TECHNICKÁ PRÍRUČKA K SLUŽBE CARDPAY

Verzia: <3.1>

Email: tpay@tatrabanka.sk
Tel.: 02/5919 1516

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

2.2 URL linka CardPay od obchodníka bude smerovať na platobný portál Tatra banky a.s.

2.3 Na platobnom portáli si klient zadá údaje zo svojej platobnej karty (číslo + expirácia + CV kód).

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

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

2.5 Klient následne potvrdí alebo zruší platbu.

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

2.7 Banka následne presmeruje klienta späť na stránku obchodníka.

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 sú označené hviezdičkou :*

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 SKK je 703.	3	-	703
VS*	Variabilný symbol	Jednoznačný identifikátor platby	max. 10	Môže byť len číselný údaj bez možnosti zadania iných znakov	1234567890
CS*	Konštantný symbol	Konštantný symbol pre CardPay nadobúda hodnotu 0558	max. 4	Môže byť len číselný údaj	0558
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 musí byť očistené od diakritiky	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	sk en de hu

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, CS, 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 HTTP)

5.1 Formát požiadavky obchodníka na realizáciu platby

Protokol platieb (cez HTTP) 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)
constant_symbol (CS) *
description (DESC)
return_url (RURL) *
IP_client (IPC) *
name_client (NAME)*
reply_sms (RSMS)
reply_email (REM)
automatic_redirect (AREDIR)
language (LANG)
podpis (SIGN) *

Request od obchodníka do banky má formát:

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp?PT=CardPay&MID=9999&AMT=1234.50&CURR=703&VS=2812&CS=0558&RURL=novak@domena.sk&IPC=207.142.131.205&NAME=NOVAK&SIGN=C845C4A58458DDCE

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

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 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">....