

Ghidul Serviciilor E-commerce ING WebPay

Cuprins

Capitolul I - Ghidul comerțului electronic

1.1. Definitii	3
1.2. Consideratii generale privind comerțul electronic	3
1.3. Cod de bune practici în comerțul electronic – Informatii esentiale care trebuie sa apara pe website	5
1.4. Riscul în comerțul electronic	6
1.4.1. Cunoasterea riscului si instruirea angajatilor	6
1.4.2. Abordarea riscului	6
1.4.3. Refuzuri de plata (chargeback)	7
1.4.3.1. Ce sunt, cum le evitam si cum recuperam sumele contestate (eventualele pierderi)	7
1.4.3.2. Monitorizarea refuzurilor	8
1.4.4. Comercianti în turism	8
1.5. Politica de securitate privind utilizarea si procesarea Datelor de card în conformitate cu PCI DSS	9
1.5.1. Date de card	9
1.5.2. Cadrul comercial	9
1.5.3. Stocarea Datelor de card	10
1.5.3.1. Mediul de stocare	10
1.5.3.2. Iata cateva recomandari pentru stabilirea si administrarea parolelor	10

Capitolul II - Manual de utilizare a interfeței Aplicației E-commerce

2.1. Cerinte tehnice necesare utilizării ING WebPay – Interfața de Administrare	11
2.1.1. Codul de utilizator si parola	11
2.1.2. Resetarea parolei	11
2.2. COT (Procedura de Inchidere de Zi/„Batch Settlement”)	11
2.3. Identificare si Deconectare	12
2.3.1. Cum se acceseaza aplicatia ING WebPay	12
2.3.2. Posibile erori de autentificare si mesaje de eroare	12
2.3.3. Deconectare	12
2.4. Vizualizarea tranzactiilor recente	12
2.4.1. Filtrarea si afisarea tranzactiilor	13
2.4.2. Descarcare tranzactii	14
2.4.3. Selectarea unei tranzactii	14
2.4.4. Anularea unei tranzactii	14
2.4.5. Completarea unei preautorizari	15
2.4.6. Detalii comenzi (status, decontare, time-out, culori)	16
2.5. Schimbarea parolei	18
2.6. Asistenta tehnica si operationala	18

Capitolul III - Manualul Utilizatorului API (Api for ING WebPay)

3.1. Scopul documentatiei	19
3.2. Definitii	20
3.3. Procesul unei tranzactii	21
3.4. Primii pasi inaintea implementarii	22
3.5. Autentificare API	22
3.6. Descriere campuri API	22
3.6.1. Initierea tranzactiei	22
3.6.1.1. Parametrii	23
3.6.1.2. Mesaje de raspuns	23
3.6.1.3. Coduri de eroare	24
3.6.1.4. Posibile mesaje de eroare	24
3.6.1.5. Exemplu mesaj de raspuns la initiere (mediu de test)	24
3.6.2. Efectuarea unei autorizari	24
3.6.3. Obtinerea statusului tranzactiei	24
3.6.3.1. Mesaj de raspuns	25
3.6.3.2. Statusul platii	26
3.6.3.3. Coduri de eroare	26
3.6.3.4. Exemple mesaj de raspuns pentru status tranzactie	26
3.6.3.5. Completarea sau reversarea tranzactiilor Preautorizate	26
3.7. Functionalitatea "email confirmation for orders"	27
3.8. Scenarii de test	27
3.9. Pasii necesari pentru promovarea serviciului ING WebPay în productie	28

Capitolul IV – Date de test pentru simularea si testarea functionalitatilor aplicatiei ING WebPay (mediu de test).

Capitolul I - Ghidul comertului electronic

1.1. Definitii

Comertul electronic (e-commerce) reprezinta cumpararea sau vanzarea de bunuri si servicii prin intermediul tehnologiilor oferite de internet. Pentru scopul prezentului document termenul de comert electronic va fi restrans numai la cumpararea/vanzarea pentru care plata s-a efectuat cu cardul pe internet.

Aplicatia ING WebPay/Aplicatia E-commerce – platforma software pusa la dispozitie de catre ING Bank pentru a fi accesata prin internet de catre Comerciant in scopul utilizarii Serviciilor e-commerce. Aceasta include interfata de efectuare a Tranzactiilor pentru Titularii de Card (MPI), conexiunile ce pot fi accesate de Comerciant pentru a facilita Tranzactiile, precum si interfata de administrare oferita Comerciantului cu scopul de a obtine informatii detaliate asupra Tranzactiilor.

Procedura de Inchidere de Zi („Batch Settlement”)/Cut of Time/COT - procedura prin care Comerciantul transmite catre ING Bank toate Tranzactiile efectuate in intervalul de timp ce decurge de la ultima astfel de procesare pana la procesarea prezenta. Aceasta procedura determina Decontarea;

Disputa/Chargeback/Refuz la Plata: o contestatie initiata de Banca Emitenta la cererea Titularului de Card pentru o Tranzactie pe care acesta o contesta, din diferite motive in temeiul regulilor Organizatiilor de Carduri sau al legii (cum ar fi, dar fara a se limita la, debitare dubla, plata prin alte mijloace, tranzactii efectuate fara consimtamantul Titularului de Card, livrare neefectuata, bunuri ce nu corespund cu descrierea Magazinului sau bunuri rambursate conform prevederilor legale). Suma de bani reprezentand valoarea Tranzactiei contestate va fi debitata de catre Organizatia de Carduri din conturile Comerciantului, prin intermediul ING Bank, in favoarea Bancii Emitente conform solicitarii Titularului de Card.

1.2. Consideratii generale privind comertul electronic

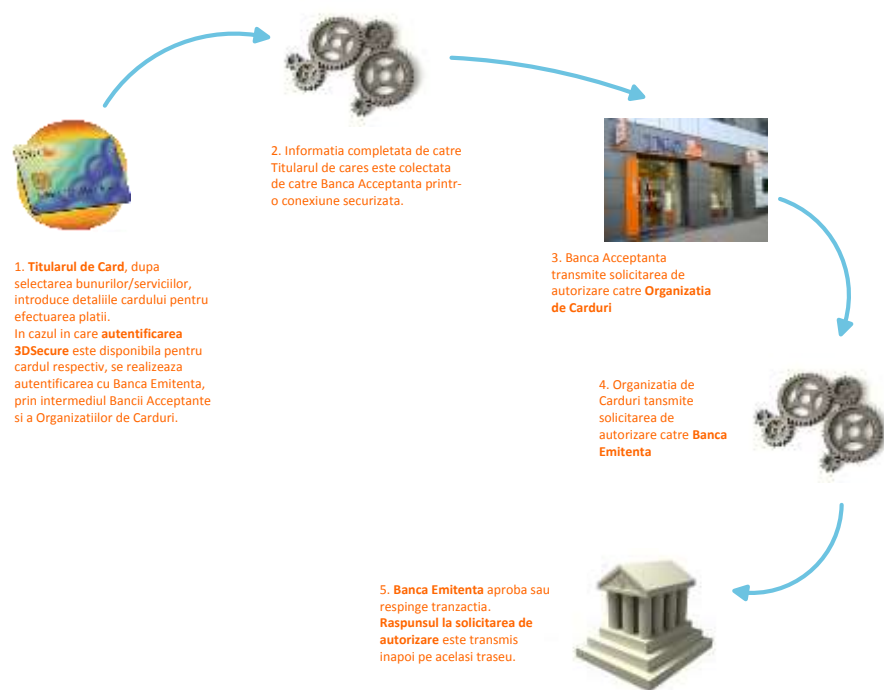
Pasi esentiali in procesarea unei tranzactii de comert electronic:

- **Autorizarea tranzactiei:** Procesul prin care banca emitenta a cardului accepta sau refuza tranzactia. Autorizarea are loc in momentul efectuarii tranzactiei.
- **Autentificarea Titularului de Card:** Procesul prin care se certifica faptul ca persoana care efectueaza tranzactia este Titularul (de drept al) Cardului ale carui date sunt utilizate in tranzactie.
- **Decontarea:** Procesul prin care suma aferenta tranzactiilor este creditata in contul Comerciantului de catre banca acceptanta, in urma livrarii bunului/serviciului care face obiectul tranzactiei.

