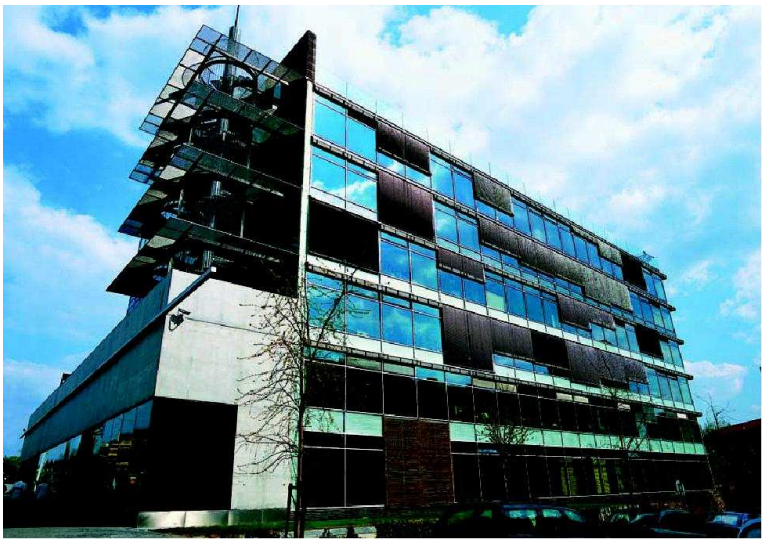


Pay MUZO

Seznámení se systémem, vytváření objednávek

Verze 1.9

Obsah

Úvod

Dokument je určen obchodníkům, kteří uvažují o možnosti rozšířit své podnikatelské aktivity i do oblasti elektronického obchodování, případně hodlají zvýšit bezpečnost svého elektronického obchodu.

Dokument obsahuje informace o možnosti komunikace se systému Pay MUZO, který umožňuje elektronickým obchodům přijímat platby provedené karetními produkty asociací MasterCard a Visa v síti Internet.

Systém Pay MUZO podporuje standard zabezpečení 3-D Secure, definovaný uvedenými asociacemi, čímž poskytuje všem zúčastněným stranám podstatně vyšší záruky než je běžné u neautentizovaných plateb.

Dokumentace je rozdělena na jednotlivé dokumenty dle dané problematiky:

- Pay MUZO – Seznámení se systémem, vytváření objednávek
- Pay MUZO – Administrace systému
- Pay MUZO – Správa objednávek – Web Services
- Pay MUZO – Praktické scénáře

Pay MUZO – popis systému

Systém **Pay MUZO** (dále jen Pay MUZO) 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.
Pay MUZO plně podporuje standard 3-D Secure a poskytuje možnost integrovat funkčnost standardního webového rozhraní formou Web Services

Komunikace s Pay MUZO je zajištěna:

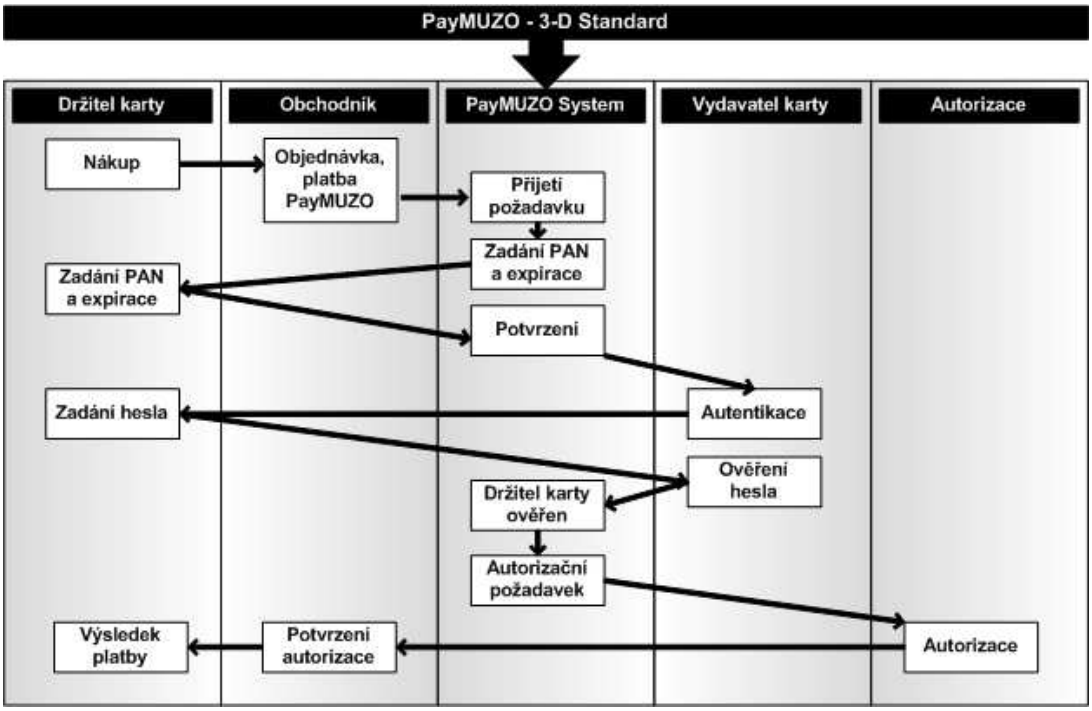
- on-line formou zaslání požadavku na vytvoření objednávky do Pay MUZO, následné zpracování požadavku a zaslání výsledku zpracování požadavku. Detailní popis je součástí tohoto dokumentu.

