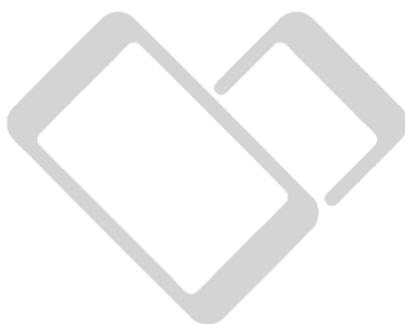




Platby obchodníkom za tovar / služby cez VIAMO

INTEGRAČNÁ PRÍRUČKA

Verzia / Február 2016

www.viamo.sk / info@viamo.sk

Obsah

1	Úvod	4
2	Firemný profil obchodníka	5
3	Inicializácia platby obchodníkovi z pohľadu používateľa	6
3.1	Platba z QR kódu	7
3.2	Platba z webovej stránky obchodníka / v eshope	8
3.2.1	Platba z webovej stránky zobrazenej na počítači	8
3.2.2	Platba z webovej stránky zobrazenej na mobilnom zariadení	9
3.3	Platba z mobilnej aplikácie obchodníka	10
3.4	Platba zo zoznamu vo VIAMO aplikácii	11
3.5	Platba zo skrátenej linky	12
4	Inicializácia platby z technického hľadiska	13
4.1	RequestString	13
4.1.1	Editovateľnosť parametrov	16
4.1.2	Vytvorenie podpisu RequestStringu	17
4.1.3	Kontrola podpisu RequestStringu	18
4.2	Generovanie QR kódu	19
4.2.1	Generovanie QR kódu pre kamenný obchod / kaviareň	19
4.2.2	Generovanie QR kódu pre eshop	19
4.3	Vytvorenie z linky	21
4.3.1	Inicializácia platby a odovzdanie platobných parametrov VIAMO aplikácii	21
4.3.2	ResponseString – odpoveď o výsledku spracovania platby	23
4.3.3	Kontrola podpisu ResponseStringu	25
4.4	Vytvorenie skrátenej linky	26
5	Notifikácia príjemcu o platbe	28
5.1	SMS notifikácia na telefónne číslo	28
5.2	Systémová e-mailová notifikácia	28
5.3	Systémová notifikácia odoslaná cez volanie HTTP/HTTPS POST	29
5.3.1	Vytvorenie a overenie podpisu systémovej notifikácie	30
5.3.2	Opakované odoslanie notifikácie	31
5.4	PUSH notifikácia do aplikácie pre obchodníka	31

1 Úvod

VIAMO umožňuje okrem jednoduchých platieb medzi fyzickými osobami (**P2P**), robiť tiež platby obchodníkom za tovar alebo služby (**P2B**). Pre platby obchodníkom sú dostupné viaceré spôsoby inicializácie platby a sú rozšírené možnosti notifikácie o zrealizovanej platbe. Tento dokument popisuje možnosti inicializácie platby, spôsoby notifikácie a poskytuje technický návod, ako má obchodník integrovať VIAMO platbu.

2 Firemný profil obchodníka

Aby obchodník mohol prijímať platby cez VIAMO, musí mať vo VIAMO vytvorený **firemný profil**.

Vo firemnom profile sú evidované:

- **základné údaje** o firme, kontaktné údaje
- **identifikátor príjemcu** pre jednoznačné určenie príjemcu platby
- **bankový účet** pre príjem platieb
- **nastavenia** (spôsob notifikácie, kľúče pre symetrické šifrovanie, email pre mesačný výpis transakcií)

Identifikátor príjemcu (BID) je unikátny alfanumerický reťazec, ktorý jednoznačne určuje príjemcu P2B platby (ekvivalent telefónneho čísla pri P2P platbách). Identifikátor príjemcu má definovaný bankový účet, v prospech ktorého sú realizované VIAMO platby, odoslané na tento identifikátor. Identifikátor príjemcu je „technický“ údaj, ktorý platca nemusí poznať. Platcovi je zobrazovaný tzv. popis identifikátora, čo by mal byť názov, pod ktorým zákazníci poznajú obchodníka. Príklad identifikátora: EUBA, popis identifikátora: „Ekonomická univerzita v Bratislave“. Vo firemnom profile je možné evidovať viacero identifikátorov, s vlastným bankovým účtom a nastaveniami.

Bankový účet slúži pre príjem platieb. Ak má firma evidované viaceré identifikátory, je možné pre každý identifikátor definovať iný účet na príjem.

Automatické smerovanie platby je funkcia, ktorej cieľom je zabezpečiť, aby VIAMO transakcie prebiehali v rámci tej istej banky. Znamená to, že ak má príjemca vo svojom profile viac bankových účtov na príjem, systém pri vytváraní prevodného príkazu použije bankový účet z tej istej banky ako je banka platcu. Ak príjemca nemá účet z tej istej banky ako platca, systém použije tzv. primárny bankový účet.

3 Inicializácia platby obchodníkovi z pohľadu používateľa

Pri P2P platbách je príjemca identifikovaný telefónnym číslom. Platca posieľa platbu na telefónne číslo, pričom je jedno či je telefónne číslo registrované vo VIAMO alebo nie. Ak je telefónne číslo registrované (systém eviduje dvojicu telefónne číslo – bankový účet), systém VIAMO platbu hneď spracuje. Ak telefónne číslo príjemcu nie je registrované, systém VIAMO zaeviduje tzv. čakajúcu platbu. O prijatí platby sa príjemca – osoba dozvie prostredníctvom SMS správy alebo PUSH notifikácie (PUSH je odoslaná, ak má príjemca aktivovanú VIAMO aplikáciu).

Pri P2B platbách je príjemca identifikovaný pomocou **identifikátora príjemcu (BID)**. Na rozdiel do P2P platieb, **P2B platby je možné posieľať len na registrované identifikátory**. Preto obchodník musí byť vo VIAMO vopred zaregistrovaný, čiže musí mať vytvorený firemný profil: mať pridelený identifikátor príjemcu a zadaný bankový účet pre príjem platieb. O prijatí platby je obchodník informovaný prostredníctvom notifikácie: cez SMS správu, e-mail alebo volanie HTTP/HTTPS POST. Spôsob notifikácie je nastavený vo firemnom profile obchodníka.

Pri P2B platbe sú dostupné **viaceré spôsoby inicializácie platby**. Obchodník si môže vybrať, ktorý spôsob vyhovuje jeho typu biznisu a potrebám; súčasne môže používať viaceré spôsoby.

Podľa spôsobu vyvolania P2B platby teda rozlišujeme:

1. **Platba z QR kódu**
2. **Platba z webovej stránky obchodníka / v eshope**
3. **Platba z mobilnej aplikácie obchodníka**
4. **Platba zo zoznamu vo VIAMO aplikácii**
5. **Platba zo skrátenej linky**

3.1 Platba z QR kódu

QR (Quick Response) kód je dvojrozmerný čiarový kód, dnes všeobecne používaný ako rýchly a jednoduchý spôsob prenosu textovej informácie do mobilného zariadenia (smartfónu alebo tabletu). V prípade VIAMO sú v QR kóde zakódované platobné údaje.

Takýto QR kód je zákazníkovi zobrazený v ľubovoľnej forme: **vytlačený na papieri napríklad faktúre, zobrazený na webovej stránke alebo doručený ako obrázok e-mailom.**

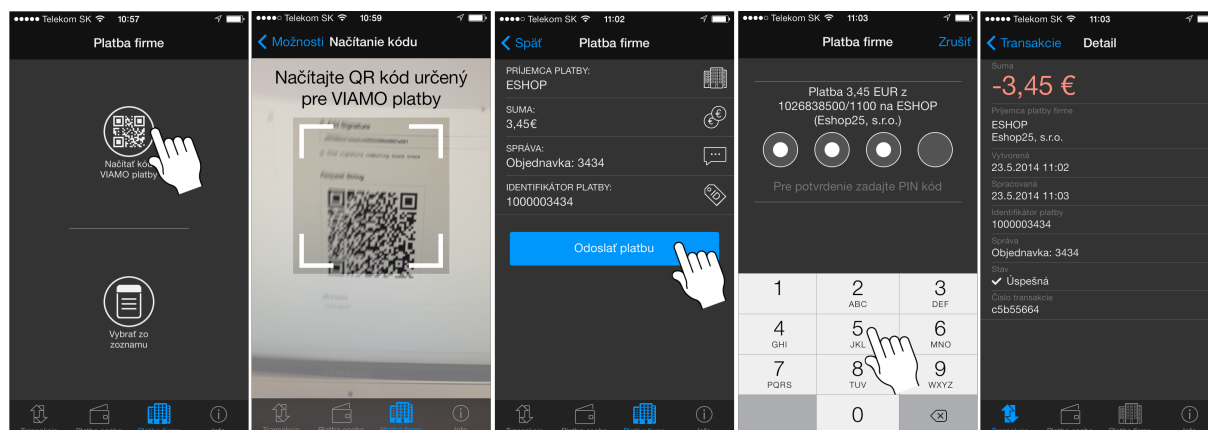
Aby mohol zákazník zaplatiť za tovar / služby obchodníkovi, musí obchodník vygenerovať QR kód s platobnými údajmi podľa špecifikácie uvedenej ďalej v tomto dokumente.

