Technická príručka k službe TatraPay

Verzia: 4.0

Email: tpay@tatrabanka.sk

Tel.: 02/5919 3800
02/5919 2129

Obsah

Úvod

Tento dokument popisuje implementáciu služby TatraPay.
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.
Dokument je určený osobám s technickými znalosťami.

Slovník pojmov

Pojem	Vysvetlenie
TatraPay	Služba umožňujúca klientom Tatra banky, ktorí majú oprávnenie pre disponovanie s bežným účtom, realizovať online platby na účet obchodníka.
HMAC	Hašovaný autentifikačný kód, ktorý je vypočítaný z reťazca (zostaveného podľa špecifikácie) a bezpečnostného kľúča, ktorý obdrží obchodník od banky. HMAC slúži pre overenie integrity správ zasielaných medzi serverom banky a serverom obchodníka.
ECDSA	Digitálny podpis algoritmom ECDSA, ktorý je posielaný v odpovediach zo servera banky a slúži pre overenie autenticity. Obchodník podpis skontroluje pomocou verejného kľúča dostupného na stránke Tatra banky.
Bezpečnostný kľúč	128 znakový kľúč, ktorý je obchodníkovi odovzdaný pri podpise zmluvy.
Verejný kľúč	Kľúč slúžiaci na kontrolu ECDSA podpisu, ktorý je zverejnený na stránke Tatra banky.

Služba TatraPay

Služba TatraPay umožňuje klientom Tatra banky (ďalej len „banka“), ktorí majú oprávnenie pre disponovanie s bežným účtom, realizovať online platby na účet obchodníka prostredníctvom špeciálneho URL odkazu, ktorý môže byť umiestnený na webovej stránke (internetovom obchode).

Služba prináša tieto výhody:

- platba z účtu zákazníka na účet obchodníka je realizovaná priamo, okamžite po potvrdení zákazníkom
- banka notifikuje obchodníka o úspešnom / neúspešnom priebehu platby a umožňuje mu overiť stav všetkých platieb realizovaných prostredníctvom služby TatraPay
- komunikácia medzi obchodníkom a bankou je zabezpečená

Realizácia platby

Primárnym využitím služby TatraPay je platba za tovar alebo služby na internetových obchodoch.

Postup:

1. Zákazník po nákupe tovaru alebo služieb v internetovom obchode klikne na symbol platby prostredníctvom TatraPay.

2. Server obchodníka presmeruje zákazníka prostredníctvom URL odkazu na Internet bankingový server banky.
3. Banka overí platnosť a správnosť parametrov zaslaných prostredníctvom URL a zobrazí aplikáciu TatraPay.
   Poznámka: Aplikácia TatraPay je zjednodušenou verziou Internet bankingu, ktorá obsahuje iba funkčnosť pre potvrdenie predvyplnenej platby.
4. Zákazník sa prihlási identifikačnými údajmi (PID, heslo a kód z autorizačného zariadenia).
5. Aplikácia zobrazí predvyplnenú platbu z bežného účtu zákazníka na účet obchodníka. Klient môže zmeniť účet platiteľa v prípade, že má oprávnenie pre vykonanie platby na viacerých bežných účtoch.
6. Zákazník potvrdí alebo zruší platbu.
7. Aplikácia zobrazí zákazníkovi informáciu o výsledku spracovania platby.
8. Zákazník stlačí tlačidlo *Pokračovať* pre návrat na stránku obchodníka.
9. Obchodník overí výsledok spracovania platby. K dispozícii má nasledovné možnosti:
   a. kontrola parametrov v návratovej URL
   b. kontrola notifikačného emailu (pokiaľ bol korektne vyplnený parameter REM v požiadavke)
   c. online rozhranie pre získanie zoznamu TatraPay platieb
      (viď kap. 0. Overenie stavov platieb vykonaných cez TatraPay)
   d. kontrola pohybov na účte prostredníctvom Internet bankingu alebo mobilnej aplikácie

Bezpečnosť komunikácie

Pre komunikáciu medzi obchodníkom a bankou platí:

- komunikácia je prenášaná a šifrovaná protokolom SSL
- server obchodníka aj banky zabezpečí integritu zasielaných údajov prostredníctvom hašovaného autentifikačného kódu (HMAC), ktorý je vypočítaný z parametrov a bezpečnostnéhokľúča, ktorý obdrží obchodník od banky
- server banky navyše odpovede podpíše digitálnym podpisom (ECDSA), ktorý si obchodník skontroluje na základe verejného kľúča dostupného na stránke Tatra banky

Obchodník je povinný overiť si pravosť odpovede z banky overením správnosti autentifikačného kódu HMAC a digitálneho podpisu ECDSA.

