TATRA BANKA
Member of Raiffeisen Bank International

TECHNICKÁ PRÍRUČKA K SLUŽBE CARDPAY

Verzia: 1.5

Email: tpay@tatrabanka.sk, Tel.: 02/5919 3435

1 Úvod

Účelom dokumentu je popísať komunikáciu medzi webovým serverom obchodníka a platobným portálom banky. Slúži ako technická príručka ku službe CardPay a obsahuje návod ako sa korektne pripojiť a komunikovať s platobným portálom banky.
Nie je určený ako návod na vytváranie web stránok, ale popisuje, aké podmienky musí stránka internetového obchodu spĺňať na správnu komunikáciu s bankovým serverom.

2 Realizácia platby

2.1 Služba CardPay umožňuje realizáciu platieb prostredníctvom transakcie typu „predaj“ a transakcie typu „predautorizácia“.

PREDAJ je typ transakcie, prostredníctvom ktorej dochádza k automatickému zúčtovaniu prostriedkov z bežného/kartového účtu držiteľa karty v sume, ktorá bola v rámci CardPay platby autorizovaná.

PREDAUTORIZÁCIA je typ transakcie, prostredníctvom ktorej banka držiteľa karty overí prostriedky na karte/účte držiteľa karty a požadovanú sumu na karte/účte zaholduje.
Prostriedky sú na účte/karte zadržané niekoľko dní v závislosti od pravidiel vydavateľskej banky. Transakcia je zúčtovaná a pripísaná na účet obchodníka až po ukončení platby zo strany obchodníka (napr. po overení dostupnosti tovaru resp. dostupnosti poskytnutia služby).

Transakcia typu „predaj“ je štandardný typ transakcie pre realizáciu CardPay platieb.
Transakciu typu „predautorizácia“ odporúčame využívať v prípade predpokladu zvýšeného počtu žiadostí o storno resp. čiastočné storno platieb z dôvodu nedostupnosti tovaru/služby, zmeny ceny objednávky a pod.

2.2 Klient obchodníka (ďalej len klient) po nákupe tovaru a jeho uložení do Nákupného košíka, klikne na stránke obchodníka na symbol platby CardPay.

URL linka CardPay od obchodníka bude smerovať na server Tatra banky a.s. Presmerovanie na portál nie je možné prostredníctvom iframe.

2.3 Na platobnom portáli si klient zadá údaje zo svojej platobnej karty (číslo + expirácia + CV kód).
V prípade, pokiaľ ide o predautorizáciu, klient je o tomto type transakcie informovaný priamo na platobnom portáli.

2.4 Banka zabezpečí, aby klient nemohol pri platbe meniť preddefinované položky:
a) účet prijímateľa (obchodníka)
b) suma
c) mena
d) variabilný symbol

2.5 Banka zobrazí klientovi informáciu o výsledku spracovania platby:
- Vaša platba prebehla úspešne.
- Vaša platba nebola spracovaná.

2.6 Banka následne presmeruje klienta späť na stránku obchodníka aj s návratovou hodnotou a následnou notifikáciou prostredníctvom email alebo SMS (ak boli zadané).

2.7 V prípade realizácie platby formou predautorizácie je obchodník povinný do 14 dní odo dňa, kedy bola predautorizácia vykonaná, zabezpečiť prostredníctvom webového rozhrania poskytnutého bankou ukončenie/storno predautorizácie.

3 Technické parametre

Bezpečnostný kľúč – bezpečnostný kľúč s popisom parametrov a algoritmami šifrovania SHA1 a AES256 obdrží obchodník po podpise Zmluvy o prevádzkovaní služby CardPay od banky. Bezpečnostný kľúč je dôverný údaj a nesmie sa zasielať nezabezpečeným komunikačným kanálom (napríklad emailom pri žiadosti o otestovanie implementácie).

Stránka obchodníka posiela na server banky prostredníctvom klienta (cez redirect) nasledujúce parametre.