Potom zákazník **načíta QR kód pomocou VIAMO aplikácie**, ktorá QR kód dekoduje a zákazníkovi zobrazí platobnú obrazovku s predvyplnenými platobnými údajmi získanými z QR kódu. Na dokončenie platby stačí, aby zákazník potvrdil platbu zadáním PIN-u.

QR kód obsahuje buď čiastočné alebo kompletné platobné údaje, potrebné na odoslanie VIAMO platby. Údaje, ktoré nie sú v QR kóde, môže používateľ po načítaní doplniť vo VIAMO aplikácii. Ktorý údaj môže zákazník doplniť alebo zmeniť definuje obchodník pri vytváraní QR kódu.

O výsledku spracovania platby je obchodník informovaný prostredníctvom notifikácie odoslanej systémom VIAMO. Viac informácií o pravidlách odosielania a nastaveniach notifikácií v kapitole ďalej.

Platba načítaním QR kódu



3.2 Platba z webovej stránky obchodníka / v eshope

V závislosti od toho, či je **platba vyvolaná z webového prehliadača mobilného zariadenia** (smartfón, tablet) **alebo webového prehliadača počítača** (stolný počítač, notebook) rozlišujeme nasledujúcej dva základné scenáre:

- **platba inicializovaná načítaním QR kódu**
- **platba z linky – presmerovanie z webového prehliadača do VIAMO aplikácie**

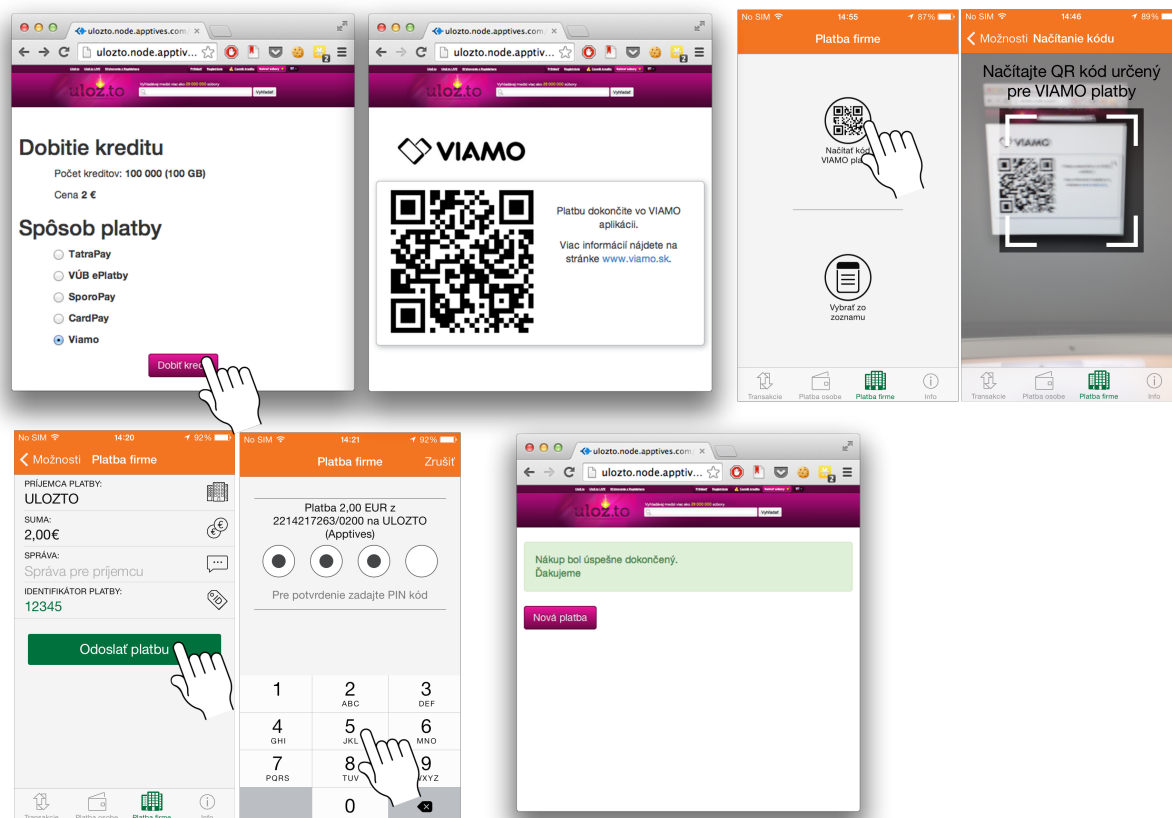
3.2.1 Platba z webovej stránky zobrazenej na počítači

Ak zákazník nakupuje **na webovej stránke obchodníka zobrazenej vo webovom prehliadači na „veľkej“ obrazovke počítača, na inicializáciu platby sa používa QR kód**. Aby mohol zákazník zaplatiť za tovar / služby obchodníkovi, musí obchodník resp. jeho eshop vygenerovať QR kód s platobnými údajmi a tento zobraziť ako obrázok. Ideálne, ak QR obsahuje kompletne platobné údaje, takže zákazník nič nemení ani nezadáva.

Potom **zákazník načíta QR kód z obrazovky počítača pomocou VIAMO aplikácie**, ktorá QR kód dekoduje a zákazníkovi zobrazí platobnú obrazovku s predvyplnenými platobnými údajmi. Na dokončenie platby stačí, aby zákazník potvrdil platbu zadaním PIN-u.

O výsledku spracovania platby je obchodník informovaný prostredníctvom notifikácie odoslanej systémom VIAMO. Po prijatí a spracovaní tejto notifikácie, eshop obnoví stránku a zákazníkovi zobrazí výsledok spracovania platby, prípadne informácie o ďalšom postupe pri vybavovaní jeho objednávky. Viac informácií o pravidlách odosielať a nastaveniach notifikácií v kapitole ďalej.

Platba z webovej stránky zobrazenej v prehliadači na počítači

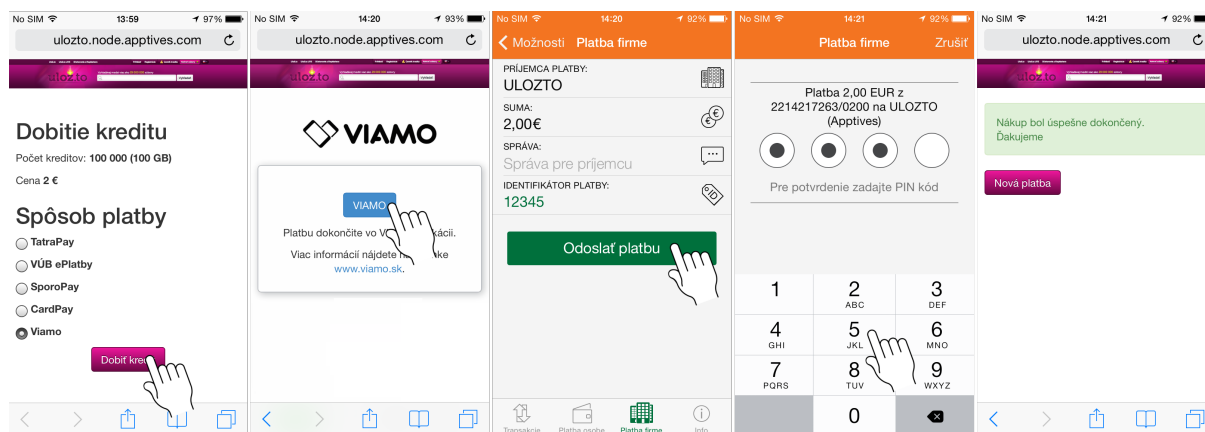


3.2.2 Platba z webovej stránky zobrazenej na mobilnom zariadení

Ak má eshop responzívny design (je optimalizovaný pre zobrazenie na mobilných zariadeniach) a zákazník nakupuje **na webovej stránke zobrazenej na „malej“ obrazovke smartfónu, je vhodné zobrazíť namiesto QR kódu (alebo spolu s QR kódom aj) linku**, napríklad ako tlačidlo „Zaplatiť cez VIAMO“. Zákazníkovi sa po kliknutí na túto linku na smartfóne otvorí VIAMO aplikácia, ktorá linku dekoduje a zákazníkovi zobrazí platobnú obrazovku s predvyplnenými platobnými údajmi. Na dokončenie platby stačí, aby zákazník potvrdil platbu PIN-om.