- prostřednictvím standardně dodávaného webového rozhraní aplikace. Detailní popis administrace Pay MUZO je součástí dokumentu – ***Administrace systému***

- on-line formou zaslání administrativního požadavku do Pay MUZO, následné zpracování přijatého požadavku a zaslání výsledku zpracování požadavku. Detailní popis je součástí dokumentu – ***Správa objednávek – Web Services.***

Pay MUZO – 3–D standard

Vzhledem k možnosti snadného zneužití plateb prostřednictvím platebních karet v prostředí sítě Internet podporuje Pay MUZO standard zabezpečení 3-D Secure definovaný asociací VISA a MasterCard.
Tento standard definuje dodatečný mechanismus pro ověření držitele platební karty a současně poskytuje všem zúčastněným stranám (držitel karty, obchodník, vydavatel karty a zúčtující banka) nesrovnatelně vyšší záruky než je tomu u neautentizovaných plateb.



Při přijetí požadavku na provedení platby platební kartou předává Pay MUZO požadavek na prověření autentičnosti držitele karty do 3-D systému asociací VISA a MasterCard a na základě obdržených výsledků povoluje / zamítá možnost dalšího zpracování objednávky.

Systém Pay MUZO předává do autorizačního centra pouze ty požadavky, pro které nebude moci banka držitele karty uplatňovat právo vrácení částky z důvodu neautentizovaného požadavku.

Zabezpečení 3-D Secure zobrazuje obrázek.

Krok	Popis
1	Držitel karty nakupuje v e-shopu a požaduje platbu platební kartou.
2	Obchodník předá požadavek na vytvoření objednávky do Pay MUZO
3	Pay MUZO zkontroluje přijatý požadavek
4	Pay MUZO zobrazí stránku pro vyplnění citlivých informací o platební kartě.
5	Držitel karty vyplní informace o kartě a potvrdí provedení platby.
6	Pay MUZO zpracuje přijaté informace o platební kartě
7	Pay MUZO předá požadavek na autentikaci držitele karty 3-D systému příslušné finanční asociace (VISA, MasterCard).
8	V případě, že je vydavatel karty zapojen do 3-D systému a je požadována autentikace držitele karty, je držitel karty přesměrován na stránku 3-D systému vydavatele karty, kde vyplní požadované autentikační údaje (heslo, e-PIN, nebo jinou tajnou informaci, kterou sdílí s vydavatelem karty) Pokud vydavatel karty nepodporuje 3-D systém, Pay MUZO obdrží tuto informaci.
9	3-D systém vydavatele karty autentikuje držitele karty a zašle výsledek autentikace do systému Pay MUZO
10	Dle výsledku autentikace držitele karty Pay MUZO určí, zda v dané transakci pokračovat a odeslat požadavek na autorizaci objednávky do autorizačního centra.
11	Pay MUZO zpracuje výsledek autorizace objednávky
12	Výsledek zpracování je oznámen obchodníkovi prostřednictvím návratových kódů.
13	Obchodník zaznamená výsledek a zobrazí výsledek platby držiteli karty.

Jestliže 3-D systém vydavatele karty ověří totožnost držitele karty, vydavatel karty se tímto současně zavazuje, že nebude popírat platnost této internetové elektronické transakce a nebude požadovat vrácení finančních prostředků od obchodníka.

Takto je rovněž možné eliminovat možný pokus o podvod v případě, kdy držitel karty není úspěšně autentikován (z důvodu chybného zadání autentikačních údajů). V takové transakci se dále nepokračuje.

Pokud se během zpracování objednávky zjistí, že vydavatel, anebo držitel karty není zapojen do 3-D systému Pay MUZO obdrží informaci o typu a míře ověření.

Na základě takto získaných informací, bude podle typu použité platební karty rozhodnuto, zda zpracování bude pokračovat odesláním požadavku do autorizačního centra či nikoliv.

VISA / MasterCard

U platebních produktů VISA / MasterCard je v případě 3-D transakce zodpovědnost za transakci plně na straně vydavatele karty.

Pokud je tedy obchodník připraven přijímat platby pomocí 3-D, ale vydavatel karty neprovozuje 3-D systém, anebo vydavatel karty nezavedl kartu do svého 3-D systému, je neověření transakce způsobeno vydavatelem, a proto nemůže požadovat vrácení částky po obchodníkovi.

Všechny transakce VISA / MasterCard kartami se tedy v případě neověření držitele karty přeposílají do autorizačního centra s příslušným příznakem.

Autorizaci objednávky **povolí/zamítne vydavatel karty** na základě obdržených informací.

Ostatní karetní produkty prozatím nejsou podporovány.

*Vzhledem k tomu, že 3-D platby se stávají standardem pro internetové platby, 3-D Secure standard v dohledné době začnou podporovat i karetní produkty společností **American Express**, **JCB a Diners Club**. Tato informace má prozatím pouze informativní charakter.*

Pay MUZO – Popis zpracování

Pay MUZO během zpracování vytváří objekt nazývaný **Objednávka,** který obsahuje všechny informace nezbytně nutné pro vytváření finančních transakcí:

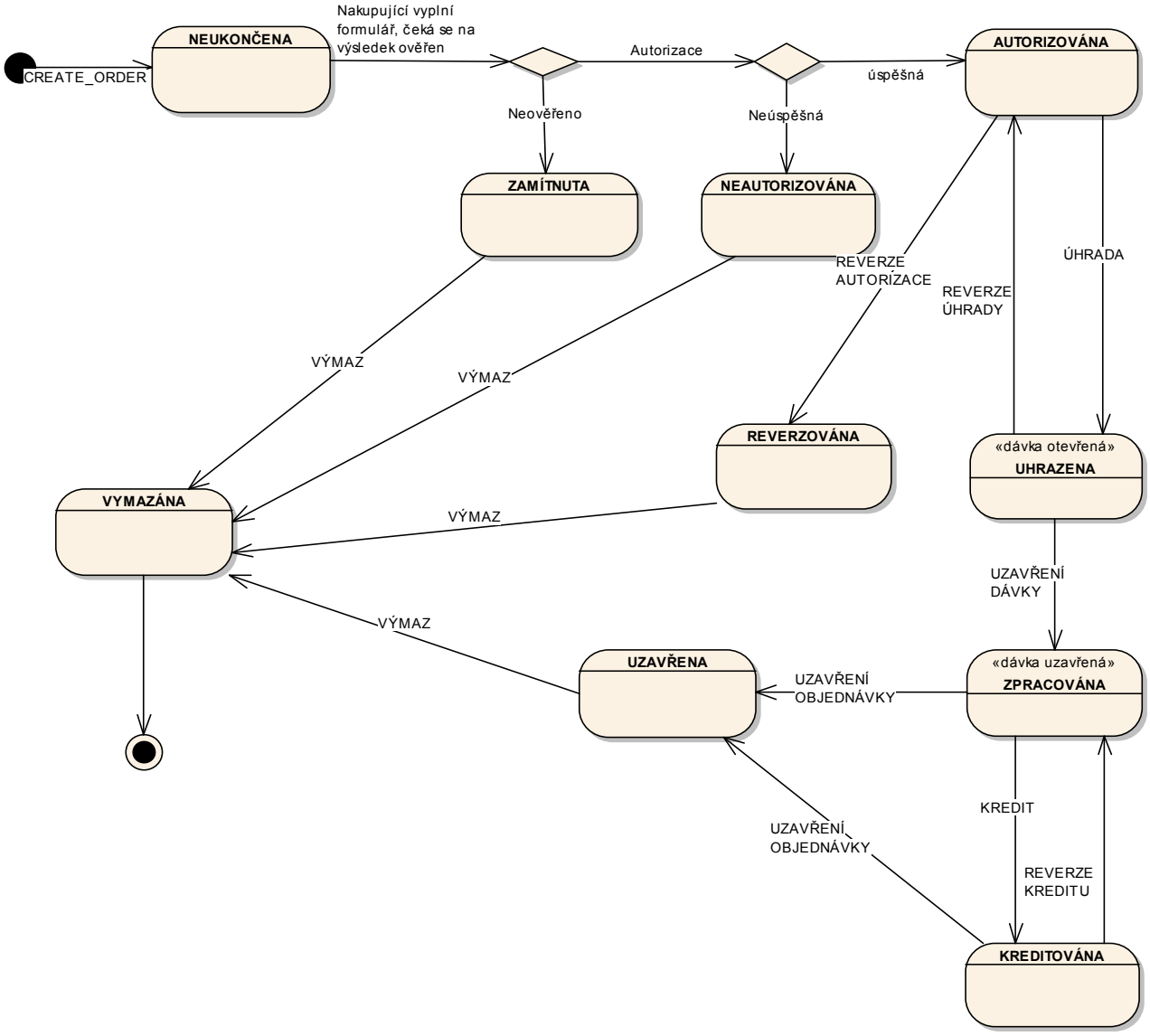
- **Autorizace** – požadavek na ověření dostupnosti finančních prostředků držitele karty a jejich zablokování;
- **Úhrada** – požadavek na přesun finančních prostředků od držitele karty k obchodníkovi;
- **Kredit** – požadavek na přesun finančních prostředků od obchodníka zpět držiteli karty z důvodu storna úhrady, částečného storna úhrady, ...

Možnosti zpracování objednávek přímo závisí na stavu, ve kterém se objednávka nachází. Popis stavu objednávky se zobrazí v jazyce, který je dán nastavením prohlížeče. Podporované jazyky jsou čeština a angličtina. Pro jiné nastavení prohlížeče se popisy zobrazují v angličtině.

Stavy objednávky:

Stav	Popis	Možné následující stavy
NEUKONČENA ***(REQUESTED)***	Objednávka byla úspěšně přijata do Pay MUZO – čeká se na vyplnění formuláře držitelem karty, nebo na výsledek dotazu zaslaného do systému asociací. Objednávka je v tomto stavu když: - držitel karty přeruší zadávání údajů karty - nebyla obdržena odpověď se systémů asociací, či vydavatelů karet	
ZAMÍTNUTA ***(DECLINED)***	Obdržen výsledek ze systému vydavatele karty – držitel karty není autentikován. **V transakci není možné pokračovat.**	**VYMAZÁNA** ***(DELETED)***
AUTORIZOVÁNA ***(APPROVED)***	Zaslán požadavek na autorizace transakce. **Transakce úspěšně autorizována.**	**UHRAZENA** ***(DEPOSITED)*** **REVERZOVÁNA** ***(REVERSED)***
NEAUTORIZOVÁNA*(UNAPPROVED)*	Zaslán požadavek na autorizace transakce. **Transakce nebyla autorizována.**	**VYMAZÁNA** ***(DELETED)***
REVERZOVÁNA ***(REVERSED)***	Zaslán požadavek na zrušení autorizace transakce. **Autorizace byla úspěšně zrušena.**	**VYMAZÁNA** ***(DELETED)***

UHRAZENA ***(DEPOSITED)***	Transakce je označena pro zpracování (přesun finančních prostředků od držitel karty k obchodníkovi) Je možné zrušit úhradu objednávky do okamžiku, než proběhne uzavření dávky, ve které se daná úhrada nachází.	**AUTORIZOVÁNA** ***(APPROVED)*** **ZPRACOVÁNA** ***(PROCESSED)***
ZPRACOVÁNA ***(PROCESSED)***	Transakce byla zpracována (banka dostala pokyn k přesunu finančních prostředků od držitele karty k obchodníkovi)	**KREDITOVÁNA** ***(CREDITED)*** **UZAVŘENA** ***(CLOSED)***
KREDITOVÁNA ***(CREDITED)***	Transakce je označena pro návrat (přesun finančních prostředků od obchodníka k držiteli karty) Pro objednávku je možné vytvořit více kreditů – až do výše původně zpracované částky. Provedení kreditu je možné zrušit do okamžiku, kdy proběhne uzavření dávky, ve které se daný kredit nachází. Po uzavření dávky zůstává objednávka v tomto stavu.	**UZAVŘENA** ***(CLOSED)***
UZAVŘENA ***(CLOSED)***	Objednávka byla uzavřena. Není možné provádět zpracování, či návraty. Jediná přípustná operace je vymazání.	**VYMAZÁNA** ***(DELETED)***
VYMAZÁNA ***(DELETED)***	Objednávka byla odstraněna. Ve skutečnosti se pouze změní stav objednávky. Objednávka zůstává v systému pro potřeby auditu. Číslo objednávky proto nelze znovu použít.	