Parameter	Typ	Názov	Povinný	Popis	Počet znakov	Pravidlá	Príklad
PT	string	Typ platby	nie	Identifikátor služby	8	Môže obsahovať iba hodnotu „CardPay“	CardPay
MID	integer	Identifikácia obchodníka	áno	Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč, určený na zabezpečenie správ.	3 - 4	-	123
AMT	float	Suma	áno	Suma, ktorú klient prevádza na obchodníkov účet. Desatinná časť je oddelená bodkou.	9+2	Max.2 desatinné miesta – oddelené vždy bodkou.	12345.50
CURR	integer	Mena	áno	Mena v ktorej bude transakcia vykonaná.	3	Môže nadobudnúť hodnoty: 978 – EUR 203 – CZK 840 – USD 826 – GBP 348 – HUF 985 - PLN 756 – CHF 208 - DKK	978
VS	string	Variabilný symbol	áno	Jednoznačný identifikátor platby	max. 10	Môže obsahovať iba číslice 0-9.	1234567890
RURL	string	Návratová URL	áno	Návratová URL adresa na ktorú banka presmeruje klienta po vykonaní platby.	max. 256	URL musí byť vytvorená v súlade s RFC 1738 a adresa zadaná v RURL po presmerovaní musí byť funkčná.	http://www.tatra-banka.sk
IPC	string	IP adresa klienta	áno	Ak nie je k dispozícii, tak IP adresa proxy servera.		-	1.1.1.1
NAME	string	Meno klienta	áno	Meno klienta z objednávkového formulára zo stránky obchodníka.	max. 30	Meno nesmie obsahovať diakritiku. Povolené znaky: 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @	Peter Novak
SIGN	string	Bezpečnostný podpis	áno	Bezpečnostný podpis vygenerovaný na strane obchodníka.	32	Môže obsahovať iba veľké písmená a čísla (A-Z, 0-9).	29C371F0B4F5A46529C371F0B4F5A465
RSMS	string	Telefónne číslo	nie	Telefónne číslo pre zaslanie notifikácie obchodníkovi o výsledku platby vo forme SMS.	max. 15	Telefónne číslo musí byť v jednom z tvarov: 9XXNNNNNN 09XXNNNNNN +4219XXNNNNN 004219XXNNNN Môže obsahovať iba jedno telefónne číslo.	0901234567

REM	string	Emailová adresa	nie	Emailová adresa pre zaslanie notifikácie obchodníkovi o výsledku platby vo forme e-mailu.	max. 35	Email musí obsahovať jeden @,minimálne 6 znakov. Pred aj za @ musí byť aspoň jeden znak. Za @ musí byť aspoň jeden znak bodka, ktorý nesmie byť hneď za @ ani na konci e-mailovej adresy. Nesmú byť uvedené dve a viac bodiek za sebou. Posledne slovo (za poslednou bodkou) musi byt zo zoznamu TLD. Môže obsahovať iba jednu e-mailovú adresu (ktorá je v súlade s RFC 2822)	novak@domena.sk
DESC	string	Popis	nie	Popis platby. Je určený pre lepšiu identifikáciu platby.	max. 20	Môže obsahovať iba znaky 0-9, A-Z, a-z, ., -, _, @ a medzeru. Nesmie obsahovať diakritiku.	Platba_za_knihy
AREDIR	integer	Príznak automatického presmerovania	nie	Príznak pre automatické presmerovanie na stránku obchodníka (RURL) po uplynutí časového intervalu.	1	Môže obsahovať hodnotu 1 alebo 0: 0 – manuálne presmerovanie po kliknutí na „Pokračovať 1 – automatické presmerovanie po 9-tich sekundách	1 0
LANG	string	Identifikácia jazyka	nie	Umožňuje nastavenie jazykovej mutácie CardPay.	2	Môže obsahovať hodnoty: sk – východzia hodnota en – anglický jazyk de – nemecký jazyk hu – maďarský jazyk cz – český jazyk es – španielsky jazyk fr –francúzsky jazyk it – taliansky jazyk pl – poľský jazyk	sk en de hu cz es fr it pl
TXN	string	Typ transakcie	nie	Typ transakcie predautorizácia.	-	Môže obsahovať iba hodnotu PA	PA
MOBILE_ DEVICE	string	Verzia pre mobilné zariadenia	nie	Zobrazenie CardPay portálu v optimalizovanej verzii pre rozhranie mobilných telefónov	1	Môže obsahovať hodnoty: 0 – CardPay portál v štandardnom zobrazení pre PC rozhranie 1 – CardPay portál optimalizovaný pre rozhranie mobilných zariadení	1 0