Po potvrdení platby zákazníkom, VIAMO aplikácia vráti zákazníka späť na webovú stránku obchodníka spolu s údajmi o výsledku spracovania platby. O výsledku spracovania platby je obchodník tiež informovaný prostredníctvom notifikácie odoslanej systémom VIAMO. Po prijatí a spracovaní tejto notifikácie, eshop obnoví stránku a zákazníkovi zobrazí výsledok spracovania platby, prípadne informácie o ďalšom postupe pri vybavovaní jeho objednávky. Viac informácií o pravidlách odosielania a nastaveniach notifikácií v kapitole ďalej.

Platba z webovej stránky zobrazenej v prehliadači na mobilnom zariadení / smartfóne



3.3 Platba z mobilnej aplikácie obchodníka

Natívna mobilná aplikácia je program určený na spustenie pre špecifickú platformu, napr. Android, iOS alebo Windows Phone.

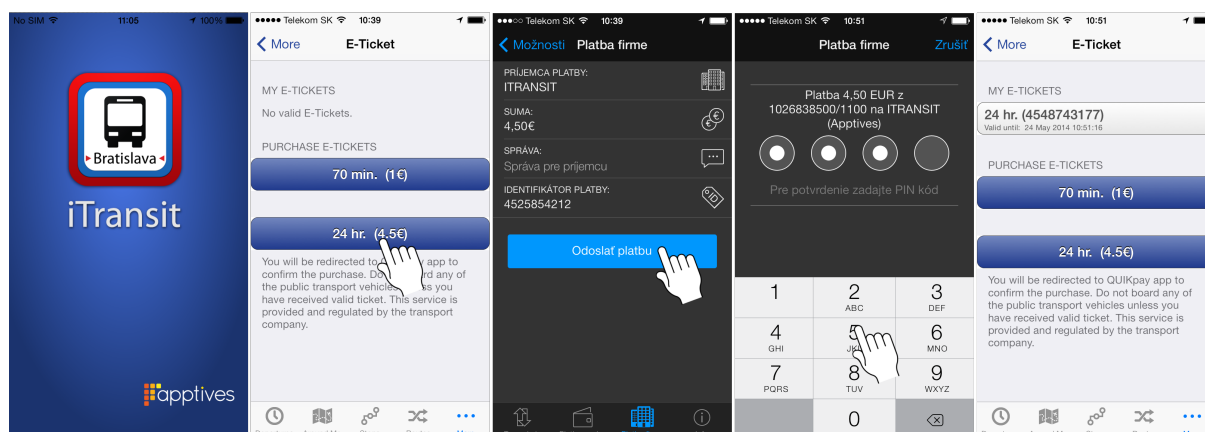
Predpokladom pre tento spôsob platby je, že obchodník upraví svoju natívnu aplikáciu tak, aby umožňovala platbu cez VIAMO.

Aby mohol zákazník zaplatiť za tovar / služby obchodníkovi, musí aplikácia obchodníka vygenerovať linku s platobnými údajmi podľa špecifikácie uvedenej ďalej v tomto dokumente.

Potom, keď zákazník v aplikácii obchodníka zvolí Platba cez VIAMO je z tejto aplikácie otvorená VIAMO aplikácia, ktorá dekoduje linku a zákazníkovi zobrazí platobnú obrazovku s predvyplnenými platobnými údajmi. Na dokončenie platby stačí, aby zákazník potvrdil platbu PIN-om vo VIAMO aplikácii. Po potvrdení platby zákazníkom, ho VIAMO aplikácia vráti späť do natívnej aplikácie obchodníka, ktorej zároveň odovzdá informácie o výsledku spracovania platby.

O výsledku spracovania platby môže byť obchodník tiež informovaný prostredníctvom notifikácie odoslanej systémom VIAMO. Viac informácií o pravidlách odosielať a nastaveniach notifikácií v kapitole ďalej.

Platba z natívnej aplikácie obchodníka



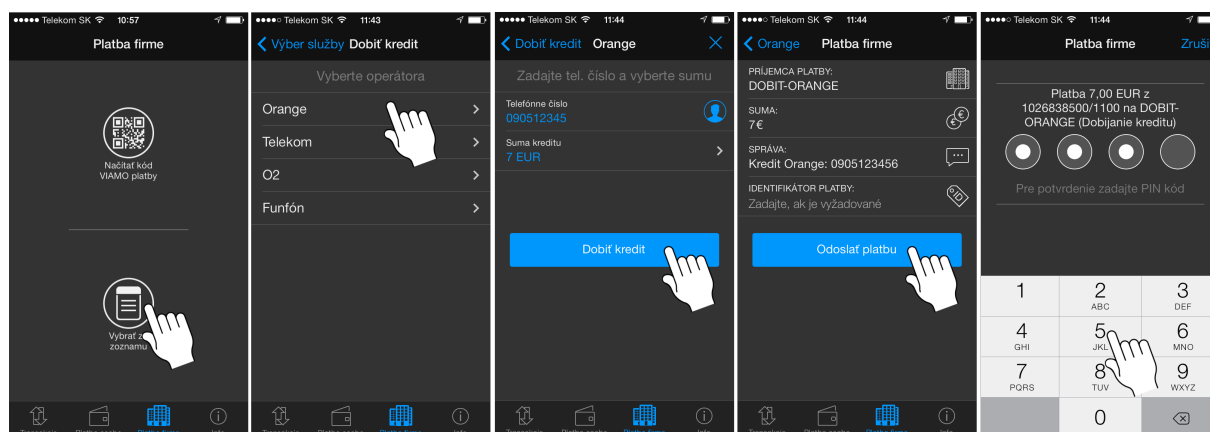
3.4 Platba zo zoznamu vo VIAMO aplikácii

Súčasťou VIAMO aplikácie je zoznam vybraných preddefinovaných príjemcov – obchodníkov. Zoznam umožňuje urobiť jednoduchú a rýchlu platbu za tovar / službu obchodníkovi priamo vo VIAMO aplikácii. Tento spôsob platby je vhodný na platby za tovar / službu, kde sú jednoduché a obmedzené možnosti pri výbere tovaru / služby napríklad parkovanie, dobíjanie kreditu, platba predplatného a podobne. Zoznam príjemcov a ich služieb udržiava VIAMO. VIAMO si vyhradzuje právo rozhodnúť, či daného obchodníka zaradiť do zoznamu.

Ak je obchodník súčasťou tohto zoznamu, potom zákazník, ak chce zaplatiť obchodníkovi za tovar / služby, vyberie zo zoznamu daného príjemcu, vyberie tovar / službu, prípadne zadá požadované údaje (napríklad EČV, číslo klienta alebo osobné číslo študenta). Zákazník na konci vidí štandardnú platobnú obrazovku s predvyplnenými platobnými údajmi. Po potvrdení platby vo VIAMO aplikácii, ostáva zákazník vo VIAMO aplikácii.

O výsledku spracovania platby je obchodník informovaný prostredníctvom systémovej notifikácie odoslanej serverom VIAMO. Viac informácií o pravidlách odosielania a nastaveniach systémových notifikácií v kapitole ďalej.

