

Uporabniški priročnik za vzpostavitev sistema elektronske trgovine

Datum priprave: 14.07.2008	Verzija: 2.0
Oznaka dokumenta:	Pričetek veljavnosti: 14.07.2008
Pripravil: Matjaž Pahor Milan Čulibrk	Zadnjo verzijo priročnika lahko naročite na spletnem naslovu: http://www.activa.si/test

Zgodovina dokumenta

Datum	Oseba	Opis
15.02.2007	Matjaž Pahor	- Predhodne verzije tega dokumenta, od verzije 1.0 do 1.4
14.07.2008	Milan Čulibrk	<ul style="list-style-type: none">- Popravki in dopolnitve v besedilih celotnega dokumenta, nova struktura dokumenta, dodane so opombe, zgodovina, dodatni viri, številčenje in vsebina dokumenta.- Dodana funkcionalnost obročnih plačil Diners in American Express.- Dodano poglavje s pogostimi vprašanji trgovcev pri implementaciji elektronskih trgovin.- Dodano poglavje vezano na delo z Back-Office portalom sistema Payment Gateway.- Verzija dokumenta: 2.0

Opombe

Oznake v dokumentu

Besedilo...	Navadno besedilo
PaymentInit	Pomembnejša besedila, definicija parametrov, klicev, sporočil
http://www.activa.si	Spletne povezave
Action=5	Programska koda

Ostali viri

Za dodatne informacije povezane z vsebino tega dokumenta lahko uporabite še naslednje uporabne spletne vire:

http://www.activa.si/e-trgovina.asp?content=prodajna_mesta
Activa e-trgovina – Opis za prodajna mesta

<http://www.activa.si/e-trgovina.asp?content=varnost>
Varnostna priporočila za poslovanje spletnih trgovcev

<http://www.activa.si/merchants.asp>
Seznam sodelujočih slovenskih e-trgovcev v programih MasterCard SecureCode in Verified by VISA

<http://www.pametna-kartica.si/securecode.asp>
Opis storitve MasterCard SecureCode

<http://www.pametna-kartica.si/vbv.asp>
Opis storitve Verified by VISA

<http://www.securecode.com>
MasterCard SecureCode (MasterCardove strani o storitvi SecureCode) – strani so v angleškem jeziku

<http://www.visaeurope.com/personal/onlineshopping/verifiedbyvisa/>
Verified by VISA (Visine strani o storitvi Verified by VISA) – strani so v angleškem jeziku

Vsebina

Zgodovina dokumenta.....	2
Opombe.....	3
Oznake v dokumentu.....	3
Ostali viri.....	3
Vsebina.....	4
1 UVOD.....	5
1.1 Payment Gateway.....	5
1.2 Hosted Payment Page (HPP).....	5
2 FAZE TRANSAKCIJE.....	6
2.1 Vidik kupca.....	6
2.2 Vidik trgovca.....	6
2.3 Vidik sistema Payment Gateway.....	6
2.4 Shematski prikaz izmenjave informacij.....	7
2.5 Opis korakov.....	8
3 INTEGRACIJA PRODAJNEGA MESTA.....	10
3.1 Potek transakcije s seznamom uporabljenih sporočil.....	10
3.1.1 Faza On-Line.....	10
3.1.2 Faze Off-Line.....	11
3.2 Opis prenosa sporočil med trgovcem in sistemom Payment Gateway.....	11
3.3 Zahtevek »PaymentInit«.....	12
3.4 Odgovor PaymentInit.....	13
3.5 Zahtevek NotificationMessage.....	13
3.6 Odgovor NotificationMessage.....	14
3.7 ErrorURL.....	15
3.8 Zahtevek Payment.....	15
3.9 Odgovor Payment.....	15
3.10 Opis vtičnika e24PaymentPipe.....	16
3.11 Specifikacija direktnega vmesnika.....	17
3.12 Demo.....	18
4 TESTNO OKOLJE IN PRILAGODITVE.....	19
4.1 Prikaz logotipov.....	19
4.2 Prilagoditev HPP strani.....	22
5 OBRAČUN TRANSAKCIJ.....	25
5.1 Neposredni obračun.....	25
5.2 Zakasneni obračun.....	26
5.3 Obročno odplačevanje Diners in American Express.....	27
6 OSNOVE DELA NA BACK-OFFICE PORTALU PAYMENT GATEWAY.....	29
6.1 Delo s transakcijami.....	29
6.2 Terminologija.....	30
7 POGOSTA VPRAŠANJA.....	32
7.1 Preusmeritev na naslov ErrorURL kljub uspešno izvedeni transakciji.....	32
7.2 Transakcije.....	34
8 NAMESTITEV DEMO SPLETNE STRANI (PRIMER ASP).....	36
PRILOGA: ERROR MESSAGES.....	37
PRILOGA: CERTIFICATION AUTHORITIES.....	41

1 UVOD

1.1 *Payment Gateway*

Storitev elektronske trgovine (Payment Gateway) sistema Activa ima vlogo vmesnega člana med kupcem, trgovcem, banko in zunanjimi kartičnimi ustanovami, med katerimi se pretakajo finančne transakcije.

Sistem Activa nudi trgovcem, ki že razpolagajo s svojo internet stranjo, možnost uporabe celovite rešitve elektronskega poslovanja (z uporabo kreditnih in debetnih kartic):

- On-line avtorizacijo: varno izvajanje nakupov v vseh fazah transakcije.
- Off-line administracijo: dostop do spletnega vmesnika, na katerem lahko izvaja administrativne vpoglede, preverja status transakcij, izvaja stornacije, izvaja postopke finančne bremenitve ter ustvarja poročila o izvršenih plačilih.

1.2 *Hosted Payment Page (HPP)*

Pri izvedbi transakcije s kreditnimi ali debetnimi karticami preko elektronske trgovine, trgovec preusmeri kupca na stran banke, kjer se izvede varen vnos podatkov o kartici. Na ta način so zagotovljeni naslednji cilji:

- Trgovec ne razpolaga s podatki o karticah in je zato razbremenjen izpolnjevanja dodatnih varnostnih zahtev (varne povezave in varno hranjenje podatkov), ki so doslej bile pogoj za tovrstno poslovanje.
- Banka dovoljuje uporabo storitev in protokolov trgovcem, glede na njihove potrebe in zahteve.
- Trgovec lahko delno prilagodi videz HPP strani (po dogovoru z banko).

Stran, na katero je preusmerjen kupec ob izvedbi plačila se imenuje Hosted Payment Page (HPP) in omogoča načine plačil, ki jih za trgovca aktivira banka. Banka bo HPP strani sama prilagajala morebitnim spremembam oziroma novim storitvam in tako trgovce razbremenila razvijanja in prilagajanja novim standardom.

2 FAZE TRANSAKCIJE

V tem poglavju so opisani posamezni koraki transakcije preko elektronske trgovine z uporabo vtičnika Payment Gateway (plug-in) in HPP strani.

2.1 *Vidik kupca*

Imetnik kartice (kupec) izvede nakup na spletni strani trgovca po naslednjih korakih:

- Izbere artikel.
- Vnese osebne podatke, potrebne za dostavo in potrdi nakup s klikom na gumb »Nakup«.
- Kupca se samodejno preusmeri na stran HPP (spletni brskalnik mora imeti vključene javascript funkcionalnosti za pravilno delovanje HPP).
- Kupec izbere način plačila in vnese podatke o plačilni kartici ter klikne na gumb »Plačilo«.
- Brskalnik ga ponovno samodejno preusmeri na stran trgovca, kjer se prikaže izid transakcije.
- Eventualno lahko kupec prejme sporočilo s strani trgovca (elektronsko pošto) s podatki o plačilu (virtualni račun).

2.2 *Vidik trgovca*

Trgovec prejme naročilo/nakup s strani kupca:

- Trgovec pošlje sporočilo o začetku plačila (PaymentInit) na sistem Payment Gateway.
- Kot odgovor prejme šifro nakupa (PaymentID) in URL naslov HPP strani.
- Zgodi se preusmeritev kupca na URL, kjer se nahaja HPP stran in priloži se podatke o nakupu ter šifro nakupa (PaymentID).
- Payment Gateway pošlje odgovor o uspešno izvedeni transakciji.
- Eventualno lahko trgovec pošlje sporočilo kupcu (elektronsko pošto) s podatki o plačilu, ki ga lahko kupec uporabi kot potrdilo (virtualni račun). V kolikor se za to odloči, mora to storitev trgovec razviti sam.
- Trgovec pošlje na Payment Gateway URL naslov, kamor se preusmeri kupca za prikazovanje izida transakcije.
- Kupcu se prikaže izid transakcije.

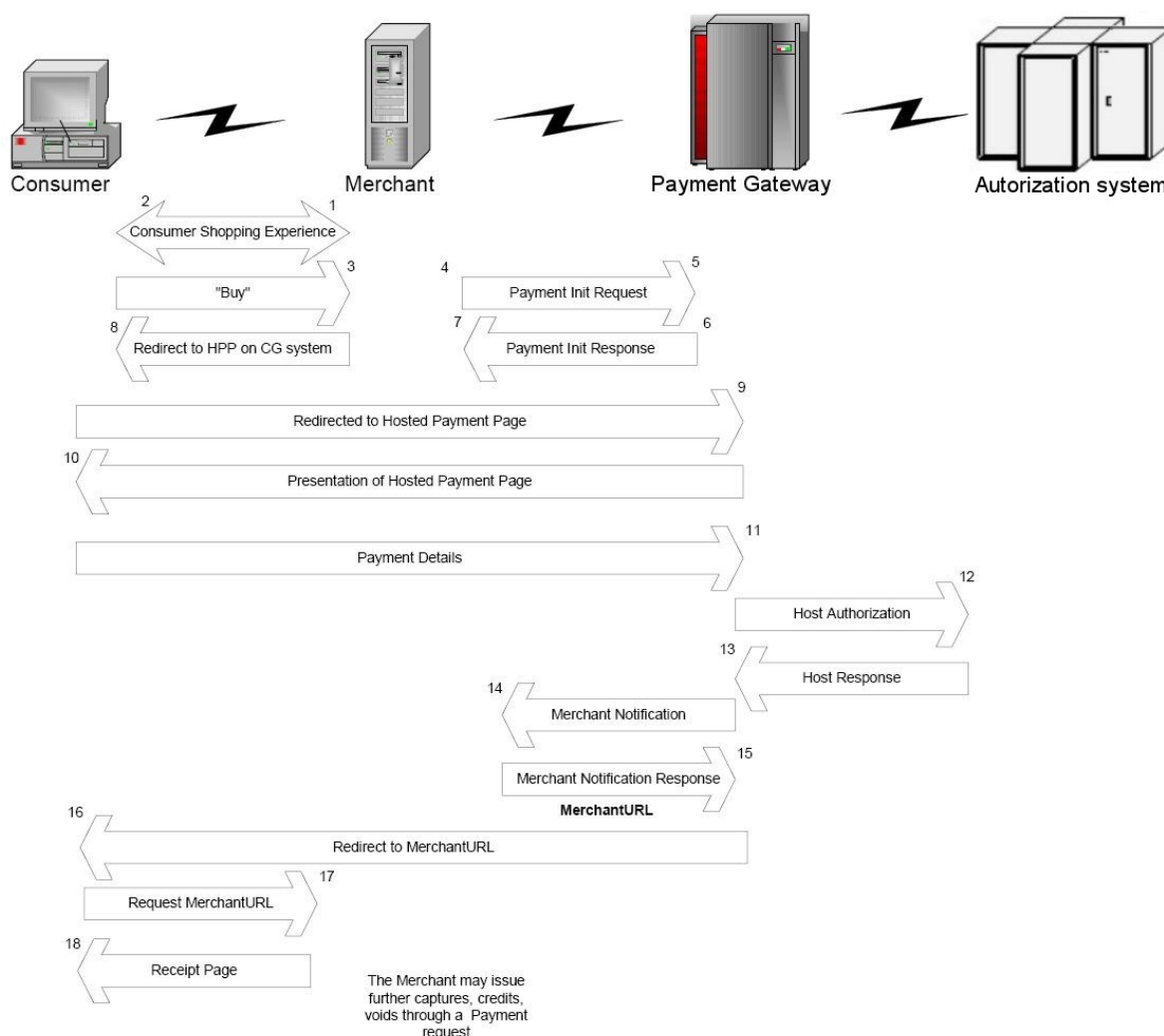
2.3 *Vidik sistema Payment Gateway*

Sistem Payment Gateway prejme sporočilo o začetku plačila (PaymentInit) s strani trgovca:

