu, 102.31 RON este trimis ca 10231.
returnUrl	AN..512	Yes	Link-ul return URL către care plătitorul va fi redirecționat de ING WebPay după autorizarea tranzacției. Link-ul URL se va trimite de forma unencoded.
language	A2	No	ro sau en în funcție de limba setată de către plătitor. O valoare implicită este setată pentru fiecare comerciant.
email	AN	No	Opțiune setată „by default” de către bancă. Adresa de email trebuie să fie validă.
reconciliationId	AN..20	No	Se completează cu informația ce se dorește a fi expusă în rapoartele financiare de reconciliere (poate conține aceeași informație precum câmpul „description”).
orderBundle	JSON	Yes	Format: {}  Acest parametru este obligatoriu de trimis în

			forma de mai sus (chiar dacă va fi trimis gol). Fără trimiterea acestui parametru în acest format nu se va aplica flow-ul agreat de VISA și Mastercard
<b>jsonParams</b>	JSON	Yes	Valoarea obligatorie a parametrului: {"FORCE_3DS2":"true"}

- \* - în cazul în care sistemul este configurat pentru a primi "OrderNumber" de pe site-ul comerciantului, ING nu va genera acest cod și va respinge tranzacția în situația în care nu a primit OrderNumber de la comerciant
- în cazul în care sistemul este configurat să genereze "OrderNumber" fără să-l primească de la site-ul comerciantului, și site-ul trimite acest parametru, atunci tranzacția va fi respinsă automat de către sistem.
- ! Recomandăm transmiterea acestor informații, în cazul în care le dețineți, întrucât în baza lor Emitentul ia decizia de autentificare a tranzacției. Este posibil ca în lipsa acestora, autentificarea să fie respinsă pe motiv că nu există suficiente informații ca să poată fi aprobată tranzacția.

ING WebPay răspunde cu informațiile necesare pentru a continua plata: link-ul paginii plății și ID-ul unic al tranzacției (OrderId)

### 3.7.1.2. Mesaje de răspuns

Name	Type	Mandatory	Value/Comment
<b>orderId</b>	AN..64	No	ID-ul unic al comenzii atribuit de către ING WebPay tranzacției în curs. Câmpul nu este prezent în cazul în care tranzacția nu s-a autorizat.
<b>formUrl</b>	AN..64	No	Link-ul URL al paginii de plată; site-ul comerciantului trebuie să redirectioneze plătitorul pe pagina de plată în vederea completării datelor de card necesare plății. Câmpul nu este prezent în cazul în care tranzacția nu a fost autorizată.
<b>errorCode</b>	N3	No	Dacă există erori în timpul inițierii plății, ING WebPay va completa câmpul cu codul de eroare aferent. Vă rugăm să consultați tabelul 3.7.1.3.Coduri de eroare
<b>errorMessage</b>	AN..512	No	Descrierea erorii returnată de către ING WebPay (afișată în limba solicitată în timpul inițierii tranzacției)



### 3.7.1.3. Coduri de eroare

Valoare	Descriere
0	Nici o eroare întâlnită.
1	Comandă duplicată
3	Valută necunoscută sau interzisă.
4	Parametrul obligatoriu nu a fost specificat.
5	Valoare eronată a unui parametru solicitat.
7	Eroare de sistem.

### 3.7.1.4. Posibile mesaje de eroare

Valoare	Descriere (adaptată de ING Bank pentru limba tranzacției)
1	O comandă cu același număr a fost deja procesată.
1	O comandă cu același număr a fost înregistrată dar nu a fost plătită
3	Valută necunoscută.
3	Valută greșită.
4	Lipsește parametrul "Currency"
4	Lipsește parametrul "Language"
4	Parametrul "orderNumber" nu este completat
4	Parametrul "Merchant name" nu este completat
4	Parametrul "amount" nu este completat
4	Parametrul "returnUrl" nu este completat
4	Parametrul "password" nu este completat
5	Parametrul "Suma" este eronat
5	Parametrul "orderNumber" este eronat
5	Numele comerciantului nu este cunoscut
5	Parametrul "Language" este eronat
5	Parametrul "OrderId" este eronat
5	Parametrul "password" este eronat
5	Codul de utilizator este inactiv
7	Eroare de sistem