Platba zo zoznamu preddefinovaných príjemcov



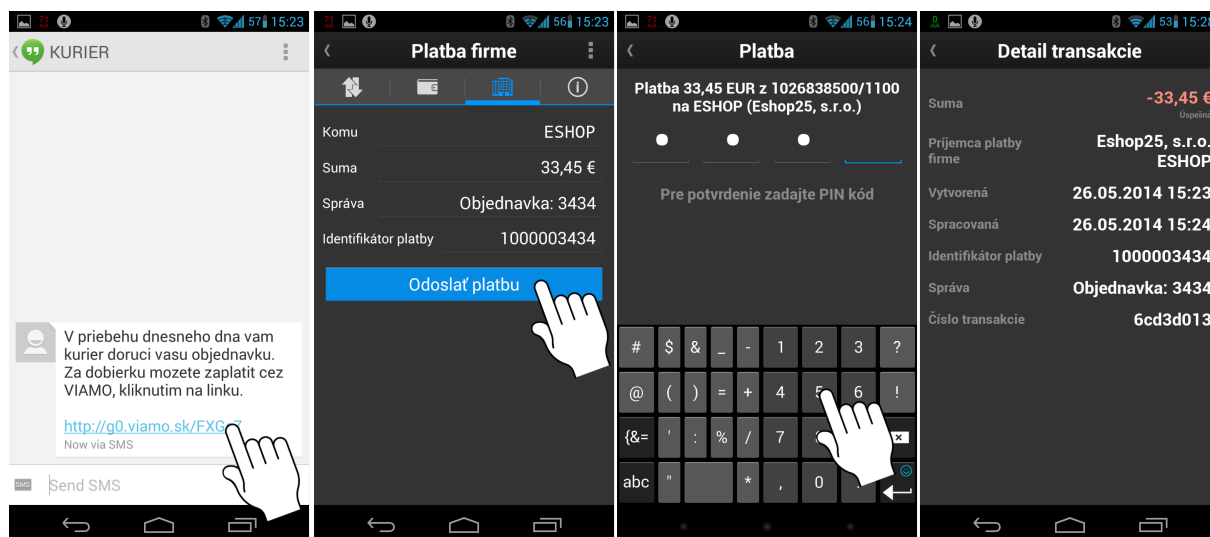
3.5 Platba zo skrátenej linky

Linka (používaná napríklad pri platbe z webovej stránky zobrazenej na mobilnom zariadení) môže byť skrátená pomocou skracovača. Takáto skrátená linka môže byť doručená na mobilné zariadenia ako SMS správa alebo ako súčasť e-mailu.

Zákazníkovi sa po kliknutí na túto linku na smartfóne otvorí VIAMO aplikácia, ktorá linku dekoduje a zákazníkovi zobrazí platobnú obrazovku s predvyplnenými platobnými údajmi. Na dokončenie platby stačí, aby zákazník potvrdil platbu PIN-om. Po potvrdení platby zákazník vo VIAMO aplikácii zostáva vo VIAMO aplikácii alebo je presmerovaný na stránku obchodníka.

O výsledku spracovania platby je obchodník informovaný prostredníctvom notifikácie odoslanej serverom VIAMO. Viac informácií o pravidlách odosielania a nastaveniach systémových notifikácií v kapitole ďalej.

Platba zo skrátenej linky odoslanej v SMS správe



4 Inicializácia platby z technického hľadiska

Podľa spôsobu vyvolania delíme platby do 2 základných skupín:

- platby inicializované **z platobnej aplikácie VIAMO** a
- platby inicializované **zo systému, stránky alebo aplikácie obchodníka**.

Do prvej skupiny patria platba zo zoznamu príjemcov vo VIAMO aplikácii a platba načítaním QR kódu. Do druhej skupiny všetky ostatné spôsoby inicializácie platby.

Všetky spôsoby P2B platby používajú **na odovzdanie platobných parametrov VIAMO aplikácii tzv. RequestString (RS)**.

4.1 RequestString

RequestString (RS) je reťazec dvojíc **kl'úč:hodnota** podľa špecifikácie uvedenej v tejto kapitole.

RequestString môže obsahovať:

- **úplné platobné údaje** vyžadované pre odoslanie požiadavky na VIAMO server alebo
- **čiastkové platobné údaje** a zvyšok musí doplniť platca vo VIAMO aplikácii.

Ak to RequestString povoľuje, môže platca niektoré údaje zmeniť alebo doplniť vo VIAMO aplikácii.

Základne pravidlá pre vytváranie RequestStringu

RequestString sa skladá z dvojíc „{kl'úč}:{hodnota}“.

Ako oddelovač medzi kl'účom a hodnotou {kl'úč}:{hodnota} sa používa znak dvojbodka „:“.

RequestString musí začínať tzv. „hlavičkou“, čo je dvojica názov protokolu a číslo verzie protokolu „**QP:1.0**“.

Ako oddelovač medzi dvoma párami „{kl'úč}:{hodnota}“ sa používa znak hviezdička „*“.

RequestString nemôže končiť znakom hviezdička „*“.

Parametre požiadavky – RequestStringu:

Kľúč	Popis	Povinný	Editovat. hodnota	Dĺžka	Povolenné znaky, hodnoty
QP	Protokol	Áno	Nie		1.0
BID	Identifikátor príjemcu	Áno	Nie	Max. 16 znakov	[0-9], [A-Z] a pomlčka
RID	Referenčné číslo platby (definované obchodníkom)	Nie	Nie	Max. 16 znakov	[0-9], [A-Z], [a-z]
AM	Suma platby	Nie	Áno	Max. 10 znakov	Max. 99999999.99. Použiť presne dve desatinne miesta, a „.“ ako oddel'ovač.
CC	Mena	Nie	Nie	Práve 3 znaky	EUR
VS	Variabilný symbol	Nie	Áno	Max. 10 číslic	[0-9]
CS	Konštantný symbol	Nie	Nie	Práve 4 číslice	[0-9]
SS	Špecifický symbol	Nie	Nie	Max. 10 číslic	[1-9]
MSG	Správa pre príjemcu	Nie	Áno	Max. 32 znakov	[0-9], [A-Z], [a-z] a špeciálne znaky
E2E	Referencia platiteľa	Nie	Nie	Max. 35 znakov	[0-9], [A-Z], [a-z] a špeciálne znaky
EXT	Rozšírené údaje	Nie	Nie	Max. 500 znakov	[0-9], [A-Z], [a-z] a špeciálne znaky
DT	Dátum platnosti	Nie	Nie	Práve 12 číslic	Dátum dokedy je RS platný vo formáte yyyyMMddHHmm
CO	Kód krajiny	Nie	Nie	Práve 2 znaky	podľa ISO 3166-1
RURL	Návratová URL	Nie	Nie	Max. 1500 znakov	[0-9], [A-Z], [a-z] a špeciálne znaky
NSMS	Telefónne číslo pre SMS notifikáciu o platbe	Nie	Nie		+421 421 00421 0 xxxxxxxx
NEML	E-mail pre EMAIL notifikáciu o platbe	Nie	Nie		[0-9], [A-Z], [a-z] a špeciálne znaky

Povinný parameter znamená, že RequestString musí obsahovať tento kľúč.

NSMS: Telefónne číslo, na ktoré je odoslaná SMS notifikácia po úspešnej platbe. Odosielanie SMS notifikácií musí byť povolené v profile firmy. Viac v kapitole Notifikácie o platbe.

NEML: E-mailová adresa, na ktorú je odoslaná e-mail notifikácia po úspešnej platbe. Odosielanie e-mailových notifikácií musí byť povolené v profile firmy. Viac v kapitole Notifikácie o platbe.

RURL: Návratová URL, na ktorú je platca presmerovaný po potvrdení platby. Presmerovanie nie je podporované pre platbu inicializovanú načítaním QR kódu, a preto RequestString zakódovaný v QR kóde nemôže obsahovať parameter RURL. Ak je v RURL použitý znak hviezdička “*”, musí sa zakódovať ako “%2A”, keďže znak “*” sa používa v RequestStringu ako oddel'ovač dvojíc kľúč:hodnota.

Do prevodného príkazu odosielaného na spracovanie do banky sa prenášajú

z RequestStringu hodnoty parametrov **AM, VS, CS, SS a MSG**. Parameter **MSG** sa prenáša do prevodného príkazu ako správa pre príjemcu.