- Payment Gateway odgovori z URL naslovom HPP strani in priloži šifro nakupa (PaymentID).
- Kupcu se prikaže HPP stran (v kolikor ta ni specifično prilagojena s strani trgovca, se uporabi prednastavljena stran banke).
- Payment Gateway prejme vse podatke o kartici, ki jih kupec vnese na HPP strani.
- Payment Gateway obdela transakcijo ter jo pošlje še v obdelavo bančnemu avtorizacijskemu sistemu. Payment Gateway počaka na odgovor avtorizacijskega sistema.
- Payment gateway pošlje trgovcu obvestilo o izidu transakcije.
- Payment Gateway prejme v odgovor URL naslov na katerega se preusmeri kupca.
- Payment Gateway preusmeri kupca na prejeti URL naslov.

2.4 Shematski prikaz izmenjave informacij

V nadaljevanju sledi shematski prikaz poteka transakcije med vpletenimi stranmi. Vsak korak je podrobno obrazložen.



2.5 Opis korakov

V tabeli je analiziran potek transakcije.

Brskalnik kupec/imetnik kartice	Spletna stran trgovec	Payment Gateway	Bančni avtorizacijski sistem
1. Doda izdelke v košarico	2. Pripravi in prikaže stran o nakupu		
3. Izpolni potrebne podatke in potrdi nakup s klikom na gumb	4. Pripravi HTTP zahtevek za PaymentInit z vsemi podrobnostmi o nakupu		
	5. Pošlje POST zahtevek na Payment Gateway	6. Po verifikaciji prejetega zahtevka, se podatki o transakciji shranijo na sistem, kjer se ustvari PaymentID šifra in pripravi URL naslov na katerega bo preusmerjen kupec	
		7. Odgovori trgovcu z URL + PaymentID	
	8. Shrani PaymentID z ostalimi podatki o transakciji in vrne brskalniku (kupcu) preusmeritev na naslov Payment Gateway-a (z dodano PaymentID šifro)		
9. Prikliče HPP stran		10. Po verifikaciji prejete PaymentID šifre, se ustvari stran za plačilo z možnostmi, ki jih podpira trgovec in jo vrne brskalniku (kupcu)	
11. Izpolni potrebne podatke in potrdi plačilo z gumbom		12. Združijo se podatki kupca in podatki trgovca ter se pošljejo v obliki zahtevka v avtorizacijski sistem banke	13. Avtorizacijski sistem obdela prejeti zahtevek ter vrne izid Payment Gateway-u
		14. Pošlje POST zahtevek trgovcu s sporočilom o izidu transakcije	

	15. Prejme sporočilo in ažurira status transakcije s prejetim izidom. Vrne URL naslov za preusmeritev brskalnika (kupca) na stran z izidom transakcije in eventualno pošlje elektronsko pošto kupcu	16. Preusmeri brskalnik (kupca) na prejeti URL naslov	
17. Prikliče/zahteva URL naslov trgovca	18. Prejme zahtevo in vrne stran z izidom transakcije		
19. Prikaže stran trgovca z izidom transakcije			

3 INTEGRACIJA PRODAJNEGA MESTA

Platforma Payment Gateway predvideva direktno komunikacijo s strežnikom trgovca za opravljanje elektronskih transakcij. Izmenjavo sporočil si lahko trgovec nadgradi na dva načina. Trgovcem priporočamo uporabo »plug-in« načina, ki ga ponuja banka. Po želji pa si lahko trgovec izdelava tudi svoj komunikacijski vmesnik.

- Plug-in e24PaymentPipe: prednost uporabe tega načina je enostavna integracija v sistem trgovca in podpora za razvojna okolja Java, C/C++, ColdFusion, ActiveX/COM, VB, in ASP.
- Izdelava lastnega komunikacijskega vmesnika: v nadaljevanju je opredeljen način izdelave lastnega komunikacijskega vmesnika za primere, ko plug-in ni kompatibilen s platformo, na kateri gostuje spletna stran trgovca (PHP).

3.1 Potek transakcije s seznamom uporabljenih sporočil

3.1.1 Faza On-Line

- Imetnik napolni košarico, izpolni osebne podatke (naslov,...) in klikne na gumb npr.: »Nakup«.
- Trgovec pošlje na Payment Gateway sporočilo **PaymentInit** s podatki o naročilu.
- S tem sporočilom trgovec poda parameter o tipu transakcije (parameter »**Action**«):
 - **Action=1**: Transakcija tipa »Purchase«; če je transakcija uspešna, je kartica imetnika obremenjena takoj.
 - **Action=4**: Transakcija tipa »Authorization«; znesek nakupa znižuje limit na kartici, dejanska bremenitev pa se zgodi šele, ko trgovec potrdi nakup (ponavadi, ko je blago odposlano).
- Trgovec dobi v odgovor URL naslov za **HPP** stran in šifro **PaymentID**, ki identificira transakcijo.
- Trgovec preusmeri kupca na naslov, kjer se nahaja HPP in priloži PaymentID kot parameter.
- Po zaključenem plačilu Payment Gateway pošlje sporočilo o izidu (**NotificationMessage**) na URL naslov, ki ga trgovec predhodno pripravi (ResponseURL) in je naveden v PaymentInit sporočilu, poslanem na Payment Gateway.
- Trgovec lahko pošlje kupcu elektronsko sporočilo o pravkar opravljeni transakciji (virtualni račun).
- Trgovec odgovori na prejeto sporočilo **NotificationMessage** z URL naslovom, na katerega bo preusmerjen brskalnik kupca.
- Payment Gateway preusmeri kupca na prejet URL naslov.
- Trgovec prikaže kupcu izid transakcije.

3.1.2 Faze Off-Line

Potrditvena transakcija (akreditiv)

Po uspešni fazi on-line avtorizacije lahko trgovec začne postopek pošiljanja blaga. Pri transakcijah tipa »Purchase« se bremenitev zgodi sočasno z avtorizacijo. Transakcije tipa »Authorization« pa morajo biti s strani trgovca naknadno potrjene z opcijo »Capture«. To se lahko izvede na dva načina:

1. Trgovec se prijavi na portal Payment Gateway, kjer lahko preko vmesnika izvaja poizvedbe po opravljenih transakcijah ter uporabi orodja in funkcionalnosti, ki jih omogoča portal Payment Gateway. V tem primeru trgovec izbere opcijo »Capture«, kar povzroči obdelavo transakcije.
 - Vstopna točka na testni portal: <http://www.activa.si/test/>
2. Trgovec pošlje **Payment** sporočilo na Payment Gateway. V sporočilu se uporabijo podatki originalne transakcije in v polju »Action« se določi vrednost 5 (**Action=5**).

Pomembno: Potrditvena transakcija je edinstvena za posamezno avtorizacijo. Znesek mora biti vedno enak ali nižji od zneska avtorizacije.

Storno transakcija

V primeru vračila blaga (v celoti ali delno) lahko trgovec izvede storno zneska - v celoti ali le delno. To povzroči bremenitev trgovca in odobritev imetniku kartice. Postopek se lahko izvede na dva načina:

1. Trgovec se prijavi na portal Payment Gateway, kjer lahko preko vmesnika izvaja poizvedbe po opravljenih transakcijah ter uporabi orodja in funkcionalnosti, ki jih omogoča portal Payment Gateway. V tem primeru trgovec izbere opcijo »Credit« (v primeru, da blago še ni bilo poslano pa opcijo »Reversal«).
 - Vstopna točka na testni portal: <http://www.activa.si/test/>
2. Trgovec pošlje **Payment** sporočilo direktno na Payment Gateway. V sporočilu se uporabijo podatki originalne transakcije in v polju »Action« se določi vrednost 2 (**Action=2**).

Lahko se izvede več manjših vračil za posamezno transakcijo, s tem da vsota posameznih storno transakcij ne presega zneska originalne avtorizacije.

3.2 Opis prenosa sporočil med trgovcem in sistemom Payment Gateway

Obstajajo trije tipi sporočil med trgovcem in Payment Gateway ("server-to-server"). Vsak tip sestoji iz zahtevka in odgovora (request & response message):

- **PaymentInit:** Začetno sporočilo transakcije, ki ga trgovec pošlje na Payment Gateway. Ta odgovori z URL naslovom HPP strani in doda PaymentID šifro.

- **NotificationMessage**: Sporočilo o izidu transakcije, ki ga Payment Gateway pošlje trgovcu. Ta odgovori z URL naslovom, na katerega se preusmeri brskalnik kupca.
- **Payment**: Sporočilo za knjiženje ali storno predhodno izvršenih transakcij, ki ga trgovec pošlje na Payment Gateway. Ta odgovori z izidom transakcije.

Sporočili **PaymentInit** in **Payment** se ustvarita na strani trgovca in za delovanje potrebujeta plug-in e24PaymentPipe ali podoben vmesnik.

Sporočilo **NotificationMessage** ustvari Payment Gateway, trgovec pa mora pripraviti dinamično stran, ki zna sprejeti parametre iz vsebine sporočila in v odgovor poslati preusmeritveni URL naslov, namenjen brskalniku kupca.

3.3 Zahtevek »PaymentInit«

Sporočilo ustvari trgovec in ga pošlje na Payment Gateway sistem. S tem se 'zažene' plačilna transakcija. V sporočilu so uporabljeni naslednji elementi (v navednicah je ime polja, ki se uporabi za pripravo sporočila):

- Tran Portal ID (»**id**«): Identifikacijska šifra trgovca, dodeljena ob aktivaciji trgovca v sistemu.
- Tran Portal Password (»**password**«): Geslo, ki je dodeljeno trgovcu v fazi aktivacije trgovca v sistem.
- Action Code (»**action**«): Tip transakcije (1 = Purchase, 4 = Authorization).
- Amount (»**amt**«): Znesek transakcije (format NNNNN.NN).
- Currency code (»**currencycode**«): ISO šifra valute (Euro = 978).
- Consumer Language (»**langid**«): Oznaka jezika, ki bo uporabljen za prikaz HPP strani.
 - »SLO« Slovenski jezik
 - »ITA« Italijanski jezik
 - »USA« Angleški jezik
 - »FRA« Francoski jezik
 - »DEU« Nemški jezik
 - »ESP« Španski jezik
- Merchant Notification URL (»**responseURL**«): URL, ki bo uporabljen za posredovanje izida trgovcu preko sporočila **NotificationMessage**. Pogoji uporabe so navedeni spodaj¹.