Participantii intr-o tranzactie de comert electronic sunt:

- **Banca Emitenta** – institutia de credit care a emis cardul si a pus la dispozitia Titularului de Card un instrument de plata electronica – Cardul - pe baza unui contract incheiat cu acesta;
- **Titularul de Card** - persoana fizica al carei nume este inscriptionat sau gravat pe un Card utilizat in efectuarea platii;
- **Banca Acceptanta** – institutia de credit care pune la dispozitia Comerciantului serviciul de acceptare la plata a cardurilor prin internet si proceseaza tranzactiile efectuate in Magazinul virtual al Comerciantului de Titularii de Card;
- **Comerciantul** - persoana juridica sau alta entitate care a solicitat ING Bank furnizarea Serviciului e-commerce;
- **Organizatia de Carduri** - o organizatie nationala sau internationala de servicii (precum Visa sau MasterCard) care reglementeaza modalitatea de distribuire si utilizare a Cardurilor emise sub licenta sa, marcile disponibile si modul de utilizare a acestora, inclusiv normele si reglementarile menite sa asigure utilizarea organizata a Cardurilor pe piata;

Prezentare schematica a unei tranzactii de e-commerce:



Ce ar trebui sa stie orice Comerciant despre comerțul electronic:

- Toate tranzactiile cu cardul trebuie autorizate (se evita astfel utilizarea unor carduri declarate pierdute/furate sau care nu au fonduri disponibile)
- Comerciantii sunt responsabili pentru tranzactiile frauduloase efectuate pe website-ul lor, indiferent de faptul ca au primit sau nu autorizare pentru respectiva tranzactie
- In cazul in care opereaza direct cu date de card (spre ex. tranzactii introduse manual la Terminalul Virtual) trebuie sa isi adapteze sistemele in conformitate cu regulile PCI DSS (Payment Card Industry – Data Security Standards, standarde obligatorii de stocare si vizualizare a informatiilor sensibile privind cardurile)
- Nu trebuie sa stocheze vreodata codurile CVV2 sau CVC2 pentru utilizari ulterioare
- Comerciantii intermediari in sistemele de plati sau in sistemele comerciale sunt solidari in responsabilitate privind tranzactiile cu comerciantul final (ex. agentii de turism cu hotelul)
- Trebuie sa accepte la plata toate cardurile VISA sau MasterCard, in conformitate cu regulile cadrului contractual al Serviciului e-commerce;
- Sa afiseze logo-urile VISA, MC, VbV, MSC si toate celelalte logo-uri privind tipurile de carduri si tipurile de servicii acceptate in platile cu cardul
- Toate taxele aditionale (accize, TVA etc.) trebuie evidentiata separat, dar incluse in suma totala a unei tranzactii
- Sa deruleze tranzactii comerciale doar in nume si interes propriu sau in baze contractuale
- In mediul electronic, data tranzactiei este considerata data livrării produsului (nu data in care s-a efectuat comanda)
- Titularul de card trebuie informat cu privire la modalitatea de livrare, perioada livrării si taxele aferente acestuia
- Politica de rambursare si anulare trebuie sa fie clar expusa si agreata de client inainte de efectuarea tranzactiei
- Tranzactiile pentru care livrarea serviciului sau produsului se deruleaza in viitor trebuie desfasurate prin procesul de preautORIZARE/autorizare
- NU trebuie sa aplice niciodata taxe suplimentare pentru utilizarea cardului la plata
- NU trebuie sa utilizeze cardul decat strict in relatie cu tranzactia consimtita de client (nu pentru alte incasari sau verificari care nu sunt necesare)
- Termenul in care o tranzactie poate fi disputata (comerciantul poate primi un refuz la plata) este de maxim 120 de zile de la data tranzactiei

1.3. Cod de bune practici in comertul electronic – Informatii esentiale care trebuie sa apara pe website

Politica de confidentialitate

- informati clientul despre datele colectate si modul in care vor fi folosite;
- informati clientul cu privire la accesul la aceste date;
- oferiti clientului posibilitatea de a nu i se prelucra datele;

Securitatea informatiilor

- afisati toate mijloacele prin care datele clientilor sunt securizate si nivelul la care sunt securizate;
- creati o pagina cu intrebari & raspunsuri frecvente despre cum se poate proteja clientul cand cumpara online;
- afisati toate logourile sistemelor de securitate pe care le folositi: de ex. Verified by VISA sau Mastercard SecureCode;

Metode de plata

- afisati metodele de plata agreate de site-ul dvs. si mentionati foarte clar optiunile: debit card, credit card etc.

Descrierea bunurilor/serviciilor

- asigurati-va ca bunurile sau serviciile oferite sunt descrise cat mai clar si complet (caracteristici tehnice, functionalitati, daca fac sau nu obiectul unei promotii/discount, tara de origine, service daca este cazul, prezentati o imagine fidela a produsului unde este posibil etc.)

Modalitati de completare a comenzii:

- descrieti/exemplificati modalitatea de completare a comenzii;
- actualizati informatiile despre stocurile disponibile;

Expedierea

- mentionati obligatoriu modalitatile de livrare;
- clientul trebuie sa opteze pentru o singura modalitate de livrare, in cazul in care exista mai multe;
- explicati optiunile de expeditie (durata si costurile);
- oferiti serviciul de urmarire a expeditiilor daca aveti posibilitatea, informati clientul daca exista intarzieri in livrarea bunului/serviciului comandat;
- informati clientul cu privire la modalitatile de returnare a bunurilor comandate si cine suporta costurile returnarii;
- mentionati responsabilitatea cu privire la deteriorarea bunurilor pe durata transportului sau a celor blocate in vama;

Facturarea

- detaliami modalitatea de facturare, perioada de timp in care suma va aparea pe extrasul de cont, datele de identificare ale comerciantului/ale tranzactiei care vor aparea pe extras. Prin aceste detalii eliminati posibilele confuzii;
- incurajati clientul sa pastreze datele cu privire la facturare;
- afisati explicit suma totala a tranzactiei, taxele si comisioanele incluse (TVA) si valuta in care este emisa factura;
- mentionati posibilitatea ca la momentul debitarii contului sa apara diferente de curs valutar;

Anularea comenzii si returnarea banilor

- asigurati-va ca aveti o politica clara si transparenta de anulare si returnare a banilor;
- oferiti clientilor de fiecare data posibilitatea de a accepta sau respinge politica site-ului;
- in cazul tranzactiilor de tip abonament, asigurati-va ca taxarea clientului inceteaza dupa anularea abonamentului si informati clientul de acest lucru;

Adresa de contact

- oferiti clientului toate datele dvs. de contact: e-mail, telefon, adresa sau chestionar spre completare pe site precum si programul de lucru al serviciului de asistenta;
- dezvoltati o politica interna de raspuns la mesajele clientilor si transmiteti aceasta politica clientilor, indicand in masura in care este posibil timpul estimativ de raspuns;

Politicile restrictive

- afisati pe site exceptiile privind acceptarea comenzilor, livrarea bunurilor, produselor, tara de origine a titularului cardului (de ex daca nu livrati in afara UE);

1.4. Riscul in comertul electronic

1.4.1. Cunoasterea riscului si instruirea angajatilor

Este important sa cunoasteti cat mai multe metode de prevenire a fraudei pe internet, sa le faceti cunoscute persoanelor din firma care sunt implicate in activitatea de acceptare si sa instruiti personalul implicat direct in gestionarea acestor riscuri. Includeti aceste riscuri in politicile de afaceri, practicile operationale, procedurile de prevenire a fraudelor si in sistemele de monitorizare. Intelegerea riscurilor reduce cheltuielile ocazionate de refuzurile la plata.

Solicitati Bancii informatii cu privire la motivele pentru care s-au primit refuzuri la plata, in special cele pe motiv de :

- probleme legate de autorizare si expirarea perioadei de autorizare;
- probleme legate de nelivrarea bunurilor si serviciilor;
- probleme legate de calitatea bunurilor si serviciilor;
- probleme legate de fraudă;

In calitate de comerciant, sunteti responsabil financiar pentru refuzurile de plata initiate de titularii de card astfel incat trebuie sa va asigurati ca folositi mijloacele necesare pentru prevenirea lor. Monitorizati personalul implicat direct in preluarea comenzilor clientilor si expedierea bunurilor/serviciilor solicitate.

Riscuri tipice pentru comertul electronic:

a. Frauda

- datele cardurilor furate sunt utilizate pentru achizitionarea de bunuri sau servicii;
- membri ai familiei utilizeaza datele cardurilor fara consimtamantului titularului;
- clienti care reclama in mod fals neprimirea bunurilor sau serviciilor;
- hackeri si alte tipuri de persoane care fura informatii din baza dvs de date pentru a le utiliza in mod organizat;

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

- bunurile si serviciile nu sunt corect descrise pe site;
- exista erori tehnice de comanda;
- nu se respecta politica de anulare si returnare de produse a firmei;
- bunurile sau serviciile nu s-au primit sau s-au primit cu intarziere;
- au existat neintelegeri cu privire la pret, comisioane, taxe;
- au existat erori tehnice de genul dublarilor de facturare;
- exista confuzii legate de denumirea comerciantului care apare pe extrasul de cont;

1.4.2. Abordarea riscului

Din perspectiva riscului este util ca fiecare comerciant, pentru protectia sa si a clientilor sai, sa-si implementeze mijloace proprii de monitorizare si prevenirea a riscului.

Una din principalele sarcini care intra in atributiile unui comerciant este, si in cazul tranzactiilor pe internet ca si in cazul celor cu prezenta cardului, autentificarea, adica identificarea celui care plaseaza comanda si ofera la plata un card.

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

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

Aceste servicii de identificare a titularului de card sunt oferite si implementate de banca dumneavoastra si este foarte important sa fie folosite conform specificatiilor.

