TECHNICKÁ PRÍRUČKA K SLUŽBE CARDPAY

Verzia: <1.3>

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 transakcie 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 transakcie 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.

2.3 URL linka CardPay od obchodníka bude smerovať na platobný portál Tatra banky a.s. Presmerovanie na portál nie je možné prostredníctvom iframe a musí sa vždy zobrazovať v novom okne, ktoré musí obsahovať viditeľnú adresu portálu banky (https://moja.tatrabanka.sk).

2.4 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.

2.5 Banka zabezpečí, aby klient nemohol pri platbe meniť preddefinované položky:

a) účet prijímateľa (obchodníka)
b) suma
c) mena
d) variabilný symbol
e) konštantný symbol

2.6 Klient následne potvrdí alebo zruší platbu.

2.7 Úspešnú realizáciu platby banka oznámi informačným oknom na obrazovku klienta.

2.8 Banka následne presmeruje klienta späť na stránku obchodníka.

2.9 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 DES obdrží obchodník po podpise Zmluvy o prevádzkovaní služby CardPay od banky. Bezpečnostný kľúč je dôverný údaj a nesmie sa zasielať nezabezpečeným komunikačným kanálom (napríklad pri žiadosti o otestovanie implementácie).

Stránka obchodníka posiela na platobný portál banky nasledujúce parametre.
** Povinné parametre*
***Paramter TXN je vyplnený iba v prípade, že CardPay transakcie budú realizované formou predautorizácie*

Parameter	Názov	Popis	Počet znakov	Pravidlá	Príklad
PT	Payment Type	Identifikátor služby	-	Môže nadobúdať iba hodnotu „CardPay“	CardPay
MID*	Merchant Identification	Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč, určený na zabezpečenie správ.	3 - 4	-	123
AMT*	Amount	Suma, ktorú klient prevádza na obchodníkov účet. Desatinná časť je oddelená bodkou.	13+2	Max.2 desatinné miesta – oddelené vždy bodkou.	12345.50
CURR*	Currency	Mena v ktorej bude transakcia vykonaná. Kód pre EUR je 978.	3	-	978
VS*	Variabilný symbol	Jednoznačný identifikátor platby	max. 10	Môže byť len číselný údaj bez možnosti zadania iných znakov	1234567890
RURL*	Return URL	Návratová URL adresa na ktorú banka presmeruje klienta po vykonaní úhrady	-	• reťazec URL nesmie byť zvýraznený boldom • nesmie ísť o premennú • nesmie obsahovať tzv. query string znaky • stránka zadaná v RURL musí byť funkčná	http://www.tatrabanka.sk
IPC*	IP adresa klienta	Ak nie je k dispozícii, tak IP adresa proxy servera.		-	1.1.1.1
NAME*	Meno klienta	Meno klienta	max. 30	Meno nesmie obsahovať diakritiku. Povolené znaky: 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @	Peter Novak
SIGN*	Bezpečnostný podpis	Parameter obsahuje bezpečnostný podpis vygenerovaný na strane obchodníka	16	Písmená musia byt veľkým písmom	A6BC1DE2F G4H8484
RSMS	Return Short Message System	Notifikácia pre obchodníka o realizácii platby vo forme SMS.	15	Zadané MT číslo musí byť v tvare: 9XX NNN NNN 09XX NNN NNN +4219XX NNN NNN	0901234567
REM	Return e-mail	Notifikácia pre obchodníka o realizácii platby vo forme e-mailu.	35	• e-mail musí obsahovať jeden @ • minimálne 6 znakov • pred aj za @ musí byť aspoň jeden znak • bodka nesmie byť hneď za @ ani na konci e-mailovej adresy v doménovej časti • nesmú byť uvedené dve a viac bodiek za sebou	novak@domena.sk

DESC	Description	Popis platby. Je určený pre lepšiu identifikáciu platby.	max. 20	V popise nesmie byť diakritika.	Platba_za_knihy
AREDIR	Automatický redirect	Umožňuje automatické presmerovanie zákazníka na stránku obchodníka (RURL).	1	0 – manuálne presmerovanie po kliknutí na „Pokračovať 1 – automatické presmerovanie po 9-tich sekundách	1 0
LANG	Identifikácia jazyka	Umožňuje presmerovanie zákazníka na platobný portál v želanej jazykovej mutácii.	2	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**	Transaction type	Typ transakcie predautorizácia	-	Môže nadobúdať iba hodnotu PA	PA
MOBILE_DEVICE	Verzia pre mobilné zariadenia	Zobrazenie CardPay portálu v optimalizovanej verzii pre rozhranie mobilných telefónov	1	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 sa vygeneruje 8 bajtový bezpečnostný kľúč (napr. ABCDEFGH).

4.2 Pred komunikáciou sa zostaví bezpečnostný podpis nasledujúcim spôsobom:

a) vytvorí sa reťazec tak, že sa zreťazia všetky podpisom chránené parametre (v uvedenom poradí): pre správu od obchodníka banke sú podpisom chránené parametre: MID, AMT, CURR, VS, RURL, IPC, NAME; pre správu banky pre obchodníka sú podpisom chránené parametre: VS, RES, AC (je generovaný len v prípade úspešnej transakcie),
b) z uvedeného reťazca sa vytvorí HASH algoritmom SHA1,
c) z vytvoreného HASHu sa vezme prvých 8 bajtov a zašifruje sa algoritmom DES pomocou vygenerovaného bezpečnostného kľúča,
d) vznikne 8 bajtový bezpečnostný podpis, ktorý sa konvertuje do 16 bajtového stringu, ktorý reprezentuje jeho zápis v hexadecimálnej sústave.

