

Technická příručka ku službě CardPay

Verzia: 2.8

01.08. 2024

Email: tpay@tatrabanka.sk

Tel.: +421 2 5919 3435

Obsah

1.	Úvod	3
1.1.	Slovník pojmov	3
2.	Služba CardPay	3
2.1.	Realizácia platby	4
2.2.	Bezpečnosť	5
3.	Implementácia na serveri obchodníka	6
3.1.	Zaslanie požiadavky prostredníctvom HTML formulára	6
3.2.	Zaslanie požiadavky zostavením URL	6
3.3.	Výpočet autentifikačného kódu HMAC	6
3.3.1.	Príklady	7
3.4.	Overenie digitálneho podpisu ECDSA	7
3.4.1.	Príklady	8
4.	Platba cez CardPay	10
4.1.	Identifikácia platby	10
4.2.	Požiadavka na realizáciu platby	10
4.2.1.	Vstupné parametre	10
4.2.2.	Odpoveď na požiadavku na realizáciu platby	14
4.3.	Overenie výsledku platby (a registrácie na službu ComfortPay)	15
4.3.1.	Návratová URL	15
4.3.2.	Notifikačný email	18
4.4.	Ukončenie a storno predautorizácie / návrat platby	19
4.4.1.	Vstupné parametre	19
4.4.2.	Odpoveď	20
4.4.3.	Číselník chýb	21
4.4.4.	Notifikačný email	22
4.5.	Príklad priebehu platby cez CardPay	22
5.	Overenie stavov platieb vykonaných cez CardPay	25
5.1.	Vstupné parametre	25
5.2.	Odpoveď	26
5.2.1.	Odpoveď v prípade chyby	28
5.3.	Zobrazenie platobnej brány v mobilnej aplikácii	29
5.3.1.	Referenčná implementácia iOS	29
5.3.2.	Referenčná implementácia Android	29

1. Úvod

Tento dokument popisuje implementáciu služby CardPay.

Účelom dokumentu je poskytnúť návod ako vytvoriť správne fungujúce a bezpečné prepojenie medzi platobným portálom banky a serverom obchodníka a popísať priebeh komunikácie medzi nimi.

Dokument je určený osobám s technickými znalosťami.

1.1. Slovník pojmov

Pojem	Vysvetlenie
CardPay	služba pre realizáciu online platieb platobnou kartou (debetnou aj kreditnou). CardPay podporuje manuálne zadanie karty, aj službu Google Pay a Apple Pay
transakcia „predaj“	typ transakcie, prostredníctvom ktorej dochádza k automatickému zúčtovaniu prostriedkov z bežného / kartového účtu držiteľa karty v sume, ktorá bola v rámci CardPay platby autorizovaná.
transakcia „predautorizácia“	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 platby zo strany obchodníka (napr. po overení dostupnosti tovaru resp. dostupnosti poskytnutia služby).
ComfortPay	služba umožňuje v rámci vopred dohodnutých pravidiel medzi obchodníkom a držiteľom karty opakovane zúčtovať platby za poskytnutý tovar a služby. Registráciu platobnej karty pre službu ComfortPay je možné vykonať iba v rámci služby CardPay. Služba ComfortPay nie je určená pre karty registrované v Apple Wallet a Google Wallet.
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 si je posielaný v odpovediach zo servera banky a slúži pre overenie autenticity. Obchodník podpis skontroluje pomocou verejného kľúča dostupného na stránke Tatra banky.

2. Služba CardPay

Služba CardPay umožňuje realizovať online platby kartou prostredníctvom špeciálneho URL odkazu, ktorý môže byť umiestnený na webovej stránke (internetovom obchode).

Služba prináša tieto výhody:

- komunikácia medzi obchodníkom a bankou je zabezpečená
- bezpečnosť je garantovaná použitím technológie 3-D Secure
- server banky notifikuje obchodníka o úspešnom / neúspešnom priebehu platby a umožňuje mu overiť stav všetkých platieb realizovaných prostredníctvom služby CardPay
- prostredníctvom služby CardPay je možné registrovať platobné karty pre službu ComfortPay
- prostredníctvom služby CardPay je možné realizovať platby prostredníctvom Click to Pay, bez potreby špeciálnej integrácie na strane obchodníka. Komunikáciu s Click to Pay zabezpečí priamo platobná brána.³⁾

- prostredníctvom služby CardPay je možné realizovať platby prostredníctvom Apple Pay, bez potreby špeciálnej integrácie na strane obchodníka. ¹⁾ Komunikáciu s Apple zabezpečí priamo platobná brána.
- prostredníctvom služby CardPay je možné realizovať platby prostredníctvom Google Pay, bez potreby špeciálnej integrácie na strane obchodníka. ²⁾ Komunikáciu s Google zabezpečí priamo platobná brána.
- V prípade, že obchodník požaduje priamu integráciu Google Pay alebo Apple Pay zo svojej webovej stránky, prípadne z mobilnej aplikácie, Tatra banka poskytne Direct API špecifikáciu pre priamu integráciu týchto služieb.

¹⁾ *Možnosť platby prostredníctvom Apple Pay je dostupná v prehliadači Safari na macOS a iOS. Na platforme iOS od verzie 16 je možnosť Apple Pay platby dostupná aj v mobilných prehliadačoch Chrome, Edge a Firefox. V prípade, že obchodník zobrazuje platobnú bránu CardPay v rámci svojej mobilnej aplikácie pre platformu iOS, musí pre správne fungovanie Apple Pay použiť pre zobrazenie platobnej brány SFViewController. Vid' kapitola 5.3.1 Referenčná implementácia iOS.*

²⁾ *Možnosť platby prostredníctvom Google Pay je dostupná vo všetkých moderných internetových prehliadačoch na desktope alebo v mobilných zariadeniach. V prípade, že obchodník zobrazuje platobnú bránu CardPay v rámci svojej mobilnej aplikácie pre platformu Android, musí pre správne fungovanie Google Pay použiť pre zobrazenie platobnej brány technológiu Chrome Tabs. Vid' kapitola 5.3.2 Referenčná implementácia Android.*

³⁾ *Obchodník je povinný uviesť k platobnej metóde, alebo do Obchodných podmienok znenie: E-mailovú adresu zákazníka pošleme do Click to Pay pre overenie, či profil/účet s uloženými platobnými kartami už existuje.*

2.1. Realizácia platby

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

Služba CardPay umožňuje realizáciu platieb prostredníctvom transakcie typu „predaj“ a transakcie typu „predautorizácia“.

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.

Pri oboch typoch transakcií je možné registrovať platobné karty na službu ComfortPay.

