



# GP webpay

## Správa objednávek, Web Services

---

verze 2.0

květen 2009



**GPE, s.r.o.**

V Olšinách 626/80

100 00 Praha 10

Telefon: +420 267 197 111

Fax: +420 267 197 690

[www.gpe.cz](http://www.gpe.cz)

**OBSAH:**

Úvod .....	3
<b>ON-LINE ADMINISTRACE PROSTŘEDNICTVÍM WEB SERVICES.....</b>	<b>3</b>
<b>DRUHY PODPOROVANÝCH POŽADAVKŮ .....</b>	<b>4</b>
Approve Reversal .....	6
Deposit .....	9
Deposit Reversal .....	12
Credit .....	15
Credit Reversal .....	18
Order Close .....	21
Delete .....	24
Batch Close .....	27
Query Order State .....	30
<b>PŘÍLOHY .....</b>	<b>33</b>
<b>PŘÍLOHA 1 – PODEPISOVÁNÍ ZPRÁV .....</b>	<b>33</b>
Podpisování požadavku .....	33
Podpisování odpovědi .....	34
Výpočet elektronického podpisu .....	34
Ověření elektronického podpisu .....	34
Grafické znázornění generování a ověření.....	35
Použité klíče .....	36
Formáty předávaných klíčů .....	36
Logování.....	37
Reference .....	37
<b>PŘÍLOHA 2 – SEZNAM NÁVRATOVÝCH KÓDŮ .....</b>	<b>38</b>
<b>PŘÍLOHA 3 – STAV OBJEDNÁVKY .....</b>	<b>40</b>

## Úvod

Dokument informuje o možnosti integrace on-line komunikace elektronického obchodu obchodníka a systému GP webpay prostřednictvím Web Services. Dokument dále obsahuje podrobný popis on-line rozhraní Web Services.

Aplikace **GP webpay** (dále jen GP webpay) je internetová platební brána, která umožňuje elektronickým obchodům (dále jen e-shop) přijímat platby, uskutečněné platebními kartami asociací VISA a MasterCard, v prostředí sítě Internet.

GP webpay plně podporuje standard 3-D Secure a poskytuje možnost integrovat funkčnost standardního webového rozhraní formou Web Services

Komunikace s GP webpay je zajištěna:

- on-line formou zaslání administrativního požadavku do GP webpay. Následuje zpracování přijatého požadavku a zaslání výsledku zpracování požadavku. Detailní popis je součástí tohoto dokumentu;
- on-line formou zaslání požadavku na vytvoření objednávky do GP webpay. Následuje zpracování přijatého požadavku a zaslání výsledku zpracování požadavku. Detailní popis je součástí dokumentu – **GP webpay – Seznámení se systémem, vytváření objednávek**;
- prostřednictvím standardně dodávaného webového rozhraní aplikace. Detailní popis administrace GP webpay je součástí dokumentu – **GP webpay - Administrace**.

## ON-LINE ADMINISTRACE PROSTŘEDNICTVÍM WEB SERVICES

Standardní administrace GP webpay je přístupná prostřednictvím standardně dodávaného grafického webového rozhraní na adrese, která bude uvedena ve smlouvě.

Kromě tohoto rozhraní je k dispozici možnost zasílat požadavky podle standardu Web Services definovaného organizací W3C (více na adrese [www.w3.org](http://www.w3.org)).

Vzhledem k tomu, že aplikace GP webpay administrativní požadavky podporuje, je možné integrovat kompletní funkčnost standardně poskytovaného webového administrativního rozhraní do systémů obchodníka.

Zasílaný požadavek (HTTPS request) pro administraci musí splňovat následující podmínky:

- Web Services standard definovaný organizací W3C;
- komunikace s GP webpay probíhá dle definice W3C Web Services.

Popis standardu Web Services, včetně komunikace prostřednictvím Web Services, není součástí dokumentu – více informací na adrese [www.w3.org](http://www.w3.org).

## DRUHY PODPOROVANÝCH POŽADAVKŮ

GP webpay definuje následující množinu požadavků, jejichž zpracování je přímo závislé na předchozím stavu objednávky/dávky.

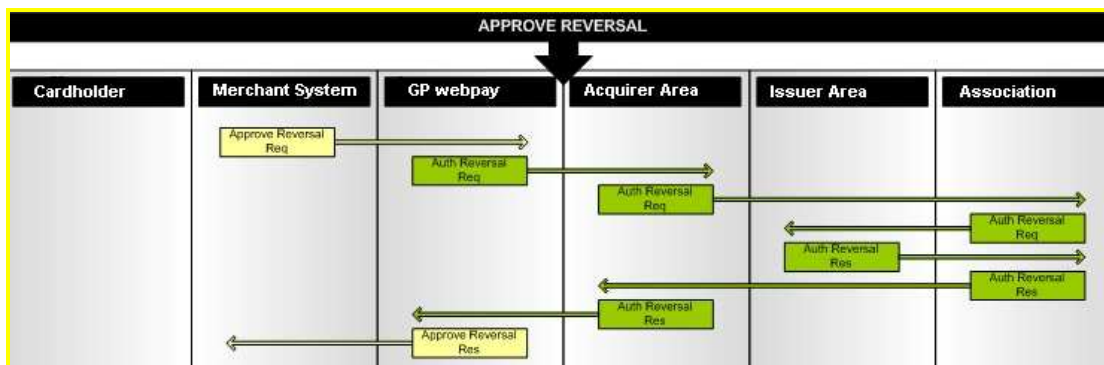
Dle výsledku zpracování požadavku se změní stav objednávky/dávky.

Detailní popis stavů objednávek/dávek je součástí dokumentu **GP webpay – Seznámení se systémem, vytváření objednávek**.

Požadavek	Význam	Popis	Předchozí možné stavy	Výsledné možné stavy
<b>approve</b>	Autorizace objednávky	Požadavek na vytvoření a zpracování autorizace k dané objednávce.  Platí pouze pro objednávku, která nebyla autorizována.	<b>Neukončena REQUESTED</b>	<b>Autorizována APPROVED</b>  <b>Neautorizována UNAPPROVED</b>
<b>approveReversal</b>	Zneplatnění autorizace objednávky	Požadavek na zneplatnění autorizace objednávky.  Platí pouze pro úspěšně autorizované objednávky.	<b>Autorizována APPROVED</b>	<b>Reverzována REVERSED</b>
<b>deposit</b>	Úhrada objednávky	Požadavek na úhradu (zaúčtování) objednávky. Označí objednávku pro následné zpracování, po kterém bude zaslán požadavek na zaúčtování finanční transakce zúčtovací bance.  Vlastní zaúčtování je v kompetenci zúčtující banky.  Platí pouze pro úspěšně autorizované objednávky.	<b>Autorizována APPROVED</b>	<b>Uhrazena DEPOSITED</b>
<b>depositReversal</b>	Zneplatnění úhrady objednávky	Požadavek na zneplatnění úhrady objednávky.  Platí pouze pro uhrazené objednávky, které ještě nebyly zpracovány – nedojde k převodu finančních prostředků od držitele karty k obchodníkovi	<b>Uhrazena DEPOSITED</b>	<b>Autorizována APPROVED</b>
<b>Credit</b>	Návrat objednávky	Požadavek na návrat úhrady objednávek, které již byly zpracovány.  Označí objednávku pro následné zpracování, po kterém budou finanční prostředky převedeny od obchodníka zpět k držiteli karty.	<b>Zpracována PROCESSED</b>  <b>Kreditována CREDITED</b>	<b>Kreditována CREDITED</b>

Požadavek	Význam	Popis	Předchozí možné stavy	Výsledné možné stavy
<b>creditReversal</b>	Zneplatnění návratu objednávky	Požadavek na zrušení, zneplatnění úhrady objednávky.  Platí pouze pro zneplatněné objednávky, které ještě nebyly zpracovány – nedojde k zpětnému převodu finančních prostředků od obchodníka k držiteli karty.	<b>Kreditována CREDITED</b>  Dávka s kreditem musí být otevřená	<b>Uhrazena DEPOSITED</b>  (v případě, že další platné kredity neexistují)  <b>Kreditována CREDITED</b>
<b>orderClose</b>	Uzavření objednávky	Požadavek na uzavření objednávky.	<b>Uhrazena DEPOSITED</b>  <b>Zpracována PROCESSED</b>  <b>Kreditována CREDITED</b>	<b>Uzavřena CLOSED</b>
<b>delete</b>	Odstranění objednávky	Požadavek na odstranění objednávky.	<b>Zamítnuta DECLINED</b>  <b>Reverzována REVERSED</b>  <b>Uzavřena CLOSED</b>	<b>Vymazána DELETED</b>
<b>batchClose</b>	Uzavření dávky objednávek	Požadavek na uzavření dávky obsahující objednávky, označené pro další zpracování.  Není nezbytně nutné zasílat tento požadavek. Uzavírání dávek probíhá automaticky před každým zpracováním dávek.		
<b>queryOrderSate</b>	Stav objednávky	Požadavek na zjištění aktuálního stavu objednávky – na dotaz se vrátí aktuální stav dané objednávky.	<b>libovolný</b>	