Mijloace suplimentare de verificare:

- este recomandata o evidenta, la nivel de comerciant, a tranzactiilor frauduloase sau suspecte (de ex.: numele celui care face comanda care trebuie sa fie acelasi cu numele titularului de card, adrese de mail, adrese de livrare, codul de utilizator si parola de inregistrare pe site, numere de telefon, numere de card etc.).
- contorizarea frecventei comenzilor; daca un client depaseste un numar normal de comenzi efectuate pe site, intr-o perioada restransa de timp, poate exista o suspiciune de fraudă. Este recomandat sa se tina evidenta pe clienti, iar la aparitia suspiciunii sa se faca verificari suplimentare.
- este bine sa se stabileasca un profil al clientului (care sunt sumele cheltuite de obicei, cumparaturile efectuate de obicei, daca un client face comenzi cu livrare la mai multe adrese sau daca mai multi clienti au aceeasi adresa de livrare sau alte date comune etc.)
- o evidenta a comenzilor returnate si gestionarea motivelor pentru care au fost returnate
- monitorizarea operatiunilor in functie de IP-urile de unde provin comenzile (atentie la comenzile provenind de la acelasi IP cu carduri diferite; acelasi card de la mai multe Ip-uri; etc)

Gestionarea tranzactiilor cu risc mare de fraudă:

- utilizati mijloacele de preventie a fraudelor pentru identificarea tranzactiilor care prezinta risc: verificati lista interna de clienti, verificati depasirea limitelor setate, etc;
- IP-urile internationale trebuie privite ca fiind cu risc mare; astfel pentru acestea trebuie luate masuri suplimentare, adica este necesara verificarea a cat mai multor elemente de siguranta: CVV2, validarea printr-un link trimis la adresa de e-mail, verificarea telefonica, solicitarea unor documente suplimentare de identificare: pasaport, factura de utilitati, etc.
- Tratatii cu atentie cazurile in care adresa de livrare nu este aceeași cu cea de facturare;
- Verificati tipul adresei de livrare; atentie sporita la locatii cu risc mare ca: inchisori, cutii postale, spitale, adrese publice in general;

1.4.3. Refuzuri de plata (chargeback)

1.4.3.1. Ce sunt, cum le evitam si cum recuperam sumele contestate (eventualele pierderi)

O disputa intre un client titular de card si un comerciant inseamna timp de procesare si costuri, un profit scazut in ceea ce priveste vanzarile si o posibila scadere a veniturilor pentru majoritatea comerciantilor.

Este important sa urmariti cu atentie si sa inregistrati/administrati refuzurile de plata pe care le primiti, sa luati masuri pentru evitarea acestora si sa va cunoasteti drepturile de a reprezenta/respinge un refuz de plata.

O cerere de documente (copy request) reprezinta o solicitare, facuta inaintea unui refuz la plata, din partea unui titular de card privind o tranzactie regasita pe extrasul sau de cont. Acesta face solicitarea la banca sa, iar banca emitenta transmite solicitarea catre banca acceptatoare (a comerciantului). Banca comerciantului trebuie sa raspunda acestei solicitari in maxim 30 de zile de la initierea acesteia de catre banca titularului de card. Banca acceptatoare solicita documentele justificative/detaliile privind tranzactia in cauza comerciantului., iar acesta trebuie sa trimita catre banca sa toate documentele aferente tranzactiei si trebuie sa se incadreze in limita de timp acordata. Lipsa unui raspuns sau un raspuns incomplet/ilizibil poate conduce la primirea unui refuz de plata si ulterior la anularea incasarii de catre comerciant.

Un refuz de plata (chargeback) inseamna transferarea responsabilitatii financiare, totala sau partiala, a valorii unei tranzactii, de la emitentul de carduri catre acceptatorul de carduri si de la aceasta catre comerciant.

In anumite conditii, impuse de Regulamentele Organizatiilor de Carduri, un refuz de plata poate fi contestat de catre comerciant (representment); in astfel de situatii comerciantul se va consulta cu banca sa acceptatoare.

Pentru a minimiza pierderile aveti nevoie de un sistem adecvat de urmarire/monitorizare a cererilor de documente si a refuzurilor de plata si o intelegere amanuntita a drepturilor de representment (reprezentarea/respingerea refuzurilor).

Urmati cele mai bune practici:

- Nu finalizati o tranzactie daca cererea de autorizare a fost respinsa (declined) si nu cereti o noua autorizare. Solicitati o alta forma de plata.
- Actionati prompt atunci cand clientilor cu dispute justificate li se cuvin returnarea banilor (creditare pe card/refund). Cand titularii de card va contacteaza direct pentru a solutiona o disputa, initiati creditarea cardului

in timp util in asa fel incat sa evitati disputele inutile si costurile de procesare aferente acestora. Trimiteti clientilor un e-mail pentru a-i instiinta imediat de initierea creditarii sumei contestate.

- Furnizati raspunsuri amanuntite la solicitarile de documente

Raspundeti la solicitarile bancii cu toate informatiile privind tranzactiile si fiti siguri ca ati inclus in raspuns urmatoarele elemente (obligatorii):

- numarul de card;
- data expirarii cardului;
- numele titularului de card;
- data tranzactiei;
- suma tranzactiei;
- codul de autorizare;
- numele comerciantului;
- adresa online/site-ul comerciantului;
- o descriere generala a bunurilor sau serviciilor furnizate;
- adresa de livrare – daca este cazul;

Puteti furniza in plus si informatii suplimentare care pot ajuta la rezolvarea solicitarii si pot reduce astfel riscul de a primi refuz de plata, cum ar fi:

- ora tranzactiei;
- adresa de e-mail a clientului;
- numere de telefon ale clientului;
- IP-ul calculatorului
- adresa de facturare a clientului;
- descriere detaliata a bunurilor sau serviciilor furnizate;
- daca este disponibila o semnatura de primire obtinuta la livrarea bunurilor sau serviciilor;

Toate documentele trebuie sa fie lizibile, complete si corecte. Un astfel de raspuns conduce in general la lamurirea situatie si preintampina un refuz de plata.

Este recomandat sa aveti un sablon pentru astfel de solicitari si doar sa il completati atunci cand este necesar.

Furnizati raspunsurile la timp pentru solicitarile de documente:

- Colaborati cu banca dumnevoastra pentru a implementa o procedura prin care sa raspundeti complet si la timp la solicitarile de documente venite de la clienti.
- Verificati solicitarea primita de la banca acceptatoare – daca este potrivita cu bunurile sau serviciile pe care le furnizati.

1.4.3.2. Monitorizarea refuzurilor

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

- Urmarirea/inregistrarea refuzurilor de plata si a contestatiilor acestora dupa motivul/codul pentru care au fost initiate. Fiecare motiv de refuz de plata implica metode specifice de a fi remediate si strategii ca acestea sa fie diminuate.
- Daca activitatea dumnevoastra combina vanzarile traditionale cu tranzactiile pe Internet, urmariti/inregistrati refuzurile de plata separat pentru aceste tipuri de activitati.
- Organizatiile de carduri monitorizeaza activitatea tuturor comerciantilor in ceea ce priveste numarul de refuzuri de plata si tipul acestora si alerteaza bancile acceptatoare atunci cand unii dintre comerciantii lor au primit refuzuri de plata in exces.

1.4.4. Comercianti in turism

Daca desfasurati activitati conexe turismului, cum ar fi: linii aeriene, hoteluri, agentii de turism, linii de croaziera si inchirieri de masini, conditiile in care puteti accepta la plata carduri, ca si conditiile in care oferiti servicii, prezinta anumite particularitati.

In mod deosebit, pentru acesti comercianti, exista obligatii, dar si drepturi suplimentare.

Dintre obligatii:

- afisarea, cat mai clara, a termenilor si conditiilor, in special conditiile de anulare si rambursare, cu evitarea clauzelor abuzive
- de a oferi serviciul pentru care s-au obligat sau ceva superior in situatia indisponibilitatii serviciului contractat
- de a transmite o confirmare a rezervarilor imediat ce acestea sunt acceptate
- in cazul anularii rezervarilor este obligatoriu sa se transmita o confirmare a acesteia in care sa apara clar legatura dintre anulare si confirmarea initiala
- de a-si asuma responsabilitatea solidar cu partenerul de afaceri, daca ofera servicii prin intermediari
- este esential sa se stabileasca o legatura de comunicare cu clientul, de aceea o adresa valida de e-mail este obligatorie
- afisati cat mai clar obligatiile clientului la momentul la care se prezinta sa utilizeze serviciul contractat (sa se prezinte cu un anume tip de card sau cu cardul cu care a facut rezervarea, sa se prezinte cu acte de identitate, sa se asigure ca are banii pentru garantii etc.)
- mentionati costurile adiacente (taxe de aeroport, bagaje suplimentare, acces la centre SPA, transport de la aeroport etc.)
- reversati operatiunile cu cardul nefinalizate, anulate. In acest mod veti pune banii la dispozitia titularului cardului.
- este important sa capturati si sa retineti IP-ul calculatorului de pe care s-a efectuat comanda

Printre drepturi:

- aveti posibilitatea sa opriti garantii de pe card si sa obtineti preautorizari inainte de a presta serviciile contractate
- puteti dispune de conditii speciale in cazul refuzurilor la plata, in functie de motivul pentru care un titular de card refuza tranzactia, detalii pe care le puteti solicita bancii la momentul respectiv

1.5. Politica de securitate privind utilizarea si procesarea Datelor de card in conformitate cu PCI DSS

1.5.1. Date de card

Cardul bancar este cel mai flexibil instrument de plata. Diversitatea metodelor de plata urmaresc deopotriwa confortul clientilor si siguranta tranzactiei.

Pentru a participa la o plata, sunt necesare anumite informatii despre card. Aceste informatii se gasesc tiparite pe card sau stocate pe banda magnetica si in cipul electronic. Pentru banda magnetica si pentru cip se folosesc cititoarele de card din componenta terminalului POS.

Pentru tranzactiile efectuate in lipsa fizica a cardului au fost stabilite o serie de date de card la care clientul/comerciantul poate avea acces direct, fara interventia unui cititor electronic. Acestea sunt: **Numele utilizatorului** asa cum a fost inscriptionat pe card, **Numarul de card**, **Data expirarii**, precum si **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") si sunt folosite in tranzactiile cu card absent. Datorita vulnerabilitatii lor sunt subiectul unei politici de protejare din partea organizatiilor de carduri.