### 3.7.1.5. Exemplu mesaj de răspuns la inițiere (mediu de test)

Resp: {"formUrl": "  
https://securepay-  
uat.ing.ro/mpi\_uat/merchants/teste\_eod/payment\_en.html?mdOrder=86faed41-  
d33b-4f10-b3bf-9c2a98ba4bd7","orderId":"86faed41-d33b-4f10-b3bf-  
9c2a98ba4bd7"}

Site-ul comerciantului ar trebui să redirectioneze plătitorul pe pagina plății în vederea completării datelor de card.

### 3.7.2. Efectuarea autorizării



Plătitorul va completa datele de card pe pagina de plată, iar ING WebPay va autoriza tranzacția. Dacă este necesar, ING WebPay va redirecționa plătitorul pe serverul emitentului pentru autentificarea 3D Secure.

După ce tranzacția este inițiată, ING Bank va redirecționa plătitorul pe pagina web din URL-ul de retur (returnUrl) descris în Parametrii, iar site-ul comerciantului poate verifica statusul tranzacției accesând API.

### 3.7.3. Obținerea statusului tranzacției

Pentru a solicita detalii cu privire la tranzacția inițiată, site-ul comerciantului va trimite un mesaj HTTPS către `https://securepay.ing.ro/mpi/rest/getOrderStatus.do` cu următoarele câmpuri:

Field	Type	Mandatory	Value/Comment
<b>orderId</b>	AN..64	No	ID unic al tranzacției atribuit de către ING WebPay tranzacției în curs. Câmpul nu este prezent în cazul în care tranzacția nu s-a autorizat.
<b>userName</b>	AN..30	Yes	Codul de utilizator API al comerciantului, așa cum a fost furnizat de către ING Bank
<b>password</b>	AN..30	Yes	Parola pentru utilizatorul de API, setată de către persoana de contact tehnic. Vă rugăm să verificați <a href="#">Autentificarea API</a>
<b>language</b>	A2	No	<a href="#">ro</a> sau <a href="#">en</a> în funcție de limba setată de către plătitor. O valoare implicită este setată pentru fiecare comerciant.

ING WebPay răspunde cu informațiile necesare:

#### 3.7.3.1. Mesaj de răspuns

GetOrderStatus:

Name	Type	Mandatory	Value/Comment
<b>OrderStatus</b>	N2	No	Statusul plății. Valoarea este selectată din variantele descrise mai jos. Acest parametru lipsește dacă statusul nu corespunde celor din listă.
<b>ErrorCode</b>	N3	No	Dacă există erori în timpul inițierii plății, ING WebPay va afișa în acest câmp codul de eroare. Vă rugăm să consultați tabelul <a href="#">3.7.3.3. Coduri de eroare</a> .

