Technická príručka k službe TatraPay

Verzia: 3.3

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

Obsah

1 Úvod

Služba TatraPay je platobný nástroj v internetovom prostredí využívaný obchodníkmi na príjem platieb za poskytnutý tovar alebo služby. Účelom dokumentu je poskytúť 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.

2.3 Na Internet bankingovom servri sa klient prihlási identifikačnými údajmi (PID, heslo a kód z autorizačného zariadenia) Tatra banky do TatraPay aplikácie.

2.4 Banka ponúkne klientovi na obrazovke predvyplnenú platbu z jeho bežného účtu na účet obchodníka.

2.5 Banka overí platnosť/správnosť uvedených predvyplenných položiek:
a) účet prijímateľa (obchodníka)
b) dátum zúčtovania
c) suma a mena
d) referencia platiteľa alebo platobné symboly (variabilný, špecifický a 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 účtov.

2.7 Klient následne potvrdí alebo zruší platbu.

2.8 Banka zobrazí klientovi informáciu o výsledku spracovania platby:
- *Vaša platba prebehla úspešne.*
- *Vaša platba nebola spracovaná.*
- *Vaša platba bola zaznamenaná. O jej výsledku dostanete správu do Schránky správ vo Vašom Internet bankingu.*
- *Platba bola zrušená*. (v prípade, že klient zrušil platbu)

2.9 Banka následne presmeruje klienta späť na stránku obchodníka aj s návratovou hodnotou a naslednou notifikáciou cez email alebo SMS (ak boli zadané).

3 Technické parametre

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

Stránka obchodníka posiela Internet bankingovému serveru 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 nadobúdať iba hodnotu „TatraPay“.	TatraPay
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.	1234.50
CURR	integer	Mena	áno	Mena, v ktorej bude transakcia vykonaná.	3	Môže nadobúdať iba hodnotu „978“ (EUR).	978
VS	string	Variabilný symbol	áno / nie	Jednoznačný identifikátor platby	max. 10	Môže obsahovať iba číslice 0-9. Parameter je povinný, pokiaľ nie je vyplnený parameter REF. Pokiaľ bude zaslaný súčasne s vyplneným parametrom REF, tak identifikátorom platby bude REF a VS bude ignorovaný.	1234567890
SS	string	Špecifický symbol	nie	Doplnkový identifikátor platby	max. 10	Môže obsahovať iba číslice 0-9. Pokiaľ bude zaslaný súčasne s vyplneným parametrom REF, tak SS bude ignorovaný	987654321
CS	string	Konštantný symbol	nie	Konštantný symbol	max. 4	Môže obsahovať iba číslice 0-9. Pokiaľ bude zaslaný súčasne v vyplneným parametrom REF, tak CS bude ignorovaný.	0308
REF	string	Referencia platiteľa	áno / nie	Jednoznačný identifikátor platby	max. 35	Môže obsahovať znaky 0-9, A-Z, a-z, ., -, / a medzeru. Parameter je povinný, pokiaľ nie je vyplnený parameter VS.	Abc/12-s
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.tatrabanka.sk
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 +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.	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 platby	nie	Popis platby. Je určený pre lepšiu identifikáciu platby. Bude predvyplnený do poľa „Informácia pre príjemcu“ v platobnom príkaze.	max. 20 1 2	Môže obsahovať iba znaky 0-9, A-Z, a-z, ., -, _, @ a medzeru. Nesmie obsahovať diakritiku.	Za_popis
AREDIR	integer	Príznak automatického presmerovania	nie	Príznak pre automatické presmerovanie na stránku obchodníka (RURL) po uplynutí časového intervalu.		Môže obsahovať hodnotu 1 alebo 0: • 0 – manuálne presmerovanie po kliknutí na „Pokračovať • 1 – automatické presmerovanie po 9-tich sekundách	1
LANG	string	Identifikácia jazyka	nie	Umožňuje nastavenie jazykovej mutácie TatraPay.		Môže obsahovať hodnoty: • sk – slovenčina (východzia hodnota) • en – anglický jazyk	en