Postup

1. Zákazník po nákupe tovaru alebo služieb v internetovom obchode klikne na symbol platby prostredníctvom CardPay. Služba Cardpay je prezentovaná logami kartových spoločností (VISA, Mastercard). Súčasne banka obchodníkovi poskytne logo Google Pay a logo Apple Pay, ktoré obchodník uvedie k platobnej metóde CardPay.
2. Server obchodníka presmeruje zákazníka prostredníctvom URL odkazu na server banky.
3. Server banky overí platnosť a správnosť parametrov zaslaných prostredníctvom URL a zobrazí platobný portál CardPay.
4. Na platobnom portáli má zákazník možnosť zadať údaje zo svojej platobnej karty (číslo karty, expiráciu a CV kód) a potvrdí platbu. Súčasne má možnosť vybrať platbu prostredníctvom Google Pay, alebo Apple Pay.

Google Pay a Apple Pay je platobná metóda, ktorá umožňuje jednoduchú, bezpečnú a rýchlu platbu pomocou karty uloženej ku Google, alebo k Apple úču.

Logo služby Google Pay alebo Apple Pay sa zobrazí na CardPay portáli v závislosti od prehliadača, alebo typu mobilného zariadenia a jeho operačného systému.

Zákazník uloží údaje o svojej platobnej karte do Google alebo Apple peňaženky. Pri následnom platení prostredníctvom služby Cardpay a výbere platobnej metódy Google Pay, alebo Apple Pay na Cardpay bráne, je zákazník presmerovaný do Google peňaženky, alebo Apple peňaženky, vyberie kartu a potvrdí platbu. Google a Apple si vymenia údaje o platbe s platobnou bránou CardPay.

5. Zákazník po presmerovaní na Cardpay bránu nemôže zmeniť sumu transakcie, menu ani číslo transakcie.

6. Platobná brána zobrazí klientovi informáciu o výsledku spracovania platby:

- *Vaša platba bola úspešne spracovaná.*
- *Vaša platba nebola vykonaná.*

Ak požiadavka na realizáciu platby obsahovala aj požiadavku na registráciu karty pre službu ComfortPay, po úspešnom spracovaní platby služba CardPay zároveň vykoná registráciu karty pre službu ComfortPay. V prípade neúspešnej transakcie neprebehne ani registrácia pre službu ComfortPay.

V prípade platby prostredníctvom Google Pay a Apple Pay, informáciu zákazník ihneď obdrží aj v Google alebo Apple peňaženke.

7. Zákazník stlačí tlačidlo *Pokračovať* pre návrat na stránku obchodníka alebo aplikácia automaticky presmeruje zákazníka späť na stránku obchodníka.

8. Server obchodníka overí výsledok spracovania platby. K dispozícii má nasledovné možnosti:

- a. kontrola parametrov v návratovej URL
- b. kontrola notifikačného emailu (pokiaľ bol vyplnený parameter REM v požiadavke)
- c. online rozhranie pre získanie zoznamu CardPay transakcií
(viď kap. 6. Overenie stavov platieb vykonaných cez CardPay)

9. V prípade realizácie platby formou predautorizácie je obchodník povinný do 7 dní odo dňa, kedy bola predautorizácia vykonaná, zabezpečiť volaním online rozhrania ukončenie / storno predautorizácie. (viď kap. 4.4)

10. Ak prebehla v rámci platby cez Cardpay aj registrácia karty pre službu ComfortPay, ďalšie transakcie zákazníka môže obchodník realizovať prostredníctvom služby ComfortPay. (viď technickú príručku služby ComfortPay).

2.2. Bezpečnosť

Komunikácia medzi obchodníkom a bankou je:

- prenášaná a šifrovaná protokolom SSL
- server obchodníka aj banky zabezpečí integritu zasielaných údajov prostredníctvom hašovaného autentifikačného kódu (HMAC)
- server banky navyše odpovede podpíše digitálnym podpisom (ECDSA)

Obchodník je povinný overiť si pravosť odpovede z banky overením správnosti HMAC a ECDSA podpisov.

Ak sa HMAC zaslaný serverom banky nezhoduje s kódom vypočítaným serverom obchodníka

ALEBO

overenie ECDSA podpisu pomocou verejného kľúča nie je úspešné, odpoveď je vyhodnotená ako podozrivá a obchodník je povinný kontaktovať banku za účelom preverenia výsledku spracovania platby resp. inej odpovede.

3. Implementácia na serveri obchodníka

Požiadavky na implementáciu:

- presmerovanie na server banky nie je možné cez iframe
- obchodník môže požiadavky zasielať na nižšie uvedené URL služby CardPay metódou GET alebo POST 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.

Obchodníkovi má k dispozícii testovaciu stránku na adrese:

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

3.1. 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>
```

3.2. 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 oddelené znakom „&“ napr. *MID=9999&AMT=1234.50*

3.3. Výpočet autentifikačného kódu HMAC

Server obchodníka:

- vypočíta autentifikačný kód HMAC a pridá ho k parametrom **požiadavky** zasielanej na server banky
- vypočíta autentifikačný kód HMAC a overí vypočítanú hodnotu voči parametru HMAC v **odpovedi** zo servera banky. V prípade, že sa hodnoty nezhodujú, vyhodnotí odpoveď ako neplatnú a kontaktuje banku za účelom preverenia transakcie.

Postup výpočtu:

1. server obchodníka pripraví reťazec, ktorý je vstupom pre výpočet bezpečnostného podpisu (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)

3.3.1. Príklady

Premenné:

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

PHP

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

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
```

3.4. Overenie digitálneho podpisu ECDSA

Server obchodníka overí digitálny podpis ECDSA, ktorý sa nachádza v **odpovediach** 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-----

...
```

- server obchodníka pripraví rovnaký reťazec ako pri overení HMAC a pripojí k nemu hodnotu HMAC (prijatú alebo vypočítanú hodnotu – musia byť zhodné)
- overí digitálny podpis volaním OpenSSL funkcie (OpenSSL knižnice 1.0.0 a vyššie) 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*
 - verejný kľúč s identifikátorom zaslaným v parametri *ECDSA_KEY*

3.4.1. Príklady

Premenné:

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

Pozn.: pred samotným overením podpisu musí server obchodníka vyhodnotiť, či má k dispozícii 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())) {
```



```
} // odpověď verifikovaná
```

4. Platba cez CardPay

4.1. Identifikácia platby

Obchodník platbu označí jednoznačným identifikátorom (parameter *VS* alebo *E2E*). Tento identifikátor:

- zašle obchodník v požiadavke na platbu cez CardPay
- zašle banka obchodníkovi v odpovediach

Každá transakcia má aj jednoznačný identifikátor priradený bankou (parameter *TID*), ktorým tiež jednoznačne identifikuje platbu. Tento identifikátor je zasielaný vo všetkých odpovediach zo servera banky.