<b>ErrorMessage</b>	AN..512	No	Descrierea erorii returnată de ING WebPay (mesajul este afișat în limba folosită la inițierea tranzacției)
<b>OrderNumber</b>	AN..32	yes	Parametru transmis de către site-ul comerciantului în <u>Parametrii</u> sau este atribuit automat de către ING Bank, în funcție de opțiunea comerciantului (verificați Capitolul 3.7.1.1.)
<b>Pan</b>	N..19	no	Numărul trunchiat al cardului utilizat în plată. Menționat doar pentru comenzile plătite.
<b>expiration</b>	N6	no	Data de expirarea a cardului în formatul YYYYMM. Menționat numai pentru comenzile plătite.
<b>cardholderName</b>	A..64	no	Numele deținătorului de card. Menționat numai pentru comenzile plătite
<b>Amount</b>	N..20	yes	Valoarea plății în unități monetare minimale (cenți, bani).
<b>depositAmount</b>	N..20	yes	Valoarea plății încasate în unități monetare minimale (cenți, bani)
<b>currency</b>	N3	no	Codul valutei plății în conformitate cu ISO 4217. 946 pentru RON, 978 pentru EUR
<b>approvalCode</b>	N6	no	IPS cod autorizare
<b>authCode</b>	N3	no	Codul autorizare al tranzacției
<b>Ip</b>	AN..20	no	Adresa IP a plătitorului
<b>clientId</b>	AN..255	no	Codul de client (identificator) în sistemul comerciantului. Folosit pentru a pune în aplicare o legătură. Prezent doar în cazul în care comerciantului îi este permis să creeze această legătură. (funcționalitate viitoare)
<b>bindingId</b>	AN..255	no	Identificatorul de legătură creat în timpul plății comenzii sau utilizat pentru a plăti. Prezent doar în cazul în care comerciantului îi este permis să creeze această legătură. (funcționalitate viitoare)

#### GetOrderStatusExtended

Name	Type	Mandatory	Value/Comment
<b>ErrorCode</b>	N3	No	Dacă există erori în timpul inițierii plății, ING WebPay va afișa în acest câmp codul de

			eroare. Vă rugăm să consultați tabelul <a href="#">3.7.3.3. Coduri de eroare</a> .
<b>ErrorMessage</b>	AN..512	No	Descrierea erorii returnată de ING WebPay (mesajul este afișat în limba folosită la inițierea tranzacției)
<b>OrderNumber</b>	AN..32	Yes	Parametru transmis de către site-ul comerciantului în <a href="#">Parametrii</a> sau este atribuit automat de către ING Bank, în funcție de opțiunea comerciantului (verificați Capitolul 3.7.1.1.)
<b>OrderStatus</b>	N2	No	Statusul plății. Valoarea este selectată din variantele descrise mai jos. Acest parametru lipsește dacă statusul nu corespunde celor din listă.
<b>ActionCode</b>	N6	Yes	Codul de răspuns generat de sistemul intern de autorizare al tranzacțiilor.
<b>ActionCodeDescription</b>	AN..600	No	Descrierea tranzacției, poate fi transmisă de către comerciant și va fi afișată în platforma ING WebPay. Câmpul poate avea valoarea "null" în cazul în care comerciantul nu transmite acest parametru la inițierea tranzacției. Este conținutul textului inclus în parametrul description trimis către serviciul register.do
<b>Amount</b>	N..20	Yes	Valoarea plății în unități monetare minimale (cenți, bani).
<b>Currency</b>	N3	No	Codul valutei plății în conformitate cu ISO 4217. 946 pentru RON, 978 pentru EUR
<b>Date</b>	TIMESTAMP6	Yes	Data tranzacției
<b>OrderDescription</b>	AN..512	No	Descrierea tranzacției, poate fi transmisă de către comerciant și va fi afișată în platforma ING WebPay. Câmpul poate avea valoarea «null» în cazul în care comerciantul nu transmite acest parametru la inițierea tranzacției.
<b>Ip</b>	AN..20	No	Adresa IP a plătitorului
<b>merchantOrderParams</b>	AN..1024	No	Sunt parametrii adiționali trimiși pentru anumite plăți. În cazul plăților standard câmpul nu se populează.
<b>attributes</b>	AN..250	No	Se returnează orderNumberul plății pentru care se interoghează. Practic este echo din request și are forma: "attributes":[{"name":"mdOrder","value":"246f1288-7ba9-4c3f-ab3d-65125ce3f73f"}]