Ak sa HMAC a ECDSA nezhodujú s vypočítanými hodnotami na strane obchodníka, odpoveď je vyhodnotená ako podozrivá a obchodník je povinný kontaktovať banku za účelom preverenia výsledku spracovania platby resp. inej odpovede.

Implementácia na strane obchodníka

Požiadavky na implementáciu:

- presmerovanie na Internet bankingový server nie je možné cez iframe
- obchodník môže požiadavky zasielať na nižšie uvedené URL služby TatraPay metódou POST alebo GET cez protokol HTTPS
- parametre budú kódované vo forme application/x-www-form-urlencoded
- každá požiadavka musí obsahovať autentifikačný kód HMAC
- odpovede servera banky obsahujú autentifikačný kód HMAC a digitálny podpis ECDSA, ktoré je povinný obchodník overiť
- obchodník od banky obdrží pri podpise zmluvy svoj identifikátor (MID) a bezpečnostný kľúč.

Zaslanie požiadavky prostredníctvom HTML formulára

Server obchodníka vygeneruje stránku so skrytým formulárom, ktorý obsahuje INPUT polia typu HIDDEN pre každý vstupný parameter.
Pre formulár sa doporučuje nastaviť parameter METHOD na hodnotu POST. V prípade, že ju daný web server nepodporuje, môže sa použiť hodnota GET.
Príklad:

```
<FORM action="[URL pre zvolené rozhranie]" METHOD="POST">
    <INPUT TYPE="HIDDEN" name="MID" value="9999" />
    <INPUT TYPE="HIDDEN" name="AMT" value="1234.50" />
    ...
</FORM>
```

Zaslanie požiadavky zostavením URL

Server obchodníka vygeneruje URL odkaz, ktorý sa skladá z URL pre zvolené rozhranie a vstupných parametrov:
*[URL pre zvolené rozhranie]***?***[reťazec vstupných parametrov]*
Pre reťazec vstupných parametrov platí:

- hodnoty parametrov sú kódované štandardnou metódou URLEncode
- názvy parametrov sú od hodnôt oddelené znakom „=“ napr. *MID=9999*
- parametre navzájom sú oddelné znakom „&“ napr. *MID=9999&AMT=1234.50*

Výpočet autentifikačného kódu HMAC

Server obchodníka musí:

- vypočítať autentifikačný kód HMAC a pridať ho k parametrom **požiadavky** zasielanej na server banky

- vypočítať autentifikačný kód HMAC a overiť vypočítanú hodnotu voči parametru HMAC v **odpovedi** zo servera banky. V prípade, že sa hodnoty nezhodujú, musí odpoveď vyhodnotiť ako neplatnú a kontaktuje banku za účelom preverenia platby.

Postup výpočtu:

1. server obchodníka pripraví reťazec, ktorý je vstupom pre výpočet autentifikačného kódu HMAC (podľa popisu v podkapitolách nižšie)
2. z tohto reťazca vygeneruje hašovaný autentifikačný kód (HMAC) použitím:
   - kryptografickej funkcie SHA-256
   - 64 bajtového bezpečnostného kľúča, ktorý je zapísaný v hexadecimálnom tvare (128 znakov)

Príklady v niektorých programovacích jazykoch

Premenné:

- *key = bezpečnostný kľúč v hexadecimálnom tvare*
- *stringToSign = reťazec hodnôt parametrov*

PHP

```php
<?php
$keyBytes = pack("H*" , $key); // konverzia do binárneho formátu
$signature = hash_hmac("sha256", $stringToSign, $keyBytes);
```

JAVA

```java
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

byte[] keyBytes = hex2bytes(key); // konverzia do binárneho formátu
SecretKeySpec keySpec = new SecretKeySpec(keyBytes, "HmacSHA256");
Mac mac = Mac.getInstance("HmacSHA256");
mac.init(keySpec);
byte[] hmacBin = mac.doFinal(stringToSign.getBytes());
String signature = bytes2hex(hmacBin); // konverzia do hexadecimálneho reťazca
```

Overenie digitálneho podpisu ECDSA

Server obchodníka overí digitálny podpis ECDSA, ktorý sa nachádza v **odpovedi** zo servera banky. V prípade, že je overenie neúspešné, vyhodnotí odpoveď ako neplatnú.
Server obchodníka overí tento digitálny podpis nasledovne:

1. obchodník si stiahne verejné kľúče zo servera Tatra banky vo forme súboru a uloží ho na server.

   Pozn.: Banka môže v prípade potreby zmeniť verejný kľúč. Z tohto dôvodu je každý verejný kľúč označený identifikátorom (KEY_ID) a stavom (STATUS). Identifikátor kľúča (KEY_ID), ktorý bol použitý na podpísanie odpovede, je vždy zasielaný v odpovedi ako parameter ECDSA_KEY.