Un aspect important de retinut este ca NU este permisa comerciantului stocarea Codului de verificare card sub nicio forma ulterior autorizarii. Banca acceptatoare poate pune la dispozitie comerciantului sistemele necesare pentru procesarea tranzactiilor de card fara manipularea sau stocarea Datelor Cardului sau ale Datelor Sensitive de Autorizare.

O definitie mai completa si mai exacta a Datelor de Card este data de PCI Consiliul Standardelor de Securitate din industria cardurilor de plata (PCI Security Standards Council) www.pcisecuritystandards.org

1.5.2. Cadrul comercial

Operatiunea de rezervare, pas premergator platii serviciilor prestate, reprezinta o modalitate de plata oferita clientilor lor de catre comerciantii din industria turistica. Aceasta modalitate de contractare a serviciilor ofera siguranta clientilor detinatori de card in ceea ce priveste programarea sejururilor. In acest sens, ING Bank v-a pus la dispozitie un terminal POS care permite incarcarea de la tastatura a Datelor Sensibile cat si o serie de alte operatiuni care sa va permita un acces util la aplicatia de plata cu cardul (pre-autorizare, completare, late charge).

Canale de receptie Contactarea clientilor si receptionarea datelor de card in vederea pre-autorizarii se poate realiza in cele mai felurite moduri de la discutia telefonica la aplicatiile securizate pe internet. Iata cateva exemple de transmitere a Datelor Sensibile:

- a) Date de Card pe suport hartie obtinute prin:
 - posta,
 - fax,
 - la receptie prin intermediul unui formular intern completat de client,
 - la telefon ;
- b) In format electronic, se pot obtine Datele de Card prin:
 - e-mail,
 - formular intern electronic completat de catre comerciant in cadrul unei convorbiri telefonice cu detinatorul 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

In vederea efectuarii si validarii rezervarii, Datele Sensitive de Autorizare sunt stocate pana la completarea tranzactiei. Mediul de stocare si accesul la informatie trebuie sa respecte normele PCI DSS.

Atentie! Dupa autorizare, codul de verificare card CVV2/CVC2 trebuie sters sau facut ilizibil. Aceasta informatie de card nu mai este necesara pentru operatiunile ulterioare (completare, late charge) si nici in procesul unui eventual refuz la plata.

1.5.3.1. Mediul de stocare

Pentru documentele pe suport hartie, se recomanda scanarea acestora si stocarea copiei electronice intr-un calculator securizat cu parola.

Dupa stocare, suportul hartie trebuie distrus!

Daca nu se poate stoca electronic, se recomanda pastrarea acestor documente in incinte securizate, sub controlul persoanei/persoanelor cu atributii in efectuarea tranzactiilor cu card.

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

1.5.3.2. Iata cateva recomandari pentru stabilirea si administrarea parolelor:

- i. Lungime: Minim 8 caractere
Componenta: Cel putin o litera mare, cel putin o cifra si cel putin un caracter special: !@#%&^*
Nu folositi date personale cunoscute si de alte persoane, nu notati, nu faceti publica parola.
- ii. Accesul va fi limitat strict la persoana/persoanele cu atributii de serviciu in efectuarea platilor cu cardul. Se recomanda urmarirea atribuirii parolelor catre angajatii noi (prin instruire) si anulara accesului pentru persoanele care inceteaza relatia de munca sau primesc atributiuni in alta activitate.
- iii. Sistemul de management a parolelor trebuie sa permita:
 - a. Schimbare periodica la intervale de maximum 90 zile. Sa nu permita folosirea aceleiasi parole la reinnoire. Schimbarea parolei ori de cate ori aveti vreo suspiciune cu privire la cunoasterea ei de catre alte persoane.
 - b. Dupa acordarea unei parole noi sa se ceara obligatoriu modificarea acesteia astfel incat utilizatorul sa foloseasca o parola stiuta numai de el.
 - c. Blocarea contului dupa introducerea gresita a parolei de trei ori consecutiv.

Mai multe detalii se pot obtine pe site-ul <https://www.pcisecuritystandards.org>. ING Bank va sta la dispozitie cu informatii suplimentare sau lamuriri la adresa rsm-mcse@ing.ro subiect: **PCI – DSS**.

Capitolul II - Manual de utilizare a interfeței Aplicației E-commerce

Serviciului e-commerce (Serviciul **ING WebPay**) reprezintă serviciul ce va 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 apălați la numărul de telefon **021 403 83 04** sau să scrieți la adresa de e-mail 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 atata timp cat exista 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 relație 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/si 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 relație 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 si Deconectare

2.3.1. Cum se acceseaza aplicatia ING WebPay

Interfata de administrare este disponibila la pagina de internet:

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

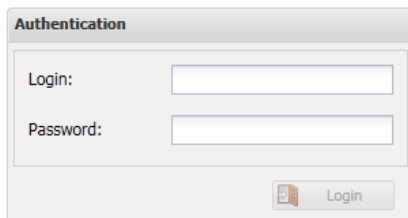
A screenshot of a web browser window showing an 'Authentication' dialog box. It contains two input fields: 'Login:' and 'Password:'. Below these fields is a 'Login' button with a small icon of a person.

Figura 1

Autentificarea se realizeaza prin introducerea codului de utilizator alocat de ING Bank si a parolei aferente (Fig 1).
!Atentie. Campurile sunt „case sensitive”, va rugam sa respectati formatul userilor si al parolelor transmise de ING Bank.

2.3.2. Posibile erori de autentificare si mesaje de eroare

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

Dupa 3 introduceri consecutive gresite contul va fi blocat. Pentru a debloca contul trebuie ca reprezentantul legal/mandatar al firmei in relatia cu banca sa contacteze ING Bank la numarul de telefon 021 403 83 04.

2.3.3. Deconectare

Pentru a inchide sesiunea, se selecteaza butonul **Logout** din partea dreapta sus a ecranului.



Figura 2

2.4. Vizualizarea tranzactiilor

Prin selectarea optiunii **Orders** din meniul principal (Fig. 3). Meniul se incarca automat in cateva secunde de la logare.



Figura 3

Platforma permite vizualizarea tranzactiilor in functie de anumite criterii de selectie disponibile in meniul Filter (in partea stanga a ecranului). Tranzactiile vor fi afisate in ordinea efectuarii lor: **cele mai recente in perioada de timp selectata**.

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

2.4.1. Filtrarea si afisarea tranzactiilor

Prin accesarea optiunilor disponibile in submeniul **Filter** (Fig. 3.1) aveti posibilitatea de a cauta si de a vizualiza tranzactiile in functie de urmatoarele criterii de selectie:

- Perioada **From – To**
 - ✓ Tranzactiile afisate vor fi cele efectuate in perioada selectata, pot fi aprobate sau respinse in functie de “Situatia platii” (Order Status), sau pot fi limitate de alte criterii de selectie
- Suma minima, maxima: **Maximum / Minimum amount**
 - ✓ Tranzactiile afisate vor fi cele cu suma de autorizare cuprinsa in intervalul selectat, pot fi aprobate sau respinse in functie de “Situatia platii” (Order Status), sau pot fi limitate de alte criterii de selectie.
Atentie! Valoarea introdusa in ambele campuri trebuie sa respecte formatul “0.00”, in caz contrar filtrarea nu se va efectua.
- Situatie platii: **Order Status** – Creată (Created), Aprobata (Approved), Refuzata (Declined), Anulata (Reversed), Depusa (Deposited), Returnata (Refunded)
- Referinta: **Reference number**
 - ✓ Permite identificarea unei singure tranzactii in functie de referinta interna “RRN” utilizata de regula de catre ING Bank; poate fi utila in comunicarea cu Banca
- Numar ordine: **Order number**
 - ✓ Permite identificarea unei singure tranzactii in functie de referinta acordata la momentul platii de catre ING Bank sau transmisa de catre comerciant (vezi Capitolul 3.6.1), si afisata in pagina de plata; poate fi utila in comunicarea cu platitorul sau cu Banca
 - ✓ Order number este setat automat pentru a fi transmis de catre ING. In cazul in care comerciantul transmite acest parametru, este foarte important sa anunte banca, pentru a modifica aceasta setare. (vezi Capitolul 3.6.1)
- Alte criterii specifice.

Figura 3.1

ATENȚIE!

Criteriile de selectie raman active pe toata durata sesiunii, ceea ce poate crea confuzii atunci cand sunt selectate tranzactii fara sa se tina cont de criteriile folosite anterior. De aceea, pentru actualizarea tranzactiilor se acceseaza butonul **Reset**, dupa care se pot aplica alte criterii de selectie sau se pot modifica criteriile selectie si apoi se acceseaza butonul **Search** pentru actualizare.

2.4.2. Descarcare tranzactii

Pentru a descarca o tranzactie sau o lista de tranzactii pe statia locala in vederea procesarii cu diverse programe informatice, se acceseaza optiunea de „Export to Excel” sau a optiunii „Export to CSV” disponibile in partea de jos stanga a ecranului (Fig. 3.2).