4 Bezpečnostný podpis

4.1 Pre každého obchodníka banka vygeneruje 32 bajtový bezpečnostný kľúč.

4.2 Pred komunikáciou sa zostaví bezpečnostný podpis nasledujúcim spôsobom:
a) vytvorí sa reťazec tak, že sa zreťazia všetky podpisom chránené parametre v definovanom poradí (viď nižšie),
b) z uvedeného reťazca sa vytvorí HASH algoritmom SHA1,
c) z vytvoreného HASHu sa vezme prvých 16 bajtov a zašifruje sa algoritmom AES256 pomocou vygenerovaného bezpečnostného kľúča,
d) vznikne 16 bajtový bezpečnostný podpis, ktorý sa konvertuje do 32 bajtového reťazca, ktorý reprezentuje jeho zápis v hexadecimálnej sústave.

4.3 Bezpečnostný podpis sa zadáva do požiadavky obchodníka resp. odpovede z banky ako hodnota parametra SIGN.

4.4 Banka alebo obchodník po prijatí správy vytvorí z prijatých parametrov, rovnakým spôsobom, kontrolný bezpečnostný podpis a porovná ho s hodnotou parametru SIGN.

4.5 Správa je platná len v prípade rovnosti bezpečnostných podpisov.

Reťazec pre bezpečnostný podpis požiadavky obchodníka:
1. MID
2. AMT
3. CURR
4. VS
5. RURL
6. IPC
7. NAME

Reťazec pre bezpečnostný podpis odpovede z banky
1. VS
2. RES
3. AC (approval code - je generovaný iba v prípade úspešnej transakcie)

Pre kontrolu správnosti generovania bezpečnostného podpisu môžete použiť testovaciu konzolu:
https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/example.jsp

5 Protokol platieb

5.1 Formát požiadavky obchodníka na realizáciu platby

Protokol platieb vyžaduje zaslanie zadefinovaných parametrov.
Web stránka obchodníka zabezpečí odovzdanie parametrov platby serveru banky. Parametre budú prenášané HTTPS dopytom metódou POST (alebo GET). Kódované budú vo forme application/x-www-form-urlencoded – t.j. ako výsledok odoslania bežného HTML formulára. Integrita prenášaných údajov je zaistená ich podpísaním. Server banky overí obdržané parametre platby a následne odošle obchodníkovi odpoveď o výsledku vykonanej platby vo forme zakódovaného reťazca.
URL servra banky je: **https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp**

a) príklad požiadavky obchodníka:
https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp?PT=CardPay&MID=9999&AMT=1234.50&CURR=978&VS=2812&-RURL=http://www.shoppingzona.sk&IPC=111.111.111.111&NAME=NOVAK&SIGN=29C371F0B4F5A46529C371F0B4F5A465
Pozn.: Uvedený formát je ilustračný

b) príklad požiadavky obchodníka v prípade realizácie predautorizácie
https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp?PT=CardPay&MID=9999&AMT=1234.50&CURR=978&VS=2812&-RURL=http://www.shoppingzona.sk&IPC=111.111.111.111&NAME=NOVAK&TXN=PA&SIGN=29C371F0B4F5A46529C371F0B4F5A465
Pozn.: Uvedený formát je ilustračný

5.2 Odpoveď z banky

Odpoveď z banky obchodníkovi o výsledku platby je zasielaná:
a) cez **URL** – presmerovaním klienta na RURL obchodníka a zaslaním parametrov odpovede z banky
b) vo forme **SMS** – zaslaním notifikačnej správy na telefónne číslo z parametra RSMS, pokiaľ bol vyplnený platnou hodnotou
c) vo forme **e-mailu** - zaslaním notifikačného emailu na email z parametra REM, pokiaľ bol vyplnený platnou hodnotou

Parametre odpovede z banky

Výsledok platby je reprezentovaný hodnotou parametra RES, ktorý môže nadobúdať hodnoty:

Hodnota	Popis
OK	Platba prebehla úspešne.
FAIL	Platba (napr. za objednaný tovar resp. služby) nebola úspešná.