URL adresa, na ktorej sú dostupné verejné kľúče:
https://moja.tatrabanka.sk/e-commerce/ecdsa_keys.txt

Formát súboru so zoznamom verejných kľúčov:

```
KEY_ID: 1
STATUS: REVOKED
-----BEGIN PUBLIC KEY-----
...
-----END PUBLIC KEY-----

KEY_ID: 2
STATUS: VALID
-----BEGIN PUBLIC KEY-----
...
-----END PUBLIC KEY-----

...
```

2. server obchodníka pripraví rovnaký reťazec ako pri overení HMAC a pripojí k nemu hodnotu HMAC (prijatú alebo vypočítanú hodnotu – musia byť zhodné)
3. overí digitálny podpis volaním OpenSSL funkcie pre overenie digitálneho podpisu ECDSA, ktorej vstupom je:
   - reťazec pre overenie digitálneho podpisu
   - voľba kryptografickej funkcie SHA-256
   - digitálny podpis zaslaný v odpovedi v parametri *ECDSA*
   - verejného kľúča s identifikátorom zaslaným v parametri *ECDSA_KEY*

Príklady

Premenné:

- *stringToVerify = reťazec hodnôt parametrov*
- *publicKey = cesta k súboru s verejným kľúčom*
- *ECDSA = digitálny podpis prijatý v odpovedi*

Pozn.: pred samotným overením podpisu musí server obchodníka vyhodnotiť, či má k dispozicii verejný kľúč s identifikátorom, ktorý bol zaslaný v odpovedi v parametri ECDSA_KEY.

Volanie knižnice OpenSSL priamo

- server uloží reťazec *stringToVerify* do súboru *parameterStringFile*
- server skonvertuje digitálny podpis *ECDSA* z Hex formátu do binárneho a uloží do súboru *ecdsaFile*

```
openssl dgst -SHA256 -verify publicKeyFile -signature ecdsaFile parameterStringFile
```

PHP

```
$verified = openssl_verify($stringToVerify, pack("H*", $ECDSA), $publicKey,
"sha256");
if ($verified === 1) {
    // odpoveď verifikovaná
}
```

JAVA

```
import java.math.BigInteger;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import javax.xml.bind.DatatypeConverter;

publicKey = publicKey.replaceAll("-----(BEGIN|END).*", "").trim();

X509EncodedKeySpec spec = new X509EncodedKeySpec(
    DatatypeConverter.parseBase64Binary(publicKey));
KeyFactory keyFactory = KeyFactory.getInstance("EC");
PublicKey pKey = keyFactory.generatePublic(spec);

Signature ecdsaSign = Signature.getInstance("SHA256withECDSA");
ecdsaSign.initVerify(pKey);
ecdsaSign.update(stringToVerify.getBytes("UTF-8"));

if (ecdsaSign.verify(new BigInteger(ECDSA, 16).toByteArray())) {
    // odpoveď verifikovaná
}
```

Platba cez TatraPay

Identifikácia platby

Obchodník musí platbu identifikovať:

- variabilným symbolom a prípadne špecifickým a konštatným symbolom

ALEBO

- referenciou platiteľa (tento identifikátor platby bol zavedený v rámci SEPA platieb)

Zvolený identifikátor / identifikátory:

- zašle obchodník v požiadavke na platbu cez TatraPay
- zašle banka obchodníkovi v návratovej URL a notifikačnom emaile

Požiadavka

Server obchodníka pošle požiadavku metódou POST alebo GET na URL adresu:

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

Vstupné parametre

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
MID	áno	Identifikátor obchodníka. *Jedinečné identifikačné číslo obchodníka*	3 - 4	MID je uvedený v Prílohe č.1 Zmluvy o prevádzkovaní služby TatraPay	9999
AMT	áno	Suma platby *Suma, ktorú má zákazník previesť na účet obchodníka.*	9 + 2	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené bodkou	1234.50
CURR	áno	Mena platby	3	- musí obsahovať hodnotu „978“ (EUR)	978
VS	áno / nie	Variabilný symbol	max. 10	- povolené znaky: 0-9 - parameter je povinný, pokiaľ nie je vyplnený parameter REF - pokiaľ budú súčasne vyplnené parametre VS a REF, identifikátorom platby bude REF a VS bude ignorovaný	1234567890
SS	nie	Špecifický symbol	max. 10	- povolené znaky: 0-9 - pokiaľ bude vyplnený súčasne s parametrom REF, bude ignorovaný	987654321
CS	nie	Konštantný symbol	max. 4	- povolené znaky: 0-9 - pokiaľ bude vyplnený súčasne s parametrom REF, bude ignorovaný	308
REF	áno / nie	Referencia platiteľa	max. 35	- povolené znaky: 0-9 A-Z a-z . - / a medzera - parameter je povinný, pokiaľ nie je vyplnený parameter VS	Abc/12-s
RURL	áno	Návratová URL *URL adresa, na ktorú banka presmeruje zákazníka po vykonaní platby*		- URL musí byť vytvorenáv súlade s RFC 1738 a musí byť funkčná	https://www.obchodnik.sk/vysledok_platby.php
REM	nie	Emailová adresa pre zaslanie notifikácie o výsledku platby	max. 50	- môže obsahovať iba jednu emailovú adresu, platnú v súlade s RFC 2822 - v prípade, že hodnota prekročí 50 znakov, notifikačný email nebude odoslaný	online_platby@obchodnik.sk
TIME STAMP	áno	Timestamp (časová pečiatka) v UTC *Server banky spracuje iba požiadavky, ktoré budú mať TIMESTAMP v intervale +/- 1 hodina voči UTC (GMT)*	14	- musí byť vo formáte **DDMMYYYYHHMISS** (DD-deň, MM-mesiac, YYYY-rok, HH-hodina, MI-minúta, SS-sekunda)	01092014125505

HMAC	áno	Autentifikačný kód HMAC z parametrov: - pokiaľ je platba identifikovaná VS: ***MID + AMT + CURR + VS + SS + CS + RURL + REM + TIMESTAMP*** - pokiaľ je platba identifikovaná REF: ***MID + AMT + CURR + REF + RURL + REM + TIMESTAMP***	64	- platné znaky: 0-9 a-f	880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56
AREDIR	nie	Príznak automatického presmerovania na stránku obchodníka (RURL) po 9-tich sekundách. Možnosti: - **0** (predvolená): vypnuté t.j. zákazník musí stlačiť tlačidlo „Pokračovať“ - **1**: zapnuté	1	- platné hodnoty: 1, 0	1
LANG	nie	Kód jazyka, v ktorom bude zobrazená aplikácia TatraPay Možnosti: - sk (predvolená): slovenčina - en: anglický jazyk	2	- platné hodnoty: sk, en	en

Odpoveď na požiadavku

V prípade, že je požiadavka platná a služba TatraPay je dostupná, zákazníkovi sa zobrazí aplikácia TatraPay. Prostredníctvom aplikácie môže potvrdiť platbu na účet obchodníka. Po potvrdení alebo zrušení platby sa zákazníkovi zobrazí jedno z hlásení:

Hlásenie	Hodnota RES	Popis
Vaša platba prebehla úspešne.	OK	
Vaša platba nebola spracovaná.	FAIL	Nastala chyba pri spracovaní. Zákazníkovi sa zobrazí aj dôvod chyby napr. nedostatok prostriedkov na účte.
Vaša platba bola zaznamenaná. O jej výsledku dostanete správu do Schránky správ vo Vašom Internet bankingu.	TOUT	Platba je realizovaná počas technickej prestávky Internet bankingu a nie je možné určiť jej finálny stav.
Platba bola zrušená	FAIL	Zobrazí sa v prípade, že zákazník platbu zrušil.

V prípade zaslania neplatnej požiadavky zobrazí server banky jedno z chybových hlásení:

Chybové hlásenie	Popis
Služba je momentálne nedostupná.	Nastala chyba pri spracovaní požiadavky.
Platbu nemožno uskutočniť z dôvodu neplatného bezpečnostného podpisu.	Neplatný autentifikačný kód v požiadavke.
Požiadavka nie je platná (neplatný TIMESTAMP).	Parameter TIMESTAMP nie je v povolenej tolerancii.
Niektorý z požadovaných parametrov nebol zadaný alebo bol nesprávne zadaný.	Niektorý zo vstupných parametrov má neplatnú hodnotu.
Obchodník nemá oprávnenie pre požadovanú službu.	Obchodník nemá požadovanú službu aktivovanú.

Overenie stavu platby

Stav platby vykonanej cez službu TatraPay môže byť:
OK
Platba prebehla úspešne, bola pripísaná na účet obchodníka
FAIL
Platba neprebehla
TOUT
Platba bola zadaná počas technickej prestávky Internet Bankingu a nie je možné určiť jej finálny stav. Po ukončení technickej prestávky sa platba spracuje a nadobudne stav OK alebo FAIL.

