Seznámení se systémem GP webpay

Vytváření objednávek

- HTTP rozhraní

Verze: 2.1

Global Payments Europe, s.r.o.

Vytvořeno **10.9.2015**

Poslední změna **14.12.2015**

SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

Autor dokumentu	Dimitrij Holovka
Správce dokumentu	
Schválil	
Verze	2.1
Stupeň utajení	Důvěrné

Historie dokumentu:

Verze	Datum	Provedl	Komentář
1.x	9.1.2015	D. Holovka	Původní dokumentace: GP_webpay_Seznameni_se_systemem_072013.pdf GP_webpay_Seznameni_se_systemem_20150109_MasterPass.doc
2.0	10.9.2015	D. Holovka	Přidání nových stavů objednávky: automaticky zrušena, automaticky uzavřena, technický problém Sjednocení dokumentů pro standardní obchodníky, obchodníky s Fastpay, obchodníky s opakovanými platbami a obchodníky se službou MasterPass Rozšíření vstupního parametru ADDINFO
2.1	14.12.2015	D. Holovka	Drobné opravy

Obsah

1. Právní doložka

Tento dokument včetně všech případných příloh a odkazů je určen výhradně pro potřeby poskytovatele služeb e-shopu (dále jen „Zákazník“).

Informace v tomto dokumentu obsažené (dále jen „Informace“) jsou předmětem duševního vlastnictví a ochrany autorských práv společnosti Global Payments Europe, s.r.o. (dále jen „GPE“) a mají povahu obchodního tajemství v souladu s ust. § 504 zák. č. 89/2012 Sb., Občanský zákoník. Zákazník si je vědom právních povinností ve vztahu k nakládání s Informacemi.

Informace nebo kterákoliv její část nesmí být bez předchozího výslovného písemného souhlasu GPE poskytnuty nebo jakýmkoliv způsobem zpřístupněny třetí straně. Informace nesmí být zároveň využity Zákazníkem pro jiné účely, než pro účely ke kterému slouží. Pro vyloučení všech pochybností nesmí být Informace nebo kterákoliv část bez předchozího výslovného písemného souhlasu GPE poskytnuty nebo jakýmkoliv způsobem zpřístupněny ani společnostem poskytujícím služby zpracování plateb v prostředí internetu.

GPE si v rozsahu dovoleném platným právem, vyhrazuje veškerá práva k této dokumentaci a k Informacím v ní obsažených. Jakékoliv rozmnožování, použití, vystavení či jiné zveřejnění nebo šíření Informací nebo její části metodami známými i dosud neobjevenými je bez předchozího písemného souhlasu společnosti GPE přísně zakázáno. GPE není jakkoliv odpovědná za jakékoliv chyby nebo opomenutí v Informacích. GPE si vyhrazuje právo, a to i bez uvedení důvodu, jakoukoliv Informaci změnit nebo zrušit.

2. 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 s aplikací GP webpay, která umožňuje elektronickým obchodům přijímat platby, provedené karetními produkty asociací MasterCard, Visa, AMEX a Diners Club[1], v síti Internet.

Aplikace GP webpay 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:

- GP webpay – Seznámení se systémem, vytváření objednávek;
- GP webpay – Administrace systému;
- GP webpay – Správa objednávek – Web Services;
- GP webpay – Praktické scénáře.

3. GP webpay

3.1 Popis aplikace

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 MasterCard, VISA, AMEX a Diners Club v prostředí sítě Internet.

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

Snadná integraci s e-shopem pomocí WS umožňuje kompletní administraci objednávek z interního prostředí obchodníka.

Komunikace s GP webpay je zajištěna:

- on-line formou zaslání požadavku na vytvoření objednávky do GP webpay, následné zpracování požadavku a zaslání výsledku zpracování požadavku. Detailní popis je součástí tohoto dokumentu;
- prostřednictvím standardně dodávaného webového rozhraní aplikace. Detailní popis administrace GP webpay je součástí dokumentu – GP webpay - Administrace systému;

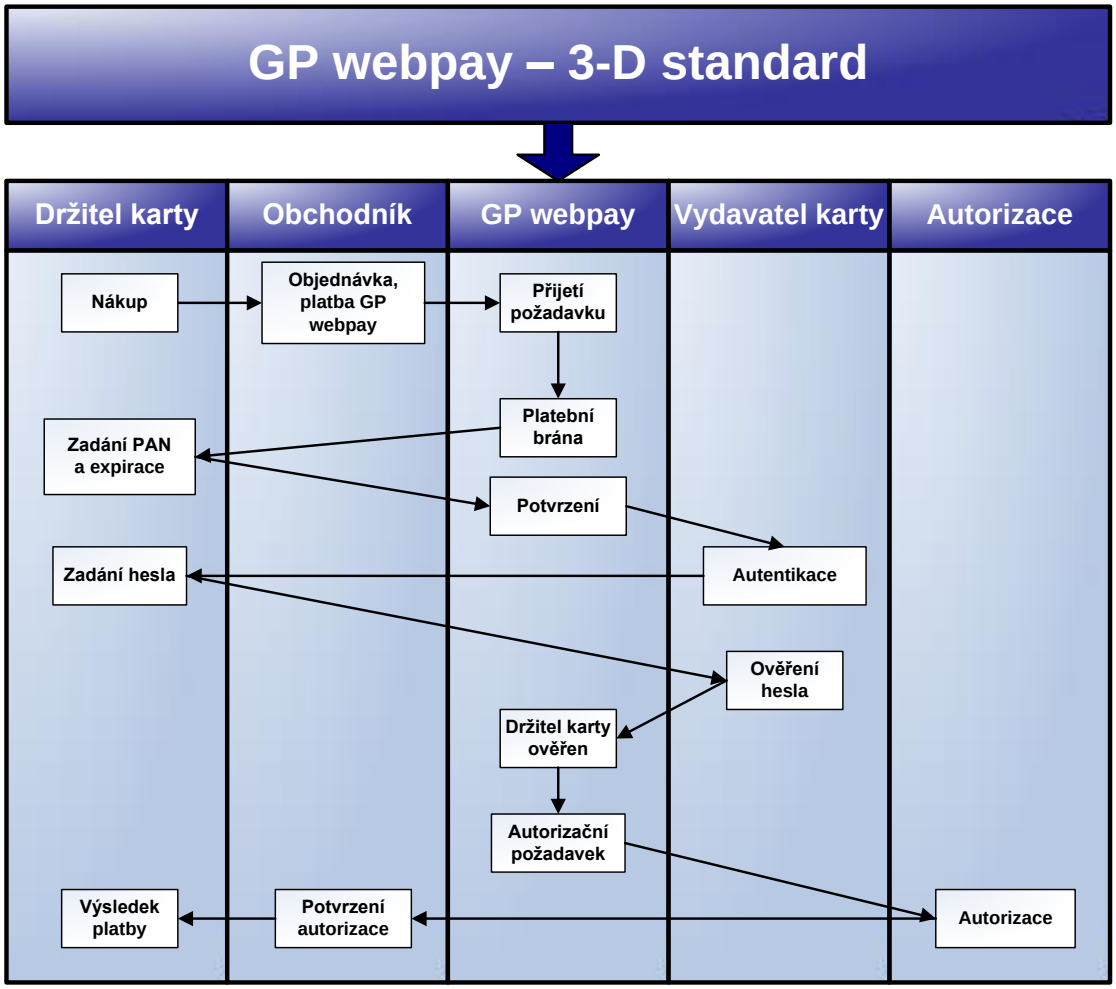
[1] O možnosti akceptace platebních karet konkrétní asociace se informujte u své banky

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

3.2 3-D standard

Vzhledem k možnosti zneužití plateb prostřednictvím platebních karet v prostředí sítě Internet, podporuje GP webpay standard zabezpečení 3-D Secure, definovaný asociacemi MasterCard, VISA a AMEX, známý též pod značkami „MasterCard SecureCode“, „Verified by VISA“ a „American Express SafeKey“.