¹ Pogoji uporabe:

- Uporabljajo se lahko le vrata (port) 80 in 443.
- Ne sme vsebovati nobenih parametrov.
- Spletne strani zaščitene z SSL certifikatom morajo uporabljati certifikate izdane s strani 'Certification Authority' (spisek v prilogi). V nasprotnem primeru, mora trgovec posredovati dokaz 'Certification Authority' ki garantira verodostojnost njegovega certifikata.

- Error URL (»**errorURL**«): URL naslov, ki ga bo Payment Gateway uporabljal za prikazovanje sporočila v primeru sistemskih in komunikacijskih napak kupcu.
- Track ID (»**trackid**«): Identifikacijska šifra transakcije. Ponavadi je to unikatna šifra naročila na sistemu trgovca.
- User Defined Fields (»**udf1**« – »**udf5**«): 5 polj na razpolago trgovcu za dodatne informacije, ki jih po želji uvrsti v sporočilo. Te informacije se lahko nespremenjeno prikažejo v NotificationMessage sporočilu.

3.4 **Odgovor PaymentInit**

Je odgovor, ki ga Payment Gateway vrne trgovcu po prejemu zahtevku PaymentInit (po verifikaciji prejetega sporočila). Vsebuje naslednja polja:

- Payment URL: URL naslov HPP strani, na katero trgovec preusmeri kupca za nadaljevanje postopka plačila.
- Payment ID: šifra nakupa, ki jo trgovec uporablja v nadaljnjih sporočilih kot identifikacijo transakcije.

3.5 **Zahtevek NotificationMessage**

Payment Gateway pošlje NotificationMessage sporočilo trgovcu kot izid transakcije. Trgovec razpolaga z dinamično stranjo, preko katere sprejme sporočilo in odgovori z URL, ki je naveden v sporočilu PaymentInit (polje responseURL).

Payment Gateway uporablja POST metodo za pošiljanje sporočila. Struktura sporočila je lahko različna, odvisno od uspešnosti transakcije:

- Pri uspešni izvedeni transakciji trgovec analizira in shrani informacije o transakciji, posebej pa 'Result Code variable' (za ugotavljanje izida).
- Pri neuspešnih transakcijah se preveri razlog napake.

Lahko se pojavi več sporočil NotificationMessage. Do tega pride, če se kupec pomotoma vrne na stran za plačilo (navigacija BACK). Payment Gateway zavrne tovrstno transakcijo (zaradi uporabe enakega PaymentID) in pošlje NotificationMessage v opozorilo. Priporočljivo je upoštevati le prvi NotificationMessage za ažuriranje statusa transakcije v lastni bazi (v izogib prepisovanju izida transakcije z naknadnimi poskusi).

Primer: Uspešna transakcija

- PaymentID (»**paymentid**«): enolična šifra za identifikacijo nakupa.
- TransID (»**tranid**«): enolična šifra za identifikacijo transakcije (dodeli Payment Gateway).
- Result Code (»**result**«): Izid transakcije, ki je lahko:
 - »APPROVED«

- »NOT APPROVED«
- »CAPTURED«
- »NOT CAPTURED«
- »DENIED BY RISK«
- »HOST TIMEOUT«
- Auth Code (»**auth**«): Šifra avtorizacije v primeru odobrene transakcije.
- Post Date (»**postdate**«): Datum transakcije.
- Track ID (»**trackid**«): Identifikacijska šifra transakcije dodeljena s strani trgovca.
- Reference ID (»**ref**«): Šifra transakcije, dodeljena s strani Banke.
- User Defined Fields (»**udf1**« – »**udf5**«): 5 polj na razpolago trgovcu za dodatne informacije, ki jih po želji uvrsti v sporočilo. Te informacije se lahko nespremenjeno prikažejo v NotificationMessage sporočilu
- Card Type (»**cardtype**«): Tip kartice je lahko npr.:
 - »VISA« = Visa
 - »MC«, »MC2« = MasterCard
 - »AMEX« = American Express
 - »DINERS« = Diners Club
 - »JCB« = JCB
- Payment Instrument (»**payinst**«): Označuje uporabo varnostnega protokola pri nakupu.

Primer: Neuspešna transakcija

- PaymentID (»**paymentid**«): enolična šifra za identifikacijo nakupa.
- Error (»**Error**«): šifra napake.
- Error Text (»**ErrorText**«): opis napake.

3.6 Odgovor NotificationMessage

V odgovoru trgovec sporočil URL naslov, na katerega želi preusmeriti kupca. Ta odgovor ima naslednjo strukturo: REDIRECT = URL naslov.

Primer: REDIRECT=http://www.trgovina.si/result.asp?paymentID=123456

Če v primeru tehničnih težav brskalnik ne prikaže naslova z izidom transakcije, se lahko zgodi, da kupec ponovi transakcijo kljub temu, da je bila prejšnja transakcija uspešna. Priporočljivo je, da se prikaz oz. uspešno vizualizacijo te strani preverja (z uporabo dinamičnega imena strani).

V primeru napake se:

- kupca obvesti o izidu transakcije z elektronsko pošto ali
- izvede avtomatski storno transakcije v on-line načinu. Ta procedura je smiselna pri transakcijah tipa Purchase (Action=1).

3.7 *ErrorURL*

V primeru napak med izmenjavo sporočil NotificationMessage, Payment Gateway preusmeri brskalnik kupca na »ErrorURL«, zaradi česar lahko sledi:

- Kljub napaki je lahko bila transakcija uspešna.
- Trgovec ne dobi obvestila in s tem izgubi nadzor nad transakcijo.
- Kupec je preusmerjen na Error URL, kjer se mu prikaže statična informacija o napaki (trgovec ne pozna izida). Kupec ponovno poskusi izvedbo transakcije.

Zaradi tega je pomembno, da trgovec pripravi Error URL na tak način, da z njim pridobi čim več uporabnih informacij za nadaljnje raziskave. Priporočljivo je, da se ob prikazu uporabi nek identifikacijski parameter (npr. TrackID), ki ga trgovec pozna že ob začetku transakcije.

3.8 *Zahtevek Payment*

Z izmenjavo sporočil »server-to-server«, lahko trgovec izvaja tudi kreditne in storno transakcije (off-line). Polja, ki se uporabljajo v takih zahtevkih, so naslednja:

- PaymentID (»**paymentid**«): enolična šifra za identifikacijo nakupa. Payment Gateway ustvari to šifro v odgovoru na zahtevek PaymentInit.
- Original TransID (»**transid**«): enolična šifra za identifikacijo transakcije. Dodeli jo Payment Gateway v odgovoru NotificationMessage.
- Tran Portal ID (»**id**«): Identifikacijska šifra trgovca, dodeljena v fazi aktivacije trgovca.
- Tran Portal Password (»**password**«): Geslo, ki je dodeljeno trgovcu v fazi aktivacije.
- Action Code (»**action**«): tip operacije (5 = Capture, 2 = Credit).
- Amount (»**amt**«): znesek.
 - Action=5 (znesek zahtevka < ali = originalnemu znesku)
 - Action=2 (znesek zahtevka < ali = originalnemu znesku)
- Track ID (»**trackid**«): Identifikacijska šifra transakcije. Ponavadi je to unikatna šifra naročila v sistemu trgovca.
- Currency code (»**currencycode**«): šifra valute.
- User Defined Fields (»**udf1**« – »**udf5**«): 5 polj na razpolago trgovcu za dodatne informacije, ki jih po želji uvrsti v sporočilo. Te informacije se lahko nespremenjeno prikažejo v NotificationMessage sporočilu.

3.9 *Odgovor Payment*

To je odgovor, ki ga Payment Gateway vrne trgovcu po prejemu zahtevku PaymentInit (po validaciji prejetega sporočila). Vsebuje naslednja polja:

- Result: izid.
- Auth : avtorizacijska koda izdana s strani izdajatelja kartice.
- Ref: referenčna številka.
- AVR: izid– ni podprto v Evropi in se zaenkrat ne uporablja
- Date: datum in ura transakcije.
- TransID: enolična šifra, ki jo dodeli Payment Gateway.
- TrackID: Identifikacijska šifra transakcije. Ponavadi je to unikatna šifra naročila na sistemu trgovca.
- User Defined Fields (»udf1« – »udf5«): 5 polj na razpolago trgovcu za dodatne informacije, ki jih po želji uvrsti v sporočilo. Te informacije se lahko nespremenjeno prikažejo v NotificationMessage sporočilu.

3.10 Opis vtičnika e24PaymentPipe

Ob aktivaciji trgovca v testno okolje, prejme trgovec tako imenovani plug-in »e24PaymentPipe«, ki ga lahko uporabi na različnih platformah:

- Java
- ASP
- ActiveX/COM
- ColdFusion

Osnovne karakteristike omenjenih platform so opisane v nadaljevanju.

Java

Java Class Object e24PaymentPipe je »platform independent« in se zato lahko uporablja v različnih okoljih. Razvijalci lahko uporabijo komponento »e24PaymentPipe« za izvajanje transakcij na svojem sistemu. Na portalu Payment Gateway je priložen primer.

Active Server Pages

Isti objekt je lahko preko vmesnika uporabljen tudi v ASP okolju. (ASP ne podpira asinhrono komunikacije, zato e24PaymentPipe ne bo vračal statusa sporočil). Na portalu Payment Gateway je priložen primer uporabe v okolju ASP.

ActiveX/COM

Objekt ActiveX/COM e24PaymentPipe podpira različne metode izvajanja varnih transakcij preko interneta v realnem času. Lahko se ga uporablja v desktop aplikacijah, CGI, web server API, ASP in ostalih. Na portalu Payment Gateway je priložen primer uporabe v Visual Basicu.

3.11 Specifikacija direktnega vmesnika

V primeru, da trgovec nima primerne platforme za uporabo plug-in načina (taka je npr. PHP platforma), si lahko izdelata lasten vmesnik. V nadaljevanju je opisan komunikacijski protokol, format pošiljanja in sprejemanja sporočil, variabilna polja in »error« sporočila.

Plug-in e24PaymentPipe je bil izdelan po enakih specifikacijah in zagotavlja enostavno uporabo ter hitro integracijo.

Specifikacija komunikacijskega protokola

- **Protokol:**
http v testnem okolju
https v produkcijskem okolju
- **Vrata (port):**
80 v testnem okolju
443 v produkcijskem okolju
- **Target (action):**
Testno okolje
za PaymentInit: <http://test4.constriv.com/cg301/servlet/PaymentInitHTTPServlet>
za Payment: <http://test4.constriv.com/cg301/servlet/PaymentTranHTTPServlet>
Produkcijsko okolje
za PaymentInit: <https://> bo sporočeno trgovcu pred preходом v produkcijo
za Payment: <https://> bo sporočeno trgovcu pred preходом v produkcijo
Method: POST
- **Content-Type:**
»application/www-form-urlencoded« ali »application/x-www-form-urlencoded«
- **Format pošiljanja podatkov:**
Url Encoded
- **Format prejemanja podatkov:**
posamezna tekst 'stringa' formirana iz polj (separator “:”)
- **Encryption Level:**
Za test ni predvidena enkripcija
SSL3 v produkciji

Format pošiljanja podatkov

Vsi podatki se pošiljajo v formatu URL encoded, ki ga sestavljata ime polja in vrednost polja.