Obchodník si môže overiť stav platby týmito spôsobmi:

1. kontrolou parametrov v návratovej URL
2. kontrolou notifikačného emailu (pokiaľ bol korektne vyplnený parameter REM v požiadavke)
3. online dopytom na server banky
   (viď kap. 0. Overenie stavov platieb vykonaných cez TatraPay)
4. kontrolou pohybov na účte prostredníctvom Internet bankingu alebo mobilnej aplikácie

V prípade stavu TOUT je dôležité čakať na finálny stav platby a overovať ho (aj opakovane) spôsobom 2 / 3 / 4.

Návratová URL a parametre

Aplikácia TatraPay zobrazí zákazníkovi výsledok platby.
V prípade, že zákazník nezatvorí okno prehliadača, ale stlačí tlačidlo *Pokračovať,* bude presmerovaný na URL stránky obchodníka (zaslanú vo vstupnom parametri RURL).
Návratová URL obsahuje parametre, vďaka ktorým môže server obchodníka overiť stav platby.

Názov	Popis	Príklad
AMT	Suma platby zaslaná v požiadavke	1234.50
CURR	Mena platby zaslaná v požiadavke	978
VS **SS** **CS** **REF**	Identifikátor / identifikátory platby na strane obchodníka Pokiaľ bol v požiadavke zaslaný parameter **REF**, bude vyplnený aj v odpovedi. Inak bude vyplnený parameter **VS** a prípadne **SS / CS**.	123456
RES	Kód výsledku platby: **OK** - platba prebehla úspešne **FAIL** - platba nebola úspešná alebo ju zákazník zrušil **TOUT** - platba zatiaľ nebola spracovaná a banka nevie jej finálny výsledok	TOUT

TID	Jednoznačný identifikátor platby na strane banky Pomocou tohto identifikátora je možné jednoducho opakovane overiť stav platby v prípade TOUT prostredníctvom rozhrania „Overenie stavov platieb vykonaných cez TatraPay“. Parameter sa v odpovedi nachádza, pokiaľ je výsledok platby **OK** alebo **TOUT**. V prípade **FAIL** iba vtedy, ak bola požiadavka platná, zákazník sa úspešne prihlásil a potvrdil platbu.	65487
TIMESTAMP	Timestamp zaslaný v požiadavke	01092014125505
HMAC	Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov: - pokiaľ bola platba identifikovaná VS: **AMT + CURR + VS + SS + CS + RES + TID + TIMESTAMP** - pokiaľ bola platba identifikovaná REF: **AMT + CURR + REF + RES + TID + TIMESTAMP**	9b559bb38b7471f7f84dec827a8ad17700806294422cb370a39921e2ec313178
ECDSA_KEY	Identifikátor verejného kľúča, ktorým je možné overiť digitálny podpis odpovede v parametri **ECDSA**	1
ECDSA	Reťazcom pre výpočet ECDSA je reťazec hodnôt parametrov: - pokiaľ bola platba identifikovaná VS: **AMT + CURR + VS + SS + CS + RES + TID + TIMESTAMP + HMAC** - pokiaľ bola platba identifikovaná REF: **AMT + CURR + REF + RES + TID + TIMESTAMP + HMAC**	304502201fb6e376a6b7bb8fe34d931e5e409721c80fb481710dac947cf913a6a3f98f5e022100f1f3066ce4a87cd139742edcd15bdb0c100ccbd7b524e6a1a866d81c273472f7

Príklad – štandardná platba

```
https://www.obchodnik.sk/potvrdenie_platby.php?
AMT=100.00
&CURR=978
&VS=123456
&SS=2205
&RES=OK
&TID=1971
&TIMESTAMP=16092014132529
&HMAC=e790515fda8a066821b37e9c2d41040b9b4ce42939474bd82ee0486ecab9a2fd
&ECDSA_KEY=1
&ECDSA=3046022100b88c4dcc3c74c8b3dac09a324f62f29c8d32bb4da8e6f73847d4ebf77ef23ddf022100bceaa33
941554f1f0dae4115572ea1398730deee4ec0f88309aff778122484b5
```

Notifikačný email

Server banky odošle notifikačný email na adresu uvedenú v parametri REM.
V prípade, že platba nadobudne stav TOUT, budú odoslané 2 notifikačné emaily:

- jeden v momente potvrdenia platby zákazníkom (so stavom TOUT)
- jeden po spracovaní platby bankou (stav OK alebo FAIL)

Telo emailu obsahuje reťazec parametrov, rovnakých ako návratová URL:

- názvy parametrov sú od hodnôt oddelené znakom „=“
- parametre navzájom sú oddelné medzerou
- pokiaľ parameter nie je vyplnený, nebude sa v reťazci nachádzať (ani názov ani hodnota)

v tomto poradí:

1. AMT
2. CURR

3. VS
4. SS
5. CS
6. REF
7. RES
8. TID
9. TIMESTAMP
10. HMAC
11. ECDSA_KEY
12. ECDSA

Príklad:

```
AMT=100.00 CURR=978 VS=123456 SS=2205 RES=OK TID=1971 TIMESTAMP=16092014132529
HMAC=e790515fda8a066821b37e9c2d41040b9b4ce42939474bd82ee0486ecab9a2fd ECDSA_KEY=1
ECDSA=3046022100b88c4dcc3c74c8b3dac09a324f62f29c8d32bb4da8e6f73847d4ebf77ef23ddf022100bceaa339
41554f1f0dae4115572ea1398730deee4ec0f88309aff778122484b5
```

Príklad

Zákazník na stránke obchodníka nakúpi tovar za *20,78 EUR*. Obchodník objednávku eviduje pod číslom *78945210*. Obchodník má od banky pridelený:

- MID: *9999*
- bezpečnostný kľúč (v hexadecimálnom tvare):
  7878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878787878

Zákazník zvolí platbu cez TatraPay.

1. server obchodníka pripraví vstupné parametre:

   ```
   MID = 9999
   AMT = 20.78
   CURR = 978
   VS = 78945210
   RURL = https://www.obchodnik.sk/potvrdenie_platby.php
   REM = online_platby@obchodnik.sk
   TIMESTAMP = 16092014132529       (pozor, dátum a čas musí byť UTC !)
               (16.9.2014 13:25:29)
   ```

2. server obchodníka zostaví reťazec pre výpočet autentifikačného kódu HMAC

   ```
   HMAC_STRING = MID + AMT + CURR + VS + RURL + REM + TIMESTAMP =
   999920.7897878945210https://www.obchodnik.sk/potvrdenie_platby.phponline_plat
   by@obchodnik.sk16092014132529
   ```

3. server obchodníka vypočíta autentifikačný kód a naplní ho do parametra HMAC

   ```
   HMAC = hash_hmac('sha256', HMAC_STRING, SECURITY_KEY) =
   d8e5927d1aa309bb48f4e32e79813e691efa37c6c5235bcca9cf9f896bbed439
   ```

   Poznámka: bezpečnostný kľúč je potrebné skonvertovať do binárneho reťazca

4. server obchodníka vytvorí z parametrov požiadavku vo forme URL (metóda GET):

   ```
   https://moja.tatrabanka.sk/cgi-bin/e-
   commerce/start/tatrapay?MID=9999&AMT=20.78&CURR=978&VS=78945210&RURL=https%3A
   %2F%2Fwww.obchodnik.sk%2Fpotvrdenie_platby.php&REM=online_platby%40obchodnik.
   sk&TIMESTAMP=16092014132529&HMAC=d8e5927d1aa309bb48f4e32e79813e691efa37c6c523
   5bcca9cf9f896bbed439
   ```

5. server obchodníka presmeruje používateľa na URL

6. zákazník sa prihlási do aplikácie TatraPay a potvrdí platbu
7. server banky odošle notifikačný email
8. server banky zobrazí zákazníkovi výsledok platby. Po stlačení tlačidla *Pokračovať* je zákazník presmerovaný na návratovú URL s výstupnými parametrami napr.:
   `https://www.obchodnik.sk/potvrdenie_platby.php?AMT=20.78&CURR=978&VS=78945210&RES=OK&TID=45678&TIMESTAMP=16092014132529&HMAC=20310658312fdf272ba5c9287084513cfacd896fc7e1a3252fbcc80097e686fe&ECDSA_KEY=1&ECDSA=304502201fb6e376a6b7bb8fe34d931e5e409721c80fb481710dac947cf913a6a3f98f5e022100f1f3066ce4a87cd139742edcd15bdb0c100ccbd7b524e6a1a866d81c273472f7`
9. server obchodníka overí autentifikačný kód – hodnotu v parametri HMAC
   - zostaví reťazec pre výpočet HMAC:
     `HMAC_STRING = AMT + CURR + VS + RES + TID + TIMESTAMP = 20.7897878945210OK4567816092014132529`
   - vypočíta HMAC:
     `HMAC_CHECK = hash_hmac('sha256', HMAC _STRING, SECURITY_KEY) = 20310658312fdf272ba5c9287084513cfacd896fc7e1a3252fbcc80097e686fe`
   - porovná vypočítaný podpis s hodnotou v parametri HMAC. **Hodnoty musia byť zhodné !**
10. server obchodníka overí digitálny podpis – hodnotu v parametri ECDSA
    - zostaví reťazec pre výpočet podpisu:
      `ECDSA_STRING = AMT + CURR + VS + RES + TID + TIMESTAMP + HMAC = 20.7897878945210OK456781609201413252920310658312fdf272ba5c9287084513cfacd896fc7e1a3252fbcc80097e686fe`
    - použije verejný kľúč s identifikátorom ECDSA_KEY zo servera banky
    - overí digitálny podpis. **Overenie digitálneho podpisu musí byť úspešné !**
      `openssl_verify(ECDSA_STRING, ECDSA, PUBLIC_KEY, 'sha256')`

Overenie dostupnosti služby (isOffline)

V prípade, že obchodník chce byť informovaný o aktuálnej dostupnosti služby TatraPay (či je služba on-line prístupná a neprebieha denná uzávierka) resp. chce informovať zákazníka, môže tak urobiť automatickým dotazovaním cez toto rozhranie.