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 GP webpay požadavek na prověření autentičnosti držitele karty do 3-D systému asociací MasterCard, VISA a AMEX, a na základě obdržených výsledků povoluje/zamítá možnost dalšího zpracování objednávky.

Zabezpečení 3-D Secure znázorňuje obrázek.

Krok	Popis
1	Držitel karty nakupuje v e-shopu a požaduje platbu platební kartou.
2	Obchodník předá požadavek na vytvoření objednávky do GP webpay
3	GP webpay zkontroluje přijatý požadavek
4	GP webpay zobrazí stránku pro vyplnění citlivých informací o platební kartě.
5	Držitel karty vyplní informace o kartě a potvrdí provedení platby.
6	GP webpay zpracuje přijaté informace o platební kartě
7	GP webpay předá požadavek na autentikaci držitele karty 3-D systému příslušné finanční asociace (MasterCard, VISA, AMEX).
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, GP webpay obdrží tuto informaci.
9	3-D systém vydavatele karty autentikuje držitele karty a zašle výsledek autentikace do systému GP webpay
10	Dle výsledku autentikace držitele karty GP webpay určí, zda v dané transakci pokračovat a odeslat požadavek na autorizaci objednávky do autorizačního centra.
11	GP webpay zpracuje výsledek autorizace objednávky
12	Výsledek zpracování je oznámen obchodníkovi prostřednictvím návratových kódů.
13	Obchodník zaznamená výsledek a zobrazí výsledek platby držiteli karty.

3-D systém eliminuje možné pokusy 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, GP webpay 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 / AMEX / DINERS

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

3.3 Popis zpracování

Aplikace GP webpay 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 (po dobu 30 dnů);
- 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,…

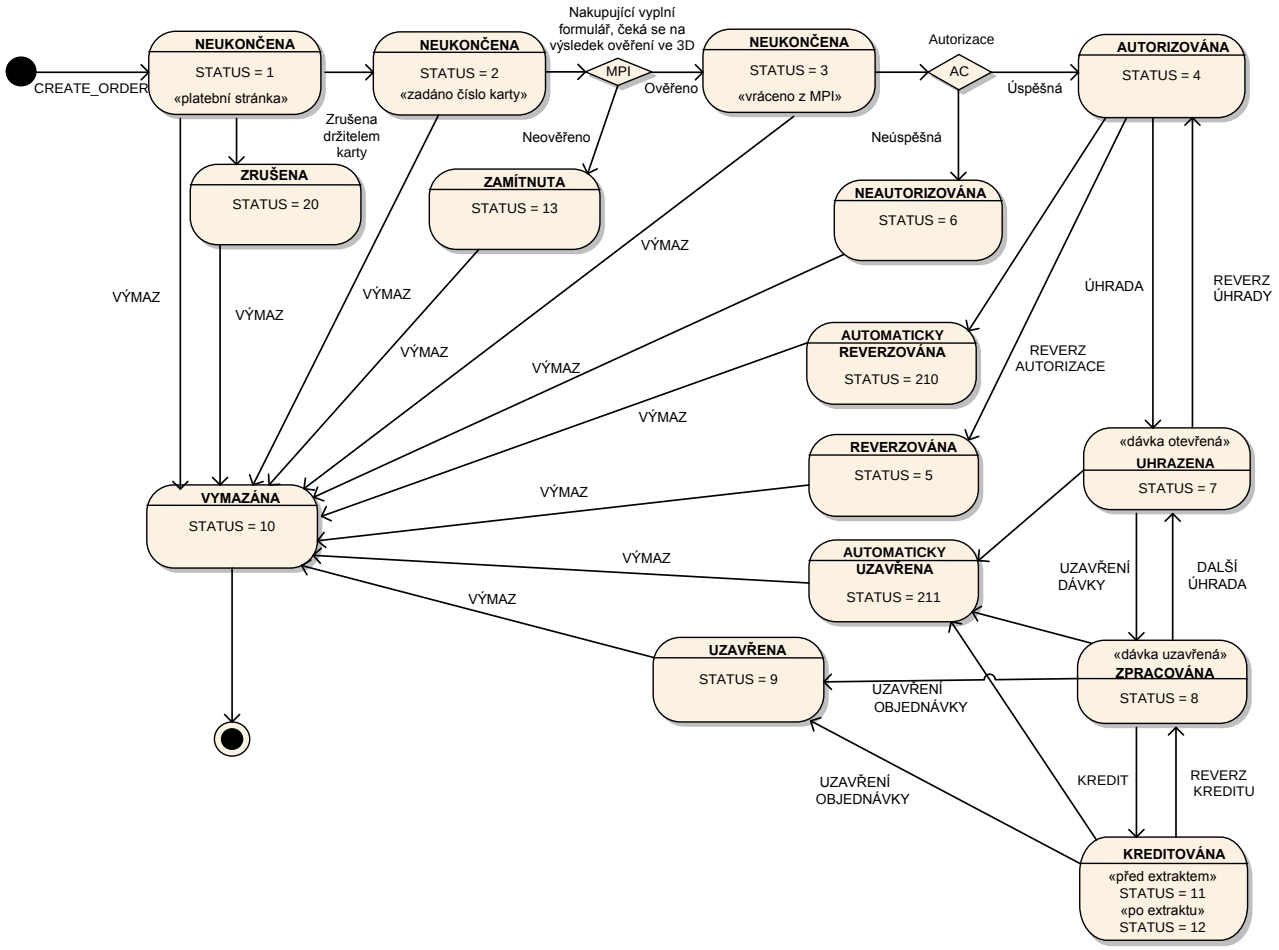
Možnosti zpracování objednávek přímo závisí na stavu, ve kterém se objednávka nachází. Popis stavu objednávky se zobrazí v jazyce, který je dán nastavením prohlížeče. Jazyk je možné manuálně přepnout.

Podporované jazyky jsou čeština, angličtina, slovenština, maďarština a rumunština. Pro jiné jazyky se popisy zobrazují v angličtině.

3.3.1 Stavy objednávky

Stav	Popis	Možné následující stavy
Neukončena **REQUESTED**	Objednávka byla úspěšně přijata do GP webpay – 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 ze systémů asociací, či vydavatelů karet.	**Vymazána** **DELETED**
Odložena **DEFERRED**	Byla odeslána odpověď obchodníkovi s žádostí o doplnění informací – např. změna částky po získání adresy z walletu.	
Zrušena **CANCELED**	Držitel karty zrušil platbu (na platební bráne zvolil možnost "Zpět do e-shopu")	**Vymazána** **DELETED**
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**
Automaticky zrušena **AUTO_CANCELED**	Automaticky zrušená „autorizovaná“ objednávka po uplynutí ochranné lhůty 30 dnů.	**Vymazána** **DELETED**
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 držitele karty k obchodníkovi) Pokud byla objednávka založena s tzv. finální částkou (tj. nastavena hodnota vstupního pole „DEPOSITFLAG“ na hodnotu 1), není možné provést zrušení úhrady. Lze pouze objednávku buď kompletně zrušit – přejde do stavu reverzována, nebo pro vrácení peněz použít funkci KREDIT. Pokud byla objednávka založena s „variabilní“ částkou (tj. nastavena hodnota vstupního pole „DEPOSITFLAG“ na hodnotu 0), je možné zrušit úhradu objednávky do okamžiku, než proběhne uzavření dávky, ve které se daná úhrada nachází. Je možné postupně provést několik úhrad (depositů) až do výše autorizované částky. Pokud provedete i operace	**Autorizována** **APPROVED** **Reverzována** **REVERSED** **Zpracována** **PROCESSED**

Stav	Popis	Možné následující stavy
	typu KREDIT, nemá to žádný vliv na součet úhrad – tzn. součet úhrad nikdy nesmí nepřekročit autorizovanou částku. Úhrady lze provádět pouze po dobu platnosti autorizačního kódu – tj. 30 dnů od data provedení autorizace částky.	
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**
Automaticky uzavřena **AUTO_CLOSED**	Automaticky uzavřená „zpracovaná“ nebo „kreditovaná“ objednávka po uplynutí ochranné lhůty 6/13 měsíců (dle nastavení banky).	**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.	
Technický problém **TECHNICAL_PROBLEM**	Nespecifikovaný stav – technický problém	



3.3.2 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.