## APPROVE REVERSAL



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Approve Reversal Req	GP webpay obdrží požadavek na zneplatnění autorizace dané objednávky.
Auth Reversal Req	GP webpay vytvoří požadavek na zneplatnění autorizace finanční transakce, který předá do autorizačního centra. Požadavek je předán prostřednictvím finančních sítí vydavateli karty, který zneplatní autorizaci dané finanční transakce.
Auth Reversal Res	GP webpay obdrží odpověď na autorizační požadavek.
Approve Reversal Res	GP webpay zašle výsledek autorizace objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka byla úspěšně autorizována – je ve stavu: **APPROVED**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay vytvoří požadavek na zneplatnění autorizace a ten předá ke zpracování do autorizačního centra.

Podle výsledku zneplatnění autorizace může být objednávka ve stavu:

- APPROVE\_REVERSED** – autorizace objednávky byla úspěšně zneplatněna;  
**APPROVED** – objednávka zůstává úspěšně autorizována – autorizaci nebylo možné zneplatnit.

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné zneplatnění autorizace objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

#### FORMÁT POŽADAVKU:

Request	approveReversal			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno zneplatnění autorizace.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

#### FORMÁT ZASLANÉ ODPOVĚDI:

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsah pole z požadavku.
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

Příklad zaslání požadavku a obdržení odpovědi:

#### Požadavek:

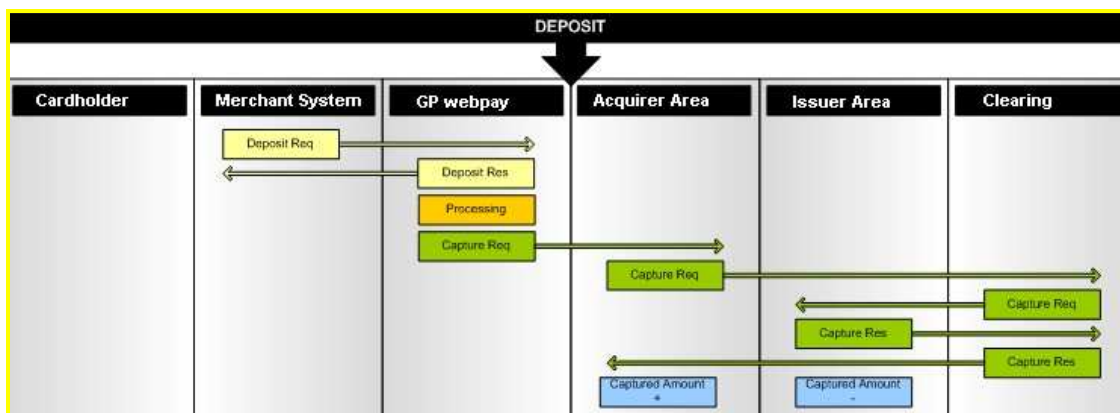
```
request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:approveReversal
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">5500216</orderNumber>
      <digest
xsi:type="xsd:string">FF3CtsvmNbrwSqWji8+WT2l4gaZn9rgj3b2tYT3wFdwTtwfi1vNxkVgL
iueKM73LVEiBYUn9wI9GqpXVbysEUy6KTDIMKa6ymtn9yDHeoQXT4l52uGwQ0UuP9kRo
vSiZ7+gt7muJeLiwLjG96qz0vhfP8k8SyvEnk5W8tBHVIlfz4aUKntoFk0nO4FXuealBz6x9s
HzZ6SMwlk+1P/bJokufsHi/9mcp0wt3HNsPkEBhOgltsWAj4u/tYhsd++aQyuVa4SKDYG93
AN65IngwvpCVj63wwrCVIMifd5ZLahw0llgR2+3wUqCqSeeH/hxlyytqNH9xMQ1Zyg/XVQ
00w==</digest>
    </ns1:approveReversal>
  </soapenv:Body>
</soapenv:Envelope>
```

#### Odpověď:

```
soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:approveReversalResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:approveReversalReturn href="#id0"/>
    </ns1:approveReversalResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">f6xQrdOdAmOeb2X3zybHgdvcq9roFIdSnWWrL2wMgPKipYDghyXp
Jtq5kiVbmGbGwo2POsrBLJK2DVB/QR2yqhrYocJQcL52dw/yEsDaWIIHuQGanerGLX1lv
JisjVye22o8m7nKkOUIyv57VinM2YTAw3ouprpX9QAhn9sGNVI7dzvmNwhzMIXNj3ilf6vl+
SgCZodOpvvn3+TGF9eqLK9rGC2a9qpWMelVCFRfiweZ0kefwbl8Bhe4fa06jETBK9JM4tP
sbJcSf4bi3ph1EHZhGZjg+oxuq3OYW3vsoHrUX2GMwRz2Z+MP3ZQd53A9Zdw17e/1ZRK
01sj7Cum2RA==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">5500216</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175164385405548660</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```



## DEPOSIT



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Deposit Req	GP webpay obdrží požadavek na úhradu dané objednávky.
Deposit Res	GP webpay označí danou objednávku pro zpracování a zašle výsledek zaúčtování objednávky.
Processing	GP webpay zpracuje všechny objednávky určené ke zpracování.
Capture Req	GP webpay vytvoří požadavek na zaúčtování objednávky. Požadavek je předán prostřednictvím mezibankovních sítí vydavateli karty, který provede zaúčtování.
Capture Res	Bance daného obchodníka je potvrzeno zaúčtování objednávky.
Capture Amount +	Na účet obchodníka je připsána zaúčtovaná částka.
Captured Amount -	Z účtu držitele karty je odepsána zaúčtovaná částka.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka byla úspěšně autorizována – je ve stavu: **APPROVED**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje požadovanou částku – zda je rovna (nebo menší) než původně autorizovaná částka;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay vytvoří požadavek na zaúčtování objednávky. Stav objednávky se změní na:  
**DEPOSITED – BATCH OPEN**

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné zaúčtování objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

#### Formát požadavku

Request	deposit			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno zaúčtování.
amount	numerický	12	ano	Částka v nejmenších jednotkách dané měny.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetězených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

#### Formát zaslané odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku.
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zaslaného požadavku a obdržené odpovědi

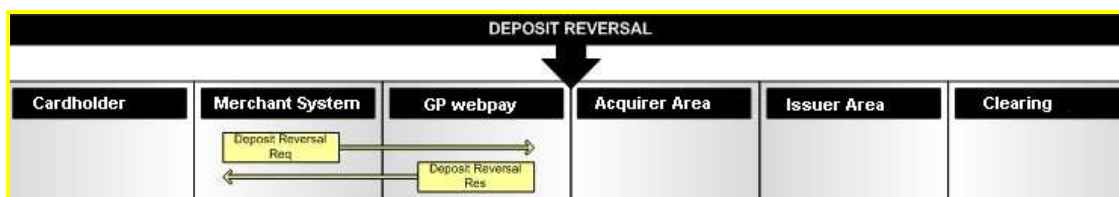
### Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:deposit soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">655210</orderNumber>
      <amount xsi:type="xsd:long">10</amount>
      <digest
xsi:type="xsd:string">RWW3TKBaL1kOJ+ZiEF/liV8xe9WiRKB67fFSPKM/KFwvDBUaZqgw
AhC1KIW/uhTTtb905tHI/LHPbqjtVen3+z/da35CgDmRxbcMYt1oBMpn5NZroQ5XPXlcFZvx
uSCXG3jADBHGjQwXphqsblQ2nwY82qlhFaMADnhFbn0xpwwO5OdjaBICieCTE9TFucd0
NZ4spmS0vFpAebmM+SgVT4UhmHuhfoVmta0Dof2EPS6iC3oqTepuHALKzvM9muDFvpc
O5PSUvwCEI/ghUakdaQqToPOiD3cp1TtSJKeTiBD/lhj7W05gL8/LQdbTS6aNcBGH2A3r0D
Eqn3IRh/cvQw==</digest>
    </ns1:deposit>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:depositResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:depositReturn href="#id0"/>
    </ns1:depositResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">Jmm1NR0tMg0BEWpvp0JrBg0VDMuC4umTXvwDNWhQsZFi5N2KLyk
5oE2Xdo6ndym9eRzjwJJ0VPPOr2PQo5RNsRaEbljURel0InPGppCs11pdyvCMT/tglFMlcn
q90jYc0CHFxiXlo5G8+20kxhjqXunG8zla18scD4rqgRBV7UBQD5vp1BoZjLJbOcPaNv2/s
S469x9e3PMtuehEum7JV51gOz/Qjskg7crfly4XxvR+iHlbdwJOJH9dfpHMYFhsnc70+U9B+
pcHvqDgA3/0+D58d/rYQhSsp7fT4CPf58ulauWsxsAPihLxD+QoVm7TiZqztP5m9MjjMISS
YpHiQ==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">655210</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175165068305351779</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```

## DEPOSIT REVERSAL



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Deposit Reversal Req	GP webpay obdrží požadavek na zneplatnění úhrady dané objednávky.
Deposit Reversal Res	GP webpay zneplatní úhradu dané objednávky a zašle výsledek zneplatnění úhrady objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka byla předána k zaúčtování, ale zaúčtování ještě neproběhlo, objednávka je ve stavu **DEPOSITED – BATCH OPEN**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje požadovanou částku – zda je rovna (nebo menší) než původně autorizovaná částka;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay vytvoří požadavek na zaúčtování objednávky. Stav objednávky se změní na: **DEPOSITED – BATCH OPEN**

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;

- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné zneplatnění zaúčtování objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

#### Formát požadavku

Request	depositReversal			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno zneplatnění zaúčtování.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

#### Formát zaslané odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku.
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zasláního požadavku a obdržené odpovědi

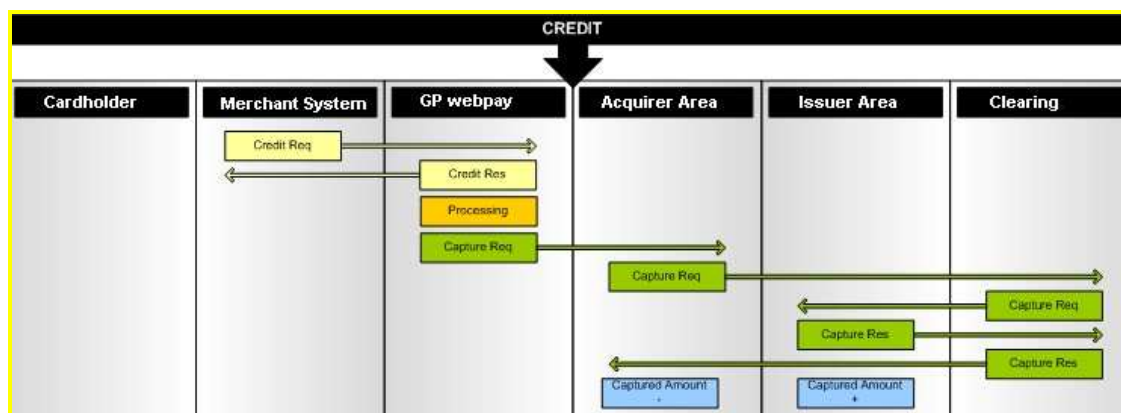
### Požadavek:

```
request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:depositReversal soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
<merchantNumber xsi:type="xsd:string">501</merchantNumber>
<orderNumber xsi:type="xsd:string">3325687</orderNumber>
<digest
xsi:type="xsd:string">Pj1e/bp6iFmrMZ5DFpgMV2e3KUNOkxsPnwR3oBOK2CAbUzW2N6s
AsRzdFIC5oZz3MNVrmN0eXgr+ljmd7dGq1f7OCX84h0m6uBGGbpqYAc6x/Uc3z1SBr7jE
+dNEWfzErwsd+fWitKmxOejdB/1nMwHJw/EXpP/PdPFZXV94xOhs8cg6QqVXry+j+Pyon
X8PtCUgh5hFNUqls/dZlwLURIA11ZXu7X3sPQk4QDyPko8IDiJdzl46OWcV5N8JBIZjF6KF
BVPVIsEBp4NT/te+MYjMKQbjstblJxTqBtzmbzDP2CJc/Z+CWYUtoXQSryN2vWFfbhuYEx
M5Uv2KPqvQ==</digest>
</ns1:depositReversal>
</soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:depositReversalResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
<ns1:depositReversalReturn href="#id0"/>
</ns1:depositReversalResponse>
<multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
<digest
xsi:type="xsd:string">johRn5xsfdO0mxSjAsyzHYOHYXCS5g7Rdz05ozam9N7ZX+yHQ3iO
HYQWUMqUDykRIHKYzgrQRGkdkp6tpm/NpFclUo5aGo6n5GWnwTlischmJzVqe8Eb0EN
aEP+LcFEMnKof2WUU+2mtAl2jPsr2LgfwYaYw0uZA5brxScOZLZbqyGAcn7/07kPI0eJuLO
51q+QZMLIFvsH6+DmfW/nz2T5MT5SY/IOGWPtAt0G6QZtzUw9HkRYEZhc3dGxUhje9DW
hHYhetulUi14+8jr3knNIIU3wi3pIUIIJZJ+LktXq6muOpBBWsljM7zLaW32i2F3RxOeZ5ohV1
6Hb1Tv/tA==</digest>
<ok xsi:type="xsd:boolean">true</ok>
<orderNumber xsi:type="xsd:string">3325687</orderNumber>
<primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
<secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
<requestId xsi:type="xsd:long">1175164527139471026</requestId>
</multiRef>
</soapenv:Body>
</soapenv:Envelope>
```

## CREDIT



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Credit Req	GP webpay obdrží požadavek na návrat již uhrazené objednávky.
Credit Res	GP webpay označí danou objednávku pro zpracování a zašle výsledek návratu uhrazené objednávky.
Processing	GP webpay zpracuje všechny objednávky určené ke zpracování.
Capture Req	GP webpay vytvoří požadavek na návrat již zaúčtované objednávky. Požadavek je předán prostřednictvím mezibankovních sítí vydavateli karty, který provede návrat zaúčtování.
Capture Res	Bance daného obchodníka je potvrzen návrat zaúčtování objednávky.
Capture Amount –	Z účtu obchodníka je odepsána zaúčtovaná částka.
Captured Amount +	Na účet držitele karty je připsána zaúčtovaná částka.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka již byla zaúčtována – je ve stavu:

**DEPOSITED – BATCH CLOSED**  
**CREDITED – BATCH OPEN**  
**CREDITED – BATCH CLOSED**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje požadovanou částku – zda je rovna (nebo menší) než zaúčtovaná částka;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay vytvoří požadavek na návrat zaúčtování objednávky. Stav objednávky se změní na: **CREDITED – BATCH OPEN**

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – neplatná částka;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšný návrat objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

#### Formát požadavku

Request	credit			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadován návrat finančních prostředků.
amount	numerický	12	ano	Částka v nejmenších jednotkách dané měny.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetězených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

#### Formát odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku.
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>



## Příklad zaslaného požadavku a obdržené odpovědi

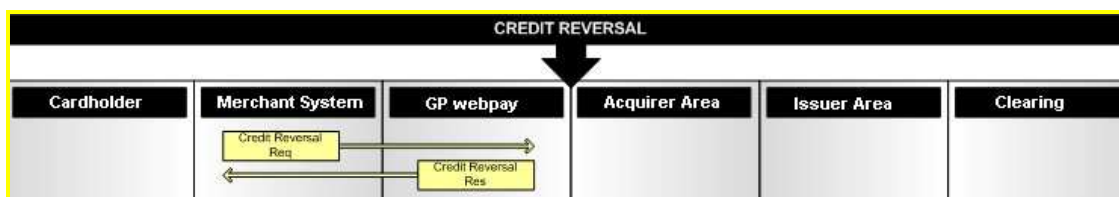
### Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:credit soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">225511</orderNumber>
      <amount xsi:type="xsd:long">0</amount>
      <digest
xsi:type="xsd:string">MTYfR82AIKXhYDPdFI24pfIR6tIkT3tQjgdNxKVOx30Mo0JW/Ma38Bz
weit/5Rt4mW6MUP9KT5lo3qkj5rxH9BPg8TEP9JTCciJMzZ16XQRo5RRux94JGcDLbqjTpX
TrA6aE9lhwyxtB/s8fZ1Q087D8EwDiooqg1Epve8VUFKunXr2BUT3XnD3rzYIYdu3Vz7N84n
NltXx7C5dnTdPWnNzCMol89uMHrtzCIHkqvPXsIOvYg4tZoDf/czIXad66shaehv2ZNXha+Y
sppiJKe9fMTwTHXbhWWswnm/Q1IGMK36+MyUSKR7VyOoEgaZoymTVWil8aqmDp6ttS7
SWb9w==</digest>
    </ns1:credit>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:creditResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:creditReturn href="#id0"/>
    </ns1:creditResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">Ng0lBz2PQUJvuwVlfqo0+gudN+V9KOCsFQQDd5TxOONRs4wmG7U
5Gjpvx42IHQ+X9/YVEH0/aAjY2bK0E7DmqSU2MWOorkuG59fS5MVIRBflbvTx+Gob1TucBV
zfulMS6Ti5yTZGTuPcfh6aorHfSlcU6+gQtOEqtNfB6Ety7C31nVLvkrOx40n1j0kMIDyPQ
GqHnCtYQDFsFQ4ZJ50n0GH8pWv4cMVJ6fVjM7fYSH8xZv8BbLRPzbQrFmXyPS/aSs1OU
p84UN4Od4t/rHtalcsGdnTKCQ0wF2d2tPHk0Lc4iGZ3DZ1uOkvg6TbNRpF+H11/HtLzoqSw
ZplnrSWYw==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">225511</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175164647398556266</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```

## CREDIT REVERSAL



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Credit Reversal Req	GP webpay obdrží požadavek na zneplatnění návratu již zaúčtované objednávky.
Credit Reversal Res	GP webpay zneplatní zaúčtování dané objednávky a zašle výsledek zneplatnění návratu již zaúčtované objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Návrat objednávky byl předán k zaúčtování, ale zaúčtování ještě neproběhlo; objednávka je ve stavu: **CREDITED – BATCH OPEN**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay vytvoří požadavek na zaúčtování objednávky. Stav objednávky se změní na:

**DEPOSITED – BATCH CLOSED**  
**CREDITED – BATCH CLOSED**

#### Chybové stavy

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné zneplatnění návratu objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

## Formát požadavku

Request	creditReversal			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno zneplatnění návratu finančních prostředků.
creditNumber	Numerický		ano	Unikátní identifikátor zneplatnění návratu v rámci dané objednávky. Z důvodu možnosti provedení několika návratů v rámci jedné objednávky je nezbytně nutné identifikovat, pro který návrat je zneplatnění požadováno.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetězených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Formát odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku.
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zaslaného požadavku a obdržené odpovědi

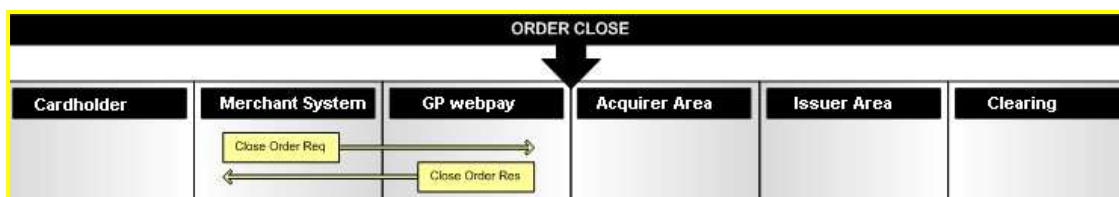
### Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:creditReversal soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">225511</orderNumber>
      <creditNumber xsi:type="xsd:int">1</creditNumber>
      <digest
xsi:type="xsd:string">MTYfR82AIKXhYDPdFI24pfIR6tIkT3tQjgdNxKVOx30Mo0JW/Ma38Bz
weit/5Rt4mW6MUP9KT5lo3qkj5rxH9BPg8TEP9JTCciJMzZ16XQRo5RRux94JGcDLbqjTpX
TrA6aE9lhwyxtB/s8fZ1Q087D8EwDiiogg1Epve8VUFKunXr2BUT3XnD3rzYIYdu3Vz7N84n
NltXx7C5dnTdPWnNzCMol89uMHrtzCIHkqvPXsIOvYg4tZoDf/czIXad66shaehv2ZNXha+Y
sppiJKe9fMTwTHXbhWWswnm/Q1IGMK36+MyUSKR7VyOoEgaZoymTVWil8aqmDp6ttS7
SWb9w==</digest>
    </ns1:creditReversal>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:creditReversalResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:creditReversalReturn href="#id0"/>