4.2. Požiadavka na realizáciu platby

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

<https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/cardpay>

4.2.1. Vstupné parametre

Názov	Popis	Pravidlá	Príklad
MID Povinný: áno Dĺžka: 3 – 5	Identifikátor obchodníka <i>Jedinečné identifikačné číslo obchodníka</i>		9999
AMT Povinný: áno Dĺžka: 1 – 12	Suma platby <i>Suma, ktorá bude pripísaná na účet obchodníka.</i>	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené bodkou	1234.50
CURR Povinný: áno Dĺžka: 3	Mena, v ktorej bude transakcia vykonaná.	Môže nadobudnúť hodnoty: 978 – EUR 203 – CZK 840 – USD 826 – GBP 348 – HUF 985 – PLN 756 – CHF 208 – DKK	978
VS Povinný: áno Dĺžka: max. 10, resp. 35	Jednoznačný identifikátor platby	Ak E2E = N : Max. dĺžka: 10 znakov Povolené znaky: 0-9 Ak E2E = Y : Max. dĺžka: 35 znakov Povolené znaky: a-zA-Z0-9/?.,:()'+- a medzera. V prípade, že obchodník použije oddeľovač „/“, banka ako KS doplní vždy hodnotu 608.	1234567890
E2E Povinný: nie	Indikuje, či je v parametri VS zadaná E2E referencia platby	Nadobúda hodnoty Y/N Y = parameter VS obsahuje E2E referenciu platby N = parameter VS obsahuje variabilný symbol Predvolená hodnota je N. V prípade hodnoty N, parameter nevstupuje do kalkulácie HMAC.	N

TXN Povinný: nie	Typ transakcie predautorizácia	Môže obsahovať iba hodnotu PA	PA '1)
RURL Povinný: áno	Návratová URL <i>URL adresa, na ktorú banka presmeruje zákazníka po vykonaní platby</i>	URL musí byť platná v súlade s RFC 1738 a musí byť funkčná	https://www.obchodnik.sk/vysledok_platby.php
IPC Povinný: áno	IP adresa klienta	IPv4 alebo IPv6 formát	1.1.1.1
NAME Povinný: áno Dĺžka: max. 64	Meno alebo mailová adresa klienta z objednávkového formulára zo stránky obchodníka	Meno nesmie obsahovať diakritiku. Povolené znaky: 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @	Peter Novak
REM Povinný: nie Dĺžka: max. 50	Emailová adresa pre zaslanie notifikácie o výsledku platby	- 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
TPAY Povinný: nie	Príznak registrácie na ComfortPay	Nadobúda hodnoty Y/N Y = registrácia na ComfortPay N (resp. iný znak ako Y) = bez registrácie na ComfortPay Predvolená hodnota je N. V prípade hodnoty N, parameter nevstupuje do kalkulácie HMAC.	Y
CID Povinný: nie Dĺžka: max. 18	ID registrácie karty(CardID) na službu ComfortPay <i>Ak príde vyplnené, tak sa ho CardPay pokúsi zaregistrovať na ComfortPay pod týmto číslom. Ak sa nepodarí zaregistrovať kartu pod týmto číslom, ComfortPay vygeneruje nové číslo a zaregistruje kartu pod ním. Pokiaľ príde nevyplnené, ComfortPay taktiež vygeneruje nové číslo a zaregistruje kartu pod ním. Card ID číslo dostane obchodník späť v odpovedi z banky.</i>	Môže byť len číselný údaj	1234

ECID Povinný: nie	ID registrovanej karty na službu ComfortPay <i>Ak je vyplnené, tak klient nemusí zadávať údaje z karty. Tie sú automaticky načítané pri zhode ECID s privátnym certifikátom vydaným obchodníkovi.</i>	ECID je poslané v requeste pre službu ComfortPay len v prípade, že transakcie registrovaných kariet sú iniciované zákazníkom (registrácia karty pre ďalší nákup na eshope). Pokiaľ sú transakcie iniciované obchodníkom (faktúry, predplatné, príspevky...), opakovaná transakcia je realizovaná cez web services a metódu popísanú vo WSDL dokumentácii. Vo formáte Base64 Hodnota parametra je výsledkom zašifrovania CID pomocou verejného kľúča obchodníka pre službu ComfortPay. Ak je vyplnené, hodnota TPAY musí byť N alebo nemôže byť vyplnená.	
TDS_CARDHOLDER Povinný: áno Dĺžka: 2 – 45	Meno držiteľa karty	Môže obsahovať 0-9, a-z, A-Z, medzera, bodka, pomlčka, podčiarkovník, zavináč (@). 2-45 alfanumerických znakov. Nesmie obsahovať diakritiku.	Peter Novak
TDS_EMAIL Povinný: áno Dĺžka: max. 254	Emailová adresa držiteľa karty	Môže obsahovať 0-9, a-z, A-Z, medzera, bodka, pomlčka, podčiarkovník, plus (+), zavináč (@). Nesmie obsahovať diakritiku. V prípade, že je vyplnený parameter TDS_MOBILE_PHONE, nie je parameter TDS_EMAIL povinný.	Peter_novak@gmail.com
TDS_MOBILE_PHONE Povinný: áno Dĺžka: max. 19	Telefónne číslo držiteľa karty	Formát: {Predvoľba}-{Telefónne číslo} Predvoľba - max. 3 numerické znaky. Telefónne číslo - max. 15 numerických znakov. V prípade, že je vyplnený parameter TDS_EMAIL, nie je parameter TDS_MOBILE_PHONE povinný.	421-911222333
TDS_BILL_CITY Povinný: nie Dĺžka: max. 50	Fakturačná adresa držiteľa karty - mesto	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Bratislava
TDS_BILL_COUNTRY Povinný: nie Dĺžka: 3	Fakturačná adresa držiteľa karty - krajina	ISO 3166-1 (číselný kód krajiny). Príklad: 703 pre Slovensko.	703
TDS_BILL_ADDRESS1 Povinný: nie Dĺžka: max. 50	Fakturačná adresa držiteľa karty - ulica	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Hlavna 1
TDS_BILL_ADDRESS2 Povinný: nie Dĺžka: max. 50	Fakturačná adresa držiteľa karty - ulica - pokračovanie	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Stare Mesto