Operace s dávkami provádí automaticky systém GP webpay. Obchodník standardně operace s dávkami nedělá.

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 byla uzavřena a čeká na následné zpracování.	**Zpracována** **EXTRACTED**
Zpracována **EXTRACTED**	Dávka byla zpracována a do mezibankovních sítí byly předány požadavky na zaúčtování objednávek.	

3.4 Vytvoření objednávky

Pokud obchodník požaduje platbu od zákazníka, musí ve svém eShopu vytvořit požadavek (objednávku), dle níže uvedené specifikace a tento požadavek zaslat na URL adresu získanou od GPE (např. https://3dsecure.gpwebpay.com/pgw/order.do).

Po obdržení validní zprávy GP webpay zobrazí zákazníkovi „platební stránku“ pro zadání údajů o platební kartě.

Jestliže obchodník na svých stránkách nabízí možnost platby prostřednictvím GP webpay, musí v případě platby GP webpay přesměrovat nakupujícího na stránky GP webpay, a to oslovením adresy GP webpay pro vytvoření objednávky.

Požadavky musí splňovat následující podmínky:

- Požadavek se do GP webpay zasílá metodou GET v případě použití Redirect, anebo formou zaslání formulářových dat z internetového prohlížeče držitele karty metodou GET nebo POST;
- Parametry požadavku musí být podepsány jednoznačným a nepopiratelným způsobem. Tento podpis (DIGEST) je tvořen z obsahu zasílaných polí s využitím soukromého klíče obchodníka – viz Příloha 1 – Podepisování zpráv
- Požadavek se zasílá na URL adresu specifikovanou ve smlouvě
    - klientský test: https://test.3dsecure.gpwebpay.com/pgw/order.do
    - produkční prostředí: https://3dsecure.gpwebpay.com/pgw/order.do;
- Data předávaná v parametrech HTTP request jsou x-www-form-urlencoded dle definice RFC 1866 – kap. 8.2.2, více info na http://www.w3.org/MarkUp/html-spec/;
- HTTP request se zasílá přes zabezpečený HTTPS kanál, za použití serverového certifikátu společnosti GPE, s.r.o.

Součástí dokumentace jsou i užitečné programy (generování klíče/certifikátu, ověřování podpisu) a příklady pro výpočet podpisu (PHP, Java, .NET).

3.4.1 Standardní objednávka

3.4.1.1 Formát požadavku

Parametr	Typ	Délka	Povinný	Poznámka
MERCHANTNUMBER **pole zahrnuto v digest**	znakový	10	ano	Přidělené číslo obchodníka.
OPERATION **pole zahrnuto v digest**	znakový	20	ano	**Hodnota CREATE_ORDER**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	**Číslo objednávky, číslo musí být v každém požadavku od obchodníka unikátní.**
AMOUNT **pole zahrnuto v digest**	numerický	15	ano	Částka v nejmenších jednotkách dané měny pro Kč = v haléřích, pro EUR = v centech

Parametr	Typ	Délka	Povinný	Poznámka
CURRENCY **pole zahrnuto v digest**	numerický	3	ano/ne *pokud není uvedeno, použije se default z obchodníka nebo banky*	Identifikátor měny dle ISO 4217. **Multicurrency (použití různých měn)** je závislé na podpoře jednotlivých bank. Je nutné se informovat u své banky.
DEPOSITFLAG **pole zahrnuto v digest**	numerický	1	ano	Udává, zda má být objednávka uhrazena automaticky. Povolené hodnoty: 0 = není požadována okamžitá úhrada 1 = je požadována úhrada
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne	Identifikace objednávky pro obchodníka. *V případě, že není zadáno, použije se hodnota ORDERNUMBER* *Zobrazí se na výpisu z banky.* ***Každá banka má své řešení/limit.***
URL **pole zahrnuto v digest**	znakový	300	ano	Plná URL adresa obchodníka. Na tuto adresu bude odeslán výsledek požadavku. Výsledek je přeposlán přes prohlížeč zákazníka – tj. je použit redirect (metoda GET). *(včetně specifikace protokolu – např. https://)* Z bezpečnostních důvodů může dojít k zamezení některých tvarů URL adresy – např. použití parametrů v adrese. Tuto kontrolu nelze vypnout a je nutné odzkoušet reálný tvar návratové adresy v testovacím prostředí.
DESCRIPTION **pole zahrnuto v digest**	znakový	255	ne	Popis nákupu. Obsah pole se přenáší do 3-D systému pro možnost následné kontroly držitelem karty během autentikace Access Control Serveru vydavatelské banky. Pole musí obsahovat pouze ASCII znaky v rozsahu 0x20 – 0x7E.
MD **pole zahrnuto v digest**	znakový	255	ano/ne	Libovolná data obchodníka, která jsou vrácena obchodníkovi v odpovědi v nezměněné podobě – pouze očištěna o „whitespace“ znaky na obou stranách. 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 255 B.**
PAYMETHOD **pole zahrnuto v digest**	znakový	255	ne	Hodnota určující preferovanou platební metodu. Podporované hodnoty: CRD – platební karta MCM – MasterCard Mobile

Parametr	Typ	Délka	Povinný	Poznámka
				MPS – MasterPass
DISABLEPAYMETHOD **pole zahrnuto v digest**	znakový	255	ne	Hodnota určující **zakázanou** platební metodu, i když ji má obchodník povolenou. **Má větší prioritu než pole „PAYMETHOD“**. Podporované hodnoty: CRD – platební karta MCM – MasterCard Mobile MPS – MasterPass
PAYMETHODS **pole zahrnuto v digest**	znakový	255	ne	Seznam povolených platebních metod. Hodnoty jsou odděleny čárkou „,“. Pokud je současně definováno pole DISABLEPAYMETHOD, vytvoří se nejprve průnik hodnot a porovná se s polem PAYMETHOD. V případě rozdílnosti hodnot je vrácena chyba o nevhodné hodnotě v odpovídajícím poli. Podporované hodnoty: CRD – platební karta MCM – MasterCard Mobile MPS – MasterPass
EMAIL **pole zahrnuto v digest**	znakový	255	ne	E-mail držitele karty, použije se pro notifikaci výsledku platby a v antifraud systémech (FDS). Pole musí obsahovat pouze **jednu** validní e-mail adresu. Pole může obsahovat jakékoli znaky, ale pokud se v e-mail adrese vyskytují národní znaky, doporučujeme použít BASE64 kódování.
REFERENCENUMBER **pole zahrnuto v digest**	znakový	20	ne	Interní ID u obchodníka Podporované ASCII znaky: x20(space), x23(#), x24($), x2A-x3B(*+,-./0-9:;), x3D(=), x40-x5A(@A-Z), x5E(^), x5F(_), x61-x7A(a-z)
ADDINFO **pole zahrnuto v digest**	XML schéma	24000	ne	Popis košíku, podklady pro FDS, doplňující informace o zákazníkovi … Může být volitelně využito pro zobrazení košíku v peněženkách (MasterPass). **Doporučujeme zasílat požadavky na platební bránu metodou POST. Odstraní se tím limit délky dat v adresním řádku (metoda GET) a zajistí zachování kódování národních znaků v UTF-8 formátu.** **Dalším doporučením je nepoužívat odřádkování a mezery/bílé znaky mezi jednotlivými elementy XML. Prohlížeče s tímto nepracují příliš korektně a při odeslání interpretují odřádkování různě. V drtivé většině případů toto končí neověřením podpisu na serveru.**
DIGEST	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením zaslaných polí v pořadí, uvedeném v této tabulce. *V případě chybného podpisu dat se chybové*

Parametr	Typ	Délka	Povinný	Poznámka
				hlášení zasílá zpět do internetového prohlížeče, ze kterého tento požadavek přišel.
LANG **pole NENÍ v digest**	znakový	2	ne	Hodnota určuje automatickou volbu jazyka na platební stránce. Musí být použita zkratka jednoho z podporovaných jazyků – viz seznam na platební bráně.