<b>cardAuthInfo</b>	AN..130	No	Acest parametru cuprinde: Data de expirarea a cardului în formatul YYYYMM; Numele deținătorului de card; codul de autorizare primit de la banca emitentă, Numărul trunchiat al cardului utilizat în plată. Detaliile sunt menționate doar pentru comenzile plătite; "cardAuthInfo":{"expiration":"201804","card holderName":"test","approvalCode":"448520","pan":"425603**0080"}
---------------------	---------	----	--

plății

### 3.7.3.2 Statusul plății

#### Explicație "orderStatus"

Valoare	Descriere
0	Comandă înregistrată, dar neplatită
1	Plată preautorizată (pentru tranzacții în 2 pasi)
2	Tranzacție autorizată
3	Tranzacție anulată
4	Tranzacție reversată
5	Tranzacție inițiată prin sistemul ACS al băncii emitente
6	Tranzacție respinsă

„getOrderStatus” nu returnează descrierea statusului. Pentru informații mai detaliate poate fi utilizat Web-Service-ul „getOrderStatusExtended”. Ambele servicii utilizează aceiași parametri, doar răspunsul este diferit.

Link-ul de producție pentru „getOrderStatusExtended” este:

<https://securepay.ing.ro/mpi/rest/getOrderStatusExtended.do>

### 3.7.3.3. Coduri de eroare

Valoare	Descriere
0	Nicio eroare de sistem
2	Tranzacția este refuzată, deoarece există erori în credențialele plății.
5	Valoare eronată a unui parametru.
6	OrderId neînregistrat

### 3.7.3.4. Exemple mesaj de răspuns pentru status tranzacție:

Exemplu pentru „getOrderStatus”

Resp:

```
{ "expiration": "201512", "cardholderName": "testc", "depositAmount": 0, "currency": "946",  
  "authCode": 2, "errorCode": "2", "errorMessage": "Payment is declined", "orderStatus": 6, "orderNumber": "12266", "Pan": "425601**0206", "Amount": 100, "Ip": "192.168.5.158" }
```

Exemplu pentru „getOrderStatusExtended”

```
{ "errorCode": "0", "errorMessage": "Success", "orderNumber": "107370", "orderStatus": 6, "actionCode": 210, "actionCodeDescription": "Transaction Denied", "amount": 100, "currency": "946", "date": "1403680642722", "orderDescription": "null", "ip": "193.17.195.110", "merchantOrderParams": [], "attributes": [ { "name": "mdOrder", "value": "ff0b026c-c319-4e0f-af1f-230834b0eaec" } ], "cardAuthInfo": { "expiration": "201604", "cardholderName": "testc", "pan": "425603**2773" } }
```

### 3.7.3.5. Completarea sau reversarea tranzacțiilor Pre-autorizate

În cazul pre-autorizărilor (inițiate prin

<https://securepay.ing.ro/mpi/rest/registerPreAuth.do>), sunt două acțiuni posibile: reversarea (anularea) sau finalizarea tranzacției (completarea).

Reversarea (anularea) unei tranzacții se poate realiza în două moduri:

1. Prin Consola de administrare, vă logați folosind Codul de utilizator de administrare, selectați tranzacția respectivă (Status Approved), apăsați butonul “Reverse”. (Vă rugăm să verificați Capitolul 2 – [2.4.4. Anularea unei tranzacții](#)).
2. Prin transmiterea unui mesaj HTTPS către <https://securepay.ing.ro/mpi/rest/reverse.do> cu următorii parametri: User, password, orderID.

Completarea se poate realiza în două moduri:

1. Prin platforma MPI, vă logați folosind Codul de utilizator de administrare, selectați tranzacția respectivă (Status Approved), apăsați butonul „Complete” și introduceți suma tranzacției. (Vă rugăm să verificați Capitolul 2 – [2.4.5. Completarea unei preautorizări](#))
2. Prin trimiterea unui mesaj HTTPS către <https://securepay.ing.ro/mpi/rest/deposit.do> cu următorii parametri: preAuth Order id (generat la inițierea PreAuth), Language, Amount, User și password. Dacă suma trimisă este 0, atunci tranzacția este finalizată automat cu suma inițială.