TDS_BILL_ZIP Povinný: nie Dĺžka: max. 16	Fakturačná adresa držiteľa karty - PSČ		81106
TDS_SHIP_CITY Povinný: nie Dĺžka: max. 50	Doručovací adresa držiteľa karty - mesto	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Bratislava
TDS_SHIP_COUNTRY Povinný: nie Dĺžka: 3	Doručovací adresa držiteľa karty - krajina	ISO 3166-1 (číselný kód krajiny). Príklad: 703 pre Slovensko.	703
TDS_SHIP_ADDRESS1 Povinný: nie Dĺžka: max. 50	Doručovací adresa držiteľa karty - ulica	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Hlavná 1
TDS_SHIP_ADDRESS2 Povinný: nie Dĺžka: max. 50	Doručovací adresa držiteľa karty - ulica - pokračovanie	Môže obsahovať 0-9, a-z, A-Z, medzera, bodky, pomlčka, podčiarkovník, @. Nesmie obsahovať diakritiku.	Stare Mesto
TDS_SHIP_ZIP Povinný: nie Dĺžka: max. 16	Doručovací adresa držiteľa karty - PSČ		81106
TDS_ADDR_MATCH Povinný: nie	Zhoda fakturačnej a doručovacej adresy	Y = doručovací adresa je rovnaká ako fakturačná N = doručovací adresa je iná ako fakturačná	Y
TIMESTAMP Povinný: áno Dĺžka: 14	Timestamp (časová pečiatka) v UTC <i>Server banky spracuje iba požiadavky, ktoré budú mať TIMESTAMP v intervale +/- 1 hodina voči UTC (GMT)</i>	- musí byť vo formáte DDMMYYYYHHMISS (DD-deň, MM-mesiac, YYYY-rok, HH- hodina, MI-minúta, SS-sekunda)	01092014125505
HMAC Povinný: áno Dĺžka: 64	Autentifikačný kód HMAC z parametrov: MID + AMT + CURR + VS + E2E + TXN + RURL + IPC + NAME + REM + TPAY + CID + ECID + TDS_CARDHOLDER + TDS_EMAIL + TDS_MOBILE_PHONE + TDS_BILL_CITY + TDS_BILL_COUNTRY + TDS_BILL_ADDRESS1 + TDS_BILL_ADDRESS2 + TDS_BILL_ZIP + TDS_SHIP_CITY + TDS_SHIP_COUNTRY + TDS_SHIP_ADDRESS1 + TDS_SHIP_ADDRESS2 + TDS_SHIP_ZIP + TDS_ADDR_MATCH + TIMESTAMP	- platné znaky: 0-9 a-f	880aeb78ffd892b 2658c9f0c739830 739c9cde0d0cd6c e4f7d4f331341bd da56

AREDIR Povinný: nie	Príznak automatického presmerovania na stránku obchodníka (RURL) po 9-tich sekundách.	- platné hodnoty: 1, 0 - 0 (predvolená): vypnuté t. j. zákazník musí stlačiť tlačidlo „Pokračovať“ - 1: zapnuté	1
LANG Povinný: nie Dĺžka: 2	Kód jazyka, v ktorom bude zobrazená aplikácia CardPay	- platné hodnoty: 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	de

*) V prípade, že obchodník realizuje transakciu typu PREDAUTORIZÁCIA pre účely registrácie karty pre službu ComfortPay, transakcia nebude zúčtovaná a držiteľovi karty ju banka držiteľa karty do pár dní uvoľní. Neodporúčame realizovať následné storno tohto typu transakcie. Dôvodom je autorizačná správa, ktorá obsahuje všetky informácie o budúcej opakovanej platbe. Existuje riziko, že v rámci storna transakcie banka zákazníka tieto informácie neuchová.

Výpočet hodnoty ECID

Pre výpočet hodnoty ECID je možné použiť napr. OpenSSL knižnicu. Nasledujúci príklad vráti hodnotu ECID pre CID 123456.

```
printf "123456" | openssl rsautl -encrypt -pubin -inkey teleplatba.public_key \
-oaep | openssl enc -e -base64
```

4.2.2. Odpoveď na požiadavku na realizáciu platby

V prípade, že je požiadavka platná a služba CardPay je dostupná, zákazníkovi sa zobrazí aplikácia CardPay, prostredníctvom ktorej môže potvrdiť platbu.

Po potvrdení platby sa zákazníkovi zobrazí jedno z hlásení:

hlásenie	Hodnota parametra RES	Popis
<i>Vaša platba bola úspešne spracovaná.</i>	OK	Platba prebehla úspešne.
<i>Vaša platba nebola vykonaná.</i>	FAIL	Nastala chyba pri spracovaní platby.

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

chybové hlásenie	Popis
<i>Platbu nemožno uskutočniť z dôvodu neplatného bezpečnostného podpisu.</i>	Neplatný MID, neplatný bezpečnostný podpis, MID nemá oprávnenie na požadovanú službu.
<i>Niektorý z požadovaných parametrov nebol zadaný alebo bol nesprávne zadaný.</i>	Niektorý zo vstupných parametrov má neplatnú hodnotu.
<i>Požiadavka nie je platná (neplatný TIMESTAMP).</i>	Parameter TIMESTAMP nie je v povolenej tolerancii.
<i>Obchodník nemá oprávnenie pre požadovanú službu.</i>	Obchodník nemá požadovanú službu aktivovanú.

4.3. Overenie výsledku platby (a registrácie na službu ComfortPay)

Výsledok platby vykonanej cez službu CardPay môže byť:

- **OK** - platba prebehla úspešne
- **FAIL** - platba neprebehla

Výsledok registrácie na službu ComfortPay môže byť:

- **OK** - registrácia prebehla úspešne
- **FAIL** - registrácia nebola úspešná

Obchodník si môže **overiť výsledok** platby (a prípadne výsledok registrácie na službu ComfortPay) týmito spôsobmi:

1. kontrolou parametrov v návratovej URL
2. kontrolou notifikačného emailu (pokiaľ bol vyplnený parameter REM v požiadavke)
3. online dopytom na server banky
(viď kap. 5. Overenie stavov platieb vykonaných cez CardPay)

4.3.1. Návratová URL

Aplikácia CardPay zobrazí zákazníkovi výsledok platby.

V prípade, že zákazník nezatvorí okno prehliadača a stlačí tlačidlo *Pokračovať*, bude presmerovaný na URL stránky obchodníka (zaslanú vo vstupnom parametri RURL). Návratová URL obsahuje parametre, prostredníctvom ktorých môže server obchodníka overiť stav platby.