Server obchodníka pošle požiadavku metódou GET alebo POST na URL adresu:

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

Vstupné parametre

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
MID	áno	Identifikátor obchodníka *Jedinečné identifikačné číslo obchodníka, ku ktorému je priradený účet obchodníka a bezpečnostný kľúč*	3 - 4	MID je uvedený v Prílohe č.1 Zmluvy o prevádzkovaní služby TatraPay	9999
TIMESTAMP	áno	Timestamp (časová pečiatka) Server banky spracuje iba požiadavky, ktoré budú mať TIMESTAMP v intervale +/- 1 hodina voči UTC (GMT)	14	- musí byť vo formáte **DDMMYYYYHHMISS** (DD-deň, MM-mesiac, YYYY-rok, HH-hodina, MI-minúta, SS-sekunda)	01092014125505

SERVICE	áno	Identifikátor služby	10	- musí obsahovať hodnotu *DOMPAYMENT*	DOMPAYMENT
HMAC	áno	Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov: MID + TIMESTAMP + SERVICE	64	- platné znaky: 0-9 a-f	880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56

Odpoveď

Odpoveď na požiadavku je vo forme XML dokumentu, ktorý obsahuje nasledovné elementy:

Element	Popis	Príklad
ecommerce	Hlavný element dokumentu, obsahuje element *request* a práve jeden element *result* alebo *error*	
ecommerce/ **request**	Element obsahuje parametre zo zaslanej požiadavky	
ecommerce/request/ **mid**	MID zaslaný v požiadavke	9999
ecommerce/request/ **timestamp**	TIMESTAMP zaslaný v požiadavke	01092014125505
ecommerce/request/ **service**	SERVICE zaslaný v požiadavke	DOMPAYMENT
ecommerce/ **result**	Element obsahuje parametre odpovede	
ecommerce/result/ **status**	Stav služby, nadobúda hodnoty: - online - offline	online
ecommerce/result/ **hmac**	Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov: MID + TIMESTAMP + SERVICE + STATUS	880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56
ecommerce/ **error**	Chybový element	
ecommerce/error **error_code**	Číselný kód chyby	1002

Príklad odpovede (stav služby online)

```
<ecommerce>
    <request>
        <mid>9999</mid>
        <timestamp>01092014125505</timestamp>
        <service>DOMPAYMENT</service>
    </request>
    <result>
        <status>online</status>
        <hmac>BF5AD57BC619B0457FB35318488C85C85C53A779507ADA24BE5E9609A4537891</hmac>
    </result>
</ecommerce>
```

Príklad chybovej odpovede

```
<ecommerce>
    <request>
        <mid>9999</mid>
        <timestamp>01092014125505</timestamp>
        <service>DOMPAYMENT</service>
```

```
    </request>
    <error>
        <error_code>1002</error_code>
    </error>
</ecommerce>
```

Číselník chýb

error_code	popis
1002	Neplatný autentifikačný kód HMAC
1003	TIMESTAMP je mimo povoleného intervalu (+/- 1 hodina voči UTC) alebo identifikátor služby SERVICE je neplatný (nie je DOMPAYMENT)
1101	Iná chyba

Overenie stavov platieb vykonaných cez TatraPay

Server obchodníka pošle požiadavku metódou GET alebo POST na URL adresu:

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

Odpoveď má formu XML dokumentu. XML dokument je zabezpečený autentifikačným kódom HMAC a digitálnym podpisom ECDSA, ktoré sú zaslané v HTTP hlavičke.

Vstupné parametre

Vstupné parametre slúžia ako kritériá vyhľadávania pre získanie zoznamu platieb. Jediný povinný parameter je MID, ďalšími parametrami je možné spresniť vyhľadávanie.