Vă rugăm să rețineți că nu puteți completa preautorizarea pe o sumă mai mare decât cea pe care a fost inițiată.

### ATENȚIE!

Termenul de valabilitate al unei preautorizări este de 14 zile calendaristice pentru tranzacțiile efectuate cu carduri VISA/Mastercard și de 7 zile calendaristice pentru tranzacțiile efectuate cu carduri Maestro, de la data efectuării tranzacției de către plătitor. Dacă acest termen se depășește, preautorizarea expiră și banii nu vor putea fi încasați. În astfel de situații, plătitorul trebuie să efectueze o nouă tranzacție aprobată.

**! Dacă se completează o preautorizare după termenul menționat mai sus, vă rugăm să verificați în meniul History (Capitolul 2.4.5. Completarea unei preautorizări) rezultatul corect al acestei operațiuni, deoarece statusul tranzacției nu se va modifica în interfață (tranzacția va avea în continuare statusul **Approved**).**

### 3.8. Funcționalitatea “email confirmation for orders”

Această funcționalitate presupune transmiterea automată pe email a confirmării de plata, atât către plătitor (vezi Capitolul 3.7.1.1.Parametrii), cât și către comerciant.

Fiecare confirmare de plată poate conține următoarele informații:

- Valoarea și valuta tranzacției (*Amount and Currency*)
- Statusul tranzacției (*Status*)
- Numărul comenzii (*OrderNumber*)
- Denumire comerciant (*Merchant name*)
- Denumire plătitor (*Cardholder name*)
- Data tranzacției (*Date*)
- Detaliile tranzacției (*Order Description*)

Activarea acestei funcționalități se realizează astfel:

- Comerciant – se activează în baza opțiunii exprimată în Cererea de acordare (ING WebPay) sau a Cererii de modificare date (ING WebPay)
- Plătitor – se activează în baza opțiunii comerciantului exprimată prin transmiterea adresei de email a Plătitorului prin aplicația ING WebPay. Comerciantul își asumă responsabilitatea de a obține acordul plătitorului pentru utilizarea de către Bancă a adresei de email ca mijloc de transmitere a confirmării de plată și de a asigura validitatea adresei de email.

### 3.9. Scenarii de test

- a. Cel puțin o tranzacție aprobată.
- b. Cel puțin o tranzacție refuzată (introducerea eronată a datei de expirare card sau CVV2)
- c. Cel puțin o tranzacție aprobată, dar reversată de „Utilizator de Administrare”.

**! Recomandare:** la efectuarea testelor, sumele trebuie să fie diferite pentru fiecare tranzacție inițiată.



Utilizatorul de API nu are drepturi să verifice tranzacțiile de test în consola de administrare.

Pentru a verifica operațiunile cu cardurile de test, utilizatorii de Administrare / Raportare trebuie să se logheze în <https://securepay-uat.ing.ro/consola/index.html> (pentru mai multe detalii vă rugăm să verificați "Capitolul 2" din acest Ghid)

*Utilizatorul de Raportare are doar drepturi de vizualizare și de întocmire rapoarte în consola de administrare ING WebPay. Utilizatorul de Administrare pe lângă drepturile Utilizatorului de Raportare, mai are posibilitatea de a anula o tranzacție în aceeași zi în care a fost efectuată, dacă acest lucru este efectuat înainte de închiderea de zi și de a modifica o tranzacție pre-autorizată.*