Stavy dávky:

Všechny transakce úhrady nebo návratu se vkládají do dávek. Tyto dávky jsou automaticky zpracovány a výstupy zpracování těchto dávek se předávají k následnému zaúčtování v rámci mezibankovních sítí.

Možnosti zpracování dávek jsou přímo závislé na stavu, ve kterém se dávka nalézá.

Stavy dávky:

Stav	Popis	Následný stav
OTEVŘENA (*OPEN)*	Dávka je otevřená. Do dávky se přidávají všechny úhrady a návraty objednávek. Dávku není nutné otevírat – nová dávka se otevírá automaticky při prvním požadavku o úhradu nebo návrat objednávky.	**UZAVŘENA *(CLOSED)***
UZAVŘENA (*CLOSED)*	Dávka je uzavřena a čeká na následné zpracování.	**ZPRACOVÁNA *(EXTRACTED)***
ZPRACOVÁNA (*EXTRACTED)*	Dávka byla zpracována a do mezibankovních sítí jsou předány požadavky na zaúčtování objednávek.	

Pay MUZO – Vytvoření objednávky

Jestliže obchodník na svých stránkách nabízí možnost platby prostřednictvím Pay MUZO, musí v případě platby Pay MUZO přesměrovat nakupujícího na stránky Pay MUZO, a to oslovením adresy Pay MUZO pro vytvoření objednávky.
Požadavky musí splňovat následující podmínky:

- Požadavek se do Pay MUZO zasílá metodou GET v případě použití Redirect, anebo formou zaslání formulářových dat z internetového prohlížeče držitele karty metodou GET nebo POST;
- Požadavek se zasílá na URL adresu specifikovanou ve smlouvě;
- Data předávaná v parametrech HTTP request jsou **x-www-form-urlencoded** (dle definice RFC 1866 – kap. 8.2.2
  vice info na http://www.w3.org/MarkUp/html-spec/);
- HTTP request se zasílá přes zabezpečený HTTPS kanál, za použití serverového certifikátu společnosti MUZO.

V požadavku musí být zaslány následující údaje

Parametr	Typ	Délka	Povinný	Poznámka
MERCHANTNUMBER	numerický		ano	Přidělené číslo obchodníka
OPERATION	znakový		ano	Hodnota **CREATE_ORDER**
ORDERNUMBER	numerický	15	ano	Pořadové číslo objednávky, číslo musí být v každém požadavku od obchodníka **unikátní**.
AMOUNT	numerický	12	ano	Částka v nejmenších jednotkách dané měny pro Kč = v haléřích
CURRENCY	numerický		ne	Identifikátor měny dle ISO 4217 (viz. dodatek ISO 4217) Pokud není parametr zadán použije se přednastavená hodnota „203“ (CZK). **Současná verze Autorizačního Centra podporuje pouze CZK = hodnotu 203**
DEPOSITFLAG	numerický	1	ano	Udává, zda má být objednávka uhrazena automaticky. Povolené hodnoty: 0 = není požadována úhrada 1 = je požadována úhrada
MERORDERNUM	numerický	16	ne	Identifikace objednávky pro obchodníka. *Zobrazí se na výpisu z banky.* *V případě, že není zadáno, použije se hodnota ORDERNUMBER*

URL	znakový	50	ano	Plná URL adresa obchodníka. *(včetně specifikace protokolu – např. https://)* Na tuto adresu bude odeslán výsledek požadavku. *V případě chybného podpisu dat se chybové hlášení zasílá zpět do internetového prohlížeče, ze kterého tento požadavek přišel.*
DESCRIPTION	znakový	125	ne	Popis nákupu. Obsah pole se přenáší do 3-D systému pro možnost následné kontroly držitelem karty během autentikace u Access Control Serveru vydavatelské banky. Pole musí obsahovat pouze ASCII znaky v rozsahu 0x20 – 0x7E.
MD	znakový	30	ne	Libovolná data obchodníka, která jsou vrácena obchodníkovi v odpovědi v nezměněné podobě. Pole se používá pro uspokojení rozdílných požadavků jednotlivých e-shopů. Pole musí obsahovat pouze ASCII znaky v rozsahu 0x20 – 0x7E. Pokud je nezbytné přenášet jiná data, potom je zapotřebí použít BASE64 kódování. (viz. Dodatek Base64). Pole nesmí obsahovat osobní údaje **Výsledná délka dat může být maximálně 30 B.**
DIGEST	znakový		ano	Kontrolní podpis řetězce, který vznikne zřetězením zaslaných polí v pořadí, uvedeném v této tabulce. *Parametr je nutné předávat URL encoded!* Popis algoritmu výpočtu pole DIGEST je uveden v příloze 1 – *Podepisování požadavku*

Formát zaslané odpovědi

Parametr	Typ	Délka	Povinný	Poznámka
OPERATION	znakový		ano	Hodnota **CREATE_ORDER**
ORDERNUMBER	numerický	15	ano	Obsah pole z požadavku
MERORDERNUM	numerický	16	ne	Obsah pole z požadavku pokud bylo uvedeno
MD	znakový	30	ne	Obsah pole z požadavku pokud bylo uvedeno
PRCODE	numerický		ano	Udává primární kód, viz. Příloha 2
SRCODE	numerický		ano	Udává sekundární kód, viz. Příloha 2
RESULTTEXT	znakový	255	ne	Slovní popis chyby, který je jednoznačně dán kombinací PRCODE a SRCODE. Pro kódování obsahu pole je použita kódová stránka Windows Central European (Code Page 1250)
DIGEST	znakový		ano	Kontrolní podpis řetězce, který vznikne zřetězením všech polí v uvedeném pořadí. Popis algoritmu výpočtu pole DIGEST je uveden v Příloze 1 – *Podepisování požadavku*