4.3 Bezpečnostný podpis sa zadáva do správy ako hodnota parametra SIGN

4.4 Banka po prijatí správy vytvorí z tých istých parametrov rovnakým spôsobom kontrolný bezpečnostný podpis a porovná sa s hodnotou parametru SIGN.

4.5 Platba sa zrealizuje len v prípade rovnosti bezpečnostných podpisov.

Pre kontrolu správnosti generovania SIGNu môžete použiť testovaciu konzolu:

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/example.jsp

5 Protokol platieb (cez HTTPS)

5.1 Formát požiadavky obchodníka na realizáciu platby

Protokol platieb (cez HTTPS) vyžaduje presun zadefinovaných parametrov.
Web stránka obchodníka zabezpečí odovzdanie parametrov platby platobnému portálu 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. Platobný portál

banky overí obdržané parametre platby a následne odošle obchodníkovi notifikačnú správu o úspešnosti vykonanej transakcie vo forme zakódovaného reťazca.

URL internet bankingového servra banky je**: https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp**

Očakávané parametre (* sú povinné):

payment_type (PT)

id_obchodníka (MID) *

amount (AMT) *

currency (CURR) *

variable_symbol (VS) * (alebo ID platby)

description (DESC)

return_url (RURL) *

IP_client (IPC) *

name_client (NAME)*

reply_sms (RSMS)

reply_email (REM)

automatic_redirect (AREDIR)

language (LANG)

transaction type (TXN)

mobile_device (MOBILE_DEVICE)

podpis (SIGN) *

a) Formát requestu od obchodníka do banky:

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=4D848C31F8E19026

Pozn.: Uvedený formát je ilustračný

b) Formát requestu od obchodníka do banky v prípade využitia 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=4D848C31F8E19026

Pozn.: Uvedený formát je ilustračný

5.2 Reply z banky obchodníkovi

Odpoveď z banky obchodníkovi o úspešnosti prijatia transakcie je možné zaslať vo formáte:

a) URL
b) SMS - nepovinné
c) e-mail - nepovinné

Požadované parametre:

a) variable_symbol (VS) (alebo ID platby)
b) result (RES)
c) approval_code (AC) (je generovaný iba v prípade úspešnej transakcie)
d) podpis (SIGN)*

URL formát	https://URL_OBCHODNIKA?VS=4325&RES=OK&AC=YYYYYY&SIGN=XXXXXXXX

Formát SMS	TBEC VS=4325 RES=OK AC=YYYYYY SIGN=XXXXXXXXX
Formát e-mail	VS=4325 RES=OK AC=YYYYYY SIGN=XXXXXXXXX

*V prípade, že hodnota parametra SIGN v odpovedi z banky (zaslaná prostredníctvom URL/e-mail/SMS) sa nezhoduje s hodnotou, ktorá je vypočítaná v parametri SIGN na strane obchodníka, transakcia je vyhodnotená ako podozrivá a obchodník je povinný kontaktovať banku za účelom preverenia výsledku transakcie.

Parameter RES môže nadobúdať hodnoty:

Parameter	**Hodnota**	**Popis**
RES	OK	Transakcia bola korektne spracovaná.
	FAIL	Transakcia nebola korektne spracovaná a teda platba za objednaný tovar, resp. služby sa nezrealizovala.

Pozn.: Zasielanie notifikačných správ na číslo mobilného telefónu alebo na e-mailovú adresu je podmienené vyplnením parametrov RSMS a REM v platobnom reťazci zasielanom od obchoníka do banky.

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. Povinné parametre sú označené hviezdičkou :*

Parameter	**Názov**	**Popis**	**Počet znakov**	**Pravidlá**	**Príklad**
MID*	Merchant Identification	Jedinečné identifikačné číslo obchodníka	3 - 4	-	1234
TXN*	Transaction type	Typ transakcie ukončenie predautorizácie, resp. storno predautorizácie	-	Môže nadobúdať hodnotu CPA – ukončenie predautorizácie SPA – storno predautorizácie	CPA/ SPA
AMT*	Amount	Suma, na ktorú bude predautorizácia/ storno preadautorizácie ukončené	13+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*	Variabilný symbol	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	1234567890

				identické. VS sa nesmie opakovať vrámci jedného obchodnika.	
FORMAT*	Formát	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*	Bezpečnostný podpis	Parameter obsahuje bezpečnostný podpis vygenerovaný na strane obchodníka	16	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 byt veľkým písmom	A6BC1DE2F G4H8484
RSMS	Return Short Message System	Notifikácia pre obchodníka o realizácii platby vo forme SMS.	15	Zadané MT číslo musí byť v tvare: 9XX NNN NNN 09XX NNN NNN +4219XX NNN NNN	0901234567
REM	Return e-mail	Notifikácia pre obchodníka o realizácii platby vo forme e-mailu.	35	• e-mail musí obsahovať jeden @ • minimálne 6 znakov • pred aj za @ musí byť aspoň jeden znak • bodka nesmie byť hneď za @ ani na konci e-mailovej adresy v doménovej časti • nesmú byť uvedené dve a viac bodiek za sebou	novak@dome na.sk

Príklad requestu od obchodníka do banky má formát:

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/txn_process.jsp?TXN=CPA&MID=011&AMT=500&VS=1234567890&SIGN=84972F5DB04F2A6E

5.4 Reply 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>474C37240DE4E4E8</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 textu:
txn=CPA|mid=3165|vs=1111|res=FAIL|error_code=13|error_reason=Processing fail|sign=9BAF425A7CE4917D

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">....