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 (ak je vyplnený)
5. SS (ak je vyplnený)
6. CS (ak je vyplnený)
7. REF (ak je vyplnený)
8. RURL

Reťazec pre bezpečnostný podpis odpovede z banky

Pokiaľ je identifikátorom platby variabilný symbol VS a prípadne špecifický symbol SS:
1. VS
2. SS (ak je vyplnený)
3. RES

Pokiaľ je identifikátorom platby referencia platiteľa REF:
1. REF
2. RES

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 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 odpoveď o výsledku vykonanej platby vo forme zakódovaného reťazca.
URL internet bankingového servra banky je: https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/e-commerce.jsp
Príklad požiadavky obchodníka:
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=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.
TOUT	Platba nebola spracovaná a banka nevie jej konečný výsledok (OK alebo FAIL). Tento status nadobúdajú platby realizované počas technickej prestávky Internet bankingu. Po ukončení technickej prestávky sa platba spracuje a jej konečný výsledok bude zaslaný obchodníkovi ďalšou notifikačnou správou (formou SMS alebo e-mailom, pokiaľ boli vyplnené platnou hodnotou).

Parametre odpovede, pokiaľ je identifikátorom platby VS a prípadne SS:
- VS – variabilný symbol z požiadavky obchodníka
- SS (ak je vyplnený) – špecifický symbol z požiadavky obchodníka
- RES – výsledok platby
- SIGN – bezpečnostný podpis parametrov odpovede z banky

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

Pokiaľ je vyplnený SS:

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

Parametre odpovede, pokiaľ je identifikátorom platby REF:
- REF – referencia platiteľa z požiadavky obchodníka
- RES – výsledok platby
- SIGN – bezpečnostný podpis parametrov odpovede z banky

URL formát	https://{parameter RURL}?REF={parameter REF}&RES={parameter RES}&SIGN={bezp. podpis}
Formát SMS	TBEC REF={parameter REF} RES={parameter RES} SIGN={bezp. podpis}
Formát e-mail	REF={parameter REF} RES={parameter RES} 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 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 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="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 klienta o aktuálnej dostupnosti služby TatraPay (či je služba on-line prístupná a neprebieha technická prestávka), môže tak urobiť automatickým dotazovaním 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	Povinný	Popis	Počet znakov	Pravidlá	Príklad
MID	Identifikácia obchodníka	áno	Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč, určený na zabezpečenie správ.	3 - 4	Kontroluje sa voči databáze obchodníkov.	9999
TIMESTAMP	Čas generovania požiadavky	áno	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	áno	Musí nadobudnúť hodnotu DOMPAYMENT.	10	SERVICE=DOMPAYMENT	DOMPAYMENT
SIGN	Bezpečnostný podpis	áno	Tvorí sa zakódovaním reťazca: MID+TIMESTAMP+SERVICE	32	Musí byť vygenerovaný na základe algoritmu uvedeného v článku 4 Bezpečnostný kľúč tohto dokumentu.	29C371F0B4F5A46529C371F0B4F5A465

Príklad požiadavky:
https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/isoffline.jsp?MID=9999&TIMESTAMP=14112005124627&SERVICE=DOMPAYMENT&SIGN=29C371F0B4F5A46529C371F0B4F5A465

6.3Formát 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>29C371F0B4F5A46529C371F0B4F5A465
</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:

a) chybný MID – obchodník nie je registrovaný v systéme, alebo je v stave OFFLINE
   chybový kód: 1001
   chybová správa: *Niektorý z požadovaných parametrov bol nesprávne zadaný. Informujte o tom, prosím, Vášho predajcu.*
b) 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: *Platbu nemožno uskutočniť z dôvodu neplatného bezpečnostného podpisu.*
c) chybné parametre – TIMESTAMP 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: *Niektorý z požadovaných parametrov nebol zadaný. Informujte o tom, prosím, Vášho predajcu.*
d) 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.
   Zaloguje sa chybový kód 1101 a správa SERVER ERROR.