Názov	Popis	Pravidlá	Príklad
AMT Povinný: áno Dĺžka: 1 – 12	Suma platby zaslaná v požiadavke	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené <u>bodkou</u>	1234.50
CURR Povinný: áno Dĺžka: 3	Mena platby zaslaná v požiadavke.	Môže nadobudnúť hodnoty: 978 – EUR 203 – CZK 840 – USD 826 – GBP 348 – HUF 985 – PLN 756 – CHF 208 – DKK	978
VS Povinný: áno Dĺžka: max. 35	Identifikátor platby na strane obchodníka	Viď kapitola 4.2.1. Vstupné parametre.	1234567890
TXN Povinný: nie	Typ transakcie predautorizácia. (v odpovedi je posielaný iba v prípade transakcie s typom predautorizácia)	Môže obsahovať iba hodnotu PA	PA

RES Povinný: áno	Kód výsledku platby	OK - platba prebehla úspešne FAIL - platba nebola úspešná alebo zákazník ju zrušil	OK
AC Povinný: nie Dĺžka: max. 6	Approval code (v odpovedi je posielaný iba v prípade úspešnej transakcie)	Povolené znaky: 0-9, A-Z, medzera	12AH24
TRES Povinný: nie	Výsledok registrácie na službu ComfortPay	OK - registrácia prebehla úspešne FAIL - registrácia nebola úspešná	OK
CID Povinný: nie	Identifikátor karty (CardID) na službu ComfortPay.	Celé číslo	1234
CC Povinný: nie Dĺžka: max. 19	maskované číslo karty Posielanie parametra musí byť povolené v konfigurácii obchodníka na strane banky.		433704*****000
RC Povinný: nie Dĺžka: 2 - 3	kód chyby (response code) Posielanie parametra musí byť povolené v konfigurácii obchodníka na strane banky.	dvojnakový kód - alfanumerický kód z výsledku autorizácie, ak transakcia bola odoslaná na autorizáciu; alebo trojnakový kód : FDS - ak transakcia zlyhala pri overení vo Fraud detection systéme; TDS - ak transakcia zlyhala pri 3D Secure overení; SYS - ak pri spracovaní transakcie nastala systémová chyba.	05
TID Povinný: nie	Jednoznačný identifikátor platby na strane banky. Pomocou tohto identifikátora je možné jednoducho opakovane overiť stav platby prostredníctvom rozhrania popísaného v kapitole 6. Overenie stavov platieb vykonaných cez CardPay. Parameter sa v odpovedi nachádza, pokiaľ je výsledok platby OK. V prípade výsledku FAIL je prítomný iba vtedy, ak bola požiadavka platná, zákazník zadal údaje z karty a potvrdil platbu.	Celé číslo	65487

TIMESTAMP Povinný: áno Dĺžka: 14	Timestamp zaslaný v požiadavke	- musí byť vo formáte DDMMYYYYHHMISS (DD-deň, MM-mesiac, YYYY-rok, HH-hodina, MI-minúta, SS-sekunda)	01092014125505
HMAC Povinný: áno Dĺžka: 64	Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov: AMT + CURR + VS + TXN + RES + AC + TRES + CID + CC + RC + TID + TIMESTAMP		880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56
ECDSA_KEY Povinný: áno	Identifikátor verejného kľúča, ktorým je možné overiť digitálny podpis odpovede v parametri ECDSA	Celé číslo	1
ECDSA Povinný: áno	Reťazcom pre výpočet ECDSA je reťazec hodnôt parametrov: AMT + CURR + VS + TXN + RES + AC + TRES + CID + CC + RC + TID + TIMESTAMP + HMAC		304502201fb6e376a6b7bb8fe34d931e5e4 09721c80fb481710dac947cf913a6a3f98f5e 022100f1f3066ce4a87cd139742edcd15bdb 0c100ccbd7b524e6a1a866d81c273472f7

Príklad – štandardná platba

https://www.obchodnik.sk/potvrdenie_platby.php?

AMT=100.00

&CURR=978

&VS=123456

&RES=OK

&AC=635594

&TID=1971

&TIMESTAMP=16092014132529

&HMAC= 59de38dac3c266998eee82d4b98388ba473fa66b326426a430bd5631e4d6bbdf

&ECDSA_KEY=1

&ECDSA=3046022100b88c4dcc3c74c8b3dac09a324f62f29c8d32bb4da8e6f73847d4ebf77ef23ddf022100bceaa33941554f1f0dae4115572ea1398730deee4ec0f88309aff778122484b5

Príklad – predautorizácia s registráciou na službu ComfortPay

```
https://www.obchodnik.sk/potvrdenie_platby.php?
AMT=100.00
&CURR=978
&VS=123456
&TXN=PA
&RES=OK
&AC=635594
&TRES=OK
&CID=987654
&TID=65487
&TIMESTAMP=16092014132529
&HMAC= 961b3efed74477375e8f109e3ca176fda1b1e42b6f227c132782e22bb068987b
&ECDSA_KEY=1
&ECDSA=3046022100b88c4dcc3c74c8b3dac09a324f62f29c8d32bb4da8e6f73847d4ebf77ef23ddf022100bceaa33
941554f1f0dae4115572ea1398730deee4ec0f88309aff778122484b5
```

Zoznam a popis response kódov (parameter RC)



response
kody_CP.XLS

4.3.2. Notifikačný email

Server banky odošle notifikačný email na adresu uvedenú v parametri REM.

Telo emailu obsahuje reťazec parametrov, rovnakých ako návratová URL, v rovnakom poradí:

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

Príklad – štandardná platba (telo emailu)

```
AMT=100.00 CURR=978 VS=123456 RES=OK AC=635594 TID=65487 TIMESTAMP=16092014132529
HMAC=1cf1f64ec3a6d233076e612a6703ce82ccf053e3d1eaa52f77ebb1ddd20874bb ECDSA_KEY=1
ECDSA=30450220542b6fb79ee071f9db6d6dac351b86052f7bab23e5ec0a5c492fbff0e3eba379022100c1eea569bf
f7b31ecb3f0be476c8e16f27071bfabc5d7e858f349ecd9b24e60d
```

4.4. Ukončenie a storno predautorizácie / návrat platby

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

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

Požiadavka musí obsahovať kód operácie, ktorá má byť vykonaná nad platbou:

- **CPA** (close preauthorization) – ukončenie predautorizácie
- **SPA** (storno preauthorization) – storno predautorizácie
- **CB** (chargeback) – návrat platby

Ukončenie a storno predautorizácie (CPA / SPA) je možné vykonať iba nad predautorizáciami (stav platby je PA).

Návrat platby je (CB) je možné vykonať iba nad úspešnými platbami, vrátane ukončených predautorizácií (stav platby je OK alebo CPA)) a taktiež nad platbami, nad ktorými už bol vykonaný návrat (stav platby je CB), pričom suma návratov nesmie prekročiť pôvodnú výšku platby (v prípade predautorizácie je to suma, s ktorou bola predautorizácia potvrdená).