Parametre odpovede:
- VS - variabilný symbol z požiadavky obchodníka
- RES - výsledok platby
- AC - approval code (v odpovedi je posielaný iba v prípade úspešnej transakcie)
- SIGN -bezpečnostný podpis parametrov odpovede z banky

URL formát	https://{parameter RURL}?VS={parameter VS}&RES={parameter RES}& AC={parameter AC}&SIGN={bezp. podpis}
Formát SMS	TBEC VS={parameter VS} RES={parameter RES} VS} AC={parameter AC} SIGN={bezp. podpis}
Formát e-mail	VS={parameter VS} RES={parameter RES} VS} AC={parameter AC} SIGN={bezp. podpis}

V prípade, že hodnota parametra SIGN v odpovedi z banky (zaslaná prostredníctvom URL, e-mail alebo SMS) sa nezhoduje s vypočítanou hodnotou na strane obchodníka, platba je vyhodnotená ako podozrivá a obchodník je povinný kontaktovať banku za účelom preverenia výsledku platby.

5.3 Ukončenie/storno predautorizácie

Na ukončenie/ storno predautorizácie je potrebné použiť webové zozhranie, obchodníkovi dostupné prostredníctvom HTTPS požiadaviek na adrese: https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/txn_process.jsp

Parametre sú prenášané metódou POST (alebo GET). Odpovede na požiadavku sa doručujú cez XML dokumenty.
Komunikácia obchodníka s bankou je šifrovaná protokolom SSL.

Obchodník posiela na ukončenie/storno predautorizácie nasledujúce parametre.

Parameter	Typ	Názov	Povinný	Popis	Počet znakov	Pravidlá	Príklad
MID	integer	Identifikácia obchodníka	áno	Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč, určený na zabezpečenie správ.	3 - 4	-	1234
TXN	string	Transaction type	áno	Typ transakcie ukončenie predautorizácie, resp. storno predautorizácie	-	Môže nadobúdať hodnotu CPA – ukončenie predautorizácie SPA – storno predautorizácie	CPA/ SPA
AMT	float	Suma	áno	Suma, ktorú klient prevádza na obchodníkov účet. Desatinná časť je oddelená bodkou.	9+2	Max.2 desatinné miesta – oddelené vždy bodkou. Pri ukončení predautorizácie (CPA), hodnota môže byť rovnaká resp. nižšia ako suma predautorizácie. V prípade storna (SPA) sa pole AMT necháva prázdne.	12345.50
VS	string	Variabilný symbol	áno	Jednoznačný identifikátor platby	max. 10	Môže byť len číselný údaj bez možnosti zadania iných znakov. Variabilný symbol transakcie pre predautorizáciu a ukončenie/storno predautorizácie musia byť identické. VS sa nesmie opakovať vrámci jedného obchodnika.	1234567890
FORMAT	string	Formát	áno	Formát výstupu XML alebo TEXT	-	XML je defaultný formát; pre generovanie výstupu vo forme textovej reprezentácie sa nastavuje content-type: text/plain, obsah: txn=|mid=|vs=|res=|sign=	-
SIGN	string	Bezpečnostný podpis	áno	Bezpečnostný podpis vygenerovaný na strane obchodníka	32	Je generovaný zakódovaním reťazca podľa typu požiadavky: SIGN = TXN (CPA/SPA) + MID + VS Podpis musí byť vygenerovaný na základe algoritmu DES alebo AES-256, podľa nastavenia šifrovania obchodníka. Písmená musia byť veľkým písmom	29C371F0B4F5A46529C371F0B4F5A465