3.4.1.2 Formát odpovědi

Parametr	Typ	Délka	Povinný	Poznámka
OPERATION **pole zahrnuto v digest**	znakový	20	ano	**Hodnota CREATE_ORDER**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	Obsah pole z požadavku.
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne	Obsah pole z požadavku, pokud bylo uvedeno.
MD **pole zahrnuto v digest**	znakový	255	ne	Obsah pole z požadavku, pokud bylo uvedeno a nebylo prázdné.
PRCODE **pole zahrnuto v digest**	numerický		ano	Udává primární kód, viz „Seznam návratových kódů“.
SRCODE **pole zahrnuto v digest**	numerický		ano	Udává sekundární kód, viz „Seznam návratových kódů“.
RESULTTEXT **pole zahrnuto v digest**	znakový	255	ne	Slovní popis chyby, který je jednoznačně dán kombinací PRCODE a SRCODE. Text je zasílán bez diakritiky.
USERPARAM1 **pole zahrnuto v digest**	znakový	64	ano/ne *pouze, pokud má obchodník tuto funkcionalitu zapnutou*	Hash čísla platební karty. Hash je unikátní hodnota pro každou kartu a každého obchodníka – tj. pokud je platba provedena stejnou kartou u stejného obchodníka je výsledný hash identický, pokud je tatáž karta použita u jiného obchodníka, tak vznikne hash jiný.
ADDINFO **pole zahrnuto v digest**	XML schéma		ne	Pole je plněné v závislosti na nastavení vstupních parametrů pro peněženky (MasterPass) a požadované návratové informace (brand platební karty …). **Pokud je požadováno zaslání tohoto pole (závisí na nastavení dat ve vstupním parametru „ADDINFO“), bude odpověď zaslána metodou POST. Důvodem je limit velikosti zaslaných dat metodou GET (adresní řádek prohlížeče) a bezpečné určení znakové sady odpovědi – UTF-8.**
DIGEST	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením všech polí v uvedeném pořadí.
DIGEST1	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením všech zaslaných polí v uvedeném pořadí (bez pole DIGEST) a navíc pole MERCHANTNUMBER (pole není zasíláno, obchodník jej musí znát, pole se přidá na konec řetězce). Tímto způsobem je zvýšena bezpečnost a jednoznačnost odpovědi. *Ověření podpisu je identické jako u pole DIGEST.*

Obchodník musí pracovat POUZE s poli, která OBDRŽÍ, nikoli s poli o kterých si „myslí“, že má obdržet.

3.4.2 Objednávka obchodníka využívající službu Fastpay

Služba „Fastpay“ umožňuje držiteli karty předvyplnit na platební stránce dříve použitou platební kartu a umožnit zadat pouze hodnotu CVC2/CVV2.

Toto předvyplnění je uskutečněno prostřednictvím uložených dat minulé objednávky. Je potřeba na rozhraní systému GP webpay zaslat identifikátor (ORDERNUMBER) transakce minulé. Systém pak předvyplní data do platební stránky. Pokud se patřičná objednávka nenajde, zpracování pokračuje standardním způsobem – tj. není nic předvyplněno.

Rozšíření standardního rozhraní:

Parametr	Typ	Délka	Povinný	Poznámka
FASTPAYID **pole zahrnuto v digest**	numerický	15	ano/ne *povinné, pokud je využita služba Fastpay*	Unikátní ORDERNUMBER objednávky, které bylo použito v minulosti a má sloužit jako podklad pro předvyplnění čísla karty. Objednávka by měla být uhrazena a nesmí být starší než 12(18) měsíců, protože by již mohla být ze systému automaticky odstraněna.

Tento parametr je řazen **za parametr MD** – viz seznam/pořadí polí.

Formát odpovědi je identický se standardním formátem.

3.4.3 Registrační objednávka (tzv. „master“ objednávka) pro opakované platby

Systém GP webpay umožňuje pracovat s tzv. opakovanými platbami. Celý proces probíhá tak, že je nejprve potřeba vytvořit tzv. registrační („master“) objednávku přes standardní HTTP rozhraní a později je možné k této registrační objednávce zakládat prostřednictvím web services (WS) další následné platby.

Než bude možné vytvořit následnou platbu, je nutné, aby objednávka byla úspěšně autorizována a zaúčtována – tj. musí dojít k fyzickému zaplacení (z pohledu systému GP webpay musí dojít k uzavření dávky s touto objednávkou).

Zneplatnění registrační platby je možné dvěma způsoby:

1. zneplatnění provede vydavatel platební karty prostřednictvím speciálního návratového kódu z autorizačního procesu
2. automaticky po roce nečinnosti – tj. k registrační objednávce nebyla více než 1 rok vytvořena žádná následná platba

Označení objednávky jako registrační se provádí přidání parametru „USERPARAM1“ do standardního HTTP rozhraní.

Rozšíření standardního rozhraní:

Parametr	Typ	Délka	Povinný	Poznámka
USERPARAM1 **pole zahrnuto v digest**	znakový	255	ano/ne *povinné pro*	Uživatelské pole. Nyní použito pro předávání parametru „R“ –

Parametr	Typ	Délka	Povinný	Poznámka
			registraci „master“ platby, jinak nepovinné	informace o požadavku registrace „master“ opakované platby.

Tento parametr je řazen **za parametr MD** – viz seznam/pořadí polí.

Formát odpovědi je identický se standardním formátem.

3.4.4 Objednávka obchodníka využívající službu MasterPass

Služba MasterPass je platba prostřednictvím elektronické peněženky. Peněženka je nainstalována v mobilním zařízení a jsou v ní registrovány platební karty. Při platbě je pak pouze potřeba sejmout aplikací QR kód, vybrat registrovanou kartu a potvrdit platbu.

O této službě pojednává samostatný dokument „GPwebpay_MasterPass_Integracni_manual_vx.x.docx“.

Standardní HTTP rozhraní podporuje tuto službu dvěma způsoby:

1. je zde možnost zaslat nákupní košík, který je následně zobrazen v peněžence a dojde k zaplacení
2. je možné platbu rozdělit na dva kroky, přičemž první krok je vytvoření objednávky standardním způsobem a získání odpovědi jakým typem karty bude zaplaceno. Druhým krokem je potvrzení platby (je možné upravit částku) a dokončit platbu

Pro odeslání košíku se používá standardní pole **ADDINFO**. V tomto poli jsou uložena data ve formátu XML.

Parametry objednávky jsou totožné jako u standardní objednávky, ale je potřeba navíc v parametru ADDINFO nastavit element „requestDeferredAuthorization“ na hodnotu „true“ (pro získání adresy je potřeba nastavit element „requestShippingDetails“ na true, pro získání věrnostního programu je potřeba nastavit element „requestLoyaltyProgram“ na true). Díky tomuto nastavení je proces platby přerušen a po získání veškerých informací z prostředí MasterPass je další zpracování přesměrováno na URL obchodníka zadanou při zakládání objednávky. Formát odpovědi je totožný/zjednodušený a obsahuje následující parametry: **PRCODE = 200, SRCODE = 0**. V poli ADDINFO (v xml) jsou obsaženy informace o držiteli karty, se kterými může následně obchodník pracovat.

Obchodník zpracuje obdržená data a voláním standardního rozhraní může upravit vstupní parametry původní objednávky.