Figura 3.2

2.4.3. Selectarea unei tranzactii

Se pot accesa detaliile suplimentare ale unei tranzactii prin dublu-click pe tranzactie. Aceste detalii vor fi afisate intr-un tab separat in browser-ul folosit. (Fig. 3.3):

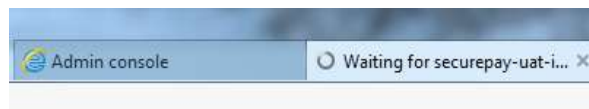


Figura 3.3

2.4.4. Anularea unei tranzactii

Dupa selectarea tranzactiei (vezi Capitolul Figura 3.2 2.4.3. *Selectarea unei tranzactii*), se poate anula o tranzactie pana la COT (ora 22.00) prin accesarea optiunii **Reverse** disponibila in tab-ul nou deschis (Fig.3.4):

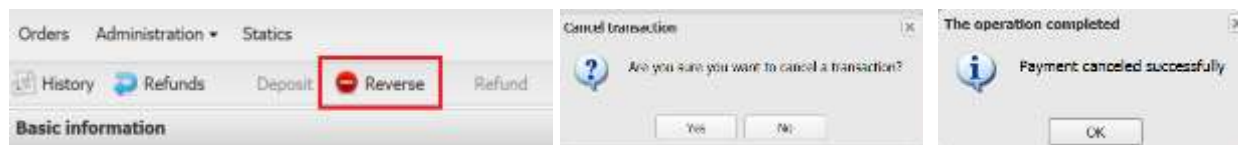


Figura 3.4

Statusul tranzactiei se va modifica in “Reversed”. Actualizarea listei de tranzactii din meniul **Orders** se poate realiza prin selectarea butonul **Search**.

Atentie! Optiunea de anulare a unei tranzactii este disponibila atat pentru autorizari, cat si pentru preautorizari pe toata durata de valabilitate a acestora sau inainte de a fi completate.

2.4.5. Completarea unei preautorizari

Dupa selectarea unei tranzactii de preautorizare (valabil doar pentru comerciantii cu optiunea respectiva, (a se vedea Figura 3.2

2.4.3. Selectarea *unei tranzactii*), aceasta se poate completa prin accesarea optiunii **Deposit** (Fig. 3.5):



Figura 3.5

Atentie! Suma se introduce cu doua zecimale folosind separatorul punct „.” (de exemplu: 20.00). O tranzactie poate fi completata doar pentru o suma mai mica sau egala cu suma preautorizata.

Dupa completarea tranzactiei, butonul **Reverse** devine inactiv iar tranzactia va avea status “Deposited” (Figura 3.7). Actualizarea listei de tranzactii din meniul **Orders** se poate realiza prin selectarea butonul **Search**.

ATENTIE!

Termenul de valabilitate al unei preautorizari este de 14 zile calendaristice pentru tranzactiile efectuate cu carduri VISA/Mastercard si de 7 zile calendaristice pentru tranzactiile efectuate cu carduri Maestro, de la data efectuarii tranzactiei de catre platitor. Daca acest termen se depaseste, preautorizarea expira si banii nu vor putea fi incasati. In astfel de situatii, platitorul trebuie sa efectueze o noua tranzactie aprobata.

! Daca se completeaza o preautorizare dupa termenul mentionat mai sus, va rugam sa verificati in meniul **History (Figura 3.6) rezultatul corect al acestei operatiuni, deoarece statusul tranzactiei nu se va modifica in interfata (tranzactia va avea in continuare statusul **Approved**).**



Figura 3.6

Completarile nu pot fi anulate ulterior, daca se doreste returnarea sumei completate este necesara contactarea departamentului de asistenta la numarul de telefon 021 403 83 04 sau depunerea in sediul ING Bank a unei cereri specifice.

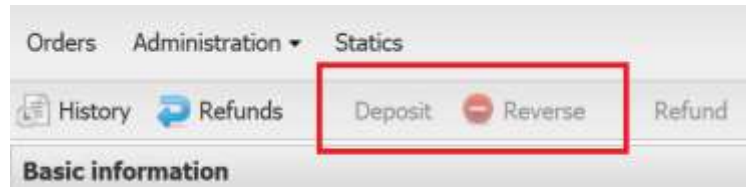


Figura 3.7

Completarea unei preautorizari se poate realiza inclusiv din interfata site-ului prin intermediul unui Webservice. Pentru mai multe detalii cu privire la aceasta optiune, va rugam sa verificati Capitolul 3.6.3.5.

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

Tabelul de mai jos reprezinta 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

Cand un posesor de card incepe sa faca plata statusul este "Created" si trece in starea de "**Deposited**" dupa autorizarea tranzactiei (atunci cand s-a realizat cu succes). In cazul in care nu se finalizeaza cu succes trece in "**Declined**", iar daca e reversata ulterior, in "**Reversed**".

Status-ul in care se poate considera tranzactia finalizata cu succes si se poate elibera bunul este "**Deposited**". Pentru aflarea online (in timp real) a rezultatului tranzactiei trebuie implementat protocolul de comunicare mentionat in Capitolul III, punctul 5.3 (pentru detalii discutate cu persoana care va asigura asistenta tehnica, cel care a implementat serviciul de plata cu cardul).

O **sesiune de plata** ramane deschisa timp de **10 minute**, dupa care tranzactia se incheie cu "time out".

Durata de trecere de la o stare la alta depinde de durata actiunilor care se fac intre stari. De ex. daca clientului magazinului (posesorul de card) ii ia mai mult timp sa valideze parola 3D Secure, trecerea de la "Created" la "Deposited" va sa fie mai lunga.

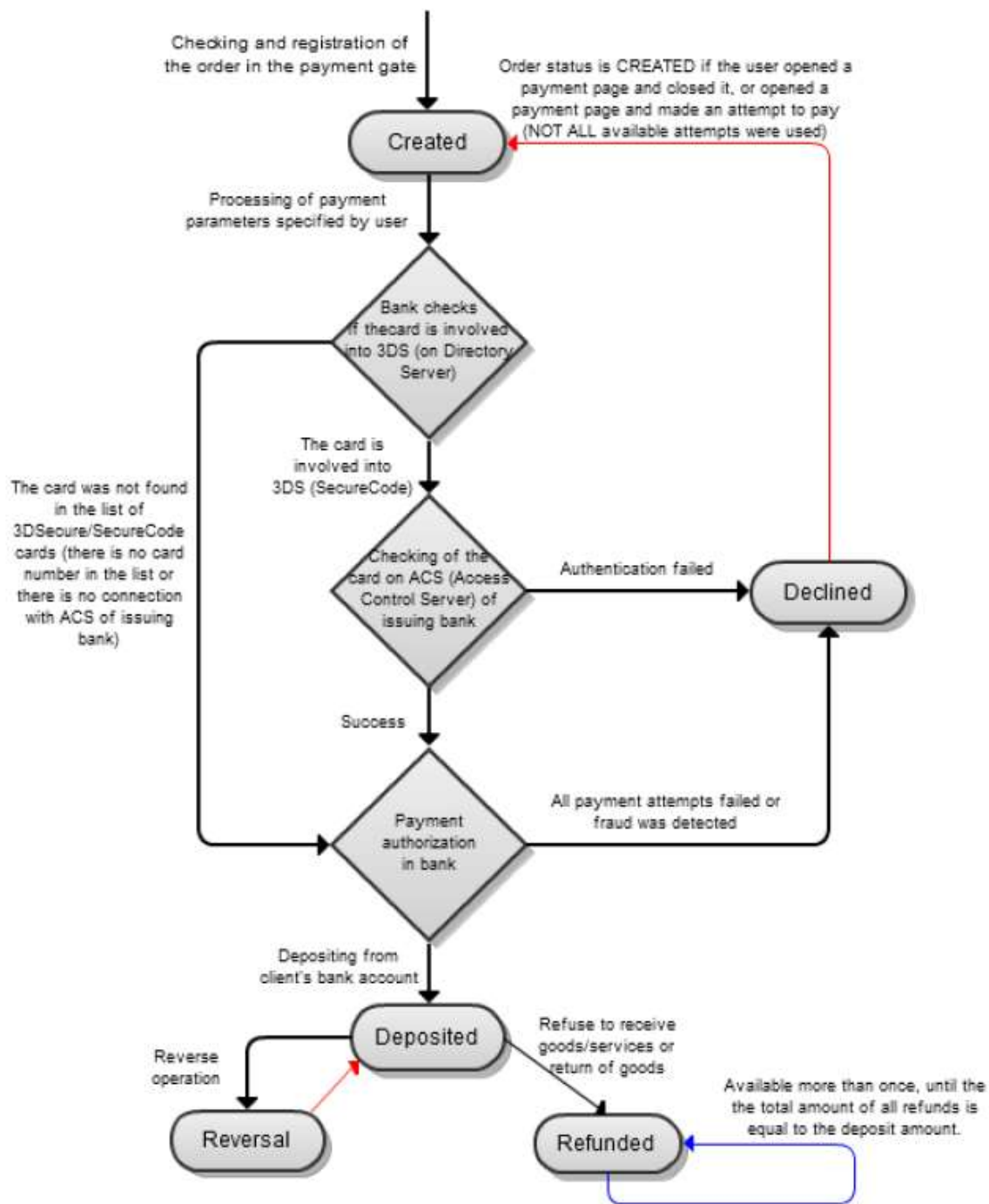
O **plata este deja incasata** in contul de comerciant daca accesand detaliile acesteia (dublu-click pe plata), in meniul History, campul stateExplanation are starea finala "Day Ended".