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

4.4.1. Vstupné parametre

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
MID	áno	Identifikátor obchodníka <i>Jedinečné identifikačné číslo obchodníka</i>	3 - 5		9999
AMT	áno, pokiaľ TXN = CPA / CB	Suma platby pre ukončenie predautorizácie alebo návratu <i>Pozn.: v prípade storna (TXN = SPA) je parameter ignorovaný.</i>	9 + 2	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené <u>bodkou</u> - pre CPA musí byť rovnaká alebo menšia ako suma predautorizácie - pre CB musí byť rovnaká alebo menšia ako suma pôvodnej transakcie, resp. rovnaká alebo menšia ako rozdiel medzi sumou už vykonaných návratov a pôvodnou výškou platby (v prípade predautorizácie je to suma s ktorou bola predautorizácia potvrdená)	1234.50
TID	áno *	Identifikátor platby (vygenerovaný bankou)		- povolené znaky: 0-9	65487
VS	áno *	Identifikátor platby (vygenerovaný obchodníkom)	max. 35	- povolené znaky: a-zA-Z0-9/?.,:()'+- a medzera	1234567890
TXN	áno	Typ operácie: CPA = ukončenie predautorizácie SPA = storno predautorizácie CB = návrat platby	-	- hodnoty: CPA = ukončenie predautorizácie SPA = storno predautorizácie CB = návrat platby	CPA

REM	nie	Emailová adresa pre zaslanie notifikácie	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 <i>Server banky spracuje iba požiadavky, ktoré budú mať TIMESTAMP v intervale +/- 1 hodina voči UTC (GMT)</i>	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: MID + AMT + TID + VS + TXN + REM + TIMESTAMP	64	- platné znaky: 0-9 a-f	880aeb78ffd892b2658c9f0c739830739c9cde0d0cd6ce4f7d4f331341bdda56

* povinný je práve jeden z parametrov VS, TID. Pokiaľ budú vyplnené oba, VS bude ignorovaný

4.4.2. Odpoveď

Odpoveď servera banky je forme XML dokumentu.

XML schéma je dostupná na URL adrese:

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/xsd/TxnProcess_2.0.xsd

XML dokument obsahuje tieto elementy:

Názov elementu	Popis
cardpay	hlavný element, obsahuje elementy <i>request</i> a <i>result</i>
request	vstupné parametre zaslané serverom obchodníka
mid	identifikátor obchodníka
amt	suma (iba pre CPA a CHCB)
tid	identifikátor platby TID (pokiaľ bol zaslaný v požiadavke)
vs	identifikátor platby VS (pokiaľ bol zaslaný v požiadavke)
txn	požadovaný typ operácie
timestamp	časová pečiatka požiadavky
result	odpoveď, obsahuje element <i>res</i> a v prípade chyby aj element <i>errorCode</i> .
res	výsledok, môže nadobudnúť hodnoty <i>OK</i> , <i>FAIL</i>
errorCode	číselný kód chyby (v prípade chyby)

Overenie HMAC

Reťazcom pre výpočet HMAC je XML dokument t.j. celé telo HTTP odpovede. HMAC sa nachádza v HTTP hlavičke, v elemente *Authorization*, pod kľúčom *HMAC*.

Overenie ECDSA

Reťazcom pre kontrolu ECDSA je XML dokument + HMAC. ECDSA sa nachádza v HTTP hlavičke, v elemente *Authorization*, pod kľúčom *ECDSA*. Identifikátor verejného kľúča sa nachádza v HTTP hlavičke, v elemente *Authorization*, pod kľúčom *ECDSA_KEY*.

Príklad

Telo HTTP odpovede – XML dokument

```
<?xml version="1.0" encoding="windows-1250"?>
<cardpay>
  <request>
    <mid>9999</mid>
    <amt>100.00</amt>
    <tid>831</tid>
    <txn>CPA</txn>
    <timestamp>16092014135559</timestamp>
  </request>

  <result>
    <res>OK</res>
  </result>
</cardpay>
```

HTTP hlavička obsahuje aj:

Authorization: HMAC=ad8f434dcbfde19ae3a8de85be540301cd839d35c2d8ba945823f18b20fcc277,
ECDSA=3046022100a4e5491ab9376f8cd9e51c176f5e75bb3664e3f852e901d36ac0a5b0f2177fad0221008794e59a
b8027c68ae74ea65d0f5b5913865db9a818044d06c114f4d84346f48, ECDSA_KEY=1

4.4.3. Číselník chýb

Kód chyby	Popis chyby
10	Neplatný identifikátor obchodníka alebo bezpečnostný podpis
11	Chýba niektorý povinný parameter.
3	Neplatná suma (AMT)
4	Neplatný variabilný symbol (VS)
9	Neplatná operácia (TXN)
15	Neplatná časová pečiatka (TIMESTAMP)
16	Nesprávny identifikátor transakcie t.j. pre zadaný VS / TID nebola nájdená žiadna transakcia
18	Nejednoznačný identifikátor transakcie (VS) t.j. existuje viacero transakcií pre daný VS s platným stavom
19	Nesprávna suma: - pre CPA musí byť menšia alebo rovná sume predautorizácie - pre CB musí platiť, že suma všetkých CB operácií musí byť menšia alebo rovná sume pôvodnej transakcie (pre CPA suma potvrdenej predautorizácie)
20	Návrat (CB) po viac ako 366 dňoch t.j. rozdiel medzi TIMESTAMP a: - dátumom vytvorenia platby <i>resp.</i> - dátumom vytvorenia predautorizácie (pre predautorizácie) je viac ako 366 dní.
13	Iná chyba

4.4.4. Notifikačný email

Server banky odošle notifikačný email na adresu uvedenú v parametri REM (okrem kódu chyby 10).

Telo emailu obsahuje parametre rovnaké, analogicky ako v XML odpovedi:

1. AMT ** pre CPA a CB*
2. TID ** pokiaľ bol zaslaný v požiadavke*
3. VS ** pokiaľ bol zaslaný v požiadavke*
4. TXN
5. RES
6. ERROR_CODE ** pokiaľ nastala chyba*
7. TIMESTAMP
8. HMAC
9. ECDSA_KEY
10. ECDSA

Platí:

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

Overenie HMAC

Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov:

AMT + TID + VS + TXN + RES + ERROR_CODE + TIMESTAMP

Overenie ECDSA

Reťazcom pre výpočet HMAC je reťazec hodnôt parametrov:

AMT + TID + VS + TXN + RES + ERROR_CODE + TIMESTAMP + HMAC

Príklad

```
AMT=100.00 TID=831 TXN=CPA RES=OK TIMESTAMP=16092014135559
HMAC=5f1ce5fe71f2a28a32469e0d67cb432db38a30d045c55084658b6b2388dac58d ECDSA_KEY=1
ECDSA=3046022100a4e5491ab9376f8cd9e51c176f5e75bb3664e3f852e901d36ac0a5b0f2177fad0221008794e59a
b8027c68ae74ea65d0f5b5913865db9a818044d06c114f4d84346f48
```

4.5. Príklad priebehu platby cez CardPay

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):
3132333435363738393031323334353637383930313233343536373839303132313233343536373839
3031323334353637383930313233343536373839303132

Zákazník zvolí platbu cez CardPay.