- **Sporočilo PaymentInit:**
*id=TranPortalID&password=password&action=action&langid=language¤cy
code=978&amt=amount&responseURL=www.merchant.com/response&errorURL=
www.merchant.com/error &trackid=unique tracking id&udfl=User Defined Field*

1&udf2=User Defined Field 2&udf3=User Defined Field 3&udf4=User Defined Field 4&udf5=User Defined Field 5

- **Sporočilo Payment:**

id=TranPortalID&password=password&action=action¤cycode=978&amt=amount&paymentid=paymentID&transid=transID&trackid=trackID&udf1=User Defined Field 1&udf2=User Defined Field 2&udf3=User Defined Field 3&udf4=User Defined Field 4&udf5=User Defined Field 5

- **Format prejemanja podatkov**

Odgovor, ki ga pošlje Payment Gateway, ima obliko 'text stringa', v katerem so prisotne vrednosti variabilnih polj (brez imen) v definirani strukturi. Trgovec mora iz sporočila izluščiti potrebne podatke:

- PaymentInit Response:
PaymentId:PaymentURL
- Payment Response:
Result:Auth:Ref:AVR>Date:TransId:TrackId:UDF1:UDF2:UDF3:UDF4:UDF5

- **Error sporočila**

V primeru napake med pripravo sporočila za Payment Gateway (**PaymentInit** ali **Payment**), se v začetku odgovora nahaja sledeča oznaka: »!ERROR!«, sledi šifra napake in opis. Pomembno je, da trgovec za vsako prejeto sporočilo (odgovor) preveri prisotnost omenjenega ERROR polja. Seznam napak je priložen na koncu dokumenta.

3.12 Demo

V paketu, ki ga prejme trgovec ob otvoritvi testnega prodajnega mesta, je poleg navodil priložen primer e-com trgovine izdelane v ASP platformi. Primer prikazuje uporabo in način povezovanja s Payment Gatewayjem z uporabo plug-in načina e24PaymentPipe (verzija DLL) ali brez njega.

Primer zajema naslednje strani:

- »Index«: prva stran prikazuje produkt, za katerega je bil določen nakup.
- »Details«: Kontrolna stran, kjer se lahko preveri vsebina košarice in drugi podatki o nakupu. Nakup se potrdi z gumbom »Nakup«.
- »Buy«: stran se aktivira z gumbom »Nakup« (v tej fazi se uporabi plug-in). Plug-in pripravi sporočilo PaymentInit in ga pošlje na Payment Gateway, ki v odgovoru preusmeri brskalnik na HPP stran.
- »Pure-Buy«: To je primer strani brez uporabe plug-in načina (potrebno je popraviti parametre v Details.asp za pravilno delovanje).
- »Receipt«: po uspešni transakciji je poslan NotificationMessage na 'Notify URL'.
- »Result«: URL trgovca, kjer je prikazan izid transakcije.
- »Error«: ob napaki je prikazana ta stran.

4 TESTNO OKOLJE IN PRILAGODITVE

Trgovec ima na razpolago testno okolje, kjer lahko izvaja transakcije in testira svoje prodajno mesto pred preходом v produkcijo. Testno okolje je trgovcem stalno na razpolago (kljub temu so možne nenapovedane prekinitve delovanja zaradi vzdrževalnih del).

Spisek spremenljivk, ki se uporabljajo v testnem okolju:

- *address*: test4.constriv.com
- *context*: /cg301
- *port*: 80
- *id*: [vsak trgovec dobi svojega]
- *password*: [sporočen po elektronski pošti]
- *action*: 1 ali 4 (2 ali 5 za naknadne transakcije)
- *currencycode*: 978
- *langid*: »USA« ali »SLO« (oznake podprtih jezikov so opisane v poglavju 3.3)

Ostali podatki se lahko prosto uporabljajo.

Ob prikazu HPP strani, se lahko uporabijo naslednji podatki o testni kartici:

- Št kreditne kartice: xxxx xxxx xxxx xxxx (testna št. bo posredovana ob aktivaciji testnega ID-ja)
- Datum veljavnosti: MM/LLLL

4.1 Prikaz logotipov

V obdobju testiranja mora trgovec banki sporočiti naslov svoje testne strani, kjer se preveri izgled in skladnost postavitve kartičnih in bančnih logotipov.

Trgovec mora kupca seznaniti o možnosti uporabe varnih načinov plačila »rust mark« »Verified by Visa« in »MasterCard SecureCode« že v fazi pregleda izbranega artikla ali na strani pregleda košarice (logotipa sta lahko pozicionirana na desnem ali spodnjem delu strani). Ločeno od omenjenih logotipov je predvideno še mesto za logotip sistema Activa in banke s katero je bila sklenjena pogodba (vsaka banka poskrbi za svoj logotip):



Naknadno, se na strani za izbor načina plačila prikaže še ostale logotipe podprtih kartičnih produktov in na dnu strani ponovno »Verified by Visa« in »MasterCard SecureCode« logotipa, ki pa morata biti odmaknjena od ostalih logotipov za minimalno 4-kratno širino logotipov.



Sledi tekst-obvestilo imetnikom kartic s povezavami do spletnih strani sistema Activa s podrobnejšim opisom varne elektronske trgovine.

Primer besedila za prikaz na spletni strani:

Plačilne kartice (MasterCard, Maestro, Visa, Visa-Electron, Activa)

Obveščamo vas, da je z novim načinom izvajanja spletnih plačil, skrb o varnosti podatkov o vaši plačilni kartici popolnoma odveč. Nov sistem spletnega plačevanja omogoča, da se podatek o številki kartice in CVV kodi vnaša izključno na varnih straneh banke. Do teh podatkov mi kot trgovec nimamo dostopa oz. vpogleda. V primeru izbire plačila s plačilnimi karticami boste zato preusmerjen na spletni strani, ki jih upravlja procesni center Activa in banka s katero imamo sklenjeno pogodbo o sprejemu kartic.

Novost predstavljajo storitve varnega spletnega plačevanja mednarodnih kartičnih sistemov Visa in MasterCard. Spodaj prikazani blagovni znamki *Verified by Visa* in *Mastercard SecureCode*² omogočata, da lahko z uporabo vaše pametne kartice in prenosnega čitalnika vsak spletni nakup elektronsko podpišete z uporabo enkratnega gesla. V Sloveniji so storitvi Verified by Visa in Mastercard SecureCode podprle banke sistema Activa (več informacij najdete na spletni strani www.activa.si).

Imetnikom plačilnih kartic nudimo trenutno najvarnejše spletno poslovanje, neodvisno od vrste kartice Activa – bodisi kreditne ali debetne. Plačujete lahko z naslednjimi plačilnimi karticami:


- MasterCard
- Maestro
- Visa
- Visa Electron

E-nakupovanje z **Maestro** kartico je možno pod pogojem, da je imetnik svojo kartico registriral na sistemu za avtentikacijo »MasterCard SecureCode«. Vse Maestro kartice sistema Activa (pametne plačilne kartice s čipom) so avtomatično že registrirane in torej usposobljene za nakupe v naši spletni trgovini. Več o tem na <http://www.activa.si/novica.asp?ID=35>. Prav tako so v program varne spletne trgovine vključene tudi vse ostale pametne kartice sistema Activa (MasterCard, Visa in Visa Electron). Več o tem na <http://www.activa.si/novica.asp?ID=91>.

² Povezavi do za imetnika koristnih informacij o sistemu MasterCard SecureCode in Verified by Visa.

- Povezava MasterCard SecureCode <http://www.pametna-kartica.si/securecode.asp>
- Povezava Verified by Visa <http://www.pametna-kartica.si/vbv.asp>

Primer postavitve logotipov ob pregledu artikla:



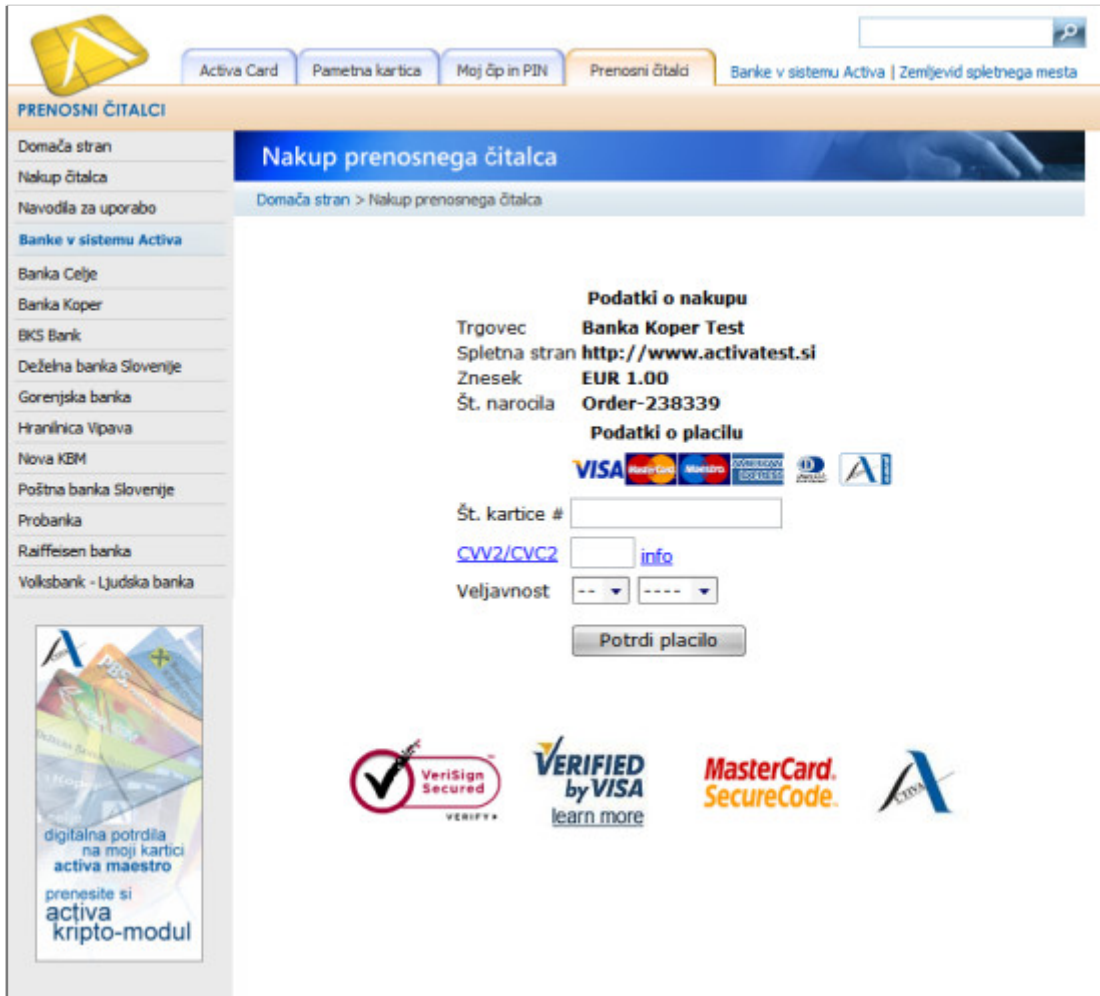
The screenshot shows the 'Nakup prenosnega čitalca' (Purchase portable reader) page. The product is a 'Prenosni čitalec - OTP TODOS eCode Signature Todos Data System AB'. The price is 20,00 EUR. The quantity is 1. Shipping options are 1,80 EUR (recommended) or 3,00 EUR (door-to-door). The 'Potrjujem nakup' (I confirm purchase) button is visible. Logos for MasterCard SecureCode, Verified by VISA, and Activa are present. A vertical double-headed arrow on the right side of the page indicates the placement of logos.