Příklad zasílaného požadavku a obdržené odpovědi

Požadavek:

1.
POST /order.do HTTP/1.1
Connection: Keep-Alive
Accept: application/xml
Host: **pay.muzo.com**
Content-Length: xxx
Content-Type: application/x-www-form-urlencoded

AMOUNT=**100**&OPERATION=**CREATE_ORDER**&ORDERNUMBER=**1234567**&DEPOSITFLAG=**0**&MERORDERNUM=**123456789**&MERCHANTNUMBER=**9999999031**&MD=**B8E5AD3CEBE760E95921FCBC4D92C7**&URL=**https://www.testmerchant.com/response.jsp**&DESCRIPTION=**Nakup**&DIGEST=Co9LzCJPQYeEKbBiqBr35hWIkQzYX%2BaEDz877q1Co9LzCJPQYeEKbBzEky6aV%2BXxD6FHIHixMV3WqJj2BX6NK9PK88pyxXIHC6INDefXKAnSEwqFLZwr8%2BSZLLImcgJWsPdb%2Fqsl3vO46llhRQor%2BdiQoH%2BFl38Vi8UQsmMSOp%2B%2Bc6US2hxTQvnspA%3D

Význam požadavku:
Obchodník, zavedený v Pay MUZO pod číslem **9999999031,** požaduje **vytvoření objednávky,** která bude mít v Pay MUZO číslo **1234567**.
Obchodník ve svém systému eviduje tuto objednávku pod číslem **123456789**, toto číslo chce mít na výpisu z platebních karet své banky.
Držitel karty bude hradit částku **1**,- **Kč bez** okamžitého požadavku na **uhrazení** objednávky.
Pokyn k úhradě částky zadá později prostřednictvím GUI nebo pomocí rozhraní WebServices.
Obchodník požaduje zaslání odpovědi na URL adresu **https://www.testmerchant.com/response.jsp**. Obchodník přikládá popis objednávky s hodnotou **Nakup** a dále pak přikládá data určená pro privátní účely obchodníka obsažena v poli **MD** – base64 kódována.
Na důkaz platnosti dat přikládá **podpis** zaslaných dat – zde uvedený podpis má pouze popisný charakter – reálná hodnota podpisu v požadavku je přímo závislá na obsažených datech a použitém klíči. Parametr **DIGEST** se zadává do požadavku URLEncoded
Pro výpočet podpisu obchodník použije hodnotu
9999999031|CREATE_ORDER|1234567|100|0|123456789https://**www.testmerchant.com/response.jsp|Nakup|B8E5AD3CEBE760E95921FCBC4D92C7**
(jednotlivá pole jsou proložena oddělovačem – viz. Příloha č. 1)

a svůj privátní klíč, vygenerovaný podle pokynů v příloze 1. MUZO použije k ověření podpisu veřejný klíč, který mu obchodník poskytne v čase podpisu smlouvy.

Odpověď:

Bude zaslána na adresu

https://www.testmerchant.com/response.jsp

(Pouze v případě, že je podpis správný. V opačném případě se odpověď zasílá zpět do internetového prohlížeče, odkud byl požadavek přijat.)

Obsah:

OPERATION=**CREATE_ORDER**&ORDERNUMBER=**1234567**&MERORDERNUM=**123456789**&MD=**B8E5AD3CEBE760E95921FCBC4D92C7**&PRCODE=**0**&SRCODE=**0**&RESULTTEXT=**OK**&DIGEST=
Co9LzCJPQYeEKbBiqBr35hWIkQzYX%2BaEDz877q1Co9LzCJPQYeEKbBzEky6aV%2BXxD6FHIHixMV3WqJj2BX6NK9PK88pyxXIHC6lNDefXKAnSEwqFLZwr8%2BSZLLImcgJWsPdb%2Fqsl3vO46llhRQor%2BdiQoH%2BFl38Vi8UQsmMSOp%2B%2Bc6US2hxTQvnspA%3D

Význam odpovědi:

Odpověď patří k požadavku na vytvoření objednávky **1234567,** obchodník v požadavku zaslal parametr **MD**, který se mu vrací zpátky, rovněž se vrací parametr **MERORDERNUM.**

Návratové kódy jsou 0 a 0, což podle tabulky návratových kódů znamená úspěšnou autorizaci.

Pole DIGEST je vypočteno z hodnoty

CREATE_ORDER|1234567|123456789|B8E5AD3CEBE760E95921FCBC4D92C7|0|0|OK

(jednotlivá pole jsou proložena oddělovačem – viz. Příloha č. 1)

Pro ověření podpisu zaslaného ze systému Pay MUZO je nutné použít všechny parametry s výjimkou DIGEST. I v případě, že je nějaký parametr prázdný jsou použity oddělovače oddělující prázdý řetězec – **"||"** (např. CREATE_ORDER|1234567||B8E5…..).

A k jeho ověření je nutné použít hodnotu veřejného klíče MUZO, uvedenou ve smlouvě.