#### 4.1. Pașii necesari pentru promovarea serviciului ING WebPay în producție:

1. După efectuarea scenariilor de test menționate în Capitolul 3.8, trebuie să transmiteți un e-mail la adresa: SupportWebPay@ing.ro și să ne informați că doriți promovarea serviciului de E-commerce în producție;
2. Echipa Support WebPay testează implementarea soluției de plată, verificând următoarele aspecte:
  - Site-ul nu expune date "sensitive" browser-ului local (Ex: cod utilizator API și parola);
  - Sunt transmise mesaje de confirmare clare pentru tranzacțiile aprobate/refuzate;
  - Toate datele sunt trimise în formatul acceptat de sistemele băncii.
3. De asemenea, în acest pas, Banca efectuează o verificare finală asupra site-ului, iar în cazul în care sunt identificate aspecte ce nu corespund Regulamentelor interne și externe (VISA/Mastercard) acestea vor fi sesizate pentru a fi remediate înainte de activarea serviciului de plată. În cazul în care problemele identificate nu pot fi remediate, Banca poate lua decizia de încetare a Contractului de Acceptare. Dacă testele se finalizează cu succes, ING Bank generează credențialele pentru mediul de producție. Fiecare utilizator, inclusiv Utilizatorul API vor primi un e-mail cu parola pentru producție și vor trebui să urmeze pașii menționați în Ghid (Capitolul 2), pentru activarea codurilor de utilizator.
4. Administratorul companiei trebuie să apeleze Serviciul Relații Clienți ING Bank la numărul de telefon (021) 403 83 04 pentru a obține codurile de utilizator ale fiecărei persoane desemnate pe Cererea de acordare serviciu E-Commerce (în e-mail este transmisă doar parola).
5. După activarea utilizatorului API, pe mediul de producție în consola MPI (<https://securepay.ing.ro/consola/index.html>), vă rugăm să modificați în scriptul dezvoltat următoarele link-uri URL (înlocuind link de TEST cu cel de LIVE):

Name	TEST	LIVE
------	------	------



Register	<a href="https://securepay-uat.ing.ro/mpi/uat/rest/register.do">https://securepay-uat.ing.ro/mpi/uat/rest/register.do</a>	<a href="https://securepay.ing.ro/mpi/rest/register.do">https://securepay.ing.ro/mpi/rest/register.do</a>
Pre-authorization	<a href="https://securepay-uat.ing.ro/mpi/uat/rest/registerPreAuth.do">https://securepay-uat.ing.ro/mpi/uat/rest/registerPreAuth.do</a>	<a href="https://securepay.ing.ro/mpi/rest/registerPreAuth.do">https://securepay.ing.ro/mpi/rest/registerPreAuth.do</a>
getOrderStatus (if you use it)	<a href="https://securepay-uat.ing.ro/mpi/uat/rest/getOrderStatus.do">https://securepay-uat.ing.ro/mpi/uat/rest/getOrderStatus.do</a>	<a href="https://securepay.ing.ro/mpi/rest/getOrderStatus.do">https://securepay.ing.ro/mpi/rest/getOrderStatus.do</a>
getOrderStatusExtended (if you use it)	<a href="https://securepay-uat.ing.ro/mpi/uat/rest/getOrderStatusExtended.do">https://securepay-uat.ing.ro/mpi/uat/rest/getOrderStatusExtended.do</a>	<a href="https://securepay.ing.ro/mpi/rest/getOrderStatusExtended.do">https://securepay.ing.ro/mpi/rest/getOrderStatusExtended.do</a>
Web Service Reversare*	<a href="https://securepay-uat.ing.ro/mpi/uat/rest/reverse.do">https://securepay-uat.ing.ro/mpi/uat/rest/reverse.do</a>	<a href="https://securepay.ing.ro/mpi/rest/reverse.do">https://securepay.ing.ro/mpi/rest/reverse.do</a>
Web Service Completare*	<a href="https://securepay-uat.ing.ro/mpi/rest/deposit.do">https://securepay-uat.ing.ro/mpi/rest/deposit.do</a>	<a href="https://securepay.ing.ro/mpi/rest/deposit.do">https://securepay.ing.ro/mpi/rest/deposit.do</a>

\* Pentru utilizarea acestor Web-Service-uri, Persoana desemnată în relația cu banca/Reprezentantul Legal trebuie să solicite băncii acordarea acestor drepturi suplimentare pe baza unui formular tip.