Sumele decontate se pot vedea in contul de e-commerce a doua zi de la data la care s-au efectuat platile (autorizarile) de catre clientii magazinului (pentru tranzactiile efectuate inainte de COT 22.00, cand are loc settlementul automat).

Rapoartele cu privire la plati se pot obtine din aplicatie, atat prin utilizatorul raportare, cat si prin utilizatorul administrare. Se acceseaza Meniul Orders -> Filter -> Se aplica criteriile de filtrare dorite -> Search-> Export to Excel/ Export to CSV (cele pentru care se vor incasa banii sunt cele cu statusul "Deposited").

Culorile din aplicatie aferente campului "State" (galben, verde, rosu) nu au legatura cu sumele incasate in cont, tranzactiile respinse sau acceptate, etc, ci sunt folosite strict pentru uzul intern al bancii.

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.

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 III - Manualul Utilizatorului API (Api for ING WebPay)

API pentru ING WebPay

Specificatii tehnice



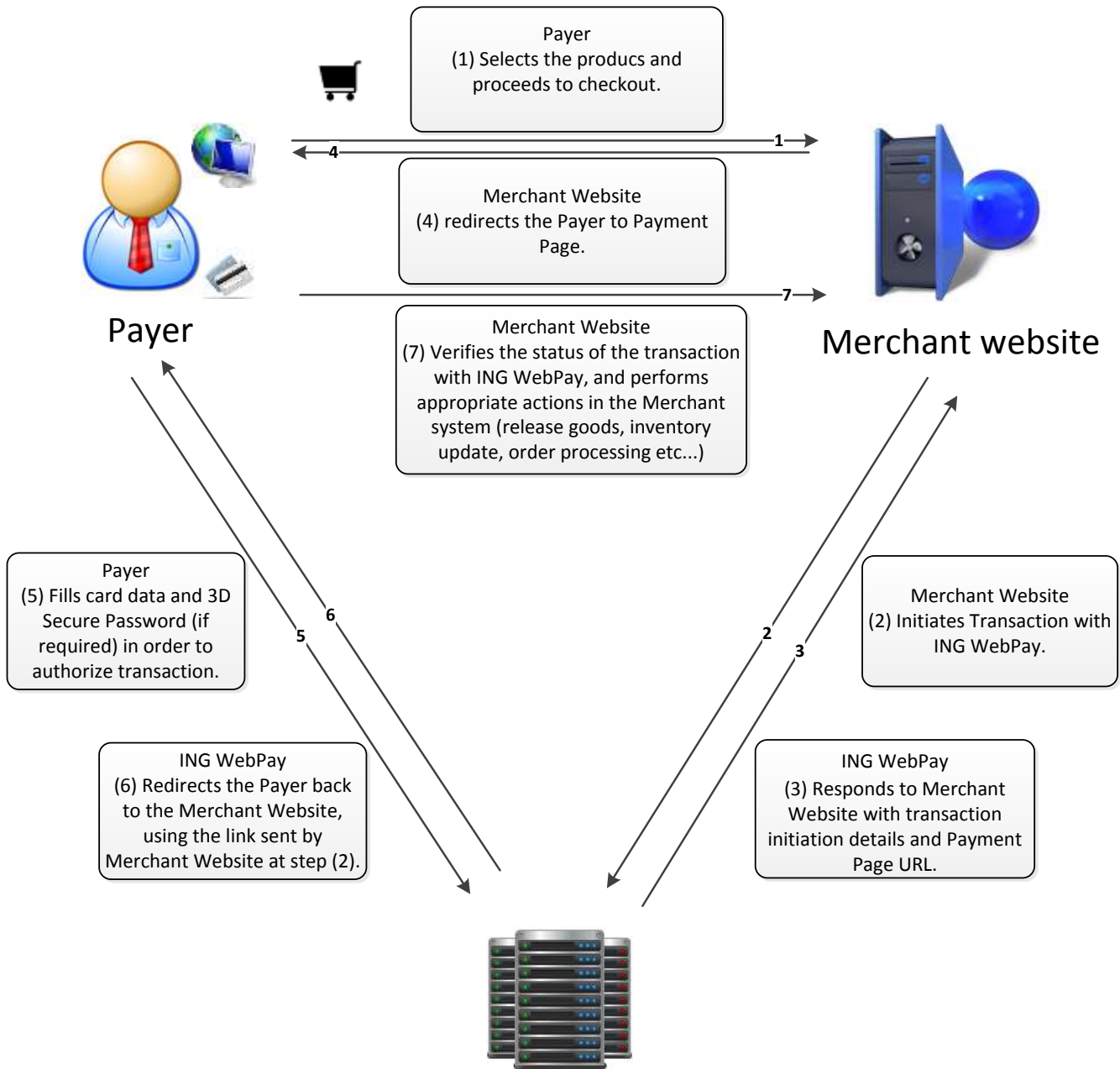
3.1. Scopul documentatiei

Acest document descrie etapele tehnice care sunt necesare pentru a conecta site-ul comerciantului la serviciul ING WebPay, pentru a initia tranzactii si a obtine statusul autorizarii pentru fiecare tranzactie. Documentatia este destinata persoanei/persoanelor de contact tehnic desemnat/e de comerciant pentru a dezvolta aplicatia.

3.2. Definitii

Consola de administrare	interfata web pentru serviciul ING WebPay, utilizata de catre comerciant pentru a Vizualiza, a anula si a edita tranzactiile
ING WebPay	serverul ING Bank care gazduieste Pagina de Plata si Consola de administrare a Comerciantului
Emitent	banca emitenta a cardului .
User-ul API	utilizatorul tehnic atribuit de catre ING Bank persoanei de contact tehnic al Comerciantului, cu scopul de a introduce si de a verifica plati prin API-ul ING WebPay.
Site-ul Comerciantului	server apartinand Comerciantului, care include cosul de cumparaturi si functionalitatile de back-office
Order ID	ID unic asignat de ING WebPay unei tranzactii.
Platitor	persoana care intentioneaza sa achizitioneze bunuri comerciale prin utilizarea cardului.
Pagina platii	pagina web gazduita pe serverul ING WebPay care va fi utilizata pentru a colecta datele detinatorului de card.

3.3. Procesul unei tranzactii E-commerce:



3.4. Primii pasi inaintea implementarii API:

1. Inainte de a incepe implementarea API, Utilizatorul API si persoana desemnata in relatia cu Banca ("Persoana de contact tehnic" / Utilizatorul API), vor primi pe adresa de e-mail, mentionata 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)
2. Urmati pasii mentionati in e-mail si a celor de mai jos.
3. Dupa primirea codurilor de utilizator API si parolele aferente mediului de test, Support WebPay va solicita, prin e-mail, logo-ul companiei in format .jpeg, dimensiune 160x60 px si informatiile subliniate mai jos, pentru personalizarea paginii de plata:

* *Tranzactia este procesata de ING Bank N.V. Amsterdam - Sucursala Bucuresti in numele XXX (nume comerciant/firma/numele companiei care detine site-ul). Datele cardului dvs. nu sunt puse la dispozitia comerciantului.*

** *In cazul in care banca emitenta a cardului dvs. si cardul dvs. sunt participante in sistemul 3DSecure, in ecranul urmator veti fi invitat sa introduceti datele de autentificare pentru 3DSecure. Pentru detalii suplimentare despre procesare comenzii dvs. va rugam sa contactati comerciantul XXX (nume comerciant/firma/numele companiei care detine site-ul) la numarul de telefon ZZZ sau la adresa de email xxx@yy.ro.*

Atentie! La implementarea serviciului ING WebPay pe mai multe valute (RON/EUR), ING Bank va crea si va transmite prin e-mail coduri de utilizator si parole diferite pentru fiecare valuta. De aceea, implementarea va fi efectuata de doua ori, pentru ambele seturi de utilizatori.

3.5. Autentificarea API

Site-ul Comerciantului va initia intodeauna cereri catre ING WebPay pentru accesarea serviciilor. Astfel, ING WebPay autentifica Site-ul Comerciantului pe baza codului de Utilizator API si a parolei atribuite responsabilului tehnic al comerciantului.



Pentru a evita atacurile web, Site-ul Comerciantului trebuie sa verifice certificatul ING WebPay, astfel se asigura ca cererea este trimisa de un serviciu securizat. Site-ul Comerciantului ar trebui sa utilizeze un mecanism care sa permita certificatului sa fie schimbat (in cazul in care ING Bank actualizeaza certificatul) si posibilitatea de a-i modifica configuratia manual (in cazul in care ING Bank utilizeaza un certificat expirat). De asemenea, va rugam sa consultati documentul "hosted_payment_page_security_visa.pdf" sau sa verificati actualizarile de securitate Visa Europe. Este necesar ca Site-ul Comerciantului sa indeplineasca standardele PCI DSS in materie de securitate si sa fie actualizat constant. Nu folositi browserul local pentru a apela API (ex: AJAX), pentru a evita divulgarea parolei comerciantului.

3.6. Descriere campuri API

Pentru a implementa serviciul de E-commerce ING WebPay, va rugam sa urmati pasii de mai jos. Daca site-ul dumneavoastra foloseste o platforma E-commerce "open source", va rugam sa informati pe e-mail serviciul nostru de suport (SupportWebPay@ing.ro) pentru a verifica posibilitatea acordarii unor Plug-in-uri pentru instalare.