Parameter **E2E** bude používaný po spustení SEPA platieb, kedy sa prestanú používať doteraz využívané parametre variabilný, konštantný a špecifický symbol.

Na detailnejšiu špecifikáciu platby je možné použiť parametre RID alebo EXT.

Referenčné číslo platby **RID** je parameter, cez ktorý si obchodník môže poslať vlastný párovací údaj o platbe. Tento údaj sa platcovi nezobrazuje a VIAMO ho vracia bez akejkoľvek transformácie vo výsledku o spracovaní platby, cez ResponseString alebo systémovú notifikáciu.

V prípade, ak je na bližšiu špecifikáciu platby potrebné preniesť viac údajov (napr. EČV alebo číslo klientskej zmluvy a pod.) je k dispozícii parameter **EXT** – rozšírené údaje o platbe. Na rozdiel od parametra VS alebo RID umožňuje prenášať dlhší alfanumerický text.

Niektoré spôsoby platby vyžadujú, aby bol RequestString podpísaný a teda výsledný RequestString obsahoval aj podpis **SIG:{podpis}**. Viac o podpisovaní RequestStringu v časti Vytvorenie podpisu RequestStringu.

Príklady validných RequestStringov

```
QP:1.0*BID:MYBID
QP:1.0*BID:MYBID*AM:6.00
QP:1.0*BID:MYBID*AM:6.00*VS:1234*MSG:PARKOVANIE
QP:1.0*BID:MYBID*AM:6.00*VS:1234*CS:0308*SS:7510206688
QP:1.0*BID:MYBID*AM:6.00*DT:201502010000
```

Príklady nevalidných RequestStringov

```
QP:1.0*BID:MYBID*AM:6.000
QP:1.0*BID:MYBID*AM:6.00*VS:ABCDEF
QP:1.0*BID:MYBID*AM:6.00*CC:HUF
QP:1.0*BID:MYBID*AM:6.00*DT:20140201
```

4.1.1 Editovateľnosť parametrov

Editovateľná hodnota znamená, že hodnotu parametra môže platca zmeniť alebo doplniť vo VIAMO aplikácii. Editovateľnosť sa povoľuje pridaním znaku dolár „\$“ k hodnote, nasledovne **{klúč}:{hodnota{\$}}** napr. AM=10.00\$.

Povoliť editovať hodnoty je možné len pre parametre **AM, MSG, VS** (tieto parametre sú zobrazené na platobnej obrazovke vo VIAMO aplikácii).

UPOZORNENIE: RequestString môže obsahovať aj prázdne parametre t.j. dvojicu klúč:hodnota bez zadanej hodnoty „{klúč}:{}“, čo spôsobí, že hodnotu parametra platca nebude vedieť doplniť. Preto **prázdny parameter bez možnosti editácie platcom nie je možné použiť v prípade parametra AM**, keďže takto by platca nemal vyplnenú hodnotu a ani by ju nevedel doplniť vo VIAMO aplikácii, a teda platba by nemohla byť vôbec odoslaná, pretože suma platby je povinný parameter.

Ak je požadované, aby niektorý z parametrov (MSG alebo VS) platca nemohol zadať, do RequestStringu sa doplní parameter bez hodnoty „{klúč}:{}“ a bez znaku dolár „\$“.

Ak sa parametre AM, MSG, VS vôbec nenachádzajú v RequestStringu, VIAMO aplikácia ich interpretuje ako editovateľné. Takže hoci ich hodnota na platobnej obrazovke nie je vyplnená, platca má možnosť hodnotu zadať ručne.

Príklady validných RequestStringov

```
QP:1.0*BID:MYBID
QP:1.0*BID:MYBID*AM:6.00
QP:1.0*BID:MYBID*AM:6.00$
QP:1.0*BID:MYBID*AM:6.00*VS:1234$
QP:1.0*BID:MYBID*MSG:$
QP:1.0*BID:MYBID*MSG:
```

Príklad nevalidných RequestStringov (parameter AM je prázdny a needitovateľný)

```
QP:1.0*BID:MYBID*AM:
```


4.1.2 Vytvorenie podpisu RequestStringu

Niektoré scenáre vyžadujú, aby súčasťou RequestString bol aj bezpečnostný podpis parametrov.

Scenár platby	Podpis
Platba z QR kódu	Voliteľný*
Platba v eshope na počítači (z QR kódu)	Voliteľný*
Platba v eshope na mobilnom zariadení (z linky)	Povinný
Platba z aplikácie obchodníka (z linky)	Povinný
Platba zo skrátenej linky	Povinný
Platba zo zoznamu vo VIAMO aplikácii	N/A

*podľa nastavenia v profile firmy

Postup vytvorenia podpisu RequestStringu

1. Z RequestStringu (hlavička + telo) sa urobí hash pomocou algoritmu SHA-256.
2. Potom sa zoberie prvých 16 bytov, ktoré sa zašifrujú algoritmom AES-128 s parametrami ECB a NoPadding pomocou kľúča K1 prideleného obchodníkovi na podpisovanie RequestStringu.

Príklad vytvorenia podpisu RequestStringu

Podpisovaný reťazec

```
QP:1.0*BID:MYBID*AM:6.00
```

Kľúč K1 pridelený na podpisovanie RequestStringu

```
11223344556677889900AABBCCDDEEFF
```

1. Vytvorenie hashu SHA-256

```
Hash = SHA-256(QP:1.0*BID:MYBID*AM:6.00) =  
bd0109a27826206141ab80d4c6ec82b7a3663458a9df87b0854e90fe2d551872
```

2. Vytvorenie podpisu AES/ECB/NoPadding a zobrazenie v HEX tvare:

```
sign(bd0109a27826206141ab80d4c6ec82b7, K1) = 30ac3cd680ba8d112a71db60977ef743
```

3. Potom výsledný RequestString doplnený o parameter podpis je:

```
QP:1.0*BID:MYBID*AM:6.00*SIG:30AC3CD680BA8D112A71DB60977EF743
```

4.1.3 Kontrola podpisu RequestStringu

VIAMO server robí kontrolu podpisu RequestStringu tak, že vytvorí podpis parametrov rovnakým spôsobom, ako je popísané vyššie a tento porovná v prijatým podpisom. Ak sa vypočítaný a prijatý podpis zhodujú, parametre platby sa považujú za správne a požiadavka na platbu je ďalej spracovaná.

RS Generátor

Na generovanie RequestStringu, testovanie vytvárania podpisu RequestStringu alebo vytvorenie linky je možné použiť RS generátor na <http://rs.viamo.sk/>. RS generátor neaplikuje kontroly na zadané údaje a preto je pomocou neho možné generovať aj nevalidné RequestStringy, ak chcete testovať negatívne scenáre.

4.2 Generovanie QR kódu

QR (Quick Response) kód je dvojdimenzionálny čiarový kód, používaný na rýchly a jednoduchý prenos textovej informácie do mobilného zariadenia. V prípade VIAMO sú v QR kóde zakódované platobné údaje vo forme RequestString.

Platba obchodníkovi je inicializovaná načítaním QR kódu pomocou fotoaparátu priamo vo VIAMO aplikácii. Generovanie QR kódu robí obchodník alebo jeho systém, webová stránka.

Postup popísaný v tejto kapitole je možné použiť pre nasledovné spôsoby platby:

- **Platba z QR kódu**
- **Platba v eshope – z webovej stránky zobrazenej na počítači**

4.2.1 Generovanie QR kódu pre kamenný obchod / kaviareň

Ak máte priradený identifikátor príjemcu, vlastný QR kód si jednoducho vygenerujete pomocou generátora QR kódov na <http://qr.viamo.sk/>. Tento generátor robí kontroly zadaných údajov, ktoré bránia vygenerovať nevalidný QR kód, preto je možné ho použiť na generovanie produkčných QR kódov.

Pre použite v kamenných obchodoch / kaviarňach odporúčame generovať QR kód ako „plagát“. Tu môžete platiť cez VIAMO, ten vytlačiť a zobrazíť zákazníkovi na viditeľnom mieste pri pokladni.