1. server obchodníka pripraví vstupné parametre:

```
MID = 9999
AMT = 20.78
```

```
CURR = 978
VS = 78945210
RURL = https://www.obchodnik.sk/potvrdenie_platby.php
IPC = 188.200.192.180
NAME = Peter Novak
REM = online_platby@obchodnik.sk
TIMESTAMP = 01112014100000 (pozor, dátum a čas musí byť UTC !)
```

2. server obchodníka zostaví reťazec pre výpočet autentifikačného kódu HMAC

```
HMAC_STRING = MID + AMT + CURR + VS + RURL + IPC + NAME + REM + TIMESTAMP =
999920.7897878945210https://www.obchodnik.sk/potvrdenie_platby.php188.200.192
.180Peter Novakonline_platby@obchodnik.sk01112014100000
```

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/cardpay?MID=9999&AMT=20.78&CURR=978&VS=78945210&RURL=http%3A%2F%2Fwww.obchodnik.sk%2Fpotvrdenie_platby.php&IPC=188.200.192.180&NAME=Peter%20Novak&REM=online_platby%40obchodnik.sk&TIMESTAMP=01112014100000&HMAC=299fc84ee60e39c4befd933d2c898894282d77a2b0551f9d9107641af6454619
```

5. server obchodníka presmeruje zákazníka na URL

6. zákazník zadá údaje z karty v aplikácii CardPay a potvrdí platbu

7. server banky odošle notifikačný email s obsahom

```
AMT=20.78 CURR=978 VS=78945210 RES=OK AC=832 TID=45678
TIMESTAMP=01112014100000
HMAC=8c5e4fb2be2b6cd2693fb0c057a4983f2b496b4a3fd8a25dd76248f9fd9b95e8
ECDSA_KEY=1
ECDSA=304502201fb6e376a6b7bb8fe34d931e5e409721c80fb481710dac947cf913a6a3f98f5e022100f1f3066ce4a87cd139742edcd15bdb0c100ccbd7b524e6a1a866d81c273472f7
```

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&AC=832&TID=45678&TIMESTAMP=01112014100000&HMAC=9fbf5a7d1a914d7806a545565b971fa480feb48e402f7a8df80dcea0fdea6049&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 + AC + TID + TIMESTAMP =`
`20.7897878945210OK8324567801112014100000`
- vypočíta HMAC:
`HMAC_CHECK = hash_hmac('sha256', HMAC_STRING, SECURITY_KEY) =`
`9fbf5a7d1a914d7806a545565b971fa480feb48e402f7a8df80dcea0fdea6049`
- porovná vypočítaný autentifikačný kód 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 + AC + TID + TIMESTAMP + HMAC =`
`20.7897878945210OK83245678011120141000009fbf5a7d1a914d7806a545565b971fa480feb48e402f7a8df80dcea0fdea6049`

- stiahne verejný kľúč s identifikátorom ECDSA_KEY zo servera banky (z definovanej URL)
- overí digitálny podpis. **Overenie digitálneho podpisu musí byť úspešné !**
`openssl_verify(ECDSA_STRING, ECDSA, PUBLIC_KEY, 'sha256')`

5. Overenie stavov platieb vykonaných cez CardPay

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

https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/cardpay_txn/v2/

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

5.1. Vstupné parametre

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

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
MID	áno	Identifikátor obchodníka <i>Jedinečné identifikačné číslo obchodníka</i>	3 - 5		9999
VS	nie	Identifikátor platby	max. 35	povolené znaky: a-zA-Z0-9/?.,:()'+- a medzera	1234567890
TID	nie	Identifikátor platby	-		125105
PA	nie	Filter podľa predautorizácie: - Y: iba transakcie s predautorizáciou - N: iba transakcie bez predautorizácie	1	hodnoty: Y, N	Y
TS_FROM	nie	Timestamp transakcie OD - DO	14	vo formáte DDMMYYYYHHMISS (DD-deň, MM- mesiac, YYYY-rok, HH- hodina, MI-minúta, SS-sekunda)	12092014100 000
TS_TO		<u>Pre predautorizované transakcie</u> platí: transakcia spĺňa toto kritérium, pokiaľ ho spĺňa timestamp vytvorenia predautorizácie ALEBO timestamp jej ukončenia / stornovania			
AMT_FROM	nie	Suma OD – DO	max. 9 + 2	- desatinné číslo - max. 9 miest pred oddeľovačom desatín - max. 2 desatinné miesta oddelené <u>bodkou</u>	1234.50
AMT_TO		<u>Pre predautorizované transakcie</u> platí: transakcia spĺňa toto kritérium, pokiaľ ho spĺňa suma predautorizácie ALEBO suma ukončenia predautorizácie			
STATUS	nie	Filter podľa stavu transakcie: OK – iba úspešne spracované transakcie FAIL – iba neúspešné transakcie PA – iba predautorizácie CPA – iba ukončené predautorizácie SPA – iba stornované predautorizácie XPA – iba exspirované predautorizácie CB – iba vrátené platby	max. 4	hodnoty: OK, FAIL, PA, CPA, SPA, XPA, CB	OK
TPAY	nie	Filter podľa registrácie pre službu ComfortPay:			

		- Y : iba transakcie s registráciou na ComfortPay - N : iba transakcie bez registrácie na ComfortPay			
CID	nie	ID registrácie karty(CardID) na službu ComfortPay	max. 18	povolené znaky: 0-9	1234
TPAY_STATUS	nie	Filter podľa stavu registrácie pre službu ComfortPay: OK – iba úspešné registrácie FAIL – iba neúspešné registrácie	max. 4	hodnoty: OK, FAIL	FAIL
HMAC	áno	Autentifikačný kód HMAC z vyššie uvedených hodnôt parametrov, v uvedenom poradí.	64	- platné znaky: 0-9 a-f	880aeb78ffd8 92b2658c9f0c 739830739c9 cde0d0cd6ce4 f7d4f331341b dda56

5.2. Odpoveď

Odpoveď obsahuje max. 100 transakcií, ktoré sú zoradené podľa TID zostupne.

Transakcie s výsledkom **FAIL** sa nachádzajú v zozname iba vtedy, ak bola požiadavka platná, zákazník zadal údaje z karty a potvrdil transakciu. Preto je potrebné neprítomnosť transakcie v zozname interpretovať ako transakciu s výsledkom **FAIL**.

XML schéma je dostupná na URL adrese:

<https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/xsd/GetCardPayTransactionsResponse.xsd>

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

Názov elementu	Popis
GetCardPayTransactionsResponse	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 transakcií (0 až 100)
transaction	element transakcie, popísaný v nasledujúcej tabuľke

Transakcia obsahuje tieto elementy:

Názov elementu	Popis
id	jednoznačný identifikátor transakcie na strane banky (TID)
amount	suma transakcie <u>Pre predautorizované transakcie</u> je vyplnená iba v stave CPA.
currency	mena transakcie
vs	jednoznačný identifikátor na strane obchodníka
ac	approval code
timestamp	timestamp vytvorenia transakcie vo formáte

	DDMMYYYYHHMISS <u>Pre predautorizované transakcie</u> je vyplnený iba v stave CPA / SPA.
status	Jedna z hodnôt: OK – úspešne spracovaná transakcia FAIL – neúspešná transakcia <u>Pre predautorizované transakcie:</u> PA – predautorizácia CPA – ukončená predautorizácia SPA – stornovaná predautorizácia XPA – exspirovaná predautorizácia Pre transakciu s návratom: CB – nad transakciou bol vykonaný aspoň jeden návrat <i>Pozn.: predautorizované transakcie majú pri vytvorení status PA. Do stavu CPA / SPA sa dostanú po <u>úspešnom</u> ukončení / storne predautorizácie. V prípade neúspešného ukončenia / storna zostávajú v stave PA.</i>
preauthorization	element obsahujú iba predautorizované transakcie
amount	suma predautorizácie
timestamp	timestamp vytvorenia predautorizácie vo formáte DDMMYYYYHHMISS
comfortpay	element obsahujú iba transakcie s registráciou pre službu ComfortPay
cid	ID registrácie karty na službu ComfortPay
status	stav registrácie pre službu ComfortPay: OK – úspešná registrácia FAIL – neúspešná registrácia
chargeback	
amount	suma návratov nad pôvodnou transakciou
timestamp	timestamp realizácie posledného návratu vo formáte DDMMYYYYHHMISS
cardNumber	maskované číslo karty <i>Posielanie parametra musí byť povolené v konfigurácii obchodníka na strane banky.</i>
rc	kód chyby (response code) dvojznakový kód – kód z výsledku autorizácie, ak transakcia bola odoslaná na autorizáciu; FDS – ak transakcia zlyhala pri overení vo Fraud detection systéme; TDS – ak transakcia zlyhala pri 3D Secure overení; SYS – ak pri spracovaní transakcie nastala systémová chyba. <i>Posielanie parametra musí byť povolené v konfigurácii obchodníka na strane banky.</i>

Príklad

Telo HTTP odpovede – XML dokument

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

  <transactions>
    <transaction>
      <id>123456</id>
      <amount>100.10</amount>
      <currency>978</currency>
      <vs>123456</vs>
      <ac>654654</ac>
      <timestamp>12092014113931</timestamp>
      <status>OK</status>

      <preauthorization>
        <amount />
        <timestamp />
      </preauthorization>

      <comfortpay>
        <cid>9885475</cid>
        <status>OK</status>
      </comfortpay>
    </transaction>

    <transaction>
      <id>234567</id>
      <amount>50.10</amount>
      <currency>978</currency>
      <vs>8854521</vs>
      <ac/>
      <timestamp>12092014113931</timestamp>
      <status>CPA</status>

      <preauthorization>
        <amount>100.00</amount>
        <timestamp>12092014113931</timestamp>
      </preauthorization>

      <comfortpay>
        <cid />
        <status />
      </comfortpay>
    </transaction>
  </transactions>
</GetCardPayTransactionsResponse>
```

