



TECHNICKÁ PRÍRUČKA K SLUŽBE TATRAPAY

Verzia: <3.2>

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

1	Úvod	3
2	Realizácia platby	3
3	Technické parametre	4
4	Bezpečnostný podpis	5
5	Protokol platieb (cez HTTP)	5
6	Získanie aktuálneho stavu dostupnosti služby „Domáci prevodný príkaz“ v aplikácii TatraPay -nepovinné	7
7	Chybové stavy	8

1 Úvod

Služba TatraPay je platobný nástroj v internetovom prostredí využívaný obchodníkmi na príjem platieb za poskytnutý tovar alebo služby. Účelom dokumentu je poskytnúť návod ako vytvoriť správne fungujúce a bezpečné prepojenie medzi Internet bankingovým serverom banky a serverom obchodníka a popísať priebeh komunikácie medzi nimi.

Nie je určený ako návod na vytváranie web stránok, ale popisuje, aké podmienky musí stránka internetového obchodu spĺňať pre 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 TatraPay.
- 2.2 URL linka TatraPay od obchodníka bude smerovať na Internet bankingový server Tatra banky a.s. Presmerovanie na Internet bankingový server nie je možné cez iframe a musí sa vždy zobrazovať v novom okne, ktoré musí obsahovať viditeľnú adresu portálu banky (<https://moja.tatrabanka.sk>).
- 2.3 Na Internet bankingovom servri sa klient prihlási identifikačnými znakmi Tatra banky do TatraPay aplikácie.
- 2.4 Banka ponúkne klientovi na obrazovke preddefinovanú platbu z jeho bežného účtu na účet obchodníka.
- 2.5 Banka zabezpečí, aby klient nemohol pri platbe meniť preddefinované položky a to:
 - a) účet prijímateľa (obchodníka)
 - b) suma
 - c) variabilný symbol
 - d) špecifický symbol
 - e) konštantný symbol
- 2.6 Klient môže zmeniť účet odosielateľa v prípade, že má v banke vedených viac bežných účtov. Tento účet si môže vybrať len zo zoznamu svojich preddefinovaných účtov.
- 2.7 Klient následne potvrdí alebo zruší platbu.
- 2.8 Úspešnú realizáciu platby banka oznámi informačným oknom na obrazovku klienta.
- 2.9 Banka následne presmeruje klienta späť na stránku obchodníka.

3 Technické parametre

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

Stránka obchodníka posielala internet bankingovému serveru banky nasledujúce parametre. *Povinné parametre sú označené hviezdíčkou** :

Parameter	Názov	Popis	Počet znakov	Pravidlá	Príklad
PT	Payment Type	Identifikátor služby	-	Môže nadobúdať iba hodnotu „TatraPay“	TatraPay
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.	1234567890
SS	Špecifický symbol	Jednoznačný identifikátor platby.	max. 10	Môže byť len číselný údaj.	987654321
CS	Konštantný symbol	Konštantný symbol	max. 4	Môže byť len číselný údaj.	0308; 0008
RURL*	Return URL	Návratová URL adresa, na ktorú banka presmeruje klienta po vykonaní úhrady.	-	<ul style="list-style-type: none"> 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.ta trabanka.sk
SIGN*	Bezpečnostný podpis	Parameter obsahuje bezpečnostný podpis vygenerovaný na strane obchodníka	16	Písmená musia byť 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	<ul style="list-style-type: none"> 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@dom na.sk
DESC	Description	Popis platby. Je určený pre lepšiu identifikáciu platby.	max. 20	V popise nesmie byť diakritika.	Platba_za_kni hy
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 internet banking 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 banka 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, SS (ak bol zadany), CS (ak bol zadany), RURL; pre správu banky pre obchodníka sú podpisom chránené parametre: VS, SS (ak bol zadany), RES,
 - 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 ho 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 internet bankingovému 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. Internet bankingový server 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)

specific_symbol (SS)

constant_symbol (CS)

description (DESC)

return_url (RURL) *

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=TatraPay&MID=9999&AMT=1234.50&CURR=978&VS=2812&RURL=http://www.shoppingzona.sk&SIGN=629C371F0B4F5A46`