    </ns1:creditReversalResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">Ng0IBz2PQUJvuwVlfqo0+gudN+V9KOCsfQQDd5TxOONRs4wmG7U
5Gjpvx42IHQ+X9/YVEH0/aAjY2bK0E7DmqSU2MWOorkuG59fS5MVIRBflbvTx+Gob1TucBV
zfulMS6Ti5yTZGTuPcfh6aorHfSlcU6+gQtOEqtNfB6Ety7C31nVLvkrOx40n1j0kMIDyPQ
GqHnCtYQDFsFQ4ZJ50n0GH8pWv4cMVJ6fVjM7fYSH8xZv8BbLRPzbQrFmXyPS/aSs1OU
p84UN4Od4t/rHtalcsGdnTKCQ0wF2d2tPHk0Lc4iGZ3DZ1uOkvg6TbNRpF+H11/HtLzoqSw
ZplnrSWYw==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">225511</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175164677463327509</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```

## ORDER CLOSE



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Close Order Req	GP webpay obdrží požadavek uzavření objednávky.
Close Order Res	GP webpay uzavře danou objednávku a zašle výsledek uzavření objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

Nutné podmínky:

Objednávka je ve stavu:

**DEPOSITED – BATCH OPEN**  
**DEPOSITED – BATCH CLOSED**  
**CREDITED – BATCH OPEN**  
**CREDITED – BATCH CLOSED**

Zpracování:

GP webpay kontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

Výsledek:

GP webpay uzavře objednávku. Pro uzavřenou objednávkou není možné zpracovat požadavek na zaúčtování. Stav objednávky se změní na: **ORDER CLOSED**

Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné uzavření objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

## Formát požadavku

Request	orderClose			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno uzavření.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Formát zaslané odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zasláního požadavku a obdržené odpovědi

### Požadavek:

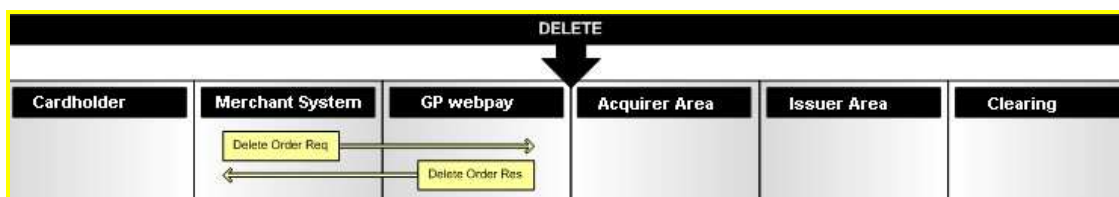
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:orderClose soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">66051</orderNumber>
      <digest
xsi:type="xsd:string">PLP9Vj1NSdCZaCivARmNS6w2UZq7BC8BvPVp/LQdk1Cza3FkQ48g
oswyF1+n1/lunw93yDqD5+DFMXDZgIOjLEiKyT1oC+IHKWp8D9I9QY7hi4Jaqlvh/ldswGU
k2Q2b5e3HYH4fjPXjO4KB0JvQUf0+2IBGEU//63eGolK06vKQkidBrYZdqDhNEixYmr6jm2Q
NTQXTGZC6JANZSHDqINrizKg3SUIrSosS3pmzZPZzmDOUPuPdQ9azeqSgJQ+B2hBP/ok
Bey713LMfGY8hTqPR3hZcDq84PPNKsN+7/9+zza5HwzGekjJ3szTvFaa3MjZiJ5c83Rva/ee
No4oFqA==</digest>
    </ns1:orderClose>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:orderCloseResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:orderCloseReturn href="#id0"/>
    </ns1:orderCloseResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">iHTq0rbVNL4jCIYw0aa7jlUryY1btHnsKUvcVeh5jW/C/52cxSVhLLg/m
eqREA0ZXcCbXC1pFXw6agWzzMnPP8yljAFAI3vW4pauwCMtVQQ1USMXQRcJLITKPYS
d9agecYlcyGt4TyQGoOBV4Lko8cEhyb6nysgesfaS2rGsy+WdW4JHqaJJAhltwuDMDS3
Hli+buZZ+0o3DFTNeeVPe0E/vBwGs9mWI5sYyJOfm+VPJUUV6Ow4FngSNMK+Luj05f9EV
gzNrGufIQvTEldXEOzYhrAKEvv/iojLLc4Gdh501+n7K55wqOGN1OidDybyAUWMh6kXRo
mhXoHv/MQx0w==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">66051</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175164501369667055</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```



## DELETE



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Delete Order Req	GP webpay obdrží požadavek na odstranění objednávky.
Delete Order Res	GP webpay odstraní danou objednávku a zašle výsledek odstranění objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka je ve stavu:

**REQUESTED**  
**PENDING**  
**DECLINED**  
**UNAPPROVED**  
**APPROVE\_REVERSED**  
**ORDER\_CLOSE**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace – zda stav objednávky povoluje požadovanou operaci;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay odstraní objednávku. Stav objednávky se změní na: **DELETED**

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné odstranění objednávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.



## Formát požadavku

Request	delete			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno odstranění.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Formát zaslané odpovědi

Response	OrderResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zaslaného požadavku a obdržené odpovědi

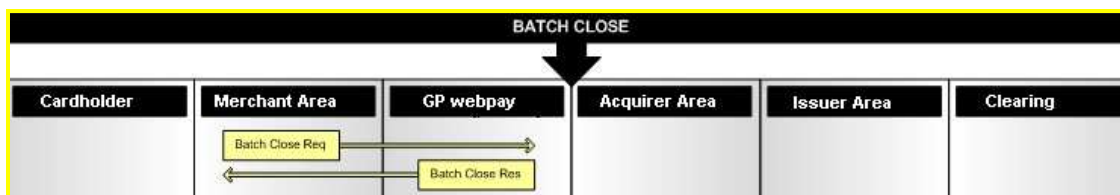
### Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:delete soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">123000154</orderNumber>
      <digest
xsi:type="xsd:string">OEPwWcsrj3EQlieVujgYheTT1ZdgOnOLSilz7C0WF0bnGyJAjepGny4
ssHE41J4NI9NIfh7KYz/CU/2JQzCeD65HstVzHUDumx83DufOXbur5zn5IPyWBR95qM3CT
ROBDliTKG9WmBO61sDVIA8QSN3Holqg1gZbjRiVRVyBBZI/rfB53RI3EsKttgZJpjqensiov
Wohkkgc3Nh5jTsfQhGwWnctCg1Opgtl9o1SxUr5RZvmvBWrrztBeTHqGQjtUXqPEbmFv3
6KNqbKALFUCAE8pRBhPdI5eDHYznPCOdEkPX0UWJzgKVP1h93ALFC8HenWwg0Wz4n
xnm7IUy/YdA==</digest>
    </ns1:delete>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:deleteResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:deleteReturn href="#id0"/>
    </ns1:deleteResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderResponse" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">NsHQi1cOFoD+Ux0AONjFU2RilysW83YihTXyYCWfUX9QmL9tHi+DR
fyPY9jpETTCbru9YXY0ko6wQLclj3BQAMX+xcNgiETqgh4uY6oElbl1+WWaGXL+L9tnwB
wrtENXmuT3Z3osk7N6uDx8Z76T89xBA3UO/O0GC3mJyBwCsSz2l9OP2BfZKw/nsGsXcb
FdCBjkMhOwqe0hioMcNt/xwjZ/VYghBiCR1FLDoQlwy2cFabL3ZcBGC8UoGmWSeXNcW
nGRbbc208nnBHtd/oALvUAgSyjzJDi6+mLxC12ku8CUyBZAqMV8YyoKjzJs/qP0/SNZERR
JZ6J1e3Ey76ug==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">123000154</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175164441240124096</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```

## BATCH CLOSE



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Batch Close Req	GP webpay obdrží požadavek na uzavření dávky objednávek určených ke zpracování.
Batch Close Res	GP webpay uzavře dávku objednávek a zašle výsledek uzavření dávky

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Dávka je ve stavu: **OPEN**

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- zkontroluje platnost zadané operace – zda stav dávky povoluje požadovanou operaci;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay odstraní objednávku. Stav dávky bude: **CLOSED**

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- neúspěšné uzavření dávky z důvodu XXX;
- požadavek nelze zpracovat – technické problémy.

## Formát požadavku

Request	batchClose			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Formát zaslané odpovědi

Response	Response			
Atribut	Typ	Délka	Povinný	Poznámka
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Příklad zaslaného požadavku a obdržené odpovědi

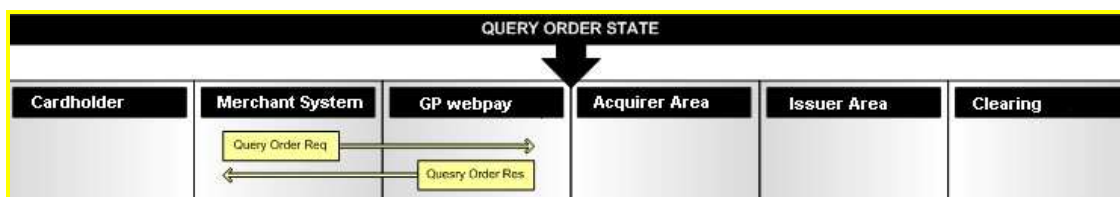
### Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:batchClose soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <digest
xsi:type="xsd:string">jqlm0drwcj+rN/nzWe57h14lWb6brEw91gtMm0dioHuksLdxX37QBXJ
92SUJhQyOX3YI7YBCK9HV33Yvm/rKRhm31qtu/xk7Tmok7HPBVRgoL8PpJfUwfgSEUIOJ
vseBIIINYuteXU4AfXc2fpV8LVFkunTqzY+Dqsr0su2hASKTRD9DNYIQunuoA5WADVaJfd9
8YARyUS2f1b3Mubs6RFdWiH5968Vfgywu7pl7GGHJI4PclHyc6ql6aPjwgvqoEV2Hh5dnC+
RHalqg+kz7XBMtEFKqM0widMG3LKb1asOIUPoibd/Nn7UILSUJQWUKzkD7OjTwTU4R7E
7wFXWwzpw==</digest>
    </ns1:batchClose>
  </soapenv:Body>
</soapenv:Envelope>
```

### Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:batchCloseResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:batchCloseReturn href="#id0"/>
    </ns1:batchCloseResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:Response" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">fBiNvJu8wNiTcSCmG6KXnQps9kE0evQrSI/fbFrAzbdav3rMy04GvSu
ba7D3wCAFzZpbd4oZo2xVyn5fvZMMgpyXThK1MazA3ZUWX18GogWxKWn0YXnK7nr1J
X9VHSY0IFmxLQ+DaVrcsgW2c7AZ5HMF16mLvJ8DRBz5uBCZ4bKII8R0Dy3MixoAr7b7
G9j1Md6nj+eyPqmbh7cp8JF6Sj5UM/bxt9+9pWe6AqeEuBZt1XH9595spxnIXKMxyO5KDjT
7bJmOKD0JtTrh/wc5XdncagDdJQ/ih3o5IIWsYz+QETH6ahlqivPmqTNN5l8dppm8p+DEor
+VYpjJUNVuQ==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <requestId xsi:type="xsd:long">1175165149909730553</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```

## QUERY ORDER STATE



### POPIS ZPRACOVÁNÍ POŽADAVKU

Akce	Popis
Query Order State Req	GP webpay obdrží požadavek na zjištění aktuálního stavu objednávky.
Query Order State Res	GP webpay zašle výsledek obsahující aktuální stav objednávky.

### PRŮBĚH ZPRACOVÁNÍ POŽADAVKU

#### Nutné podmínky:

Objednávka je v libovolném stavu.

#### Zpracování:

GP webpay zkontroluje platnost zadaných údajů:

- vyhledá požadovaného obchodníka;
- vyhledá požadovanou objednávku;
- zkontroluje platnost zadané operace;
- zkontroluje podpis požadavku;
- zkontroluje platnost obsahu (délka, typ, hodnota) všech prvků.

#### Výsledek:

GP webpay předá detailní informace o objednávce.