Primer postavitve logotipov pri izbiri plačila:



The screenshot shows the 'Nakup prenosnega čitalca' page at the payment selection stage. The 'Plačilo:' (Payment) section has 'Plačilne kartice' (Credit cards) selected. Below it, the 'Košarica:' (Basket) section shows the product and a total price of 22,30 EUR. The 'Potrjujem nakup' button is at the bottom. Logos for Activa, MasterCard, Maestro, VISA, and VISA-ELECTRON PAY are displayed. A text block explains the secure payment system. Logos for MasterCard SecureCode and Verified by VISA are also shown. A vertical double-headed arrow on the right side of the page indicates the placement of logos.

Primer prikaza »bančne« HPP strani



PRENOSNI ČITALCI

Activa Card | Pametna kartica | Moj čip in PIN | Prenosni čitalci | Banke v sistemu Activa | Zemljevid spletnega mesta

Nakup prenosnega čitalca

Domača stran > Nakup prenosnega čitalca

Podatki o nakupu

Trgovec: **Banka Koper Test**
 Spletna stran: **http://www.activatest.si**
 Znesek: **EUR 1.00**
 Št. narocila: **Order-238339**

Podatki o placilu

VISA | MasterCard | Maestro | American Express | Diners Club | A1

Št. kartice #

CW2/CVC2 [info](#)

Veljavnost -- -- ---- --

VeriSign Secured | **VERIFIED by VISA** learn more | **MasterCard SecureCode** | **ACTIVA**

digitalna potrdila na moji kartici **activa maestro**
 prenesite si **activa kripto-modul**

4.2 Prilagoditev HPP strani

Trgovec lahko poljubno prilagodi grafični izgled »Hosted Payment Page« (HPP) strani. Namen te možnosti je, da kupec ne zazna preusmeritve na HPP. Prilagoditev je možna samo v produkcijskem okolju.

Trgovec lahko pripravi naslednje 3 datoteke, ki vplivajo na izgled HPP strani, v nasprotnem primeru bo uporabljen prednastavljen izgled, ki ga določi banka:

- **Header.html:** HTML koda, ki je uporabljena za prikaz zgornjega dela strani (nad polji za vnos podatkov o kartici).
- **Footer.html:** HTML koda, ki je uporabljena za prikaz spodnjega dela strani (pod polji za vnos podatkov o kartici).
- **Style.css:** datoteka za definiranje »sloga« strani in prikazovanja vnosnih polj.

V nadaljevanju so navedeni pogoji, ki se jih je potrebno držati pri personalizaciji HPP strani.

Primer personalizirane HPP strani:



Header.html

Prikazuje zgornji del strani.

- Tag <HTML>, <HEAD>, <BODY> in ostali meta-tagi ne smejo biti prisotni.
- Trgovec lahko zamenja barvo, prikaže logotipe in informacije vezane na nakup.
- Niso dovoljene povezave do zunanjih strani (linki) - uporabi se lahko le povezave do grafičnih vsebin lastne strani.
- Niso dovoljena reklamna sporočila – uporabi se lahko le informacije vezane na lastno e-com trgovino.

Footer.html

Prikazuje spodnji del strani. Tudi v tem primeru so popravki omejeni:

- Trgovec lahko zamenja barvo ozadja.

Na tem mestu, bo banka uvrstila svoje logotipe vezane na varnostne protokole in kartične produkte, ki jih podpira spletna trgovina (barva ozadja ne sme vplivati na prikaz logotipov).

Style.css

Je datoteka za definiranje videza strani in vnosnih polj (nastavitve se lahko uporabljajo tudi za header in footer del strani). Popravki so možni le med tagi: `<STYLE> ... </STYLE>`

Navodila za pripravo datotek:

1. Med izvajanjem transakcij v testnem okolju, si shranimo kopijo HPP strani na lokalni disk.
2. Datoteko je mogoče spreminjati. Ko je dosežen željen videz, se popravke kopira v sledeče datoteke:
 - a. Header:
 - i. Popravimo videz in vsebino pod pogoji, ki jih določa banka.
 - ii. Spremembe shranimo v datoteko »header.html«.
 - b. Style:
 - i. Popravimo vsebino med tagi `<STYLE> </STYLE>`.
 - ii. Popravke shranimo v datoteko »style.css«.
 - c. Footer:
 - i. Popravimo videz in vsebino pod pogoji, ki jih določa banka.
 - ii. Spremembe shranimo v datoteko »footer.html«.
3. Popravljenе 3 datoteke (in morebitne druge datoteke kot so razne grafike, slike, logotipi, ozadja) je potrebno poslati v pregled banki (e-mail naslov bo sporočen naknadno), kjer bodo prenesene v produkcijsko okolje prodajnega mesta. Priloži se tudi popravljeno HPP stran, za hiter predogled popravkov.

Banka ima pravico zavrniti predlagane popravke in uporabiti svojo prednastavljeno HPP stran. Vsak trgovec lahko pošlje spremembe datotek za personalizacijo HPP strani največ trikrat. Po treh menjavah bo trgovcu onemogočeno ponovno spreminjanje strani.

5 OBRAČUN TRANSAKCIJ

Obračun prometa spletnih nakupov se lahko izvede sočasno z izvedbo transakcije ali pa naknadno v predvidenem roku, ki ga določi banka (npr. 15 dni). Sistem Payment Gateway daje trgovcem možnost, da za posamezno transakcijo določi način obračuna.

5.1 Neposredni obračun

Neposredni način obračunavanja prometa se sproži, ko je v sporočilu PaymentInit definiran parameter `Action=1`. V tem primeru se transakcija obravnava kot »Purchase«. Uspešno avtorizirane »Purchase« transakcije so obdelane v redni dnevni obdelavi prometa in imajo datum obdelave nakupa enak datumu avtorizacije le-tega.

Pomembno: Neposredni obračun se uporablja v primerih, ko trgovec ponuja storitev, ki jo kupec lahko koristi neposredno po opravljeni transakciji.

V primerih, ko kupec želi stornirati nakup iz neznanega razloga, lahko trgovec izvede vračilo »Credit« ali »Void Purchase« v delnem ali celotnem znesku.

Postopek vračila se lahko izvede na dva načina:

- Z uporabo plug-in načina: trgovec pošlje »Payment« sporočilo s parametrom `Action=2` ali `Action=3`.
- Preko Payment Gateway portala: postopek se izvede tako, da se v arhivu označi sporno transakcijo, vnese znesek vračila ter potrdi vnos.
(*Znesek $Credit1 + Credit2 + Credit3 + \dots + CreditN$ je manjši ali enak originalnemu znesku*).

Shema 1:

Operation:	Purchase	→	Credit
Action:	1		2

Možno je izvesti več »Credit« transakcij za eno »Purchase« transakcijo (Vsota vseh »Credit« transakcij je lahko manjša ali enaka originalnemu znesku).

Shema 2:

Operation:	Purchase	→	Credit #1	→	Credit #2	→	Credit #3...
Action:	1		2		2		2

Shema 3:

Operation:	Purchase	→	Void Purchase
Action:	1		3

5.2 Zakasneni obračun

Zakasnen način obračunavanja prometa se sproži, ko je v sporočilu PaymentInit definiran parameter **Action=4**. V tem primeru se transakcija obravnava kot »**Authorization**«.

Odobrena transakcija zniža limit kartice v vrednosti avtoriziranega zneska, promet pa se obdela šele po posredovanju trgovca. Ko je blago poslano, trgovec potrdi transakcijo s funkcijo »**Capture**«. Znesek transakcije »Capture« je lahko nižji ali enak avtoriziranemu znesku. Postopek potrditve transakcije trgovca se lahko izvede na dva načina:

- Z uporabo plug-in načina: trgovec pošlje »Payment« sporočilo s parametrom **Action=5**.
- Preko Payment Gateway portala: postopek se izvede tako, da se v arhivu izbere zelena avtorizacija, vnese končni znesek ter potrdi z možnostjo "Capture" (znesek je manjši ali enak znesku avtorizacije).

V primeru, da kupec želi vrniti prejeto blago, lahko trgovec izvede vračilo »**Credit**« v celotnem ali delnem znesku. Postopek vračila se lahko izvede na dva načina:

- Z uporabo plug-in načina: trgovec pošlje »Payment« sporočilo s parametrom **Action=2**.
- Preko Payment Gateway portala: postopek se izvede tako, da se v arhivu označi sporno transakcijo, vnese znesek vračila ter potrdi vnos
(*Znesek Credit1 + Credit2 + Credit3 + ... + CreditN je manjši ali enak originalnemu znesku.*)

Shema 1:

Operation:	Authorization	→	Capture	→	Credit
Action:	4		5		2

Mogoče je izvesti več »Credit« transakcij za eno »Capture« transakcijo (vsota »Credit« zneskov je lahko manjša ali enaka »Capture« znesku).

Shema 2:

Operation:	Authorization	→	Capture	→	Credit #1	→	Credit #2...
Action:	4		5		2		2

Shema 3:

Operation:	Authorization	→	Void Authorization
Action:	4		9

Vrednosti parametra »Action«:

- | | |
|--------------------------|--|
| ▪ 1 = Purchase | Neposredni obračun |
| ▪ 2 = Credit | Vračilo (delnega zneska ali zneska v celoti) |
| ▪ 3 = Void Purchase | Vračilo / storno celotnega zneska |
| ▪ 4 = Authorization | Avtorizacija |
| ▪ 5 = Capture | Potrditev avtorizacije |
| ▪ 9 = Void Authorization | Storno avtorizacije |

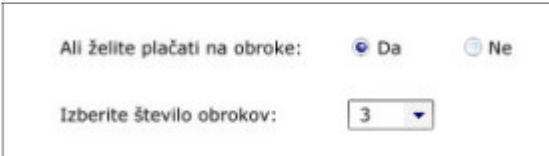
5.3 Obročno odplačevanje Diners in American Express

To poglavje velja samo za trgovce, ki v svojih spletnih trgovinah sprejemajo kartične produkte Diners in/ali American Express. S karticama Diners in American Express lahko imetniki namreč plačujejo blago in storitve tudi na obroke. Če želi trgovec ponuditi obročno odplačevanje tudi v svoji spletni trgovini mora slediti naslednjim navodilom:

- Imetnik izbere izdelke, ki jih želi kupiti, izpolni osebne podatke in klikne na gumb za nakup.
- Trgovec preveri s katerim plačilnim sredstvom želi imetnik opraviti nakup. Primer:



- Če imetnik izbere kartico Diners oz. American Express, trgovec najprej preveri, če nakup ustreza pogojem za plačilo na obroke in posledično imetniku ponudi možnost obročnega plačila. Primer:



- Trgovec pošlje sporočilo o začetku plačila (**PaymentInit**) na sistem Payment Gateway tako kot to počne za vsa ostala kartična plačila. Podatke o obročnem plačilu posreduje preko parametra »**udf2**« na naslednji način:

- Parameter »**udf2**« je potrebno poslati v dolžini 24 znakov, kjer od pozicije 23 definiramo število obrokov. Polje formirano na naslednji način:

```
udf2=PI 1 40 000000000XX
```

kjer XX predstavlja število obrokov.