4.2.2 Generovanie QR kódu pre eshop

Generovať QR kódy pre platby na eshope je možné pomocou niektorej voľne dostupnej knižnice na generovanie QR kódov alebo je možné použiť API VIAMO QR generátora, ktoré vracia QR kód ako PNG obrázok.

Príklad volania API QR generátora

```
http://qr.viamo.sk/api/?text=
QP%3A1.0*BID%3AMOJOBCHOD*AM%3A10.99*VS%3A45654&template=300
```

Odporúčame, aby obchodník implemetoval generovanie QR kódu do svojho systému / eshopu, keďže API VIAMO QR generátora nie je garantovaná služba.

Podobne, ak potrebujete generovať väčšie množstvo QR kódov (napríklad pre automatizované rozposielanie cez e-mail), urobte tak priamo vo vašom systéme, pomocou niektorej voľne dostupnej knižnice pre generovanie QR kódov.

Príklad pre RequestString pre jednoduchý QR kód, sumu doplní zákazník

```
QP:1.0*BID:KAVIAREN-ZRNKO
```

Príklad pre RequestString so všetkými údajmi povinnými pre odoslanie platby

```
QP:1.0*BID:MYBID*AM:140.20$*VS:45678*CS:0308*SS:16700*MSG:Platba na eshope
```



Tu môžete platiť cez VIAMO



1 Naskenujte
QR kód

2 Dopĺňte
sumu

3 Platbu
potvrďte
PIN-om

Služba VIAMO je dostupná pre klientov

**VÚB BANKA**
Member of Raiffeisen Bank International
by Raiffeisen Bank International

4.3 Vytvorenie z linky

Postup popísaný v tejto kapitole je platný pre nasledovné spôsoby platby:

- **Platba z mobilnej aplikácie obchodníka**
- **Platba v eshope – z webovej stránky zobrazenej na mobilnom zariadení**

Na odovzdanie platobných parametrov z mobilnej aplikácie alebo webovej stránky obchodníka VIAMO aplikácii sa používa štandardný RequestString. RequestString môže tiež obsahovať voliteľný parameter **RURL – návratovú URL adresu**, na ktorú je platca presmerovaný po potvrdení platby PIN-om.

Pre platbu z linky je vyžadované, aby bol **RequestString podpísaný** a teda výsledný RequestString obsahoval aj podpis **SIG:{podpis}**. Na vytvorenie podpisu sa používa symetrické šifrovanie pomocou kľúča K1 prideleného obchodníkovi na podpisovanie RequestStringu.

DÔLEŽITÉ UPOZORNENIE: Nie je vhodné, aby podpis RequestStringu vytvárala priamo mobilná aplikácia, pretože by musela obsahovať kľúč K1. **Vytvorenie podpisu by sa malo robiť výlučne na backende obchodníka!**

4.3.1 Inicializácia platby a odovzdanie platobných parametrov VIAMO aplikácii

1. Zákazník v mobilnej aplikácii obchodníka (alebo webovej stránke zobrazenej na smartfóne) vyberie typ a parametre služby / tovaru a zvolí platbu cez VIAMO.
2. Mobilná aplikácia obchodníka (alebo webová stránka) z parametrov platby:
 - a) vytvorí RequestString,
 - b) podpíše tento RequestString (s pomocou backendu obchodníka) a
 - c) tento použije na vytvorenie linky s VIAMO URL schémou (viamo://).
3. Mobilná aplikácia obchodníka (alebo webová stránka) otvorí túto linku, čo spôsobí, že je otvorená VIAMO aplikácia*, v ktorej sa zobrazí platobná obrazovka v predvyplnenými údajmi odovzdanými v RequestStringu.
4. Zákazník vo VIAMO aplikácii potvrdí platbu zadaním PIN-u. Pred potvrdením môže zmeniť alebo doplniť údaje, v závislosti od RequestStringu.
5. VIAMO aplikácia po spracovaní platby na backende VIAMO presmeruje používateľa na URL adresu prijatú v RequestStringu, čiže späť do mobilnej aplikácie obchodníka (alebo na webovú stránku).

O výsledku spracovania platby je informovaný aj backend obchodníka prostredníctvom systémovej notifikácia (e-mail alebo HTTP POST volanie).

*Ak má zákazník na mobilnom zariadení nainštalovaných viacero VIAMO aplikácií (napr. TB VIAMO a VUB VIAMO) je mu zobrazený zoznam týchto VIAMO aplikácií. Zákazník vyberie aplikáciu, v ktorej chce platbu urobiť.

Pri iOS natívna mobilná aplikácia zistí, ktoré URL schémy sú podporované, a podľa toho zobrazí dialóg so zoznamom nainštalovaných VIAMO aplikácií (poskytnutý zdrojový kód alebo knižnica). Podľa výberu zákazníka sa použije konkrétna URL schéma aplikácie (viamo-tb://, viamo-vub://), ktorá realizuje zobrazenie zvolenej VIAMO aplikácie.

Pri Androide, alebo Windows Phone, použije natívna mobilná aplikácia všeobecnú URL schému (viamo://) a dialóg s podporovanými aplikáciami je realizovaný na úrovni OS.

Webová aplikácia zobrazí zoznam všetkých existujúcich VIAMO aplikácií, zákazník realizuje voľbu konkrétnej VIAMO aplikácie a podľa výberu zákazníka je potrebné použiť konkrétnu URL schému aplikácie (viamo-tb://, viamo-vub://).

Príklad vyvolania platby cez RequestString z natívnej aplikácie

Identifikátor príjemcu: MYBID
 Návratová URL: itransit://
 Kľúč K1 pre podpisovanie RequestStringu = 11223344556677889900AABBCCDDEEFF

1. Vytvorenie RequestStringu z parametrov platby:

QP:1.0*BID:MYBID*AM:16.00*VS:1234*RURL:itransit://

Poznámka: Ak sa v návratovej URL nachádza znak hviezdička „*“, ktorý je zároveň používaný ako oddelovač dvojíc kľúč:hodnota, musí byť pred podpísaním nahradený „%2A“.

2. Vytvorenie podpisu RequestStringu (SHA-256, AES/ECB/NoPadding):

QP:1.0*BID:MYBID*AM:16.00*VS:1234567890*RURL:itransit://*SIG:6AD86397E7674F4F377C71611947C427

3. Zakódovanie podpísaného RequestStringu pomocou URL kódovania:

QP%3A1.0*BID%3AMYBID*AM%3A16.00*VS%3A1234*RURL%3Aitransit%3A%2F%2F*SIG%3A6AD86397E7674F4F377C71611947C427

4. Vytvorenie URL pridaním VIAMO schémy

viamo:///requestString=QP%3A1.0*BID%3AMYBID*AM%3A16.00*VS%3A1234*RURL%3Aitransit%3A%2F%2F*SIG%3A6AD86397E7674F4F377C71611947C427

5. Aplikácia obchodníka (alebo webová stránka zobrazená na mobilnom zariadení) otvorí túto linku, čo spôsobí otvorenie VIAMO aplikácie, ktorej sú cez RequestString odoslané parametre platby.

4.3.2 ResponseString – odpoveď o výsledku spracovania platby

VIAMO aplikácia na **odovzdanie informácie o výsledku spracovania platby** natívnej aplikácii obchodníka (alebo webovej stránky) používa tzv. **ResponseString**.

Pre tvorbu ResponseStringu platia rovnaké pravidlá ako pre tvorbu inicializačného RequestStringu, popísané vyššie v tomto dokumente. Zoznam parametrov je doplnený o parameter vracajúci výsledok spracovania platby **RES** (result).

ResponseString **je vždy podpísaný**, kľúčom K1 pridelený obchodníkovi, evidovaný v profile firmy určený na podpisovanie RequestStringu.

Pre úplnosť je dobré uviesť, že o výsledku spracovania platby môže byť informovaný aj backend obchodníka prostredníctvom systémovej notifikácie (e-mail alebo HTTP POST volanie).