#### Chybové stavy:

- požadavek nelze zpracovat – obchodník nenalezen;
- požadavek nelze zpracovat – objednávka nenalezena;
- požadavek nelze zpracovat – neplatná operace;
- požadavek nelze zpracovat – chybný podpis dat;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovaný typ;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou délku;
- požadavek nelze zpracovat – prvek XXX neobsahuje požadovanou hodnotu;
- požadavek nelze zpracovat – technické problémy.

## Formát požadavku

Request	queryOrderState			
Vstupní parametr	Typ	Délka	Povinný	Poznámka
merchantNumber	numerický		ano	Přidělené číslo obchodníka.
orderNumber	numerický	15	ano	Číslo objednávky, pro kterou je požadováno zjištění aktuálního stavu.
digest	znakový		ano	Kontrolní podpis všech výše uvedených polí, zřetěžených se sdílenou tajnou informací, za využití hash funkce SHA1. Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

## Formát zaslané odpovědi

Response	OrderStateResponse			
Atribut	Typ	Délka	Povinný	Poznámka
orderNumber	numerický	15	ano	Obsahuje orderNumber z požadavku.
state	numerický		ano	Obsahuje aktuální stav objednávky, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
primaryReturnCode	numerický		ano	Obsahuje primární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
secondaryReturnCode	numerický		ano	Obsahuje sekundární kód, viz <a href="#">Příloha 2 – Seznam návratových kódů</a>
digest	znakový		ano	Popis algoritmu výpočtu pole DIGEST viz <a href="#">Příloha 1 – Podepisování zpráv</a>

# Příklad zaslaného požadavku a obdržené odpovědi

## Požadavek:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:queryOrderState soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <merchantNumber xsi:type="xsd:string">501</merchantNumber>
      <orderNumber xsi:type="xsd:string">655210</orderNumber>
      <digest
xsi:type="xsd:string">RWW3TKBaL1kOJ+ZiEF/liV8xe9WiRKB67fFSPKM/KFwvDBUaZqgw
AhC1KIW/uhTTtb905tHI/LHPbqjtVen3+z/da35CgDmRxbcMYt1oBMpn5NZroQ5XPXlcFZvx
uSCXG3jADBHGJQwXphqsblQ2nwY82qlhFaMADnhFbn0xpwwO5OdjaBICieCTE9TFucd0
NZ4spmS0vFpAebmM+SgVT4UhmHuhfoVmta0Dof2EPS6iC3oqTepuHALKzvm9muDFvpc
O5PSUvwCEl/ghUakdaQqToPOiD3cp1TtSJKeTiBD/lhj7W05gL8/LQdbTS6aNcBGH2A3r0D
Eqn3IRh/cvQw==</digest>
    </ns1:queryOrderState>
  </soapenv:Body>
</soapenv:Envelope>
```

## Odpověď:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:queryOrderStateResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://webservices.pgw.muzo.com">
      <ns1:queryOrderStateReturn href="#id0"/>
    </ns1:queryOrderStateResponse>
    <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:OrderStateResponse"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://request.pgw.muzo.com">
      <digest
xsi:type="xsd:string">pg2MQgnrkoIKFyA3uj2KBkMXLa+Oj4K6fC6TKlu2QZmQ3rfAtAe3hCt
0sgZy3Nqj1dNWP/jk2LMBKBoGqVF50WLFsKPshBoYLBqRWtKTuWuFBVfVS7pT4zSpLX
UIVgKDbueC4A8MQ2FW9Jmr94xpBjnSonigqcQEuYX7iKvlt5jc4fFKic3WPo0+3XPyLxDqc
qaSkx2FqqTBUM/Z68nTQ7wNcAhaDbL77yJrSjDTve0RsQvefJozc3bqps++MXXxl6CeN57i
qXC7QW8e3EVQVYYbPQD8ykR11cKxFx+YR6WuqZQ1tWERu1142j7Cg96ON2BuckvAP6
DLbRv90HkVw==</digest>
      <ok xsi:type="xsd:boolean">true</ok>
      <orderNumber xsi:type="xsd:string">655210</orderNumber>
      <primaryReturnCode xsi:type="xsd:int">0</primaryReturnCode>
      <secondaryReturnCode xsi:type="xsd:int">0</secondaryReturnCode>
      <state xsi:type="xsd:int">8</state>
      <requestId xsi:type="xsd:long">1175165175679534435</requestId>
    </multiRef>
  </soapenv:Body>
</soapenv:Envelope>
```



## **PŘÍLOHY**

### **PŘÍLOHA 1 – PODEPISOVÁNÍ ZPRÁV**

#### **PODEPISOVÁNÍ POŽADAVKU**

---

GP webpay přijímá pouze ty požadavky, u kterých lze doložit, že původcem požadavku byl oprávněný subjekt, tedy obchodník, se kterým GPE, s.r.o. uzavřela smlouvu o poskytování služby GP webpay.

K prokázání původu požadavku slouží pole DIGEST. Jeho obsah byl vypočten na základě:

- zaslaných dat - tím je prokázáno, že obsah jednotlivých polí nebyl cestou změněn,
- soukromého klíče – tím je prokázáno, že požadavek pochází od daného obchodníka.

Při uzavírání smlouvy obchodník vygeneruje dvojici soukromý/veřejný klíč s parametry, uvedenými ve smlouvě.

Soukromý klíč obchodník bezpečně uloží. Veřejný klíč ve formátu DER poskytne obchodník poskytovateli na některém z médií (CD, disketa). Tento klíč bude uložen v databázi a před přijetím libovolného požadavku od obchodníka se pomocí veřejného klíče v GP webpay bude kontrolovat, zda obchodník podepsal požadavek prostřednictvím svého soukromého klíče.

Požadavky bez pole DIGEST, anebo s neodpovídajícím obsahem pole DIGEST budou zamítnuty s důvodem:

"SRCODE=5 nebo 31, SRCODE=34 a popisem "Chybi povinne pole, DIGEST" anebo "Chybny podpis".

Pole DIGEST, obsažené v předávaných datových zprávách, obsahuje elektronický podpis všech ostatních polí zprávy. Tento podpis zajišťuje integritu a nepopiratelnost předávané zprávy.

Pro výpočet a ověření elektronického podpisu slouží jako datová zpráva řetězec, sestavený jako součet (concatenation) textové interpretace hodnot všech polí v zasílaném požadavku, s výjimkou pole DIGEST. Při sestavení vstupní zprávy je nutné dodržet pořadí polí stejné, jaké je v definici příkazu.

U příkazu CREATE\_ORDER se tedy zdrojem pro výpočet pole DIGEST stane hodnota, která vznikne zřetěžením obsahů polí v tomto pořadí:

MERCHANTNUMBER + OPERATION + ORDERNUMBER + AMOUNT + CURRENCY + DEPOSITFLAG + MERORDERNUM + URL + DESCRIPTION + MD.

V případě, že v požadavku není obsaženo některé z nepovinných polí, pole se přeskočí. Pokud obchodník posílá pouze povinné parametry, k výpočtu pole DIGEST slouží hodnota:

MERCHANTNUMBER+OPERATION+ORDERNUMBER+AMOUNT+DEPOSITFLAG+URL.

## PODEPISOVÁNÍ ODPOVĚDI

---

Všechny odpovědi z GP webpay obsahují také pole DIGEST, jehož obsah byl vypočten:

- na základě údajů, obsažených v odpovědi;
- a současně na základě soukromého klíče GP webpay.

Při podpisu smlouvy bude druhé straně poskytnut veřejný klíč GP webpay, který slouží obchodníkovi k ověření obsahu pole DIGEST.

Tímto způsobem se zasilatel požadavku může přesvědčit, že:

- odpověď pochází skutečně od GP webpay;
- odpověď nebyla cestou změněna.

## VÝPOČET ELEKTRONICKÉHO PODPISU

---

Vstupy: datová zpráva (zpráva)

privátní RSA klíč (s modulem délky K)

Výstupy: elektronický podpis (BASE64 kódovaný), délka přibližně  $K \cdot 1,5$

Výpočet elektronického podpisu probíhá následujícím způsobem

- ze zprávy je vypočtena hodnota hash funkce SHA-1 [3]
- hash je zakódován na vstupní hodnotu pro RSA podpis algoritmem EMSA-PKCS1-v1\_5-ENCODE podle části 9.2.1 [1].

Toto kódování je provedeno takto:

01 | FF\* | 00 | 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 | hash

kde znaky FF se opakují tolikrát, až je celková délka řetězce o jeden oktet kratší než modulus klíče. Znak | značí spojení řetězců (concatenation).