- Primer za 3 obroke: `udf2=PI 1 40 00000000003`
- Primer za 12 obrokov: `udf2=PI 1 40 00000000012`

- Podroben pregled formata polja udf2:

Pozicija 1 – 2:	PI
Pozicija 3:	<presledak>
Pozicija 4:	1
Pozicija 5 – 6:	<2 presledka>
Pozicija 7 – 8:	40
Pozicija 9 – 13:	<5 presledkov>
Pozicija 14 – 22:	000000000
Pozicija 23 – 24:	<2 poziciji za število obrokov, glej zgornji primer>

- Kupec nato na HPP strani vpiše številko svoje Diners ali Amex kartice, podatki o plačilu se nato avtorizirajo pri enem od izdajateljev, trgovec pa prejme sporočilo o uspešno oz. neuspešno obdelani transakciji, ki ga prikaže kupcu.
- Vse nadaljnje aktivnosti povezane z obračunom se izvajajo enako kot pri ostalih kartičnih produktih.

6 OSNOVE DELA NA BACK-OFFICE PORTALU PAYMENT GATEWAY

Vse podatke za prijavo na Back-Office portal sistema Payment Gateway prejmejo trgovci v PDF dokumentu bodisi ob prejemu testnega dostopa, bodisi ob prejemu dostopa do produkcijskega okolja. Povezava za dostop do testnega portala je <http://www.activa.si/test>.

6.1 Delo s transakcijami

Pregled transakcij

- V Back-Office portalu sistema Payment Gateway v meniju »**Orders**« izberite »**Detail Report**«.
- V formi, ki se prikaže izberite časovno obdobje in morebitne druge podatke o transakcijah, ki jih želite prikazati.
- Pritisnite gumb »**Generate Report**«.

Potrditev avtorizacije

- Kadar v spletni trgovini izvajate transakcije s parametrom `Action=4` (avtorizacija) je potrebno ob pošiljanju blaga vsako avtorizacijo tudi potrditi. Če potrditve nimate razvite avtomatično oziroma vam avtomatika potrditve ne izvede samodejno, lahko to naredite preko BackOffice portala Payment Gateway.
- Na seznamu transakcij kliknete gumb »**Trans**« poleg avtorizacije, ki jo želite potrditi (to so tiste transakcije, ki imajo na seznamu kodo transakcije (Result Code) enako »APPROVED«).
- V formi, ki se prikaže pod »**Available Actions**« v polju »**Capture Euros**« potrdite avtorizacijo v znesku nižjem ali enakem avtoriziranemu s klikom na gumb »**Proceed**«.

Storno avtorizacije

- Storno avtorizacije sprosti zasežena sredstva (limit) na imetnikovi kartici.
- Na seznamu transakcij kliknete gumb »**Trans**« poleg avtorizacije, ki jo želite stornirati (to so tiste transakcije, ki imajo na seznamu kodo transakcije (Result Code) enako »APPROVED«).
- V formi, ki se prikaže pod »**Available Actions**« v polju »**Void the transaction**« stornirajte avtorizacijo s klikom na gumb »**Proceed**«.

Storno finančne transakcije

- Na seznamu transakcij kliknete gumb »**Trans**« poleg transakcije, ki jo želite stornirati (to so tiste transakcije, ki imajo na seznamu kodo transakcije (Result Code) enako »CAPTURED«).

- V formi, ki se prikaže pod »**Available Actions**« v polju »**Reverse the transaction**« stornirajte transakcijo s klikom na gumb »**Proceed**«.

Delni storno finančne transakcije

- Na seznamu transakcij kliknete gumb »**Trans**« poleg transakcije, za katero želite delno ali v celoti povrniti sredstva (to so tiste transakcije, ki imajo na seznamu kodo transakcije (Result Code) enako »**CAPTURED**«).
- V formi, ki se prikaže pod »**Available Actions**« v polju »**Credit Euros**« potrdite storno transakcije v znesku nižjem ali enakem znesku transakcije s klikom na gumb »**Proceed**«.

6.2 Terminologija

Order Statuses (statusi naročil)

Tukaj so opisani statusi naročil, kot jih vidite v Back-Office portalu sistema Payment Gateway v koloni »**Order status**«:

- **AUTH ERROR** – Najpogosteje se ta napaka pojavi kadar imetnik v okno za vnos podatkov vnese napačne ali nepopolne podatke o kartici (npr. številko kartice, ki ne obstaja).
- **INITIALIZED** – Status »Initialized« pomeni, da je bila transakcija samo inicializirana, ni pa prišlo niti do klica za prikaz okna za vnos podatkov o plačilni kartici.
- **PRESENTED** – Status »Presented« pomeni, da je bila prikazana stran za vnos podatkov o kartici, vendar je uporabnik na tem mestu zapustil stran oz. zaprl okno brskalnika brez da bi vnesel podatke o kartici.
- **PROCESSED** – Naročilo je bilo uspešno procesirano. To pomeni, da je Payment Gateway prejel odgovor o uspešnosti oz. neuspešnosti avtorizacije oz. transakcije.
- **TIMEOUT** – Naročilo je poteklo zaradi nezmožnosti povezave s procesnim centrom izdajatelja imetnikove kartice.

Result Codes (kode transakcij)

Tukaj so opisani možni odgovori na izvedbo transakcije, kot jih vidite v Back-Office portalu sistema Payment Gateway v koloni »**Financial status**«:

- **APPROVED** – Avtorizacija uspešna. Izvedete lahko dejansko bremenitev sredstev z uporabo funkcije CAPTURE. Odobrena avtorizacija zniža limit kartice v vrednosti avtoriziranega zneska. Ko je blago poslano, trgovec potrdi avtorizacijo s funkcijo CAPTURE. Znesek transakcije CAPTURE je lahko nižji ali enak avtoriziranemu znesku. Po potrditvi avtorizacije dobi transakcija status CAPTURED oz. NOT CAPTURED.
- **NOT APPROVED** – Avtorizacija neuspešna. To se zgodi kadar ima kartica presežen periodni limit, premalo sredstev na razpolago, je blokirana ali kaj podobnega.

- **CAPTURED** – Predstavlja uspešno finančno bremenitev. Po opravljeni avtorizaciji je namreč potrebno transakcijo potrditi. Funkcija CAPTURE omogoča potrditev zneska enakega ali manjšega znesku avtorizacije.
- **NOT CAPTURED** – Potrditev transakcije neuspešna. Neuspešna finančna bremenitev.
- **DENIED BY RISK** – Na samem sistemu Payment Gateway je mogoče s strani banke nastavljati t.i. risk parametre (št. kartic s sumljivimi transakcijami, prodajna mesta s sumljivimi posli itd.). V primeru, da pride do transakcije s kartico oz. na prodajnem mestu, ki je na tem seznamu, dobite izid transakcije označen s sporočilom DENIED BY RISK.
- **UNKNOWN** – Izida transakcije ni mogoče določiti. V primeru takega izida se obrnite na banko.
- **HOST TIMEOUT** – Do izida HOST TIMEOUT pride v primeru, ko avtorizacijski sistem ne vrne odgovora sistemu Payment Gateway v določenem časovnem intervalu.

7 POGOSTA VPRAŠANJA

7.1 Preusmeritev na naslov ErrorURL kljub uspešno izvedeni transakciji

Razlogov za preusmeritev na naslov ErrorURL kljub uspešno izvedeni transakciji je lahko več, vsekakor pa gre za napako v implementaciji same spletne trgovine.

Ne glede na uspešen ali neuspešen izid transakcije vas Payment Gateway vedno preusmeri na stran ResponseURL, na kateri nato prikažete izid transakcije. ErrorURL se uporablja samo v primerih, ko pride do raznoraznih zapletov v komunikaciji oz. delovanju sistema, npr. ko Payment Gateway ne more dostopati do vaše ResponseURL strani.

Eden od razlogov je lahko ta, da ResponseURL stran ni dosegljiva sistemu PaymentGateway, ki sicer na ResponseURL posreduje podatke o uspešnosti transakcije. Razlogi za to so lahko različni varnostni sistemi, npr. požarne pregrade (firewall) in podobni varnostni sistemi. ResponseURL stran mora biti sistemu PaymentGateway namreč vedno dosegljiva.

Druga (sicer najbolj pogosta) napaka pa je lahko tudi napaka v sami kodi spletnega vmesnika. Velikokrat namreč trgovci pri implementaciji pozabijo na določen korak zaključnega procesa transakcije in tako ne dobijo rezultata ne glede na to, ali je sama transakcija uspešna ali ne.

V nadaljevanju je prikazana kratka obrazložitev bistvenih strani plačilnega procesa na primeru ASP:

Po vnosu vseh potrebnih podatkov na straneh vaše trgovine in pritisku na gumb "plačilo" je potrebno parametre, ki so vezani na plačilo (cena...) prenesti na drugo stran, kot je prikazano v spodnjem primeru (buy.asp).

< ZAČETEK Buy.asp STRANI >

```
<%Dim MyObj
Set MyObj = Server.CreateObject("e24PaymentPipe.e24PaymentPipe.1")
MyObj.WebAddress = "www.constriv.com"
MyObj.PortStr = "443"
MyObj.Context = "/cg"
MyObj.ID = "XXXXXXXXXX"           'TranPortal ID
MyObj.Password = "XXXXXXXXXX"    'TranPortal PWD
MyObj.Action = "4"               'vrsta plačila
MyObj.Amt = Request.form("PRICE") 'znesek plačila
MyObj.Currency = "978"           'valuta, 978 = EURO
MyObj.Language = "SLO"           'jezik za prikaz HPP strani
```

```
' Vnesete URL naslove vašega strežnika
MyObj.ResponseURL = "http://www.vas-streznik.si/response.asp"
' na ta naslov PaymentGateway pošlje podatke o izidu transakcije
```

```
MyObj.ErrorURL = http://www.vas-streznik.si/error.asp
' V primeru sistemskih ali komunikacijskih napak se izvede preusmeritev na
to stran.
```

```
randomize
Ord_id = cstr(cLng(rnd(50) * 1000000))

MyObj.TrackId = "Order-" & Ord_id 'strTrackID -- TODO create a new trackid
for each transaction'

MyObj.Udf1 = Request.form("ime")
MyObj.Udf2 = Request.form("naslov")
MyObj.Udf3 = Request.form("posta")
MyObj.Udf4 = Request.form("kraj")
MyObj.Udf5 = Request.form("e-mail")

'perform the transaction'

Dim TransVal, varPaymentId, varPaymentPage, varErrorMsg, varRawResponse,
varRedirectURL

TransVal = MyObj.PerformInitTransaction 'returns 0 for succes -1 for
failure varRawResponse = MyObj.RawResponse varPaymentId = MyObj.PaymentId
varPaymentPage = MyObj.PaymentPage varErrorMsg = MyObj.ErrorMsg
varRedirectURL = varPaymentPage & "?PaymentID=" & varPaymentId

Response.Redirect varRedirectURL
```

< **KONEC Buy.asp STRANI** >

ResponseURL stran mora sprejeti parametre, ki ji jih posreduje Payment Gateway in nato formirati naslov (ReceiptURL), na katerem bo prikazan izid transakcije. Ta korak trgovci oz. njihovi razvijalci pri implementaciji v veliko primerih preskočijo, zato pride do napake pri preusmeritvi.