Parametre odpovede – ResponseStringu:

Kľúč	Povinný	Dĺžka	Hodnota	Príklad
QP	Áno		Verzia 1.0	1.0
BID	Áno	Max. 16 znakov	Identifikátor príjemcu platby	MYBID
RES	Áno		Výsledok platby (OK, FAIL, BANK_PROC)	OK
RID	Nie	Max 16 znakov	Referenčný identifikátor platby pre príjemcu.	ABC123
AM	Áno	Max 10 znakov	Maximálne dve desatinne miesta, bodka ako oddelovač.	12.23
CC	Nie	Práve 3 znaky	Zatiaľ povolená hodnota 'EUR'	EUR
VS	Nie	Max 10 číslíc	Variabilný symbol. Povolene znaky [0-9]	123459
SS	Nie	Práve 4 číslice	Špecifický symbol. Povolene znaky [0-9]	0308
E2E	Nie	Max 35 znakov	Referencia platiteľa	
SIG	Áno		Bezpečnostný podpis	

Stav platby RES môže nadobudnúť nasledovné hodnoty:

- **OK** – platba úspešná
- **FAIL** – platba neúspešná
- **BANK_PROC** – platba bola odoslaná na spracovanie do banky. Po spracovaní platby v banke bude odoslaná systémová notifikácia, kde konečný stav je buď OK alebo FAIL.

VIAMO aplikácia nerobí presmerovanie do mobilnej aplikácie obchodníka (alebo na webovú stránku) ak:

- inicializačný RequestString neobsahoval parameter RURL
- ak používateľ zruší platbu, nezačne autorizáciu
- ak používateľ zruší platbu počas autorizácie

Príklad odpovede cez ResponseString a presmerovania na webovú stránku

Ak návratová RURL definovaná v inicializačnom RequestStringu je:

```
http://moj.biznis.sk/viamo/receiver/
```

potom výsledná URL linka, ktorú otvorí VIAMO aplikácia je:

```
http://moj.biznis.sk/viamo/receiver/?requestString=QP%3A1.0*BID%3AMYPID*AM%3A6.00*VS%3A1234*RES%3AOK*SIG%3A8493BE1FCAE7B152EEEC2A2406D005C
```

Príklad odpovede cez ResponseString a presmerovania do natívnej aplikácie obchodníka:

Ak návratová RURL definovaná v inicializačnom RequestStringu je:

```
itransit://
```

potom výsledná URL linka, ktorú otvorí VIAMO aplikácia je:

```
itransit://?requestString=QP%3A1.0*BID%3AMYPID*AM%3A6.00*VS%3A1234*RES%3AOK*SIG%3A8493BE1FCAE7B152EEEC2A2406D005C
```


4.3.3 Kontrola podpisu ResponseStringu

DÔLEŽITÉ UPOZORNENIE: Nie je vhodné, aby podpis ResponseStringu vytvárala alebo kontrolovala priamo natívna aplikácia obchodníka, pretože by musela obsahovať kľúč K1. **Vytvorenie a overenie podpisu by sa malo robiť výlučne na backende obchodníka.**

Príklad: Overenie podpisu po presmerovaní do natívnej aplikácie obchodníka

1. Natívna aplikácia z prijatej URL prečíta parameter *ResponseString*:

```
itransit://?responseString=QP%3A1.0*BID%3AMYBID*AM%3A6.00*VS%3A1234*RES%3AOK*SIG%3A8493BE1FCAE7B152EEECC2A2406D005C
```

2. Z hodnoty parametra responseString sa urobí URL decode, výsledkom čoho je podpísaný responseString:

```
QP:1.0*BID:MYBID*AM:6.00*VS:1234*RES:OK*SIG:8493BE1FCAE7B152EEECC2A2406D005C
```

3. Z responseStringu sa oddelí podpis (parameter SIG):

```
QP:1.0*BID:MYBID*AM:6.00*VS:1234*RES:OK*SIG:8493BE1FCAE7B152EEECC2A2406D005C
```

4. Z responseStringu sa pomocou kľúča K1 pre podpísovanie RequestStringu vytvorí podpis:

```
sign(QP:1.0*BID:MYBID*AM:6.00*VS:1234*RES:OK, K1) =  
8493BE1FCAE7B152EEECC2A2406D005C
```

5. Porovnanie podpisov: ak sa vypočítaný a prijatý podpis zhodujú, správa je v poriadku.

Príklad: Overenie podpisu na webovú stránku obchodníka

Zákazník je presmerovaný na webovú stránku nasledovnou linkou, z ktorej sa získa parameter ResponseString:

```
http://moj.biznis.sk/viamo/receiver/?responseString=QP%3A1.0*BID%3AMYBID*AM%3A6.00*VS%3A1234*RES%3AOK*SIG%3A8493BE1FCAE7B152EEECC2A2406D005C
```

Ďalší postup pre overenie podpisu na webovej stránke obchodníka je rovnaký ako v prípade overenia podpisu natívnou aplikáciou: URL decode, oddelenie parametra SIGN, vytvorenie podpisu a porovnanie podpisov.

4.4 Vytvorenie skrátenej linky

VIAMO poskytuje obchodníkom vlastný skracovač URL adres dostupný na adrese **http://go.viamo.sk**.

Skracovať linky je možné cez webové rozhranie alebo je možné použiť API, ak je potrebné skrátiť veľké množstvo liniek. Na používanie skracovača je vyžadované prihlásenie cez meno+heslo pridelené obchodníkovi.

VIAMO skracovač poskytuje aj štatistiku otvorenia skrátených liniek.

API rozhranie skracovača

API skracovača vyžaduje aby požiadavky boli typu HTTP POST a požiadavky obsahovali povinné parametre: *login*, *password*, *url*.

Príklad skrátenia URL linky pomocou API

URL linka so zakódovanými parametrami platby:

```
viamo://?requestString=QP%3A1.0*BID%3AMYBID*AM%3A6.00*VS%3A1234*RURL%3Ahttp%3A%2F%2Fmoj.biznis.sk%2Fviamo%2Freceiver%2F*SIG%3A65AC25CA33D92C6F59F43744A242FFA6
```

Príklad požiadavky

```
POST http://go.viamo.sk/api/ HTTP/1.1
login=mojlogin&password=mojeheslo&url=viamo://?requestString=QP%3A1.0*BID%3AMYBID*AM%3A6.00*VS%3A1234*RURL%3Ahttp%3A%2F%2Fmoj.biznis.sk%2Fviamo%2Freceiver%2F*SIG%3A65AC25CA33D92C6F59F43744A242FFA6
```

Príklad odpovede – skrátenej linky

Správna odpoveď má vždy status kód 200. Prvý riadok odpovede obsahuje skrátenú URL adresu pripravenú na použitie. Napríklad:

```
HTTP/1.1 200 OK
http://go.viamo.sk/3WGoV
```

Ak počas spracovania požiadavky dôjde k chybe, odpoveď má status kód iný ako 200 a prvý riadok obsahuje za slovom ERROR dôvod chyby. Napríklad:

```
HTTP/1.1 400 Badá Request
ERROR:UNSUPPORTED_URL_SCHEME
```

Časová platnosť skrátenej linky

Pri vytváraní skrátenej linky je možné nastaviť časovú platnosť linky použitím nepovinného parametra *expire*. Hodnota sa zadáva vo formáte DD.MM.YYYY napr. 30.04.2016. Skrátená adresa je platná do 23:59 toho dňa.

Príklad požiadavky s časovou platnosťou

POST http://go.viamo.sk/api/ HTTP/1.1

login=mojlogin&password=mojeheslo&url=viamo://?requestString=QP%3A1.0*BID%3AMYBID*AM%3A6.00*VS%3A1234*RURL%3Ahttp%3A%2F%2Fmoj.biznis.sk%2Fviamo%2Freceiver%2F*SIG%3A65AC25CA33D92C6F59F43744A242FFA6&expire=30.04.2014

5 Notifikácia príjemcu o platbe

O výsledku spracovania platby je obchodník informovaný prostredníctvom notifikácie odoslanej serverom VIAMO. VIAMO ponúka niekoľko spôsob notifikácie:

- **SMS notifikácia na telefónne číslo**
- **Systémová e-mailová notifikácia**
- **Systémová notifikácia cez volanie HTTP/HTTPS POST**
- **PUSH notifikácia do aplikácie pre obchodníka**

Spôsob notifikácie je zvolí obchodník, podľa spôsobu použitia VIAMO platby. Konfiguráciu notifikácii v profile firmy zabezpečuje VIAMO administrátor. Nastavenie notifikácií môže byť vlastné pre každý identifikátor príjemcu.

