



**a-sms, s.r.o.**  
Sulekova 70  
811 03 Bratislava

## **myPAY online API**

verzia 2.4

# 1. Úvod

Účelom tohto dokumentu je popísať komunikáciu medzi serverom obchodníka a platobným systémom MyPay.

## 2. Realizácia platby

- 2.1. Zákazník je presmerovaný pomocou webového formuláru na stránke obchodníka na platobnú stránku systému myPAY.
- 2.2. Na platobnej stránke systému myPAY zákazník vykoná platbu odoslaním SMS na zobrazené číslo s unikátnym SMS kódom ako text správy. Platba je potvrdená odoslaním SMS a úspešným spoplatnením zákazníka. Zákazník môže platbu zrušiť.
- 2.3. Úspešná alebo neúspešná platba je zobrazená ako informácia na webovej stránke systému myPAY.
- 2.4. Systém myPAY následne presmeruje zákazníka na stránku obchodníka.

### **3. Technické parametre prepojenia (API)**

#### **Smer Obchodník -> myPAY**

Web stránka obchodníka zabezpečí odovzdanie parametrov platby platobnému systému MyPay po zvolení takého druhu platby zákazníkom. Parametre budú prenášané HTTPS dopytom metódou 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.

URL adresa systému myPAY pre platbu: TBD

Pre testovacie rozhranie: TBD

SMS kód je platný 10 minút. Následne je zákazník presmerovaný na stránku obchodníka so statusom FAIL.

Parameter	Názov	Popis	Počet znakov	Pravidlá	Príklad
CID	Client ID	Unikátny identifikátor klienta	-	Max. 32 alfanumerických znakov	12345ABC
AMT	Amount	Suma spoplatnenia v EUR	3+2	Iba hodnoty explicitne povolené pre klienta. Max. dve desatinné miesta oddelené bodkou	2.49
VS	Variabilný symbol	Jednoznačný identifikátor platby pre klienta	Max. 10	Len kladný číselný údaj	1234567890
RURL	Return URL	Návratová URL adresa na ktorú systém myPAY presmeruje zákazníka po vykonaní platby	-	URL musí byť funkčná Nesmie obsahovať query string znaky Musí obsahovať protokol (http/https)	http://www.mypay.sk
COUNTRY	Kód krajiny	Kód krajiny pre platbu	Max. 3	SK alebo CZ	SK
SIGN	Bezpečnostný podpis	Bezpečnostný podpis zložený z predchádzajúcich parametrov	40	Písmená musia byť veľkým písmom	7660A6EE64 534E44DB82 AAB6222A15 5AF2B84BA6
MSG	SMS Message	Text odpovednej SMS správy	Max. 160	Znaky bez diakritiky	Dakujeme za platbu.

Všetky parametre okrem COUNTRY a MSG sú povinné. Ak si obchodník vytvára sám texty odpovedných SMS správ, potom je potrebné vyplniť aj parameter MSG (text musí byť schválený). Implicitná hodnota parametra COUNTRY je SK.

Parameter CID a Bezpečnostný kľúč pre tvorbu SIGN budú vopred pridelené.

## **Smer myPAY -> Obchodník**

System myPAY po ukončení platby zabezpečí presmerovanie zákazníka na webové stránky obchodníka na URL z parametra rurl. K tejto URL sa pridajú parametre VS, MSISDN, RES a SIGN.

VS – variabilný symbol zadaný obchodníkom

MSISDN – telefónne číslo zákazníka (len pri úspešnej platbe)

RES – výsledok spracovania transakcie, môže nadobúdať dve hodnoty

OK – úspešná transakcia

FAIL – neúspešná transakcia

SIGN – bezpečnostný podpis vytvorený z parametrov VS, MSISDN a RES

Obchodník musí vytvoriť vlastný SIGN na svojej strane a porovnať ho s tým v requeste. Parametre sa musia zhodovať.

## 4. Bezpečnostný podpis

Každému obchodníkovi bude vygenerovaný 8 bajtový bezpečnostný kľúč (reťazec), napr. ABCDEFGH.

Parameter SIGN pre komunikáciu sa vygeneruje nasledovným spôsobom:

1. Vytvorí sa reťazec pre šifrovanie:
  - Komunikácia obchodník -> myPAY – zreťazením parametrov CID, AMT, VS, RURL, COUNTRY (len ak je prítomné v parametroch) a MSG (len ak je prítomné v parametroch).
  - Komunikácia myPAY -> obchodník – zreťazením parametrov VS, MSISDN RES v prípade úspešnej transakcie, a VS, RES v prípade neúspešnej transakcie
2. Z reťazca vytvoríte hash algoritmom HMAC SHA1 pomocou kľúča
3. Znaky hashu prevedťe na veľké písmená

Bezpečnostný podpis sa zadáva do správy ako hodnota parametra SIGN.

Systém myPAY po prijatí správy vytvorí z tých istých parametrov rovnakým spôsobom kontrolný bezpečnostný podpis a porovná sa s hodnotou parametra SIGN.

Platba sa zrealizuje len v prípade rovnosti bezpečnostných podpisov.

### Zoznam chybových kódov:

<b>Kód</b>	<b>Popis</b>
1010	CID neexistuje
1020	Cenová hladina nie je povolená pre dané CID
1030	SIGN sa nezhodujú
2000	DB error
Ostatné	Chyba systému, report chyby administrátorovi systému myPAY

## Funkcie v jazyku PHP pre výpočet parametra SIGN:

```
<?php
/*
 * CID, AMT, VS, RURL, COUNTRY, MSG - parametre
 * PWD - sifrovaci kluc
 */
function CalculateSIGN ($PWD , $CID, $AMT, $VS, $RURL, $COUNTRY="", $MSG =
"")
{
    $data = $CID . $AMT . $VS . $RURL . $COUNTRY . $MSG;
    return strtoupper( hash_hmac('SHA1', $data, $PWD) );
}
```

```
<?php
/*
 * VS, MSISDN, RES - parametre
 * PWD - sifrovaci kluc
 */
function CalculateSIGN ($VS , $MSISDN="", $RES) {
    $data = $VS . $MSISDN . $RES;
    return strtoupper( hash_hmac('SHA1', $data, $PWD) );
}
```