< **ZAČETEK ResponseURL STRANI** >

```
<% Dim PayID, TransID, ResCode, AutCode, PosDate, TrckID, UD1, UD2, UD3,
UD4, UD5, ReceiptURL
```

```
PayID = Request.Form("paymentid")
TransID= Request.Form("tranid")
ResCode = Request.Form("result")
AutCode = Request.Form("auth")
PosDate = Request.Form("postdate")
TrckID = Request.Form("trackid")
```

```
UD1 = Request.Form("udf1")
UD2 = Request.Form("udf2")
UD3 = Request.Form("udf3")
UD4 = Request.Form("udf4")
UD5 = Request.Form("udf5")
```

' V spodnji URL vnesete točen naslov vašega strežnika, npr.:

```
ReceiptURL = "REDIRECT=http://www.vas-streznik.si/uspesna.asp?PaymentID=" &
PayID & "&TransID=" & TransID & "&TrackID=" & TrckID & "&postdate=" &
PosDate & "&resultcode=" & ResCode & "&auth=" & AutCode%>
```

```
<%=ReceiptURL%>
```

< **KONEC ResponseURL STRANI** >

Na končni strani (v zgornjem primeru »www.vas-streznik.si/uspesna.asp«) nato izpišete zaključno poročilo transakcije, npr.:

< ZACĀETEK ReceiptURL STRANI >

```
<%  
' get Merchant Notification parameters  
Dim payID  
payID = request.QueryString("PaymentID")  
  
if IsEmpty(payID) Then  
    response.Redirect("error.asp")  
end if  
  
if ( request.QueryString("resultcode")="CAPTURED" or _  
request.QueryString("resultcode")="APPROVED" ) Then%>  
  
    <FONT color="GREEN" face="Verdana" style="font-size: 12px">  
        Transakcija JE odobrena. Hvala za nakup.  
    </FONT>  
  
<% else %>  
  
    <FONT color="RED" face="Verdana" style="font-size: 12px">  
        Transakcija NI odobrena.  
        Prosimo, obrnite se na vašo banko in poskusite znova.  
    </FONT>  
  
<% end if %>
```

< KONEC ReceiptURL STRANI >

Na končni strani lahko prav tako prikažete tudi podatke o transakciji, npr.:

```
Podatki o nakupu:<br>  
Track ID: <%=request.QueryString("TrackID")%><br>  
Auth Code: <%=request.QueryString("auth")%><br>  
Post Date: <%=request.QueryString("postdate")%><br>  
Result Code: <%=request.QueryString("resultcode")%><br>  
Payment ID: <%=request.QueryString("PaymentID")%><br>  
Transaction ID: <%=request.QueryString("TransID")%>
```

7.2 Transakcije

V nadaljevanju je opisano nekaj najpogostejših vprašanj vezanih na izide transakcij in njihov pregled na Back-Office portalu sistema Payment Gateway.

Q: Glede na to, da plačilni proces poteka na strani vašega strežnika me zanima, ali prejmemo povratno informacijo, če stranka v tistem trenutku zapre brskalnik in ne dokonča plačila. Mi moramo namreč sprostiti zaloge v primeru, da je stranka prekinila plačilo?

A: V primeru, ko uporabnik prekine transakcijo na strani, ki od njega zahteva vnos podatkov o kartici, dobite samo podatek o inicializirani transakciji s statusom PRESENTED, če pa ni bilo prikazano niti okno za vnos podatkov o kartici, ima transakcija status INITIALIZED. Če uporabnik zapre okno brskalnika po kliku na gumb za plačilo, torej med samim procesiranjem transakcije, sam ne bo dobil informacije o izidu transakcije, taka transakcija pa je lahko odobrena ali pa ne. Vsekakor pa so podatki o izidu transakcije na voljo preko Back-Office portala Payment Gateway.

Q: Po prejemu statistike in podatkov o prometu na našem prodajnem mestu opažamo izjemno velik izpad z izidom PRESENTED ali INITIALIZED.

A: Take težave ne izvirajo iz nedelovanja plačilnega sistema ampak so odvisne od same narave spletnega mesta (še posebej močno obiskana spletna mesta). Večina transakcij je samo inicializiranih, to pa pomeni, da je obiskovalec s klikanjem res prišel do okna za vnos podatkov o plačilni kartici, nakar je stran zapustil brez vnosa kakršnihkoli podatkov. Takih inicializiranih transakcij je veliko in niso nič čudnega, če predvidevamo, da spletno mesto dnevno obiše kar veliko število uporabnikov, med temi pa nekateri iz same radovednosti pridejo tudi do plačilne strani.

Q: Prosimo preverite kaj se dogaja, ali so kakšne napake oziroma kakšni so razlogi za izpad transakcij. Opazili smo kar nekaj uporabnikov, ki so imeli težave s plačili s karticami.

A: Navadno so razlogi za neuspešnost nekaterih transakcij popolnoma običajni. Velikokrat je na primer vnesena napačna številka kartice, neobstoječa številka kartice in podobne kombinacije takih in drugačnih števil (napačen CVC/CVV, napačna veljavnost), ki so posledica neuspešne avtorizacije plačila. Veliko je tudi imetnikov, ki vnašajo številke Maestro kartic, čeprav njihove kartice ne podpirajo spletnega plačevanja. Spletno plačevanje z Maestro karticami je namreč mogoče samo v primeru, ko je kartica registrirana v program MasterCard SecureCode. Takšne Maestro kartice trenutno v Sloveniji izdajajo samo banke sistema Activa.

Q: Kako poteka postopek avtorizacije Maestro plačilnih kartic?

A: Plačilo z Maestro kartico je mogoče le v primeru, ko imetnikova banka izdaja kartice, ki omogočajo uporabo storitve MasterCard SecureCode. Konkretno v Sloveniji take Maestro kartice trenutno izdajajo vse banke članice sistema Activa. Postopek avtorizacije pa se v ničemer ne razlikuje od avtorizacije ostalih kartičnih produktov.

8 NAMESTITEV DEMO SPLETNE STRANI (PRIMER ASP)

Registracija DLL

- Vsebino datoteke (nahaja se na portalu Payment Gateway) **Plugin301.zip** razpakiramo – shranimo v mapo »c:\e24plugin«.
- V DOS oknu se pomaknemo v podmapo »c:\e24plugin\DLL\Release«.
- Odtipkamo naslednji ukaz: »regsvr32 e24PaymentPipe.dll«.
- Pojavi se obvestilo o uspešni namestitvi. Potrdimo z »OK«.
- V primeru napake poskusimo ukaz »regsvr32 e24PaymentPipe.dll« pognati iz mape »c:\e24plugin\DLL\Debug«.

Namestitev spletne strani

- Po potrebi namestimo Microsoft IIS.
- Vsebino datoteke **DEMO_ASP.zip** kopiramo v novo mapo, in sicer: »c:\inetpub\wwwroot\demo«.
- V IIS aktiviramo novo stran »**MerchantDemo**« (Execute Permissions: »**Scripts only**«).
- Sprožimo reset IIS.
- Preverimo delovanje v brskalniku: <http://localhost/demo/index.asp>.

PRILOGA: ERROR MESSAGES

GW00100-Institution ID required.	GW00250-Transaction denied: Negative Card
GW00101-Brand ID required.	GW00251-Maximum transaction count exceeded.
GW00102-Brand Description required.	GW00252-Maximum transaction volume exceeded.
GW00150-Missing required data.	GW00253-Maximum credit volume exceeded.
GW00151-Invalid Action type	GW00254-Maximum card debit volume exceeded.
GW00152-Invalid Transaction Amount.	GW00255-Maximum card credit volume exceeded.
GW00153-Invalid Transaction ID.	GW00256-Maximum card transaction count exceeded.
GW00154-Invalid Terminal ID.	GW00257-Maximum transaction amount exceeded.
GW00155-Invalid Batch Track ID.	GW00258-Transaction denied: Negative BIN.
GW00156-Batch track ID not unique.	GW00259-Transaction denied: Declined Card.
GW00157-Invalid Payment Instrument.	GW00260-Transaction denied: Credits exceed Captures.
GW00158-Card Number Not Numeric.	GW00261-Trans. denied: Captures exceed Authorizations
GW00159-Card Number Missing.	GW00300-Institution ID required.
GW00160-Invalid Brand.	GW00302-Currency code required.
GW00161-Invalid Card/Member Name data.	GW00350-Merchant has terminals.
GW00162-Invalid User Defined data.	GW00351-Merchant ID required.
GW00163-Invalid Address data.	GW00352-Institution ID required.
GW00164-Invalid Zip Code data.	GW00353-Invalid Login.
GW00165-Invalid Track ID data.	GW00354-Invalid Login.
GW00166-Invalid Card Number data.	GW00355-New password mismatch.
GW00167-Invalid Currency Code data.	GW00356-New password same as old.
GW00168-Institution ID mismatch.	GW00357-Console password required.
GW00169-Merchant ID mismatch.	GW00358-Invalid Login.
GW00170-Terminal ID mismatch.	GW00359-ISO Country code is invalid.
GW00171-Payment Instrument mismatch.	GW00360-Website address is invalid.
GW00172-Card Verification Code Mismatch.	GW00361-Console Password Confirmation required.
GW00173-Currency Code mismatch.	GW00362-Console Password Confirmation invalid.
GW00174-Card Number mismatch.	GW00363-Password Confirmation mismatch.
GW00175-Invalid Result Code.	GW00364-Name is invalid.
GW00176-Failed Previous Captures check.	GW00378-Currency Code is invalid.
GW00177-Failed Capture Greater Than Auth check.	GW00380-Merchant ID not numeric.
GW00178-Void Greater Than Original Amount check.	GW00381-Merchant Password data invalid.
GW00179-Failed Previous Voids check.	GW00383-Merchant Password Confirmation invalid.
GW00180-Failed Previous Credits check.	GW00384-Merchant New Password invalid.
GW00181-Failed Credit Greater Than Capture check.	GW00385-Merchant New Password is required.
GW00200-Address verification failed.	GW00386-Merchant New Confirm Password is required.
GW00201-Transaction not found.	GW00387-Merchant User Password is expired.
GW00203-Invalid access: Must use POST method.	GW00388-Merchant User Name is required.
GW00205-Invalid Original Transaction ID.	GW00389-Merchant User Pswd Confirmation is required.
GW00390-Password and Confirmation mismatch.	GW00478-Invalid Terminal Card Acceptor ID.
GW00391-Merchant User password length is too short.	GW00479-Invalid Terminal Card Acceptor Terminal ID.
GW00392-Merchant User Status is required.	GW00480-Invalid Terminal Acquirer Institution.
GW00393-Merchant User Status is invalid.	GW00481-Invalid Terminal Base24 Terminal Data.

