GP webpay API HTTP

Technická specifikace pro vývojáře

Verze: 1.4

Global Payments Europe, s.r.o.

Vytvořeno **08.06.2016**

Poslední změna **22.10.2018**

Autor dokumentu	GPE Product
Správce dokumentu	GPE Application Development
Schválil	
Verze	1.4
Stupeň utajení	Důvěrné

Historie dokumentu:

Verze	Datum	Provedl	Komentář
0.1	08.06.2016	GPE Product	Vznik dokumentu – přepracování dokumentu GP_webpay_Seznameni_se_systemem_v2.1
0.2	13.06.2016	GPE Product	Drobné opravy
1.0	17.06.2016	GPE Application Development	Revize dokumentu
1.1	01.08.2016	GPE Application Development	Přidání polí pro verifikaci platební karty
1.2	15.06.2017	GPE Application Development	Přidání Card on file specifikace: - úprava hodnoty vstupního parametru USERPARAM1 - přidání nových polí v odpovědi
1.3	19.09.2018	GPE Application Development	Nová hodnota v poli „PAYMETHOD“ a „PAYMETHODS“ pro GooglePay
1.4	17.10.2018	GPE Application Development	Nová hodnota v poli „DISABLEPAYMETHOD“ pro GooglePay Vyzdvihnutí možnosti použití metody POST při odeslání odpověďi zpět k obchodníkovi

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

Technická specifikace pro vývojáře „GP webpay API HTTP“ je určena pro vývojáře e-commerce obchodníků (dále jen vývojář), kteří provádí integraci e-shopu s platební bránou GP webpay s využitím API HTTP.

Integrace s využitím API WS je popsána v technické specifikaci pro vývojáře „GP webpay API WS“.

Důležité upozornění: jednotlivé platební metody a funkce povoluje obchodníkovi jeho poskytovatel (acquirer). Informace ohledně objednání platební brány GP webpay a kontakty na všechny poskytovatele jsou k dispozici na www.gpwebpay.cz.

3. Proces platby

3.1 Požadavek

Obchodník při požadavku na online platbu od zákazníka vytvoří ve svém e-shopu požadavek na vytvoření platby (dále jen požadavek) a zašle jej na rozhraní platební brány GP webpay API HTTP.

Formát požadavku pro jednotlivé platební metody je popsán níže. Kompletní seznam a pořadí parametrů požadavku uvádí tato tabulka:

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 registrační platbu pro funkci Opakovaná platba, jinak nepovinné*
FASTPAYID	numerický	15	ano/ne

pole zahrnuto v digest			*povinné, pokud je využita služba Fastpay*
PAYMETHOD **pole zahrnuto v digest**	znakový	255	ne
DISABLEPAYMETHOD **pole zahrnuto v digest**	znakový	255	ne
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
PANPATTERN **pole zahrnuto v digest**	znakový	255	ne
TOKEN **pole zahrnuto v digest**	znakový	64	ne
DIGEST	znakový	2000	ano
LANG **pole NENÍ v digest**	znakový	2	ne

GP webpay API HTTP přijme pouze ty požadavky, u kterých lze doložit, že původcem požadavku byl oprávněný subjekt, tedy obchodník, se kterým poskytovatel uzavřel smlouvu.

K prokázání původu požadavku slouží parametr DIGEST. Jeho obsah je vypočten na základě:

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

Při zahájení integrace obchodník vygeneruje s využitím portálu GP webpay soukromý klíč, který si obchodník bezpečně uloží a poskytne ho vývojáři pro integraci. Veřejný klíč obchodníka je během tohoto procesu automaticky uložen na server GP webpay a před přijetím požadavku od obchodníka se pomocí něj bude kontrolovat, zda obchodník podepsal požadavek svým soukromým klíčem.

Parametr DIGEST, obsažené v předávaných požadavcích, obsahuje elektronický podpis všech ostatních polí požadavku. Tento podpis zajišťuje integritu a nepopiratelnost předávaného požadavku.

Požadavek musí splňovat následující podmínky:

- Požadavek se na API HTTP 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 č. 1: Podepisování zpráv)
- Požadavek se zasílá na URL adresu dle používaného prostředí:

1. Klientské testovací prostředí: https://test.3dsecure.gpwebpay.com/pgw/order.do
2. 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

V aplikaci portál GP webpay jsou ke stažení další zdroje pro integraci s platební bránou GP webpay s využitím API HTTP (např. příklady pro výpočet podpisu (PHP, Java, .NET)).