RSMS	string	Telefónne číslo	nie	Telefónne číslo pre zaslanie notifikácie obchodníkovi o výsledku platby vo forme SMS.	Max. 15 Max. 35	Telefónne číslo musí byť v jednom z tvarov: 9XXNNNNNN 09XXNNNNNN +4219XXNNNNNN 004219XXNNNNNN Môže obsahovať iba jedno telefónne číslo.	0901234567
REM	string	Emailová adresa	nie	Emailová adresa pre zaslanie notifikácie obchodníkovi o výsledku platby vo forme e-mailu.		Email musí obsahovať jeden @,minimálne 6 znakov. Pred aj za @ musí byť aspoň jeden znak. Za @ musí byť aspoň jeden znak bodka, ktorý nesmie byť hneď za @ ani na konci e-mailovej adresy. Nesmú byť uvedené dve a viac bodiek za sebou. Posledne slovo (za poslednou bodkou) musi byt zo zoznamu TLD. Môže obsahovať iba jednu e-mailovú adresu (ktorá je v súlade s RFC 2822)	novak@domena.sk

Príklad požiadavky obchodníka:
https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/txn_process.jsp?TXN=CPA&MID=011&AMT=500&VS=1234567890&-SIGN=29C371F0B4F5A46529C371F0B4F5A465

5.4 Odpoveď z banky obchodníkovi

Odpoveď z banky na ukončenie/ storno predautorizácie je realizovaná vo forme XML dokumentu, ktorý môže obsahovať nasledujúce elementy:

Názov elementu	Popis
cardpay	root element dokumentu, musí obsahovať jeden element request a jeden element result alebo error
request	parametre požiadavky, obsahuje elementy txn, mid, vs
txn	typ požadovanej transakcie poslaný v požiadavke
mid	MID obchodníka poslaný v požiadavke
vs	variabilný symbol poslaný v požiadavke
result	odpoveď na požiadavku, musí obsahovať jeden element res a element sign
res	výsledok operácie, môže nadobudnúť OK, FAIL
sign	podpis výstupu
error	odpoveď na požiadavku v prípade chyby, obsahuje element code a reason
code	číselný kód chyby
reason	popis chyby

Príklady odpovede:

```
<?xml version="1.0" encoding="windows-1250"?>
<cardpay>
 <request>
  <txn>CPA</txn>
  <mid>011</mid>
  <vs>1234567890</vs>
 </request>
 <result>
  <res>OK</res>
  <sign>29C371F0B4F5A46529C371F0B4F5A465</sign>
 </result>
</cardpay>
```

Chyba pri spracovávaní:

```
<?xml version="1.0" encoding="windows-1250"?>
<cardpay>
 <request>
  <txn>CPA</txn>
  <mid>011a</mid>
  <vs>1234567890</vs>
 </request>
 <error>
  <code>12</code>
  <reason>Invalid MID</reason>
 </error>
</cardpay>
```

Príklad odpovede vo formáte TXT:

txn=CPA|mid=3165|vs=1111|res=FAIL|error_code=13|error_reason=Processingfail|sign=29C371F0B4F5A46529C371F0B4F5A465

5.5 Chybové stavy vo výstupe:

Číslo chyby	Popis	Poznámka
1	MID fail	chybný identifikátor MID
2	Amount fail	chyba pri formáte sumy
3	Amount fail	suma nie je číselná hodnota
4	VS fail	VS nie je číslo, resp. nie je vyplnené
5	Operation not allowed	obchodník nemá povolené vykonávať operáciu
6	AES fail	nesprávny formát podpisu
7	DES fail	nesprávny formát podpisu
8	Unknown error	
9	Txn fail	nepodporovaná operácia
10	Bad signature	Nesprávny podpis
11	Missing or unknown parameter	chýba niektorý povinný parameter
12	Invalid MID	obchodník nie je registrovaný v systéme, alebo je v stave OFFLINE
13	Processing fail	

5.6 Skrytie protokolu pred užívateľmi

Na CardPay stránkach doporučujeme hore uvedené parametre zadávať ako INPUT polia typu HIDDEN. Pre formulár sa doporučuje nastaviť parameter METHOD na hodnotu POST. V prípade že ju daný web server nepodporuje môže sa použiť hodnota GET.

Časť obchodníckej stránky so skrytými parametrami bude vyzerať nasledovne :

```
<FORM name="meno_formu" action="https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp" METHOD=POST>
<INPUT TYPE="HIDDEN" name="PT" value="CardPay">
<INPUT TYPE="HIDDEN" name="MID" value="123">
<INPUT TYPE="HIDDEN" name="AMT" value="12345.60">....
```