GW00394-Merchant User Password is required.	GW00482-Invalid Terminal Retailer ID.
GW00395-Merchant User Password mismatch.	GW00483-Invalid Terminal Retailer Group ID.
GW00396-Merchant User new password same as old.	GW00484-Invalid Terminal Retailer Region ID.
GW00397-Merchant User inactive.	GW00485-Invalid Terminal Cutover Hour.
GW00398-Merchant User Password length too long.	GW00486-Invalid Terminal Cutover Minute.
GW00399-Merchant User ID is invalid.	GW00550-Category Code missing or invalid.
GW00400-Merchant User Password is invalid.	GW00600-Card number required.
GW00401-Merchant New Password is invalid.	GW00601-Card BIN required.
GW00402-Merchant User Name is invalid.	GW00602-Invalid BIN length.
GW00403-Merchant Password Expire Code is invalid.	GW00603-Institution ID required.
GW00404-Merchant Password Expires Date is invalid.	GW00604-Merchant ID required.
GW00405-Merchant exists with this Merchant Category.	GW00605-Terminal ID required.
GW00420-Currency Code data is not available.	GW00606-Card number required.
GW00421-Currency Code minor digits is invalid.	GW00607-Invalid Card Number.
GW00450-Institution ID required.	GW00608-Invalid Currency Code.
GW00451-Merchant ID required.	GW00609-Invalid Decline Reason.
GW00452-Terminal ID required.	GW00610-Invalid Card Number.
GW00453-TranPortal ID required.	GW00611-Invalid Negative Reason.
GW00454-TranPortal password required.	GW00612-Invalid Card Bin.
GW00455-TranPortal ID not unique.	GW00613-Invalid Negative Reason.
GW00456-Invalid TranPortal ID.	GW00614-Please click correct button or tab.
GW00457-Action not supported.	GW00700-No processes available.
GW00458-Invalid Transaction Attempt.	GW00701-Batch not processed.
GW00459-Terminal not active.	GW00702-Batch could not be started.
GW00460-TranPortal ID required.	GW00703-Institution ID required.
GW00461-Invalid Transaction amount.	GW00704-Batch ID not numeric.
GW00462-Invalid Tranportal Password.	GW00705-Batch ID required.
GW00463-Invalid Terminal Institution ID.	GW00706-Invalid Batch Response File Name
GW00464-Invalid Terminal Merchant ID.	GW00750-Error hashing card number.
GW00465-Invalid Terminal Terminal ID.	GW00850-Missing required data.
GW00466-Invalid Terminal Description.	GW00851-Invalid Action Type.
GW00467-Invalid Terminal External Connection ID.	GW00852-Invalid Card Number.
GW00468-Invalid Terminal Risk Profile.	GW00853-Invalid Card Number.
GW00469-Invalid Terminal Currency Code List.	GW00854-Invalid Expiration Date.
GW00470-Invalid Terminal Action Code List.	GW00856-Invalid Card Verification Code.
GW00471-Invalid Terminal Payment Instrument List.	GW00875-Missing required data.
GW00472-Invalid Terminal Brand List.	GW00876-Invalid Action Type.
GW00473-Invalid Terminal Option Code List.	GW00877-Invalid Card Number.
GW00474-Invalid Terminal Risk Flag.	GW00878-Invalid Card Number.
GW00475-Invalid Terminal Address Verification List.	GW00879-Invalid Expiration Date.
GW00476-Invalid Terminal Tranportal ID.	GW00880-Invalid Card Verification Code.
GW00477-Invalid Terminal Status.	GW00881-Card Type unknown
GW00950-Batch Upload Directory Required.	GW01072-Merchant exists with this Currency Code.
GW00951-Batch Download Directory Required.	GW01180-Hex required.
GW00952-Batch Archive Directory Required.	GW01181-Invalid Key length.
GW00953-Access Log Retention Days Required.	GW01182-Key encryption failed.

GW00954-Transaction Log Retention Days Required.
GW00955-Declined Card Retention Minutes Required.
GW00956-Declined Card Maximum Count Required.
GW00957-Access Log Retention Days Invalid.
GW00958-Transaction Log Retention Days Invalid.
GW00959-Declined Card Retention Minutes Invalid.
GW00960-Declined Card Maximum Count Invalid.
GW00961-Multiple Capture Flag Invalid.
GW00962-Multiple Capture Amount Flag Invalid.
GW00963-Multiple Void Flag Invalid.
GW00964-Compare Void Amount Flag Invalid.
GW00965-Multiple Credit Debit Flag Invalid.
GW00966-Compare Credit Debit Amount Flag Invalid.
GW00967-Batch Upload Directory Invalid.
GW00968-Batch Download Directory Invalid.
GW00969-Batch Archive Directory Invalid.
GW00970-Invalid Terminal Cutover Hour.
GW00971-Invalid Terminal Cutover Minute.
GW00975-FAQ Question ID required.
GW00976-Invalid Language ID.
GW00977-Invalid Question ID.
GW00978-Invalid Question content.
GW00979-Invalid Answer content.
GW00990-Card Number Encryption Failure.
GW01020-Invalid Language ID.
GW01021-Invalid System News Header.
GW01022-Invalid System News Body.
GW01040-Invalid Language ID.
GW01041-Invalid Merchant Guideline Header.
GW01042-Invalid Merchant Guideline Body.
GW01060-Currency Code Required.
GW01061-Institution ID Required.
GW01062-Invalid Minor Digits Range.
GW01063-Currency Code Not Numeric.
GW01064-Currency Code Not Valid ISO Code.
GW01065-Invalid Minor Digits.
GW01066-Invalid Amount.
GW01067-Invalid Currency Code Data.
GW01068-Invalid Currency Description Data.
GW01069-Invalid Minor Digits Data.
GW01070-Invalid Currency Symbol Data.
GW01071-Terminal exists with this Currency Code.
PY20015-Invalid Card Name.
PY20016-Invalid Card Address.
PY20017-Invalid Zip Code.
PY20018-Invalid Card Verification Code.

CM00001-External message timeout.
CM00002-External message system error.
CM00026-External connection ID required.
CM00027-External connection description required.
CM00028-External connection Protocol code required.
CM00029-External connection Formatter class name invalid.
CM00030-External connection Protocol not supported.
CM00051-Institution ID required.
CM00052-Invalid Institution Data Encryption Key Name.
CM00053-Missing Institution Data Encryption Key.
CM00054-Institution Data Encryption Key does not exist.
CM00055-Missing Institution Data Encryption Key.
CM00056-Institution Data Encryption Key does not exist.
CM90000-Database error.
CM90001-Database configuration error.
CM90002-Data format error.
CM90003-No Records Found.
CM90004-Duplicate found error.
CM90005-TimeStamp Mismatch error.
CM90100-Message formatter class failure.

PY20000-Missing required data.
PY20001-Invalid Action Type.
PY20002-Invalid amount.
PY20003-Invalid Order Status.
PY20004-Non Numeric Card Number.
PY20005-Missing Card Number.
PY20006-Invalid Brand.
PY20007-Invalid Order Status.
PY20008-Invalid Currency Code.
PY20009-Transaction Not Found.
PY20010-Invalid Merchant URL.
PY20011-Invalid Merchant Error URL.
PY20012-Invalid Track ID.
PY20013-Invalid Language Code.
PY20014-Invalid User Defined Field.

PY20019-Invalid Transaction ID.

PY20080-Invalid Payment Page Style File.

PY20081-Invalid Payment Page Header File.

PY20082-Invalid Payment Page Footer File.

PY20050-Card Number Encryption Failure.

ERROR 3-D Secure

GV00001-Unknown VPAS version

GV00002-Cardholder not enrolled

GV00003-Not a VPAS Card

GV00004-PARes status not successful

GV00005-Certificate chain validation failed

GV00006-Certificate chain validation error

GV00007-Signature validation failed

GV00008-Signature validation error

GV00009-Invalid root certificate

GV00010-Missing data type

GV00011-Invalid expiration date

GV00012-Invalid action type

GV00013-Invalid Payment ID

ERROR plug-in 3-D Secure

GV00100-Invalid action type

GV00101-Missing data type

GV00102-Invalid Amount

GV00103-Invalid Brand

GV00104-Payment ID not numeric

PRILOGA: CERTIFICATION AUTHORITIES

Web strani zaščitene z SSL certifikatom, morajo uporabljati certifikate izdane s strani »Certification Authority«. V nasprotnem primeru, mora trgovec posredovati dokaz o »Certification Authority«, ki garantira verodostojnost njegovega certifikata.

Verisign Root CA

Creation date: Wed Feb 04 17:49:20 CET 2004
Owner: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Serial number: 2ad667e4e45fe5e576f3c98195eddc0
Valid from: Wed Nov 09 01:00:00 CET 1994 until: Fri Jan 08 00:59:59 CET 2010
Certificate fingerprints:
MD5: 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
SHA1: 44:63:C5:31:D7:CC:C1:00:67:94:61:2B:B6:56:D3:BF:82:57:84:6F

Verisign Root CA

Creation date: Tue Feb 03 10:01:08 CET 2004
Owner: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Serial number: 70bae41d10d92934b638ca7b03ccbaf
Valid from: Mon Jan 29 01:00:00 CET 1996 until: Wed Aug 02 01:59:59 CEST 2028
Certificate fingerprints:
MD5: 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
SHA1: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

Verisign Intermediate CA

Creation date: Tue Feb 03 10:25:45 CET 2004
Owner: OU=www.verisign.com/CPS Incorpor.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSign International Server CA - Class 3, OU="VeriSign, Inc.", O=VeriSign Trust Network
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Serial number: 78ee48de185b2071c9c9c3b51d7bddc1
Valid from: Thu Apr 17 02:00:00 CEST 1997 until: Tue Oct 25 01:59:59 CEST 2011
Certificate fingerprints:
MD5: 81:C8:88:53:0A:FC:AD:91:6F:BE:71:D9:41:7B:F1:0C
SHA1: DE:0F:3A:63:CA:D1:38:41:E9:B6:2C:94:50:2C:B1:89:D7:66:1E:49

Thawte

Creation date: Tue Feb 03 09:13:17 CET 2004
Owner: EmailAddress=server-certs@thawte.com, CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
Issuer: EmailAddress=server-certs@thawte.com, CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
Serial number: 1
Valid from: Thu Aug 01 02:00:00 CEST 1996 until: Fri Jan 01 00:59:59 CET 2021
Certificate fingerprints:
MD5: C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
SHA1: 23:E5:94:94:51:95:F2:41:48:03:B4:D5:64:D2:A3:A3:F5:D8:8B:8C

Equifax

Creation date: Tue Jan 27 13:21:15 CET 2004
Owner: OU=Equifax Secure Certificate Authority, O=Equifax, C=US
Issuer: OU=Equifax Secure Certificate Authority, O=Equifax, C=US

Serial number: 35def4cf
Valid from: Sat Aug 22 18:41:51 CEST 1998 until: Wed Aug 22 18:41:51 CEST 2018
Certificate fingerprints:
MD5: 67:CB:9D:C0:13:24:8A:82:9B:B2:17:1E:D1:1B:EC:D4
SHA1: D2:32:09:AD:23:D3:14:23:21:74:E4:0D:7F:9D:62:13:97:86:63:3A

Infocamere CA

Creation date: Tue Feb 03 09:18:16 CET 2004
Owner: CN=InfoCamere Servizi di Certificazione, OU=Ente Certificatore del Sistema Camerale,
O=InfoCamere SCpA, C=IT
Issuer: CN=InfoCamere Servizi di Certificazione, OU=Ente Certificatore del Sistema Camerale,
O=InfoCamere SCpA, C=IT
Serial number: 1c
Valid from: Tue Jan 16 10:17:00 CET 2001 until: Mon Jan 17 00:59:00 CET 2011
Certificate fingerprints:
MD5: 8C:0A:E8:00:D8:22:3C:38:DF:33:CC:B9:7B:7E:A0:A1
SHA1: DC:58:3E:76:06:46:BC:5C:CD:2B:8A:28:CF:7A:87:13:38:03:8B:C9