6. Dacă ați reușit implementarea serviciului în producție, vă rugăm să trimiteți un e-mail către [SupportWebPay@ing.ro](mailto:SupportWebPay@ing.ro) cu adresa site-ului.
7. Echipa tehnică ING va verifica serviciul ING WebPay prin efectuarea unei tranzacții cu un card valid, însă care va apărea ca fiind respinsă (se va verifica doar faptul că sistemele se conectează și se primește un răspuns).
8. Administratorul firmei va primi un e-mail de confirmare că totul este în regulă și că plata cu cardul devine accesibilă clienților site-ului. Până la primirea acestui e-mail serviciul este suspendat. În acest e-mail de confirmare se vor transmite inclusiv datele financiare ale serviciului (Merchant ID, Terminal ID, IBAN, etc.).

**Pentru orice problemă tehnică, nu ezitați să contactați serviciul de suport ING WebPay la adresa de e-mail: [SupportWebPay@ing.ro](mailto:SupportWebPay@ing.ro).**

## Capitolul 4

### Date de test pentru simularea tranzacțiilor

### și testarea funcționalităților aplicației

#### ING WebPay – mediu de test

Pentru simularea unor tranzacții și testarea funcționalităților aplicației ING Web Pay în Consola de administrare, puteți utiliza datele de test de mai jos. Tranzacțiile efectuate pe mediul de test nu implică un transfer real de fonduri.

#### Coduri de utilizator:

- Cod de utilizator API: **TEST\_API** & Parola: **q1w2e3r4Q!**
  - Cod de utilizator Administrare: **TEST\_ADMINISTRARE** & Parola: **Ing.123456!**
- !Atenție** Vă rugăm să nu modificați parolele de autentificare ale userilor menționați mai sus, deoarece datele pot fi utilizate și de către alți comercianți.

Consola de administrare: <https://securepay-uat.ing.ro/consola/index.html>

Link simulare tranzacții: [https://securepay-uat.ing.ro/mpi\\_uat/merchants/testecomerciant/test.html](https://securepay-uat.ing.ro/mpi_uat/merchants/testecomerciant/test.html)

#### Date de card (test):

Type	Details
Visa	4771187399025612 Cardholder Name: ING VISA Exp. Date: 06/24 CVV2: 279

**!Atenție** Consola de administrare (mediu de test) este pusă la dispoziția solicitantului, în scop informativ, doar ca mediu de test. Datele de test mai sus menționate pot fi folosite doar în scopul menționat în primul paragraf al acestui Capitol. Ghidul Serviciilor E-commerce ING WebPay este pus la dispoziția solicitantului, doar cu titlu de prezentare a soluției tehnice oferite de ING Bank aferente serviciilor de acceptare la plată a cardurilor prin internet și a caracteristicilor aplicației ING Web Pay.

Prin accesarea Consolei de administrare - mediu de test, solicitantul acceptă condițiile menționate în prezentul capitol și înțelege că punerea la dispoziția sa a datelor de test mai sus menționate și a Ghidului Serviciilor E-commerce ING WebPay este făcută în scop pur informativ, nu reprezintă o ofertă din partea ING Bank și nici o asumare de către ING Bank a oricărei obligații de a încheia un contract cu solicitantul pentru servicii de acceptare la plată a cardurilor prin internet.

În consecință, orice implementare/ dezvoltare efectuată de beneficiarul Consolei de administrare - mediu de test asupra dotărilor sale informatice, în baza datelor de test menționate în prezentul Capitol, în scopul efectuării simulărilor de tranzacții și testării funcționalitatilor aplicației ING Web Pay în mediul de test, se află în deplina responsabilitate a beneficiarului acestor date de test și pe costul acestuia, neputând fi atrasă răspunderea ING Bank pentru eventualele costuri suportate de beneficiar, în cazul în care solicitarea acestuia de acordare a serviciului de E-Commerce (ING WebPay) nu este aprobată de către ING Bank.