Pozn.: Uvedený formát je ilustračný

5.2 Reply z banky obchodníkovi

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

- URL
- SMS - nepovinné
- e-mail - nepovinné

Požadované parametre:

- variable_symbol (VS)* (alebo ID platby)
- specific_symbol (SS) (ak bol zadany v requeste od obchodníka)
- result (RES)*
- podpis (SIGN)*

URL formát	<code>https://URL_OBCHODNIKA?VS=4325&RES=OK&SIGN=XXXXXXXXXX</code>
Formát SMS	<code>TBEC VS=4325 RES=OK SIGN=XXXXXXXXXX</code>
Formát e-mail	<code>VS=4325 RES=OK SIGN=XXXXXXXXXX</code>

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.
	TOUT	Transakcia nebola spracovaná a banka nevie jej konečný výsledok. Tento status majú transakcie realizované počas technickej prestávky Internet bankingu banky. Po ukončení technickej prestávky sa transakcia spracuje a jej konečný výsledok dostane prevádzkovateľ virtuálneho obchodu ďalšou notifikačnou správou (formou SMS alebo e-mailom). Výsledok TOUT nie je konečným výsledkom transakcie, a preto ho nie je možné pokladať za určujúci pre vybavenie danej objednávky.

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 obchodníka do banky.

5.3 Skrytie protokolu pred užívateľmi

Na TatraPay stránkach doporučujeme vyššie 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 vyzeráť 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="TatraPay">
```

```
<INPUT TYPE="HIDDEN" name="MID" value="9999">
```

```
<INPUT TYPE="HIDDEN" name="AMT" value="12345.60">....
```

6 Získanie aktuálneho stavu dostupnosti služby „Domáci prevodný príkaz“ v aplikácii TatraPay - nepovinné

V prípade, že obchodník chce byť informovaný, resp. chce informovať kupujúceho o aktuálnej dostupnosti služby TatraPay (či je služba on-line prístupná a neprebieha technická prestávka), môže tak urobiť automatickým dotazovaním sa cez rozhranie dostupné prostredníctvom HTTPS požiadaviek na adrese: <https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/isoffline.jsp>. Parametre sa odovzdávajú cez metódu POST (alebo GET). Odpovede na požiadavku sa doručujú cez XML dokumenty. Komunikácia obchodníka s bankou je šifrovaná protokolom SSL.

6.1 Komunikácia cez webové rozhranie na získanie aktuálneho stavu dostupnosti služieb v aplikácii TatraPay prebieha nasledovne:

- 1) obchodník vygeneruje požiadavku so všetkými požadovanými parametrami
- 2) požiadavku odošle na server banky cez HTTPS protokol
- 3) na serveri banky prebehne kontrola parametrov a bezpečnostného podpisu
- 4) server banky zobrazí odpoveď vo formáte XML

Možné výsledky komunikácie:

- a) V prípade správnych parametrov a podpisu sa zistí a zobrazí aktuálny stav dostupnosti služby.
- b) V prípade chybných parametrov, podpisu alebo údajov obchodníka sa zobrazí kód chyby a chybová správa.
- c) V prípade inej chyby na strane servera sa zobrazí dotazovaná služba v stave offline.

Pozn.: Kontrola bezpečnostného podpisu je popísaná v článku 4 Bezpečnostný kľúč tohto dokumentu.

6.2 Požiadavka na kontrolu dostupnosti služieb musí obsahovať nasledujúce parametre (* Všetky parametre sú povinné):

Parameter	Názov	Popis	Počet znakov	Pravidlá	Príklad
MID*	Merchant Identification	Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč, určený na zabezpečenie správ. MID prideluje obchodníkovi banka	3 - 4	Kontroluje sa voči databáze obchodníkov.	9999
TIMESTAMP*	Čas generovania požiadavky	Musí byť aktuálny čas +/- 1 hodina podľa časovej zóny UTC (GMT), ak je zasielaný čas mimo tohto dvojhodinového intervalu, požiadavka skončí s chybou.	14	Formát: DDMMYYYYHHMISS (DD -deň, MM - mesiac, YYYY - rok, HH - hodina, MI - minúta, SS - sekunda).	14112005124627
SERVICE*	Identifikátor služby	Musí nadobudnúť hodnotu DOMPAYMENT.	10	SERVICE=DOMPAYMENT	DOMPAYMENT
SIGN*	Bezpečnostný podpis	Tvorí sa zakódovaním reťazca: MID+TIMESTAMP+SERVICE	16	Musí byť vygenerovaný na základe algoritmu uvedeného v článku 4 Bezpečnostný kľúč tohto dokumentu.	8EBBB7D488371223

Príklad požiadavky:

<http://tatra.sun.tatrabanka.sk/cgi-bin/e-commerce/start/isoffline.jsp?MID=9999&TIMESTAMP=14112005124627&SERVICE=DOMPAYMENT&SIGN=8EBBB7D488371223>

6.3 Formát odpovede z banky

Odpoveď z banky na požiadavku obchodníka je realizovaná vo forme XML dokumentu. Môže obsahovať nasledujúce elementy:

Názov elementu	Popis
ecommerce	root element dokumentu, musí obsahovať práve jeden element result alebo error
result	odpoveď na požiadavku, musí obsahovať jeden element service a jeden element status
service	názov služby
Status	stav služby, môže nadobudnúť hodnoty offline alebo online
Error	odpoveď v prípade chyby, musí obsahovať jeden element error_code a jeden element error_message
error_code	číselný kód chyby
error_message	chybová správa

Kódovanie odpovede je Windows-1250. Podpis výstupu sa generuje pomocou algoritmu uvedeného v článku 4 Bezpečnostný kľúč z reťazca: MID + TIMESTAMP + SERVICE + STATUS

Príklady odpovede:

Služba je offline:

```
<?xml version="1.0" encoding="windows-1250"?>
<ecommerce>
<request>
<mid>9999</mid>
<timestamp>21122005101827</timestamp>
<service>DOMPAYMENT</service>
</request>
<result>
<status>offline</status>
<sign>2EE78B37AA5AEB3D</sign>
</result>
</ecommerce>
```

Chyba pri spracovávaní parametrov:

```
<?xml version="1.0" encoding="windows-1250"?>
<ecommerce>
<request>
<mid>9999</mid>
<timestamp>21122005101827</timestamp>
<service>DOMPAYMENT</service>
</request>
<error>
<error_code>1002</error_code>
</error>
</ecommerce>
```

7 Chybové stavy

Počas spracovávania odpovede môžu nastať nasledovné chybové stavy:

- chybný MID – obchodník nie je registrovaný v systéme, alebo je v stave OFFLINE
chybový kód: 1001
chybová správa: *Lutujeme, ale tento obchodník nie je registrovaný v našom systéme.*
- chybný bezpečnostný podpis – bezpečnostný podpis nie je vygenerovaný v súlade s algoritmom generovania podpisu, bol generovaný s nesprávnym kľúčom alebo s nesprávnymi parametrami
chybový kód: 1002
chybová správa: *Lutujeme, ale Vašu platbu nemožno z dôvodu neplatného bezpečnostného podpisu uskutočniť!*
- chybné parametre – TIMESTAMP nie je mimo intervalu +/- 1 hodina k aktuálnemu času v časovej zóne UTC (GMT), alebo je identifikátor služby iný ako povolené služby (DOMPAYMENT)
chybový kód: 1003
chybová správa: *Žiaľ, niektorý z požadovaných parametrov nebol zadáný. Informujte o tom, prosím, Vášho predajcu.*
- všetky ostatné chyby na strane servera banky (nefunkčné overovanie podpisu, chyba spojenia s bankovým systémom a pod.)
V takomto prípade sa vráti výsledok so statusom OFFLINE.
Zaluguje sa chybový kód 1101 a správa SERVER ERROR.