3.4.4.1 Formát požadavku

Parametr	Typ	Délka	Povinný	Poznámka
MERCHANTNUMBER **pole zahrnuto v digest**	znakový	10	ano	Přidělené číslo obchodníka.
OPERATION **pole zahrnuto v digest**	znakový	20	ano	**Hodnota FINALIZE_ORDER**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	**Číslo objednávky – musí odpovídat číslu původní objednávky**
AMOUNT	numerický	15	ano	Částka v nejmenších jednotkách dané měny

Parametr	Typ	Délka	Povinný	Poznámka
pole zahrnuto v digest				pro Kč = v haléřích, pro EUR = v centech
URL **pole zahrnuto v digest**	znakový	300	ano	Plná URL adresa obchodníka. Na tuto adresu bude odeslán výsledek požadavku. Výsledek je přeposlán přes prohlížeč zákazníka – tj. je použit redirect (metoda GET). *(včetně specifikace protokolu – např. https://)* Z bezpečnostních důvodů může dojít k zamezení některých tvarů URL adresy – např. použití parametrů v adrese. Tuto kontrolu nelze vypnout a je nutné odzkoušet reálný tvar návratové adresy v testovacím prostředí.
DIGEST	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením zaslaných polí v pořadí, uvedeném v této tabulce. *V případě chybného podpisu dat se chybové hlášení zasílá zpět do internetového prohlížeče, ze kterého tento požadavek přišel.*

3.4.4.2 Formát odpovědi

Parametr	Typ	Délka	Povinný	Poznámka
OPERATION **pole zahrnuto v digest**	znakový	20	ano	**Hodnota FINALIZE_ORDER**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	Obsah pole z požadavku.
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne	Obsah pole z požadavku operace CREATE_ORDER, pokud bylo uvedeno.
MD **pole zahrnuto v digest**	znakový	255	ne	Obsah pole z požadavku operace CREATE_ORDER, pokud bylo uvedeno a nebylo prázdné.
PRCODE **pole zahrnuto v digest**	numerický		ano	Udává primární kód, viz „Seznam návratových kódů“.
SRCODE **pole zahrnuto v digest**	numerický		ano	Udává sekundární kód, viz Seznam návratových kódů.
RESULTTEXT **pole zahrnuto v digest**	znakový	255	ne	Slovní popis chyby, který je jednoznačně dán kombinací PRCODE a SRCODE. Text je zasílán bez diakritiky.
USERPARAM1 **pole zahrnuto v digest**	znakový	64	ano/ne *pouze, pokud má obchodník tuto funkcionalitu zapnutou*	Hash čísla platební karty. Hash je unikátní hodnota pro každou kartu a každého obchodníka – tj. pokud je platba provedena stejnou kartou u stejného obchodníka je výsledný hash identický, pokud je tatáž karta použita u jiného obchodníka, tak vznikne hash jiný.
ADDINFO **pole zahrnuto v digest**	XML schéma		ne	Pole je plněné v závislosti na nastavení vstupních parametrů pro peněženky (MasterPass) a požadované návratové informace (brand platební karty …). **Pokud požadováno zaslání tohoto pole (závisí na nastavení dat ve vstupním**

Parametr	Typ	Délka	Povinný	Poznámka
				parametru „ADDINFO“), bude odpověď zaslána metodou POST. Důvodem je limit velikosti zaslaných dat metodou GET (adresní řádek prohlížeče) a bezpečné určení znakové sady odpovědi – UTF-8.
DIGEST	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením všech polí v uvedeném pořadí.
DIGEST1	znakový	2000	ano	Kontrolní podpis řetězce, který vznikne zřetězením všech zaslaných polí v uvedeném pořadí (bez pole DIGEST) a navíc pole MERCHANTNUMBER (pole není zasíláno, obchodník jej musí znát, pole se přidá na konec řetězce). Tímto způsobem je zvýšena bezpečnost a jednoznačnost odpovědi. *Ověření podpisu je identické jako u pole DIGEST.*

Obchodník musí pracovat POUZE s poli, která OBDRŽÍ, nikoli s poli o kterých si „myslí“, že má obdržet.

3.5 Kompletní seznam polí na vstupu – pořadí parametrů

Parametr	Typ	Délka	Povinný
MERCHANTNUMBER **pole zahrnuto v digest**	znakový	10	ano
OPERATION **pole zahrnuto v digest**	znakový	20	ano
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano
AMOUNT **pole zahrnuto v digest**	numerický	15	ano
CURRENCY **pole zahrnuto v digest**	numerický	3	ano/ne *pokud není uvedeno, použije se default z obchodníka nebo banky*
DEPOSITFLAG **pole zahrnuto v digest**	numerický	1	ano
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne
URL **pole zahrnuto v digest**	znakový	300	ano
DESCRIPTION **pole zahrnuto v digest**	znakový	255	ne
MD **pole zahrnuto v digest**	znakový	255	ano/ne
USERPARAM1 **pole zahrnuto v digest**	znakový	255	ano/ne *povinné pro registraci „master“ platby, jinak nepovinné*
FASTPAYID **pole zahrnuto v digest**	numerický	15	ano/ne *povinné, pokud je využita služba Fastpay*
PAYMETHOD **pole zahrnuto v digest**	znakový	255	ne
DISABLEPAYMETHOD	znakový	255	ne

pole zahrnuto v digest			
PAYMETHODS **pole zahrnuto v digest**	znakový	255	ne
EMAIL **pole zahrnuto v digest**	znakový	255	ne
REFERENCENUMBER **pole zahrnuto v digest**	znakový	20	ne
ADDINFO **pole zahrnuto v digest**	XML schéma	24000	ne
DIGEST	znakový	2000	ano
LANG **pole NENÍ v digest**	znakový	2	ne

4. Přílohy a dodatky

4.1 Příloha č. 1 – Podepisování zpráv

4.1.1 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 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, DVD) nebo zašle e-mailem na adresu zákaznické podpory – gpwebpay@gpe.cz. 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 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** (definovaných v HTTP rozhraní, ostatní pole se ignorují) v **zasílaném požadavku** s výjimkou pole DIGEST. Při sestavení vstupní zprávy je nutné dodržet stejné **pořadí polí** (viz tabulka pořadí), jako v definici příkazu a oddělovat jednotlivá pole oddělovačem “|“ (pipe, ascii 124, hexa 7C), kterému nesmí předcházet, ani nesmí být následován **whitespace**. URLEncode parametrů se použije pouze pro přenos dat, pro výpočet podpisu se musí použít původní data.

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 + | + CURRENCY + | + DEPOSITFLAG + | + MERORDERNUM + | + URL + | + DESCRIPTION + | + MD

V případě, že v požadavku není obsaženo některé z nepovinných polí, pole se přeskočí. Jestliže je zasíláno pole prázdné, pak je potřeba jej také zahrnout do výpočtu pro DIGEST a budou v řetězci dva oddělovače vedle sebe – ||.

Pokud obchodník posílá pouze povinné parametry, k výpočtu pole DIGEST slouží hodnota:

MERCHANTNUMBER + | + OPERATION + | + ORDERNUMBER + | + AMOUNT + | + CURRENCY + | + DEPOSITFLAG + | + URL

4.1.2 Ověření 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 je 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.

Dále odpověď obsahuje také pole DIGEST1, které dále zvyšuje bezpečnost odpovědi. Pole DIGEST1 je tvořeno stejně jako pole DIGEST, ale je k parametrům pro ověření pole DIGEST přidán parametr „MERCHANTNUMBER“. Tento parametr není zasílán v odpovědi a obchodník si jej musí přidat sám, protože zná jeho hodnotu.