3.6.1. Initierea tranzactiei

Site-ul Comerciantului initiaza o tranzactie prin trimiterea unui mesaj HTTPS catre <https://securepay.ing.ro/mpi/rest/register.do> pentru efectuarea vanzarii (daca nu sunteti sigur de tipul tranzactiei pe care trebuie sa o initiati, va rugam sa verificati cu reprezentantul ING Bank variantele posibile) sau <https://securepay.ing.ro/mpi/rest/registerPreAuth.do> pentru varianta de plata prin preautorizare cu specificatiile de mai jos. Pentru mai multe detalii privind preautorizarile verificati capitolul 3.6.3.5. *Completarea sau reversarea tranzactiilor Preautorizate.*

(Pentru mediul test, va rugam sa verificati link-urile URL prezentate in cadrul capitolului 3.9. *Pasii necesari pentru promovarea serviciului ING WebPay in productie*)

3.6.1.1. Parametrii

Field	Type	Mandatory	Value/Comment
userName	AN..30	Yes	Codul de utilizator API al comerciantului asa cum este furnizat de catre ING Bank
password	AN..30	Yes	Parola pentru codul de utilizator API al comerciantului, reprezentantul tehnic al comerciantului. Pentru mai multe detalii verificati autentificarea API
currency	N3	Yes	Parametru obligatoriu 946 pentru tranzactii in RON. 978 pentru tranzactii in EUR.
orderNumber	AN..32	Yes/No	Element unic de identificare a unei tranzactii; poate fi stabilit de catre comerciant sau poate fi atribuit automat de catre ING WebPay. Parametrul orderNumber va fi atribuit in mod automat de catre ING WebPay. Daca este setat de catre comerciant, ING trebuie sa fie informat pentru a evita rejectarea tranzactiei. Va rugam sa verificati detaliile de mai jos*
description	AN..512	No	Descrierea tranzactiei, poate fi transmisa de catre comerciant si va fi afisata in platforma ING WebPay. Campul poate fi lasat necompletat.
amount	N..20	Yes	Valoarea tranzactiei fara separator de zecimale. De exemplu, 102.31 RON este trimis ca 10231.
returnUrl	AN..512	Yes	Link-ul return URL catre care platitorul va fi redirectionat de ING WebPay dupa autorizarea tranzactiei. Link-ul URL se va trimite de forma unencoded.
language	A2	No	ro sau en in functie de limba setata de catre platitor. O valoare implicita este setata pentru fiecare comerciant.
email	AN	No	Optiune setata „by default” de catre banca. Adresa de email trebuie sa fie valida.

* - in cazul in care sistemul este configurat pentru a primi "OrderNumber" de pe site-ul comerciantului, ING nu va genera acest cod si va respinge tranzactia in situatia in care nu a primit OrderNumber de la comerciant
- in cazul in care sistemul este configurat sa genereze "OrderNumber" fara sa-l primeasca de la site-ul comerciantului, si site-ul trimite acest parametru, atunci tranzactia va fi respinsa automat de catre sistem.

ING WebPay raspunde cu informatiile necesare pentru a continua plata: link-ul paginii platii si ID-ul unic al tranzactiei (OrderId)

3.6.1.2. Mesaje de raspuns

Name	Type	Mandatory	Value/Comment
orderId	AN..64	No	ID-ul unic al comenzii atribuit de catre ING WebPay tranzactiei in curs. Campul nu este prezent in cazul in care tranzactia nu s-a autorizat..
formUrl	AN..64	No	Link-ul URL al paginii de plata; site-ul comerciantului trebuie sa redirectioneze platitorul pe pagina de plata in vederea completarii datelor de card necesare platii. Campul nu este prezent in cazul in care tranzactia nu a fost autorizata.
errorCode	N3	No	Daca exista erori in timpul initierii platii, ING WebPay va completa campul cu codul de eroare aferent. Va rugam sa consultati tabelul 3.6.1.3.Coduri de eroare
errorMessage	AN..512	No	Descrierea erorii returnata de catre ING WebPay (afisata in limba solicitata in timpul initierii tranzactiei)

3.6.1.3. Coduri de eroare

Valoare	Descriere
0	Nici o eroare intalnita.
1	Comanda duplicata
3	Valuta necunoscuta sau interzisa.
4	Parametrul obligatoriu nu a fost specificat.
5	Valoare eronata a unui parametru solicitat.
7	Eroare de sistem.

3.6.1.4. Posibile mesaje de eroare

Valoare	Descriere (adaptata de ING Bank pentru limba tranzactiei)
1	O comanda cu acelasi numar a fost deja procesata.
1	O comanda cu acelasi numar a fost inregistrata dar nu a fost platita
3	Valuta necunoscuta.
3	Valuta gresita.
4	Lipseste parametrul "Currency"
4	Lipseste 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

3.6.1.5. Exemplu mesaj de raspuns la initiere (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 sa redirectioneze platitorul pe pagina platii in vederea completarii datelor de card.

3.6.2. Efectuarea autorizarii

Platitorul va completa datele de card pe pagina de plata, iar ING WebPay va autoriza tranzactia. Daca este necesar, ING WebPay va redirectiona platitorul pe serverul emitentului pentru autentificarea 3D Secure.

Dupa ce tranzactia este initiata, ING Bank va redirectiona platitorul pe pagina web din URL-ul de retur (returnUrl) descris in **Parametrii**, iar site-ul comerciantului poate verifica statusul tranzactiei accesand API.

3.6.3. Obtinerea statusului tranzactiei

Pentru a solicita detalii cu privire la tranzactia initiata, site-ul comerciantului va trimite un mesaj HTTPS catre [https:// securepay.ing.ro/mpi/rest/getOrderStatus.do](https://securepay.ing.ro/mpi/rest/getOrderStatus.do) cu urmatoarele campuri:

Field	Type	Mandatory	Value/Comment
orderId	AN..64	No	ID unic al tranzactiei atribuit de catre ING WebPay tranzactiei in curs. Campul nu este prezent in cazul in care tranzactia nu s-a autorizat.
userName	AN..30	Yes	Codul de utilizator API al comerciantului, asa cum a fost furnizat de catre ING Bank
password	AN..30	Yes	Parola pentru utilizatorul de API, setata de catre persoana de contact tehnic. Va rugam sa verificati Autentificarea API
language	A2	No	ro sau en in functie de limba setata de catre platitor. O valoare implicita este setata pentru fiecare comerciant.

ING WebPay raspunde cu informatiile necesare:

3.6.3.1. Mesaj de raspuns

Name	Type	Mandatory	Value/Comment
OrderStatus	N2	No	Statusul platii. Valoarea este selectata din variantele descrise mai jos. Acest parametru lipseste daca statusul nu corespunde celor din lista.
errorCode	N3	No	Daca exista erori in timpul initierii platii, ING WebPay va afisa in acest camp codul de eroare. Va rugam sa consultati tabelul 3.6.3.3. Coduri de eroare .
errorMessage	AN..512	No	Descrierea erorii returnata de ING WebPay (mesajul este afisat in limba folosita la initierea tranzactiei)
OrderNumber	AN..32	yes	Parametru transmis de catre site-ul comerciantului in Parametrii sau este atribuit automat de catre ING Bank, in functie de optiunea comerciantului (verificati Capitolul 3.6.1.1.)
Pan	N..19	no	Numarul trunchiat al cardului utilizat in plata. Mentionat doar pentru comenzile platite.
expiration	N6	no	Data de expirarea a cardului in formatul YYYYMM. Mentionat numai pentru comenzile platite.
cardholderName	A..64	no	Numele detinatorului de card. Mentionat numai pentru comenzile platite
Amount	N..20	yes	Valoare platii in unitati monetare minimale (centi, bani).
currency	N3	no	Codul valutei platii in conformitate cu ISO 4217. 946 pentru RON, 978 pentru EUR
approvalCode	N6	no	IPS cod autorizare
authCode	N3	no	Codul autorizare al tranzactiei
Ip	AN..20	no	Adresa IP a platitorului
clientId	AN..255	no	Codul de client (identificator) in sistemul comerciantului. Folosit pentru a pune in aplicare o legatura. Prezent doar in cazul in care comerciantului ii este permis sa creeze aceasta legatura. (functionalitate viitoare)
bindingId	AN..255	no	Identificatorul de legatura creat in timpul platii comenzii sau utilizat pentru a plati. Prezent doar in cazul in care comerciantului ii este permis sa creeze aceasta legatura. (functionalitate viitoare)

3.6.3.2. Statusul platii

Valoare	Descriere
0	Comanda inregistrata, dar neplatita
1	Plata preautorizata (pentru tranzactii in 2 pasi)
2	Tranzactie autorizata
3	Tranzactie anulata
4	Tranzactie reversata
5	Tranzactie initiata prin sistemul ACS al bancii emitente
6	Tranzactie respinsa

„getOrderStatus” nu returneaza descrierea statusului. Pentru informatii mai detaliate poate fi utilizat Web-Service-ul „getOrderStatusExtended”. Ambele servicii utilizeaza aceiasi parametri, doar raspunsul este diferit.