HTTP hlavička obsahuje aj:

Authorization: HMAC=ad8f434dcbfde19ae3a8de85be540301cd839d35c2d8ba945823f18b20fcc277, ECDSA=3046022100a4e5491ab9376f8cd9e51c176f5e75bb3664e3f852e901d36ac0a5b0f2177fad0221008794e59ab8027c68ae74ea65d0f5b5913865db9a818044d06c114f4d84346f48, ECDSA_KEY=1

5.2.1. Odpoveď v prípade chyby

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

Číselník chýb:

Kód chyby	Popis chyby
1	Neplatný identifikátor obchodníka alebo bezpečnostný podpis
2	Chyba vstupného parametra
9	Iná chyba Chyba vstupného parametra

5.3. Zobrazenie platobnej brány v mobilnej aplikácii

Platobnú bránu CardPay je možné zobraziť aj priamo v mobilnej aplikácii obchodníka, bez potreby otvárania aplikácie internetového prehliadača. Pre správne fungovanie platobných metód Apple Pay a Google Pay je však potrebné použiť pri zobrazení platobnej brány technológie, ktoré na danej platforme zaručia správnu funkčnosť týchto platobných metód.

V nasledujúcich kapitolách uvádzame príklady implementácie zobrazenia platobnej brány CardPay priamo v mobilnej aplikácii, pri ktorej sú spomínané platobné metódy funkčné.

5.3.1. Referenčná implementácia iOS

V prípade, že chce obchodník zobraziť platobnú bránu CardPay v rámci svojej mobilnej aplikácie pre platformu iOS, musí pre správne fungovanie Apple Pay použiť pre zobrazenie platobnej brány **SFSafariViewController**.

```
let urlString = "URL_ADRESA_Z_KTOREJ_DOJDE_K_PRESMEROVANIU_NA_BRANU"
if let url = URL(string: urlString) {
    let vc = SFSafariViewController(
        url: url,
        configuration: SFSafariViewController.Configuration()
    )

    self?.present(vc, animated: true)
}
```

Pre viac informácií viď https://developer.apple.com/documentation/apple_pay_on_the_web.

5.3.2. Referenčná implementácia Android

V prípade, že chce obchodník zobraziť platobnú bránu CardPay v rámci svojej mobilnej aplikácie pre platformu Android, musí pre správne fungovanie Google Pay použiť pre zobrazenie platobnej brány technológiu **Chrome Tabs**.

```
val url = "URL_ADRESA_Z_KTOREJ_DOJDE_K_PRESMEROVANIU_NA_BRANU"
val customTabsIntent = CustomTabsIntent.Builder().apply {
    setShowTitle(true)
    setShareState(CustomTabsIntent.SHARE_STATE_OFF)
    setInstantAppsEnabled(false)
}.build()
customTabsIntent.launchUrl(this, Uri.parse(url))
```