Výsledný řetězec pro ověření pole DIGEST1 vypadá takto:

<řetězec pro pole DIGEST> + | + MERCHANTNUMBER

4.1.3 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

4.1.4 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 GPE je vybrán správný veřejný klíč a ověřena jeho integrita;

b) elektronický podpis je BASE64 dekódován;

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

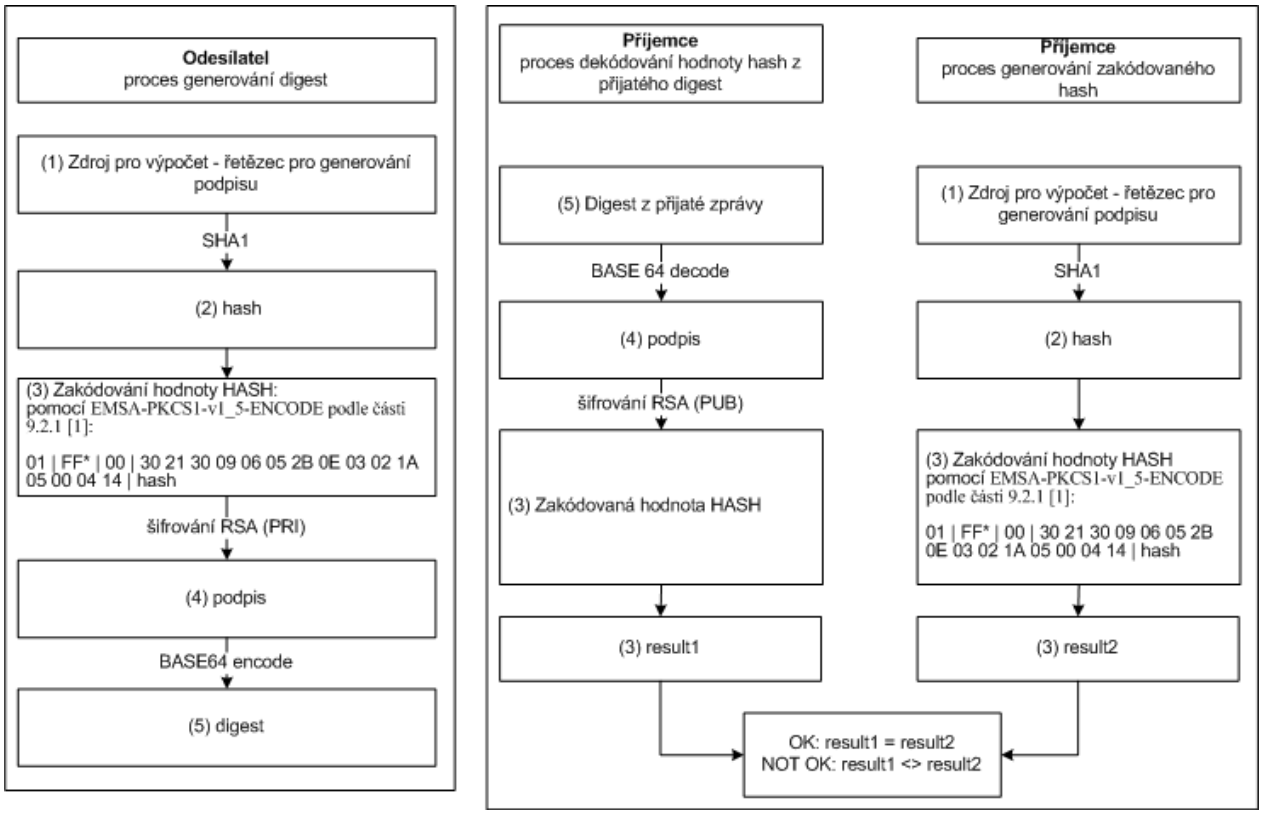
d) d) ze zprávy je vypočtena miniatura (hash) a zakódována v souladu s předchozí částí “Výpočet elektronického podpisu“ body a) b);

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).

4.1.5 Grafické znázornění generování a ověření



4.1.6 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:

KeyPair GPE	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
KeyPair obchodníka	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.. Lze použít i komerčně vydávané klíče, ale jejich platnost je omezena 1-2 roky (na rozdíl od klíče vytvořeného aplikací, kde je platnost 10 let).

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).

4.1.7 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[2].

Parametr	Hodnota	Poznámky
Version	3	
Subject a Issuer	CN=<Jméno obchodníka>:<Merchant ID>:<banka>, OU=GP webpay, O=GPE,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 nebo datum a čas vytvoření	V případě obnovy nebo výměny klíče musí být pořadové číslo zvýšeno vždy o 1 nebo vygenerováno jednoznačné sériové číslo v rámci společnosti.
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.

4.1.8 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.

4.1.9 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/;

[2] Parametry odpovídají RFC 2459 [4]

[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.

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

4.2 Příloha č. 2 – Seznam návratových kódů

Výsledek zpracování v GP webpay 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“.

4.2.1 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
25	Uživatel není oprávněn k provedení operace	Operation not allowed for user
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
35	Expirovaná session Nastává při vypršení webové session při zadávání karty	Session expired
50	Držitel karty zrušil platbu	The cardholder canceled the payment
200	Žádost o doplňující informace	Additional info request

1000	Technický problém	Technical problem

4.2.2 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. *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. *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. *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. *Note: Cardholder wasn't authenticated – Issuer or Cardholder not participating in 3D.* *Transaction can continue.*

Hodnota	Význam CS	Význam EN
3004	Neověřeno v 3D. Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. *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. *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. *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. *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. *Info: Byla použita karta, která není v 3D systémech podporována.* *V transakci není možné pokračovat.*	Declined in 3D. Unsupported card product. *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**[3] *Zahrnuje důvody, které naznačují zneužití platební karty – kradená karta, podezření na podvod, ztracená karta apod.* *Karta je označena jako:* *Ztracená* *K zadržení* *K zadržení (speciální důvody)* *Ukradená* *Většinou pokus o podvodnou transakci.*	Declined in AC, Card blocked
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 PIN.*	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 poskytovatele 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).

[3] 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.