- na výstupní hodnotě z b) je proveden RSA podpis v souladu s částí 8.1.1 [1] RSASSA-PKCS1-V1\_5-SIGN
- Výstup c) je zakódován pomocí BASE64

## OVĚŘENÍ ELEKTRONICKÉHO PODPISU

---

Vstupy: datová zpráva

elektronický podpis (BASE64 kódovaný)

veřejný RSA klíč

Výstupy: logická hodnota - ano – podpis je platný;

- ne – podpis není platný nebo nebylo jeho ověření možné.

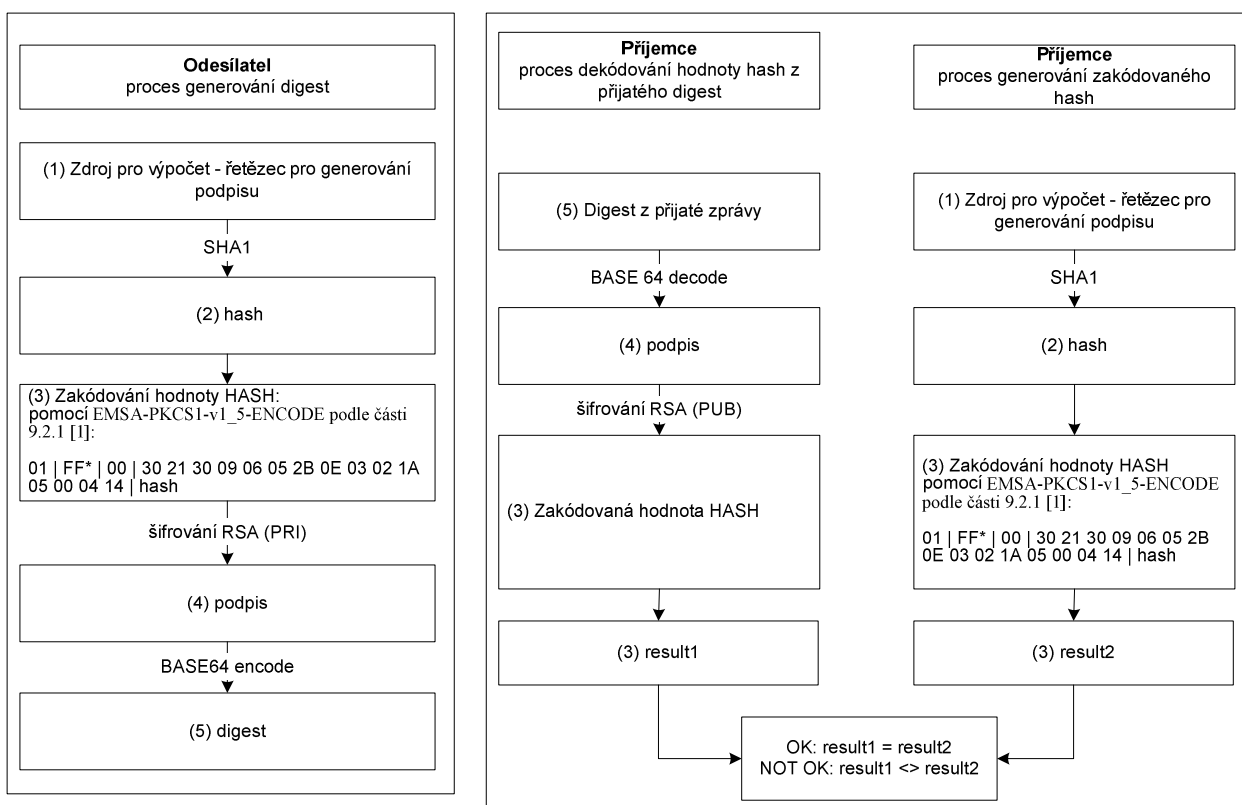
Verifikace elektronického podpisu probíhá v souladu s částí 8.1.2 [1] v těchto hlavních krocích:

- podle nastavení obchodníka v systému GPE je vybrán správný veřejný klíč a ověřena jeho integrita;
- elektronický podpis je BASE64 dekodován;
- výstup b) je dešifrován pomocí vybraného veřejného klíče;
- ze zprávy je vypočtena miniatura (hash) a zakódována v souladu s předchozí částí "Výpočet elektronického podpisu" body a) - b);

- e) elektronický podpis dešifrovaný podle c) je porovnán s výsledkem podle d) a pokud jsou shodné, vrací funkce logickou pravdu (podpis je platný).  
V opačném případě vrací funkce logickou nepravdu (podpis není platný).

Aplikace, která vyhodnocuje elektronický podpis, musí vyhodnotit podpis jako neplatný i v případě, kdy jeho ověření nebylo možné (například kvůli nedostupnosti klíče).

## GRAFICKÉ ZNÁZORNĚNÍ GENEROVÁNÍ A OVĚŘENÍ



## POUŽITÉ KLÍČE

Pro vytvoření podpisu budou použity RSA klíče (keyPair) o délce modulu 2048 bitů. Při komunikaci mezi GP webpay a obchodníkem budou využity následující páry klíčů:

<b>KeyPair GPE</b>	Privátní klíč GPE ( $GPE_{PRI}$ )	Použit pro výpočet elektronického podpisu zpráv odesílaných GPE.	
	Veřejný klíč (certifikát) GPE ( $GPE_{PUB}$ )	Použit obchodníkem k ověření elektronického podpisu zpráv zasílaných GPE .	Bude předáván ve formě X509 certifikátu
<b>KeyPair obchodníka</b>	Privátní klíč obchodníka ( $MERCH_{PRI}$ )	Použit pro výpočet elektronického podpisu zpráv odesílaných obchodníkem.	
	Veřejný klíč (certifikát) obchodníka ( $MERCH_{PUB}$ )	Použit v GPE k ověření elektronického podpisu zpráv zasílaných obchodníkem.	Předáván ve formě X509 self-signed certifikátu

Aplikaci pro vytvoření self-signed certifikátu obdrží obchodník při zažádání o uzavření smlouvy mezi obchodníkem a firmou GPE, s.r.o.

Veřejný klíč bude předán určenému správci v GPE při podpisu smlouvy. Součástí smlouvy je formulář s identifikačními údaji o certifikátu obchodníka. Po podpisu smlouvy obdrží obchodník veřejný klíč GPE a detailní postupy pro manipulaci s klíči (výměna, odvolání platnosti).

## FORMÁTY PŘEDÁVANÝCH KLÍČŮ

Formát privátních klíčů, používaných pro vytváření elektronického podpisu zpráv, závisí na použité technologii a není tímto dokumentem předepsán.

Veřejné klíče budou předávány ve formě self-signed X509 certifikátů šifrovaných ve formátu DER a s následujícími parametry profilu<sup>1</sup>.

Parametr	Hodnota	Poznámky
Version	3	
Subject a Issuer	CN=<Jméno obchodníka>:<Merchant ID>:<banka>, OU=PayMUZO, O=MUZO,C=CZ	Jméno obchodníka tvoří obchodní jméno (podnikatelský název) obchodníka, bez diakritiky, včetně dodatků. MerchantID je jednoznačný identifikátor obchodníka přiřazený bankou. Banka je označení Acquirer banky, se kterou má obchodník uzavřenou smlouvu.

<sup>1</sup> Parametry odpovídají RFC 2459 [4]

Parametr	Hodnota	Poznámky
CertificateSerialNumber	MerchantID+pořadové číslo certifikátu	V případě obnovy nebo výměny klíče musí být pořadové číslo zvýšeno vždy o 1.
signatureAlgorithm	sha-1WithRSAEncryption	
Validity	10 let od okamžiku vystavení	
keyUsage	nonRepudiation && digitalSignature	
extendedKeyUsage	Nenastaveno	
SubjectPublicKeyInfo::= algorithm	RSA	Délka modulu klíče musí být 2048 bitů.

Ostatní hodnoty profilu certifikátu nejsou předepsány.

## LOGOVÁNÍ

Aplikace, která ověřuje elektronický podpis, musí ve svých auditních záznamech uchovávat všechny informace o úspěšných i neúspěšných verifikacích elektronického podpisu. Pro ověření záznamů je nutné logovat veškeré údaje nutné k ověření, respektive opětovnému ověření elektronického podpisu. Jedná se především o elektronický podpis, pole, která byla využita pro jeho vytvoření a výsledek jeho ověření. V případě chybějících nebo nekompletních záznamů nebude možné uznat autentičnost takových transakcí.