5.1 SMS notifikácia na telefónne číslo

SMS notifikácia **je odoslaná po úspešnej platbe na telefónne číslo**, ktoré:

- je evidované pri identifikátore príjemcu (BID), na ktorý bola platba odoslaná a/alebo
- je súčasťou RequestStringu (NSMS), z ktorého bola platba inicializovaná.

5.2 Systémová e-mailová notifikácia

Systémové notifikácie používajú na výmenu dát štandard JSON. Každá systémová notifikácia má pridelený identifikátor *notificationId*, na jej jednoznačnú identifikáciu.

Systémová notifikácia obsahuje nasledovné údaje:

- **údaje o platbe:**
 - interný identifikátor VIAMO platby (payment.id)
 - stav platby (payment.result)
 - suma (payment.amount),
 - mena (payment.currency),
 - identifikátor príjemcu, na ktorý bola platba odoslaná (payment.bid),
 - dátum a čas spracovanie platby (payment.processedOn),
 - správa pre príjemcu (payment.message),
 - variabilný symbol (payment.vs),
 - konštantný symbol (payment.cs),
 - špecifický symbol (payment.ss)
 - referenčné číslo definované obchodníkom (payment.rid)
 - referencia platiteľa (payment.e2e)
 - rozšírený parameter (payment.ext)
- **údaje o platcovi:**
 - meno a priezvisko (payer.name),
 - telefónne číslo (payer.phone),
 - e-mail (payer.email)
- **podpis** (signature.sign)

Údaje o platbe a podpis sú vždy súčasťou notifikácie, údaje o platcovi podľa nastavenia v profile firmy.

Podpis je vytvorený pomocou symetrického kľúča K2 prideleného pre identifikátor príjemcu na podpisovanie systémových notifikácií.

Súbor vo formáte JSON je odoslaný ako príloha na e-mailovú adresu:

- evidovanú pri identifikátore príjemcu a/alebo
- je súčasťou RequestStringu (NEML), z ktorého bola platba inicializovaná.

Systémová notifikácia **je odoslaná v prípade**, ak je platba:

- úspešná
- neúspešná a platba bolo inicializovaná z RequestStringu z aplikácie obchodníka alebo linky (MOBILE)
- odoslaná na spracovanie do banky a platba bolo inicializovaná z RequestStringu z aplikácie obchodníka alebo linky (MOBILE)

Parameter stav platby (payment.result) môže nadobudnúť nasledovné hodnoty:

- **OK** – platba úspešná
- **FAIL** – platba neúspešná
- **BANK_PROC** – platba bola odoslaná na spracovanie do banky. Po spracovaní platby v banke je odoslaná nová notifikácia, kde stav je buď OK alebo FAIL.

5.3 Systémová notifikácia odoslaná cez volanie HTTP/HTTPS POST

Platia rovnaké pravidlá ako pre systémovú notifikáciu odosielanú na e-mailovú adresu.

Systémová JSON notifikácia je odoslaná na URL adresu evidovanú pri identifikátore príjemcu v profile firmy určenú na doručovanie týchto notifikácií.

Príklad JSON notifikácie

```
{
  "notificationId": "8fb32697-ca50-47d2-bf34-841b9a7cf547",
  "payment": {
    "result": "OK",
    "amount": "222.00",
    "currency": "EUR",
    "bid": "MYBID",
    "rid": "5566",
    "id": "42929ecb-b75f-4911-92f3-74fcc7a36eb3",
    "processedOn": "2014-05-02T12:52:53+0200",
    "message": "dakujem",
    "vs": "12345",
    "ss": "9753",
    "cs": "0308",
    "e2e": "/VS12345",
    "ext": "ECV=BA555XL"
  },
  "payer": {
    "name": "Milan T.",
    "phone": "0903000123",
    "email": "milan.test@viamo.sk"},
  "signature": {
```

```

    "description": "SHA-256 UTF-8 AES/ECB/NoPadding",
    "sign": "29d307e6d4c864d973c66d2e11033d9a"
  }
}

```

5.3.1 Vytvorenie a overenie podpisu systémovej notifikácie

Postup pre vytvorenie podpisu systémovej notifikácie

1. V prvom kroku treba vytvoriť reťazec „text na podpis“ naukladaním hodnôt parametrov bez oddel'ovača v nasledovnom poradí:

```
rid|vs|e2e,result,amount,id
```

Pre parametre RID, VS a E2E platí: ak je zadané RID, tak sa použije RID. Ak RID nie je zadané a je zadán VS, použije sa VS. Ak RID a VS nie je zadané a je zadané E2E – použije sa E2E. Ak sú hodnoty všetkých parametrov RID, VS a E2E prázdne (null), tak v texte na podpis neuvádzajú.

2. Z vytvoreného reťazca sa urobí hash pomocou algoritmu SHA-256.
3. Potom sa zoberie prvých 16 bytov, ktoré sa zašifrujú algoritmom AES-128 s parametrami ECB a NoPadding pomocou kľúča K2 prideleného pre identifikátor príjemcu na podpisovania systémových notifikácií.

Príklad 1

Kľúč K2 pridelený pre identifikátor príjemcu na podpisovania systémových notifikácií

```
AABBCCDDEEFF11223344556677889900
```

1. Vytvorenie reťazca „text na podpis“, z platby v ktorej RID nie je definovaný, VS = 12345, suma je 22.00 EUR a identifikátor VIAMO platby je 42929ecb-b75f-4911-92f3-74fcc7a36eb3.

```
123450K22.0042929ecb-b75f-4911-92f3-74fcc7a36eb3
```

2. Vytvorenie hashu SHA-256

```
Hash = SHA-256(123450K22.0042929ecb-b75f-4911-92f3-74fcc7a36eb3) =
362ba2fcb071cb842abbfe32604c2d6b56483312294ec917eb931eafede1768d
```

3. Vytvorenie podpisu AES/ECB/NoPadding z prvých 16 bytov

```
sign(362ba2fcb071cb842abbfe32604c2d6b, K2) = 849f00f8f512547a3146a1b8f063acd1
```

4. Pridanie podpisu do tela notifikačnej správy

```

{
  "notificationId": "8fb32697-ca50-47d2-bf34-841b9a7cf547",
  "payment": {
    "result": "OK",
    "amount": "22.00",

```

```

    "currency": "EUR",
    "bid": "MYBID",
    "id": "42929ecb-b75f-4911-92f3-74fcc7a36eb3",
    "processedOn": "2014-05-02T12:52:53+0200",
    "message": "dakujem",
    "vs": "12345",
    "ss": "9753",
    "cs": "0308",
    "e2e": "/VS12345",
    "ext": "ECV=BA555XL"
  },
  "payer": {
    "name": "Milan T.",
    "phone": "0903000123",
    "email": "milan.testner@viamo.sk"},
  "signature": {
    "description": "SHA-256 UTF-8 AES/ECB/NoPadding",
    "sign": "849F00F8F512547A3146A1B8F063ACD1"
  }
}

```

Odporúčame, aby obchodník po prijatí systémovej notifikácie robil **kontrolu podpisu systémovej notifikácie** – vytvoril podpis rovnakým spôsobom ako je popísané vyššie. Ak je prijatý podpis rovnaký s vypočítaným, správa je v poriadku.

Príklad 2: Príklad reťazca “text na podpis”, ak RID, VS ani E2E nie je známe

```
OK22.0042929ecb-b75f-4911-92f3-74fcc7a36eb3
```

5.3.2 Opakované odoslanie notifikácie

V prípade, že odoslanie systémovej notifikácie zlyhalo (nedostupný SMTP server alebo HTTP služba), systém VIAMO sa pokúsi odoslať notifikáciu znova N-krát v určitom časovom odstupe, v závislosti od konfigurácie VIAMO systému. Odporúčame, aby obchodník po prijatí notifikácie pred pokračovaním v svojom procese kontroloval unikátnosť parametra *notificationId*, a ošetril prípady, keď by tá istá notifikácia mohla vyvolať opakovanú akciu, napr. expedovanie tovaru.

5.4 PUSH notifikácia do aplikácie pre obchodníka

K identifikátoru príjemcu je možné aktivovať aplikáciu pre obchodníka. Potom po úspešnej platbe odoslanej na tento identifikátor je na toto zariadenie odoslaná PUSH notifikácia. PUSH notifikácia je odosielaná len po úspešnej platbe.