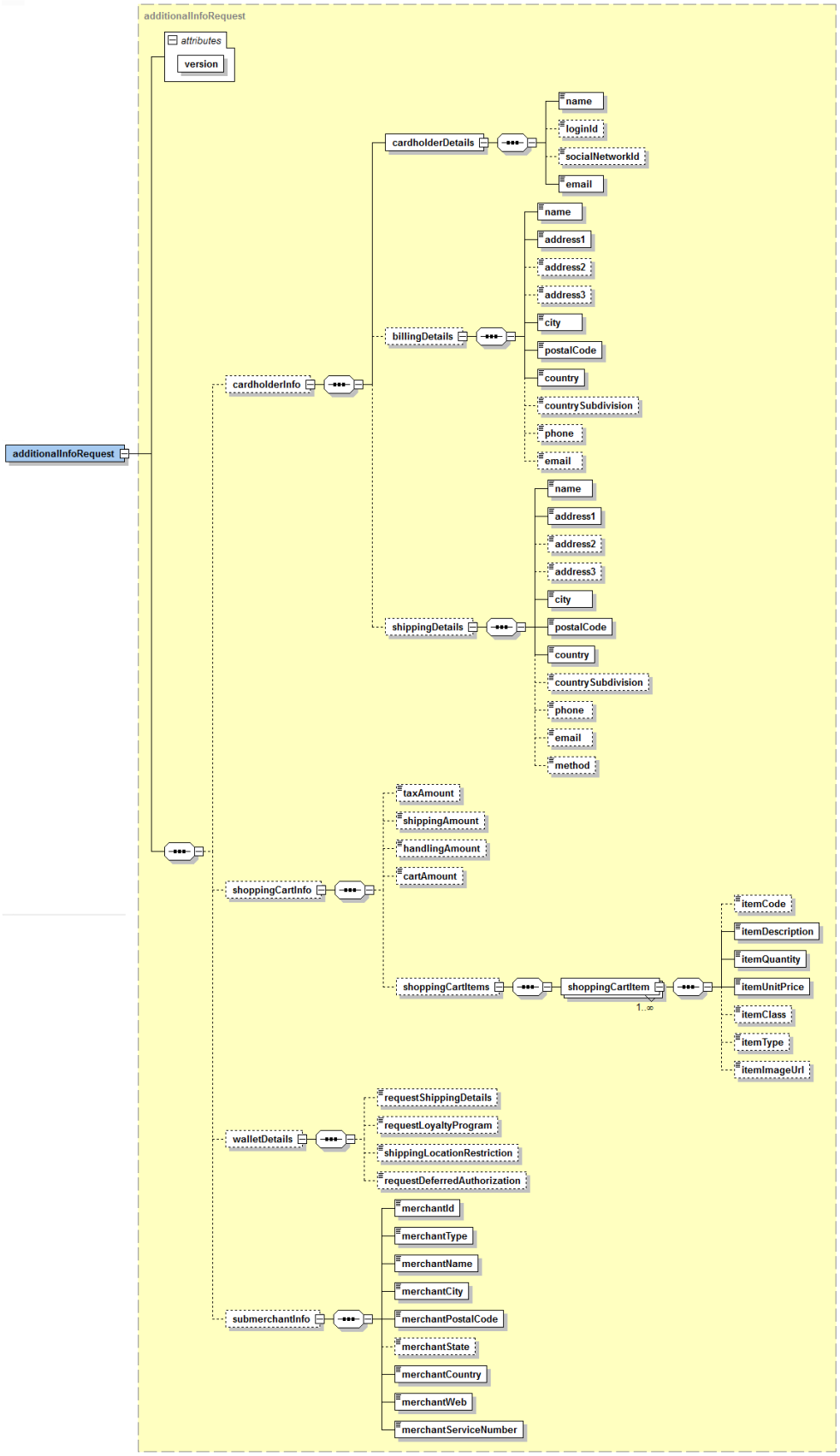
4.3 Příloha č. 3 – formát polí ADDINFO

Seznam typů elementů

Název typu	Popis
Složený typ	Element je složen z více elementů různého typu
Částka	Číslo o max. délce 12 číslic. Hodnota částky musí být uvedena v nejmenších jednotkách dané měny bez desetinné částky

4.3.1 Vstupní parametr „ADDINFO“

4.3.1.1 Popis elementů



Název elementu	Popis	P/N[4]	Typ
additionalInfoRequest	Hlavní element zahrnující veškeré požadované informace	P	Složený typ
version="x.x"	*Součástí je atribut s informací o použité verzi šablony.*	*P*	*Číselný typ ve tvaru např. "1.0".*
Data o nakupujícím použitá ve anti-fraud systému			
cardHolderInfo	Informace o zákazníkovi	N	Složený typ
cardHolderDetail	Základní informace o zákazníkovi	A	Složený typ
name	Jméno zákazníka	A	Text, max. 255 znaků
loginId	LoginID do e-shopu	N	Text, max. 255 znaků
socialNetworkId	LoginID do e-shopu pokud je použito přihlášení přes sociální síť (Facebook, Google…)	N	Text, max. 255 znaků
email	E-mail zákazníka	A	E-mail, max. 255 znaků
billingDetails	Fakturační adresa	N	Složený typ
name	Jméno	A	Text, max. 255 znaků
address1	Ulice – první řádek	A	Text, max. 255 znaků
address2	Ulice – druhý řádek	N	Text, max. 255 znaků
address3	Ulice – třetí řádek	N	Text, max. 255 znaků
city	Město	A	Text, max. 255 znaků
postalCode	Poštovní směrovací číslo	A	Text, max. 255 znaků
country	Stát	A	Text, max. 255 znaků
countrySubdivision	Oblast	N	Text, max. 255 znaků
phone	Telefonní číslo	N	Text, max. 20 znaků
email	E-mail	N	E-mail, max. 255 znaků
shippingDetails	Doručovací adresa	N	Složený typ
name	Jméno	A	Text, max. 255 znaků
address1	Ulice – první řádek	A	Text, max. 255 znaků
address2	Ulice – druhý řádek	N	Text, max. 255 znaků
address3	Ulice – třetí řádek	N	Text, max. 255 znaků
city	Město	A	Text, max. 255 znaků
postalCode	Poštovní směrovací číslo	A	Text, max. 255 znaků
country	Stát	A	Text, max. 255 znaků
countrySubdivision	Oblast	N	Text, max. 255 znaků
phone	Telefonní číslo	N	Text, max. 20 znaků
email	E-mail	N	E-mail, max. 255 znaků
method	Metoda doručení `personal pick-up, courier, electronic delivery …`	N	Text, max. 255 znaků
Data o nákupním košíku použitá ve anti-fraud systému a elektronických peněženkách			
shoppingCartInfo	Element obsahující informace o nákupním košíku	N	Složený typ
taxAmount	Částka DPH	N	Částka
shippingAmount	Poštovné	N	Částka
handlingAmount	Balné	N	Částka

[4] Povinnost pole P – povinné, N – nepovinné

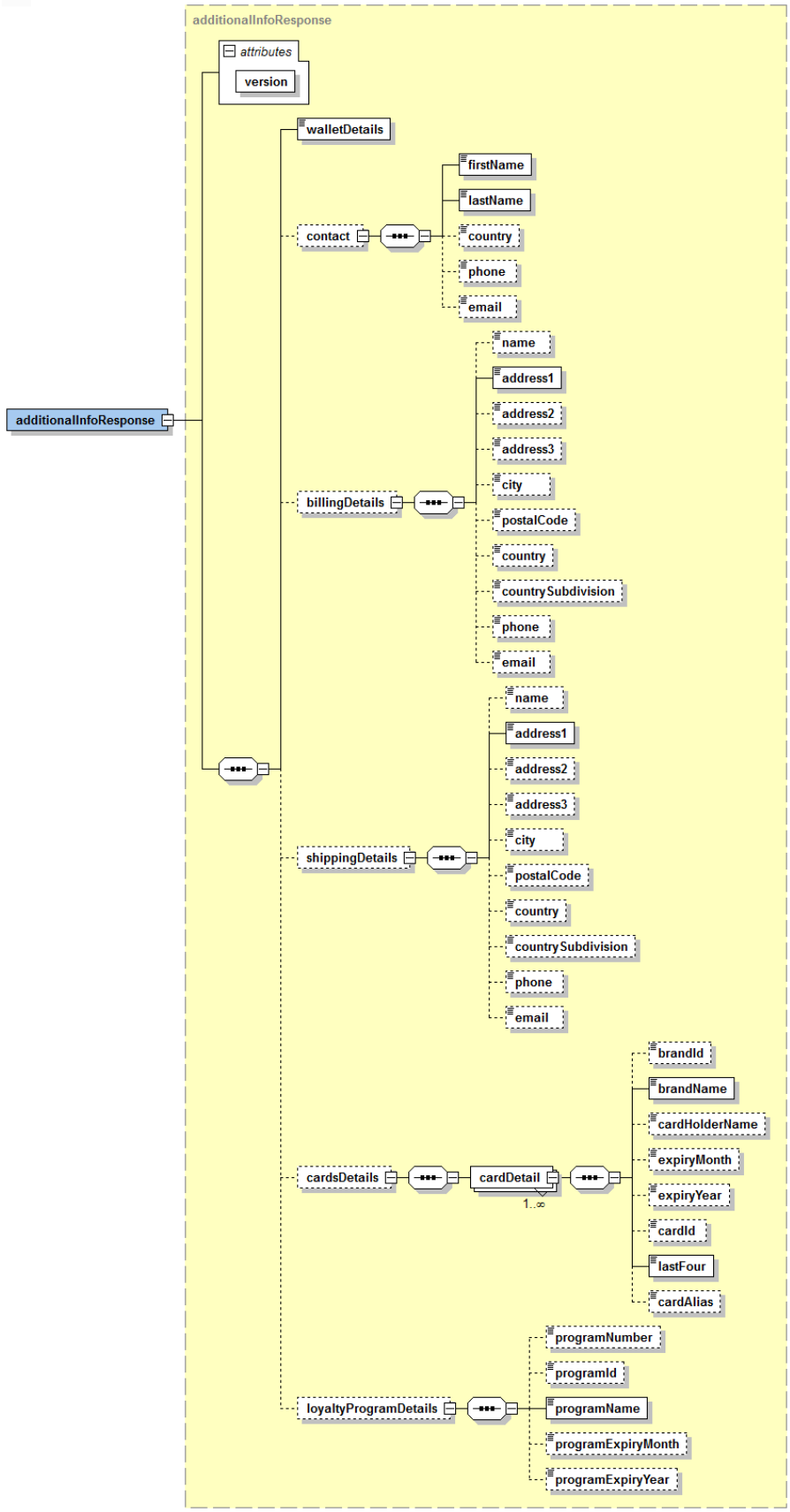
cartAmount	Čistá hodnota nákupního košíku bez DPH. Hodnota se vypočítá takto: `(shoppingCartItem1[itemQuantity] * shoppingCartItem1[itemUnitPrice]) + (shoppingCartItem2[itemQuantity] * shoppingCartItem2[itemUnitPrice]) + …`	N	Částka
shoppingCartItems	Jednotlivé položky nákupního košíku. Je možné uvést více položek.	P	Složený typ
shoppingCartItem	Položka nákupního košíku	P	Složený typ
itemCode	Kód položky, např. „položka 1“	N	Text, max. 20 znaků
itemDescription	Popis položky	P	Text, max. 50 znaků
itemQuantity	Počet kusů položky	P	Číslo, max. 12 pozic
itemUnitPrice	Cena za 1 kus položky bez DPH	P	Částka
itemClass	Třída položky, např. „třída A“	N	Text, max. 20 znaků
itemType	Typ položky, např. „pánské oblečení“	N	Text, max. 20 znaků
itemImageUrl	Kompletní URL cesta k obrázku položky. Při použití MasterPass peněženky bude u položky zobrazen obrázek.	N	URL, max. 2000 znaků
Sekce dat při využití některé z elektronických peněženek			
walletDetails	Element upravující chování peněženky	N	Složený typ
requestShippingDetails	Přepínač nastavující, zda je požadována v odpovědi informace o dodací adrese	N	true/false
requestLoyaltyProgram	Přepínač nastavující, zda je požadována v odpovědi informace o věrnostním programu	N	true/false
shippingLocationRestriction	Seznam podporovaných zemí pro doručování zásilek	N	Omezení výběru dodací adresy. Podporované hodnoty: CZ – Česká republika SK – Slovensko HU – Maďarsko EU – Evropská unie US – USA WW – celý svět (bez omezení) Defaultní hodnota je nastavena podle sídla banky. V případě požadavku na doručování do jiných zemí kontaktujte prosím aplikační podporu.
requestDeferredAuthorization	Nastavení elementu na „true“ umožní přerušit zpracování objednávky v systému GP webpay a vyžádání finalizačních dat od obchodníka	N	true/false
requestCardsDetails	Požadavek na zaslání detailu platební karty/karet v odpovědi	N	true/false
Sekce dat pro velké poskytovatele platebních služeb			
submerchantInfo	Informace o obchodníkovi realizujícím své obchody prostřednictvím platebního agregátora (payment facilitator model)	N	Složený typ
merchantId	Číslo obchodníka	A	Max. 15 znaků