## REFERENCE

Další informace o mechanismu výpočtu pole DIGEST lze nalézt v těchto dokumentech:

- [1] **RFC 2437**, PKCS #1: RSA Cryptography Specifications, October 1998;
- [2] **XML-Signature Syntax and Processing**, W3C Recommendation 12 February 2002, <http://www.w3.org/TR/xmlsig-core/>;
- [3] **RFC 3174** - US Secure Hash Algorithm 1 (SHA1), September 2001;
- [4] **RFC 2459** – Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999

Pro vytvoření elektronického podpisu je možné použít například následující kryptografické knihovny a komponenty:

JCE Cryptix: alternativní JCE Provider, poskytující algoritmus pro RSA/SHA1/PKCS#1 podpis, [www.cryptix.org](http://www.cryptix.org) (dočasně nedostupné)

Bouncy Castle: alternativní JCA Provider, poskytující knihovny pro generování certifikátů a práci s PKCS#12 úložišti certifikátů, [www.bouncycastle.org](http://www.bouncycastle.org).

Crypto++ volně šiřitelná C++ knihovna kryptografických funkcí podporující také RSA/SHA1/PKCS#1 algoritmus, [www.cryptopp.com](http://www.cryptopp.com)

Chilkat Easy RSA – ActiveX componenta pro Windows od Chilkat software (developerská licence cca 75 USD), podporující RSA algoritmus.

## PŘÍLOHA 2 – SEZNAM NÁVRATOVÝCH KÓDŮ

Výsledek zpracování v GP webpay je dán dvojicí návratových kódů. V případě, že jsou různé od nuly, PRCODE obsahuje typ chyby, a nenulové SRCODE obsahuje upřesnění chyby.

### Příklad:

PRCODE=1 SRCODE=8 oznamuje, že v příchozím požadavku bylo pole DEPOSITFLAG příliš dlouhé. RESULTTEXT, vrácený v tomto případě má hodnotu "Pole příliš dlouhé, DEPOSITFLAG".

RESULTTEXT je vhodné zobrazit nakupujícímu v případě, že se vrátí PRCODE = 28 a 30, případně 1000. V ostatních případech je chyba pravděpodobně na straně software obchodníka.

### PRCODE / PRIMARYRETURNCODE

PRCODE / primaryReturnCode		
Hodnota	Význam CS	Význam EN
0	OK	OK
1	Pole příliš dlouhé	Field too long
2	Pole příliš krátké	Field too short
3	Chybný obsah pole	Incorrect content of field
4	Pole je prázdné	Field is null
5	Chybí povinné pole	Missing required field
11	Neznámý obchodník	Unknown merchant
14	Duplikátní číslo objednávky	Duplicate order number
15	Objekt nenalezen	Object not found
17	Částka k úhradě překročila autorizovanou částku	Amount to deposit exceeds approved amount
18	Součet kreditovaných částek překročil uhrazenou částku	Total sum of credited amounts exceeded deposited amount
20	Objekt není ve stavu odpovídajícím této operaci	Object not in valid state for operation
26	Technický problém při spojení s autorizačním centrem	Technical problem in connection to authorization center
27	Chybný typ objednávky	Incorrect order type
28	Zamítnuto v 3D Důvod zamítnutí obsahuje SRCODE	Declined in 3D
30	Zamítnuto v autorizačním centru Důvod zamítnutí obsahuje SRCODE	Declined in AC
31	Chybný podpis	Wrong digest
1000	Technický problém	Technical problem

## SRCODE / secondaryReturnCode

SRCODE / secondaryReturnCode		
Hodnota	Význam CS	Význam EN
0	Bez významu	
<b>V případě PRCODE 1 až 5, 15 a 20 se mohou vrátit následující SRCODE</b>		
1	ORDERNUMBER	ORDERNUMBER
2	MERCHANTNUMBER	MERCHANTNUMBER
6	AMOUNT	AMOUNT
7	CURRENCY	CURRENCY
8	DEPOSITFLAG	DEPOSITFLAG
10	MERORDERNUM	MERORDERNUM
11	CREDITNUMBER	CREDITNUMBER
12	OPERATION	OPERATION
18	BATCH	BATCH
22	ORDER	ORDER
24	URL	URL
25	MD	MD
26	DESC	DESC
34	DIGEST	DIGEST
<b>V případě PRCODE 28 se mohou vrátit následující SRCODE</b>		
3000	Neúspěšné ověření držitele karty. Kontaktujte vydavatele karty.	Cardholder not authenticated in 3D. Contact your card issuer.
3001	Držitel karty ověřen	Authenticated
3002	Vydavatel karty nebo karta není zapojena do 3D. Kontaktujte vydavatele karty.	Issuer or Cardholder not participating in 3D. Contact your card issuer.
3004	Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. Kontaktujte vydavatele	Issuer not participating or Cardholder not enrolled. Contact your card issuer.
3005	Technický problém při ověření držitele karty. Kontaktujte vydavatele karty.	Technical problem during Cardholder authentication. Contact your card
3006	Technický problém při ověření držitele karty.	Technical problem during Cardholder authentication.
3007	Technický problém v systému zúčtování banky. Kontaktujte obchodníka.	Acquirer technical problem. Contact the merchant.
3008	Použit nepodporovaný karetní produkt. Kontaktujte vydavatele karty.	Unsupported card product. Contact your card issuer.
<b>V případě PRCODE 30 se mohou vrátit následující SRCODE</b>		
1001	Neúspěšná autorizace – karta blokována	Unsuccessful authorization – blocked card.
1002	Autorizace zamítnuta	Authorization declined.
1003	Neúspěšná autorizace – problém karty. Kontaktujte vydavatele karty.	Unsuccessful authorization – Card problem. Contact your card issuer.
1004	Neúspěšná autorizace – technický problém v autorizačním centru	Unsuccessful authorization – technical problem in authorization process.
1005	Neúspěšná autorizace – problém účtu. Kontaktujte vydavatele karty.	Unsuccessful authorization – Account problem. Contact your card issuer.

### PŘÍLOHA 3 – STAV OBJEDNÁVKY

State – stav objednávky		
Hodnota	Stav	Popis stavu
1	Neukončena <b>REQUESTED</b>	Objednávka byla úspěšně přijata do GP webpay – čeká se na výsledek vyplnění citlivých informací držitele karty.
2	Neukončena <b>PENDING</b>	Pokud držitel karty vyplnil citlivé informace, je zaslán dotaz do 3D systému, zda je požadována autentikace držitele karty. Čeká se na výsledek z 3D systému.
3	Neukončena <b>CREATED</b>	Jestliže držitel karty přeruší zadávání údajů karty, je to finální stav objednávky.
4	Autorizována <b>APPROVED</b>	Výsledek autentikace držitele karty v 3D systému byl úspěšný, byl poslán požadavek na autorizaci do autorizačního centra. Výsledek autorizace objednávky je úspěšný.
5	Reverzována <b>APPROVE_REVERSED</b>	Autorizace objednávky byla zneplatněna. Na straně držitele karty došlo k odblokování původně autorizovaných finančních prostředků.
6	Neautorizována <b>UNAPPROVED</b>	Výsledek autorizace objednávky je neúspěšný, objednávku není možné uhradit. Není možné pokračovat.
7	Uhrazena <b>DEPOSITED_BATCH_OPENED</b>	Objednávka byla označena pro uhrazení během následného dávkového zpracování. Je možné zneplatnit úhradu objednávky do okamžiku, než proběhne uzavření dávky, ve které se daná úhrada nachází.
8	Zpracována <b>DEPOSITED_BATCH_CLOSED</b>	Proběhl automatický proces uzavírání dávek a přenos dat do finančních systémů.
9	Uzavřena <b>ORDER_CLOSED</b>	Objednávka byla uzavřena. Jediná přípustná operace je vymazání.
10	Vymazána <b>DELETED</b>	Objednávka byla odstraněna.
11	Kreditována <b>CREDITED_BATCH_OPENED</b>	Objednávka byla označena pro návrat během následného dávkového zpracování.
12	Kreditována <b>CREDITED_BATCH_CLOSED</b>	Je možné zneplatnit návrat objednávky do okamžiku, než proběhne uzavření dávky, ve které se daná objednávka nachází. Po uzavření dávky zůstává v tomto stavu. Pro objednávku je možné vytvořit více kreditů.
13	Zamítnuta <b>DECLINED</b>	Výsledek autentikace držitele karty v 3D systému je neúspěšný. Držitel karty není autentikován – není možné pokračovat. Objednávku je možné odstranit.