Link-ul de productie pentru „getOrderStatusExtended” este:

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

3.6.3.3. Coduri de eroare

Valoare	Descriere
0	Nicio eroare de sistem
2	Tranzactia este refuzata, deoarece exista erori in credentialele platii.
5	Valoare eronata a unui parametru.
6	OrderId neinregistrat

3.6.3.4. Exemple mesaj de raspuns pentru status tranzactie:

Exemplu pentru „getOrderStatus”

Resp:

```
{ "expiration": "201512", "cardholderName": "testc", "depositAmount": 0, "currency": "946", "authCode": 2, "ErrorMessage": "Payment 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": "TransactionDenied", "amount": 100, "currency": "946", "date": "1403680642722", "orderDescription": null, "ip": "193.17.19 5.110", "merchantOrderParams": [], "attributes": [ { "name": "mdOrder", "value": "ff0b026c-c319-4e0f-af1f-230834b0eaec" } ], "cardAuthInfo": { "expiration": "201604", "cardholderName": "testc", "pan": "425603**2773" } }
```

3.6.3.5. Completarea sau reversarea tranzactiilor Preautorizate

In cazul preautorizarilor (initiate prin <https://securepay.ing.ro/mpi/rest/registerPreAuth.do>), sunt doua actiuni posibile: reversarea (anularea) sau finalizarea tranzactiei (completarea).

Reversarea (anularea) unei tranzactii se poate realiza in doua moduri:

1. Prin Consola de administrare, va logati folosind Codul de utilizator de administrare, selectati tranzactia respectiva (Status Approved), apasati butonul “Reverse”. (Va rugam sa verificati Capitolul 2 – [2.4.4. Anularea unei tranzactii](#)).
2. Prin transmiterea unui mesaj HTTPS catre <https://securepay.ing.ro/mpi/rest/reverse.do> cu urmatorii parametri: User, password, orderID.

Completarea se poate realiza in doua moduri:

1. Prin platforma MPI, va logati folosind Codul de utilizator de administrare, selectati tranzactia respectiva (Status Approved), apasati butonul „Complete” si introduceti suma tranzactiei. (Va rugam sa verificati Capitolul 2 - [2.4.5. Completarea unei preautorizari](#))
2. Prin trimiterea unui mesaj HTTPS catre <https://securepay.ing.ro/mpi/rest/deposit.do> cu urmatorii parametrii: preAuth Order id (generat la initierea PreAuth), Language, Amount, User si password. Daca suma trimisa este 0, atunci tranzactia este finalizata automat cu suma initiala.

Va rugam sa retineti ca nu puteti completa preautorizarea pe o suma mai mare decat cea pe care a fost initiata.

ATENTIE!

Termenul de valabilitate al unei preautorizari este de 14 zile calendaristice pentru tranzactiile efectuate cu carduri VISA/Mastercard si de 7 zile calendaristice pentru tranzactiile efectuate cu carduri Maestro, de la data efectuării tranzactiei de catre platitor. Daca acest termen se depaseste, preautorizarea expira si banii nu vor putea fi incasati. In astfel de situatii, platitorul trebuie sa efectueze o noua tranzactie aprobata.

! Daca se completeaza o preautorizare dupa termenul mentionat mai sus, va rugam sa verificati in meniul [History](#) (Capitolul [2.4.5. Completarea unei preautorizari](#)) rezultatul corect al acestei operatiuni, deoarece statusul tranzactiei nu se va modifica in interfata (tranzactia va avea in continuare statusul [Approved](#)).

3.7. Functionalitatea “email confirmation for orders”

Aceasta functionalitate presupune transmiterea automata pe email a confirmarii de plata, atat catre platitor (vezi Capitolul [3.6.1.1.Parametrii](#)), cat si catre comerciant.

Fiecare confirmare de plata poate contine urmatoarele informatii:

- Valoarea si valuta tranzactiei (*Amount and Currency*)
- Statusul tranzactiei (*Status*)
- Numarul comenzii (*OrderNumber*)
- Denumire comerciant (*Merchant name*)
- Denumire platitor (*Cardholder name*)
- Data tranzactiei (*Date*)
- Detaliile tranzactiei (*Order Description*)

Activarea acestei functionalitati se realizeaza astfel:

- Comerciant – se activeaza in baza optiunii exprimata in Cererea de acordare (ING WebPay) sau a Cererii de modificare date (ING WebPay)
- Platitor - se activeaza in baza optiunii comerciantului exprimata prin transmiterea adresei de email a Platitorului prin aplicatia ING WebPay. Comerciantul isi asuma responsabilitatea de a obtine acordul platitorului pentru utilizarea de catre Banca a adresei de email ca mijloc de transmitere a confirmarii de plata si de a asigura validitatea adresei de email.

3.8. Scenarii de test

- a. Cel putin o tranzactie aprobata.
- b. Cel putin o tranzactie refuzata (introducerea eronata a datei de expirare card sau CVV2)
- c. Cel putin o tranzactie aprobata, dar reversata de „Utilizator de Administrare”.

! Recomandare: la efectuarea testelor, sumele trebuie sa fie diferite pentru fiecare tranzactie initiata.

Utilizatorul de API nu are drepturi sa verifice tranzactiile de test in consola de administrare.

Pentru a verifica operatiunile cu cardurile de test, utilizatorii de Administrare / Raportare trebuie sa se logheze in <https://securepay-uat.ing.ro/consola/index.html> (pentru mai multe detalii va rugam sa verificati "Capitolul 2" din acest Ghid)

Utilizatorul de Raportare are doar drepturi de vizualizare si de intocmire rapoarte in consola de administrare

ING WebPay. Utilizatorul de Administrare pe langa drepturile Utilizatorului de Raportare, mai are posibilitatea de a anula o tranzactie in aceeași zi in care a fost efectuată, dacă acest lucru este efectuat înainte de închiderea de zi și de a modifica o tranzactie preautorizată.

3.9. Pași 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 ca 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 bancii.
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	https://securepay- uat.ing.ro/mapiuat/rest/register.do	https://securepay.ing.ro/mapi/rest/register.do
Pre-authorization	https://securepay- uat.ing.ro/mapiuat/rest/registerPreAuth.do	https://securepay.ing.ro/mapi/rest/registerPreAuth.do
getOrderStatus (if you use it)	https://securepay- uat.ing.ro/mapiuat/rest/getOrderStatus.do	https://securepay.ing.ro/mapi/rest/getOrderStatus.do
getOrderStatusExtended (if you use it)	https://securepay- uat.ing.ro/mapiuat/rest/getOrderStatusExtended.do	https://securepay.ing.ro/mapi/rest/getOrderStatusExtended.do
Web Service Reversare*	https://securepay- uat.ing.ro/mapiuat/rest/reverse.do	https://securepay.ing.ro/mapi/rest/reverse.do
Web Service Completare *	https://securepay- uat.ing.ro/mapi/rest/deposit.do	https://securepay.ing.ro/mapi/rest/deposit.do

* Pentru utilizarea acestor Web-Service-uri, Persoana desemnată în relația cu banca/Reprezentantul Legal trebuie să solicite bancii 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 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 problema tehnica, nu ezitati sa contactati serviciul de suport ING WebPay la adresa de e-mail: SupportWebPay@ing.ro.

Capitolul IV – Date de test pentru simularea tranzactiilor si testarea functionalitatilor aplicatiei ING WebPay – mediu de test

Pentru simularea unor tranzactii si testarea functionalitatilor aplicatiei ING Web Pay in Consola de administrare, puteti utiliza datele de test de mai jos. Tranzactiile efectuate pe mediul de test nu implica un transfer real de fonduri.

Coduri de utilizator:

- Cod de utilizator API: TEST_API & Parola: q1w2e3r4
- Cod de utilizator Administrare: TEST_ADMINISTRARE & Parola: Test1234567890!1

!Atentie Va rugam sa nu modificati parolele de autentificare ale userilor mentionati mai sus, deoarece datele pot fi utilizate si de catre alti comercianti.

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

Link simulare tranzactii: https://securepay-uat.ing.ro/mpi_uat/merchants/testecomerciant/test.html

Date de card (test):

Type	Details
Visa	4256031168525366 Cardholder Name: ING VISA Exp. Date: 05/19 CVV2: 855 3D Secure Password: test123!

!Atentie Consola de administrare (mediu de test) este pusa la dispozitia solicitantului, in scop informativ, doar ca mediu de test. Datele de test mai sus mentionate pot fi folosite doar in scopul mentionat in primul paragraf al acestui Capitol. Ghidul Serviciilor E-commerce ING WebPay este pus la dispozitia solicitantului, doar cu titlu de prezentare a solutiei tehnice oferite de ING Bank aferente serviciilor de acceptare la plata a cardurilor prin internet si a caracteristicilor aplicatiei ING Web Pay.

Prin accesarea Consolei de administrare - mediu de test, solicitantul accepta conditiile mentionate in prezentul capitol si intelege ca punerea la dispozitia sa a datelor de test mai sus mentionate si a Ghidului Serviciilor E-commerce ING WebPay este facuta in scop pur informativ, nu reprezinta o oferta din partea ING Bank si nici o asumare de catre ING Bank a oricarei obligatii de a incheia un contract cu solicitantul pentru servicii de acceptare la plata a cardurilor prin internet.

In consecinta, orice implementare/ dezvoltare efectuata de beneficiarul Consolei de administrare - mediu de test asupra dotarilor sale informatice, in baza datelor de test mentionate in prezentul Capitol, in scopul efectuarii simularilor de tranzactii si testarii functionalitatilor aplicatiei ING Web Pay in mediul de test, se afla in deplina responsabilitate a beneficiarului acestor date de test si pe costul acestuia, neputand fi atrasa raspunderea ING Bank pentru eventualele costuri suportate de beneficiar, in cazul in care solicitarea acestuia de acordare a serviciului de E-Commerce (ING WebPay) nu este aprobata de catre ING Bank.