Zpracování

Pay MUZO zkontroluje platnost zadaných údajů:

- Přítomnost parametru URL – jestliže není přítomen, v HTTP response k zaslanému požadavku se odešle chybové hlášení
- vyhledá obchodník s uvedeným MERCHANTNUMBER
- zaslaný podpis požadavku v poli DIGEST
- pro všechny prvky platnost obsahu – délka, typ, hodnota
- zda objednávka s tímto ORDERNUMBER už není zavedena

Výsledek

Je vytvořena objednávka a čeká se na její dokončení – doplnění citlivých informací od držitele karty, autentikaci držitele karty a výsledek autorizace objednávky. Podle výsledku dokončení zpracování může objednávka nabýt jednoho z následujících stavů

NEUKONČENA ***(REQUESTED)***	Čeká se na doplnění citlivých informací od držitele karty, případně na odpověď z 3D. V případě, že držitel karty

	přeruší proces zadávání údajů, objednávka zůstává v tomto stavu.
ZAMÍTNUTA ***(DECLINED)***	Ověření v 3D bylo neúspěšné
AUTORIZOVÁNA ***(APPROVED)***	Objednávka úspěšně autorizována, úhrada nebyla požadována (DEPOSITFLAG byl 0)
NEAUTORIZOVÁNA ***(UNAPPROVED)***	Žádost o autorizaci v autorizačním centru byla neúspěšná
UHRAZENA ***(DEPOSITED)***	Žádost o autorizaci v autorizačním centru byla úspěšná, v žádosti byl zaslán DEPOSITFLAG=1, takže pro objednávku byla vytvořena finanční transakce úhrady

Přílohy a dodatky

Příloha 1 – Podepisování zpráv

Podepisování požadavku

Pay MUZO přijímá pouze ty požadavky, u kterých lze doložit, že původcem požadavku byl oprávněný subjekt, tedy obchodník, se kterým MUZO, a.s. uzavřelo smlouvu o poskytování služby Pay MUZO.

K prokázání původu požadavku slouží pole DIGEST. Jeho obsah je 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 Pay MUZO zkontroluje, zda byl požadavek podepsán obchodníkem za pomoci jeho soukromého klíče.

Požadavky bez pole DIGEST nebo s neodpovídajícím obsahem pole DIGEST budou zamítnuty s důvodem:

PRCODE=5 SRCODE=34 “Chybi povinne pole, DIGEST” nebo PRCODE =31 “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 i 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 a oddělovat jednotlivá pole oddělovačem „|“ (pipe, ascii 124, hexa 7C), kterému nesmí předcházet, ani být následován whitespace.

U příkazu CREATE_ORDER se tedy zdrojem pro výpočet pole DIGEST stane hodnota, která vznikne zřetězením obsahů polí v tomto pořadí:

MERCHANTNUMBER + **|** + OPERATION + **|** + ORDERNUMBER + **|** + AMOUNT + **|** + CU
RRENCY + **|** + 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 + **|** + DEP
OSITFLAG + **|** + URL

Podepisování odpovědi

Všechny odpovědi z Pay MUZO obsahují také pole DIGEST, kterého obsah je vypočten:

- na základě údajů, obsažených v odpovědi,
- a současně na základě soukromého klíče Pay MUZO.

Při podpisu smlouvy je druhé straně poskytnut veřejný klíč Pay MUZO, který slouží obchodníkovi k ověření obsahu pole DIGEST. Tímto způsobem se zasilatel požadavku může přesvědčit, že:

- odpověď pochází skutečně od Pay MUZO,
- 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*1,5

Výpočet elektronického podpisu probíhá následujícím způsobem

a) ze zprávy je vypočtena hodnota hash funkce SHA-1 [3]

b) 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).

c) na výstupní hodnotě z b) je proveden RSA podpis v souladu s částí 8.1.1 [1] RSASSA-PKCS1-V1_5-SIGN

d) 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:

a) podle nastavení obchodníka v systému MUZO je vybrán správný veřejný klíč a ověřena jeho integrita;

b) elektronický podpis je BASE64 dekódován;

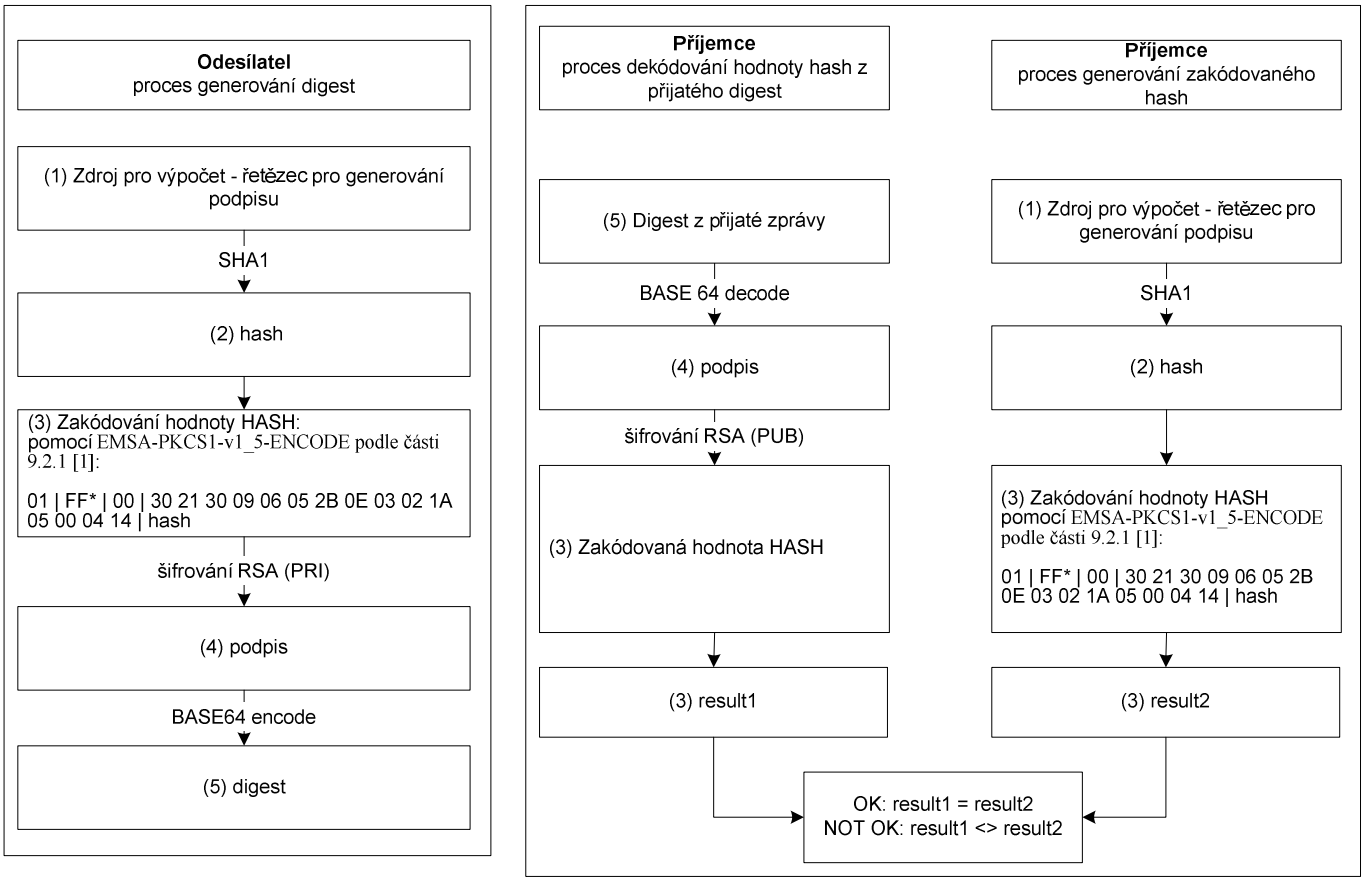
c) výstup b) je dešifrován pomocí vybraného veřejného klíče;