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
MID	áno	Identifikátor obchodníka *Jedinečné identifikačné číslo obchodníka*	3 - 4		9999
REF	nie	Referencia platiteľa	max. 35	- povolené znaky: 0-9 A-Z a-z . - / a medzera	Abc/12-s
VS	nie	Variabilný symbol	max. 10	- povolené znaky: 0-9	1234567890
SS	nie	Špecifický symbol	max. 10		987654321
CS	nie	Konštantný symbol	max. 4		308
TID	nie	Jednoznačný identifikátor platby na strane banky	-		125105
TS_FROM **TS_TO**	nie	Timestamp platby OD - DO	14	vo formáte **DDMMYYYYHHMISS** (DD-deň, MM-mesiac, YYYY-rok, HH-hodina, MI-minúta, SS-sekunda)	12092014100000
AMT_FROM **AMT_TO**	nie	Suma OD – DO	max. 9 + 2	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené bodkou	1234.50

STATUS	nie	Filter podľa stavu platby: **OK** – iba úspešne spracované platby **FAIL** – iba neúspešné platby **TOUT** – iba platby čakajúce na spracovanie	max. 4	hodnoty: OK, FAIL, TOUT	OK
HMAC	áno	Autentifikačný kód HMAC z vyššie uvedených hodnôt parametrov, v uvedenom poradí.	64	- platné znaky: 0-9 a-f	880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56

Odpoveď

Odpoveď obsahuje max. 100 platieb, ktoré sú zoradené podľa TID zostupne.
V zozname sa nachádzajú platby s výsledkom **OK** alebo **TOUT**. Platby s výsledkom **FAIL** sa nachádzajú v zozname iba vtedy, ak bola požiadavka na platbu platná, zákazník sa úspešne prihlásil a potvrdil platbu. Preto je potrebné neprítomnosť platby v zozname interpretovať ako platbu s výsledkom FAIL.
XML schéma odpovede je dostupná na URL adrese:

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/xsd/GetTatraPayTransactionsResponse.xsd

Odpoveď servera banky je vo forme XML dokumentu, ktorý obsahuje tieto elementy:

Názov elementu	Popis
GetTatraPayTransactionsResponse	hlavný element XML dokumentu
mid	identifikátor obchodníka z požiadavky
responseTimestamp	časová pečiatka vygenerovania odpovede v UTC (GMT) vo formáte **DDMMYYYYHHMISS** (DD-deň, MM-mesiac, YYYY-rok, HH-hodina, MI-minúta, SS-sekunda)
hasMoreTransactions	Hodnota „true“ indikuje, že existuje viac záznamov, ktoré spĺňajú požadované kritériá a v odpovedi sa nachádza iba prvých 100 záznamov.
transactions	element, ktorý obsahuje zoznam platieb (0 až 100)
transaction	element platby, popísaný v nasledujúcej tabuľke

Platba obsahuje tieto elementy:

Názov elementu	Popis
id	jednoznačný identifikátor platby na strane banky (TID)
amount	suma platby
currency	mena platby
postingDate	dátum spracovania platby
ref	referencia platiteľa
vs	variabilný symbol
ss	špecifický symbol
cs	konštantný symbol
timestamp	timestamp zadania platby vo formáte **DDMMYYYYHHMISS**
status	Jedna z hodnôt: **OK** – úspešne spracovaná platba **FAIL** – neúspešná platba **TOUT** – platba čakajúca na spracovanie

Príklad

Telo HTTP odpovede – XML dokument

```
<GetTatraPayTransactionsResponse>
    <mid>9999</mid>
    <responseTimestamp>12092014113931</responseTimestamp>
    <hasMoreTransactions>true</hasMoreTransactions>

    <transactions>
        <transaction>
            <id>123456</id>
            <amount>100.10</amount>
            <postingDate>2014-09-12Z</postingDate>
            <currency>978</currency>
            <vs>123456</vs>
            <timestamp>12092014113931</timestamp>
            <status>OK</status>
        </transaction>

        <transaction>
            <id>123456</id>
            <amount>100.10</amount>
            <postingDate>2014-09-12Z</postingDate>
            <currency>978</currency>
            <ref>ax5778</ref>
            <timestamp>12092014113931</timestamp>
            <status>FAIL</status>
        </transaction>

        ...

    </transactions>

</GetTatraPayTransactionsResponse>
```

HTTP hlavička obsahuje:

Authorization: HMAC=*[HMAC autentifikačný kód]*, ECDSA=*[ECDSA digitálny podpis]*, ECDSA_KEY=*[identifikátor použitého verejného kľúča]*

Odpoveď v prípade chyby

Názov elementu	Popis
GetTatraPayTransactionsResponse	hlavný element XML dokumentu
mid	identifikátor obchodníka z požiadavky
errorCode	kód chyby z číselníka nižšie

Číselník chýb:

Kód chyby	Popis chyby
1	Chyba vstupného parametra
2	Neplatný autentifikačný kód
9	Iná chyba