			ASCII x20-x7E
merchantType	MCC kód obchodníka	A	4 čísla
merchantName	Název obchodníka Výsledný název obchodníka bude složenina názvu agregátora a obchodníka	A	Max. 22 znaků ASCII x20-x7E
merchantStreet	Ulice	A	Max. 25 znaků ASCII x20-x7E
merchantCity	Město	A	Max. 13 znaků ASCII x20-x7E
merchantPostalCode	Poštovní směrovací číslo	A	Max. 10 znaků
merchantState	Stát	N	Max. 3 znaky
merchantCountry	Kód země – ISO 3166-1 Alpha-2	A	2 znaky
merchantWeb	Webová adresa obchodníka	A	25 znaků ASCII x20-x7E
merchantServiceNumber	Telefonní číslo obchodníka	A	13 číslic

4.3.1.2 Schéma parametru

4.3.2 Návratový parametr „ADDINFO“

4.3.2.1 Popis elementů



Název elementu	Popis	P/N	Typ
additionalInfoResponse *version="x.x"*	Hlavní element zahrnující veškeré požadované informace. *Součástí je atribut s informací o použité verzi šablony.*	P *P*	Složený typ *Číselný typ ve tvaru např. „1.0".*
Informace o použité elektronické peněžence			
walletDetails	Informace o použité peněžence. Aktuálně podporované hodnoty: MPS	P	Text, max. 255 znaků
Data získaná z elektronické peněženky			
contact	Kontakt na držitele karty	N	Složený typ
firstName	Jméno	P	Text, max. 255 znaků
lastName	Příjmení	P	Text, max. 255 znaků
country	Země	P	Text, max. 255 znaků
phone	Telefon	N	Text, max. 20 znaků
email	E-mail	N	Text, max. 255 znaků
billingDetails	Zúčtovací/fakturační data kupujícího	N	Složený typ
name	Jméno	N	Text, max. 255 znaků
address1	1. linka adresy	P	Text, max. 255 znaků
address2	2. linka adresy	N	Text, max. 255 znaků
address3	3. linka adresy	N	Text, max. 255 znaků
city	Město	P	Text, max. 255 znaků
postalCode	PSČ/ZIP	N	Text, max. 255 znaků
country	Země	P	Text, max. 255 znaků
countrySubdivision	Region v zemi	N	Text, max. 255 znaků
phone	Telefon	N	Text, max. 20 znaků
email	E-mail	N	Text, max. 255 znaků
shippingDetails	Doručovací adresa	N	Složený typ
name	Jméno	N	Text, max. 255 znaků
address1	1. linka adresy	P	Text, max. 255 znaků
address2	2. linka adresy	N	Text, max. 255 znaků
address3	3. linka adresy	N	Text, max. 255 znaků
city	Město	P	Text, max. 255 znaků
postalCode	PSČ/ZIP	N	Text, max. 255 znaků
country	Země	P	Text, max. 255 znaků
countrySubdivision	Region v zemi	N	Text, max. 255 znaků
phone	Telefon	N	Text, max. 20 znaků
email	E-mail	N	Text, max. 255 znaků
Data získaná z elektronické peněženky			
cardsDetails	Detaily karet registrovaných v elektronické peněžence a vyhovující podmínkám zadaným ve vstupním požadavku	N	Složený typ
cardDetail	Detail karty, může jich být více (při použití v rámci elektronické peněženky)	A	Složený typ
brandId	ID karetní asociace	N	Text, max. 255 znaků
brandName	Název karetní asociace	A	Text, max. 255 znaků
cardHolderName	Jméno držitele karty	N	Text, max. 255 znaků
expiryMonth	Měsíc expirace karty	N	1-2 čísla

expiryYear	Rok expirace karty	N	4 čísla
cardId	ID karty v elektronické peněžence	N	Text, max. 255 znaků
lastFour	Poslední 4 číslice z čísla karty	A	4 čísla
cardAlias	Pojmenování karty v elektronické peněžence	N	Text, max. 255 znaků
Data získaná z elektronické peněženky			
loyaltyProgramDetails	Informace o věrnostním programu	N	Složený typ
programNumber	Číslo programu	N	Text, max. 255 znaků
programId	Id programu	N	Text, max. 255 znaků
programName	Jméno programu	P	Text, max. 255 znaků
programExpiryMonth	Měsíc ukončení programu	N	Číslo, 1-12
programExpiryYear	Rok ukončení programu	N	Číslo, 2014-2099

4.3.2.2 Schéma parametru

4.4 Dodatek č. 1 – BASE64 kódování / dekódování

Base64 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 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 1 znak = 8 bitů. Vstupní proud se následně rozdělí do skupin 6bitů, 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 8mi bitech a tyto skupiny jsou převedeny zpět do původní podoby vstupních dat.

Přesné znění base64 kódování je možné nalézt v RFC 3548.

4.5 Dodatek č. 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 for the Identification of Languages

4.6 Dodatek č. 3 – Maximální délka MERORDERNUM

Maximální délka MERORDERNUM pro jednotlivé banky zobrazená na výpisech pro obchodníky:

Banka	Max. počet číslic v MERORDERNUM zobrazených na výpise banky
Komerční banka	16
ČSOB CZ	
Raiffiesen bank	10
UniCredit bank	12
ČSOB SK	
ČSAS	