d) 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 Pay MUZO a obchodníkem budou využity následující páry klíčů:

KeyPair MUZO	Privátní klíč MUZO ($MUZO_{PRI}$)	Použit pro výpočet elektronického podpisu zpráv odesílaných MUZO	
	Veřejný klíč (certifikát) MUZO ($MUZO_{PUB}$)	Použit obchodníkem k ověření elektronického podpisu zpráv zasílaných MUZO	Bude předáván ve formě X509 certifikátu

KeyPair obchodníka	Privátní klíč obchodníka ($MERCH_{PRI}$)	Použit pro výpočet elektronického podpisu zpráv odesílaných obchodníkem	
	Veřejný klíč (certifikát) obchodníka ($MERCH_{PUB}$)	Použit v MUZO 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 MUZO, a.s.

Veřejný klíč bude předán určenému správci v MUZO při podpisu smlouvy. Součástí smlouvy je také formulář s identifikačními údaji o certifikátu obchodníka. Po podpisu smlouvy obdrží obchodník veřejný klíč MUZO 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 profilu1.

Parametr	Hodnota	Poznámky
Version	3	
Subject a Issuer	CN=<Jméno obchodníka>:<Merchant ID>:<banka>, OU=Pay MUZO, 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 zúčtující banky, se kterou má obchodník uzavřenou smlouvu
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.

[1] Parametry odpovídají RFC 2459 [4]

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 k 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/xmldsig-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 (dočasně nedostupné)

Bouncy Castle: alternativní JCA Provider, poskytující knihovny pro generování certifikátů a práci c PKCS#12 úložišti certifikátů, www.bouncycastle.org.

Crypto++ volně šiřitelná C++ knihovna kryptografických funkcí podporující také RSA/SHA1/PKCS#1 algoritmus. www.cryptopp.com

Příloha 2 – Seznam návratových kódů

Výsledek zpracování v Pay MUZO je dán dvojicí návratových kódů. V případě, že jsou různé od nuly, PRCODE udává typ chyby a v případě, že SRCODE je nenulové, udává 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 *Info:Pokud v případě vytváření objednávky (CREATE_ORDER) obdrží obchodník tento návratový kód, vytvoření objednávky již proběhlo a objednávka je v určitém stavu – tento návratový kód je zapříčiněn aktivitou držitele karty (například pokusem o přechod zpět, použití refresh ... ...)*	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 *Info: důvod zamítnutí udává SRCODE*	Declined in 3D
30	Zamítnuto v autorizačním centru *Info: Důvod zamítnutí udává 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	
V případě PRCODE 1 až 5, 15 a 20 se mohou vrátit následující SRCODE		
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
V případě PRCODE 28 se mohou vrátit následující SRCODE		
3000	Neověřeno v 3D. Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. Kontaktujte vydavatele karty. *Info: Ověření držitele karty bylo neúspěšné (neplatně zadané údaje, stornování autentikace, uzavření okna pro autentikaci držitele karty se zpětnou vazbou … ...). V transakci se nesmí pokračovat.*	Declined in 3D. Cardholder not authenticated in 3D.Contact your card issuer. *Note: Cardholder authentication failed (wrong password, transaction canceled, authentication window was closed … …) Transaction Declined.*
3001	Držitel karty ověřen *Info: Ověření držitele karty v 3D systémech proběhlo úspěšně. Pokračuje se autorizací objednávky.*	Authenticated *Note: Cardholder was successfully authenticated – transaction continue with authorization.*
3002	Neověřeno v 3D. Vydavatel karty nebo karta není zapojena do 3D. Kontaktujte vydavatele karty. *Info: V 3D systémech nebylo možné ověřit držitele karty – karta, nebo její vydavatel, není zapojen do 3D. V transakci se pokračuje/.*	Not Authenticated in 3D. Issuer or Cardholder not participating in 3D. Contact your card issuer. *Note: Cardholder wasn't authenticated – Issuer or Cardholder not participating in 3D. Transaction can continue.*

3004	Neověřeno v 3D. Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. Kontaktujte vydavatele karty. *Info: V 3D systémech nebylo možné ověřit držitele karty – karta není aktivována, nebo její vydavatel, není zapojen do 3D. V transakci je možné pokračovat. .*	Not Authenticated in 3D. Issuer not participating or Cardholder not enrolled. Contact your card issuer. *Note: Cardholder wasn't authenticated – Cardholder not enrolled or Issuer or not participating in 3D. Transaction can continue.*
3005	Zamítnuto v 3D.Technický problém při ověření držitele karty. Kontaktujte vydavatele karty. *Info: V 3D systémech nebylo možné ověřit držitele karty – vydavatel karty nepodporuje 3D, nebo technický problém v komunikaci s 3D systémy finančních asociací, či vydavatele karty. V transakci není možné pokračovat povoleno z důvodu zabezpečení obchodníka před případnou reklamací transakce držitelem karty.*	Declined in 3D. Technical problem during Cardholder authentication. Contact your card issuer. *Note: Cardholder authentication unavailable – issuer not supporting 3D or technical problem in communication between associations and Issuer 3D systems. Transaction cannot continue.*
3006	Zamítnuto v 3D. Technický problém při ověření držitele karty. *Info: V 3D systémech nebylo možné ověřit držitele karty – technický problém ověření obchodníka v 3D systémech, anebo v komunikaci s 3D systémy finančních asociací, či vydavatele karty. V transakci není možné pokračovat.*	Declined in 3D. Technical problem during Cardholder authentication. *Note: Technical problem during cardholder authentication – merchant authentication failed or technical problem in communication between association and acquirer. Transaction cannot continue.*
3007	Zamítnuto v 3D. Technický problém v systému zúčtující banky. Kontaktujte obchodníka. *Info: V 3D systémech nebylo možné ověřit držitele karty – technický problém v 3D systémech. V transakci není možné pokračovat.*	Declined in 3D. Acquirer technical problem. Contact the merchant. *Note: Technical problem during cardholder authentication – 3D systems technical problem. Transaction cannot continue.*
3008	Zamítnuto v 3D. Použit nepodporovaný karetní produkt. Kontaktujte vydavatele karty. *Info: Byla použita karta, která není v 3D systémech podporována. V transakci není možné pokračovat.*	Declined in 3D. Unsupported card product. Contact your card issuer. *Note: Card not supported in 3D. Transaction cannot continue.*
V případě PRCODE 30 se mohou vrátit následující SRCODE		
1001	**Zamitnuto v autorizacnim centru, karta blokovana**[2] *Zahrnuje důvody, které naznačují zneužití platební karty – kradená karta, podezření na podvod, ztracená karta a pod.* *Karta je označena jako:* - *ztracená* - *k zadržení* - *k zadržení (speciální důvody)*	Declined in AC, Card blocked

[2] Pouze tučně vytištěné části v této a níže uvedených buňkách tohoto sloupce budou obsaženy v poli RESULTTEXT *(NEPOVINNÉ POLE)* v odpovědi zaslané obchodníkovi. Ostatní text je pouze vysvětlení pro obchodníky.

	- *ukradená* *Většinou pokus o podvodnou transakci.*	
1002	**Zamitnuto v autorizacnim centru, autorizace zamítnuta** *Z autorizace se vrátil důvod zamítnutí „Do not honor“* *Vydavatel, nebo finanční asociace zamítla autorizaci BEZ udání důvodu.*	Declined in AC, Declined
1003	**Zamitnuto v autorizacnim centru, problem karty** *Zahrnuje důvody:* *expirovaná karta, chybné číslo karty, nastavení karty - pro kartu není povoleno použití na internetu, nepovolená karta, expirovaná karta, neplatná karta, neplatné číslo karty, částka přesahuje maximální limit karty, neplatné CVC/CVV, neplatná délka čísla karty, neplatná expirační doba, pro kartu je požadována kontrola PINu.*	Declined in AC, Card problem
1004	**Zamitnuto v autorizacnim centru, technicky problem** *Autorizaci není možné provést z technických důvodů – technické problémy v systému vydavatele karty, nebo finančních asociací a finančních procesorů.*	Declined in AC, Technical problem in authorization process
1005	**Zamitnuto v autorizacnim centru, Problem uctu** *Důvody: nedostatek prostředků na účtu, překročeny limity, překročen max. povolený počet použití...*	Declined in AC, Account problem

V případě zamítnutí autorizace získává platební brána návratový kód přímo od vydavatele karty (případně od jeho poskytovate služeb, či finanční asociace). V případě reklamace zamítnuté autorizace musí držitel karty kontaktovat svoji vydavatelskou banku, která mu odpoví přímo, případně tato banka řeší reklamaci s bankou, která zúčtovala transakci (bankou obchodníka).

Dodatek 1 – BASE64 kódování / dekódování

Basae64 je kódovací algoritmus umožňující zakódovat libovolná binární data do textové – běžně tisknutelné a snadno přenositelné podoby.
Výsledek Base64 kódování je možné přenášet bez jakéhokoliv nebezpeční, že zakódovaná data budou zkonvertována a tím i zničena.

Base64 kódování využívá definovanou abecedu 65-ti US-ASCII znaků (64 znaků + mezeru), které obsahuje následující tabulka:

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w	(pad)	=
15	P	32	g	49	x		
16	Q	33	h	50	y		

Zdrojová data se převedou do dvojkové soustavy jako proud vstupních bitů $\rightarrow$ 1 znak = 8 bitů. Vstupní proud se následně rozdělí do skupin 6-ti bitů a takto získané hodnoty se převedou dle kódu definované abecedy.
Každé 3 vstupní znaky (3 * 8 = 24) se zakódují jako 4 výstupní znaky (24 / 6 = 4). Zbude-li na konci vstupních dat po jejich rozdělení méně než 24 bitů, doplní se vstupní data nulovými bity zprava. Přidání nulových bitů je indikováno znakem “=“.

Dekódování base64 kódovaných dat je pak procesem přesně opačným k procesu base64 kódování. Ze zakódovaných dat se podle definované tabulky získá proud bitů. Tento proud je následně rozdělen na skupiny o 8-mi bitech a tyto skupiny jsou převedeny zpět do původní podoby vstupních dat.

Přesné znění base64 kódování je možné nalézt v RFC 3548.

Dodatek 2 – Dokumentace a informační zdroje

- ISO 639-1:2002 Codes for the representation of names of languages Part 1: Alpha-2 code
- ISO 639-2:1998 Codes for the representation of names of languages Part 2: Alpha-3 code
- ISO 4217:2001 Codes for the representation of currencies and funds
- RFC 3066 – Tags fotr the Identification of Languages