Platební brána GP webpay po přijetí požadavku vytvoří objekt nazývaný ORDER (viz kapitola 4. Stavy platby) a přesměruje prohlížeč zákazníka na platební stránku pro výběr platební metody.

3.2 Odpověď

Platební brána GP webpay po provedení platby zasílá obchodníkovi výsledek platby. Odpověď je zaslána prostřednictvím prohlížeče zákazníka s využitím redirectu (metoda GET), nebo pomocí automaticky odesílaného formuláře (metoda POST). Typ použité metody záleží na druhu požadovaných parametrů v odpovědi a podle poskytnutých služeb (DCC, splátkový prodej …). Systém obchodníka musí být schopen přijímat data odeslaná oběma metodami.

Formát odpovědí pro jednotlivé platební metody je popsán níže.

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

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

Při zahájení integrace si obchodník v portálu GP webpay stáhne veřejný klíč GPE, který mu slouží k ověření obsahu pole DIGEST.

Tímto způsobem se obchodník může přesvědčit, že:

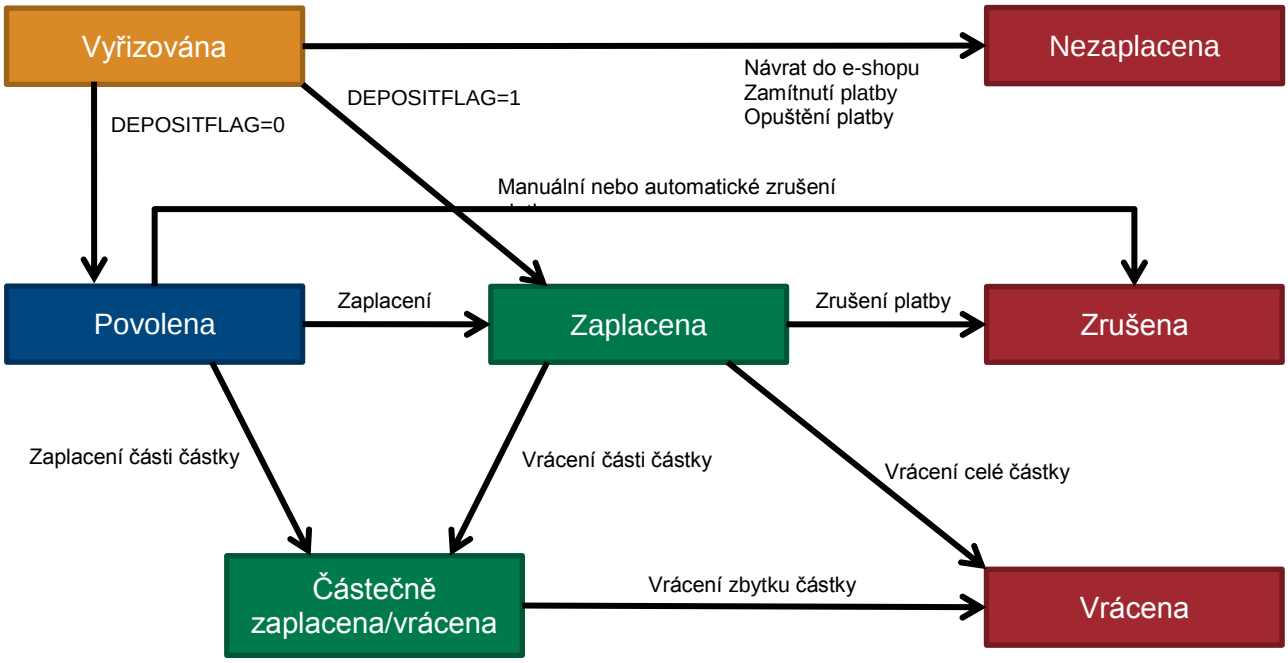
- odpověď pochází skutečně od GP webpay
- odpověď nebyla cestou změněna.

Důležité upozornění: při zpracování odpovědi je potřeba používat pouze parametry, které jsou zaslány zpět platební bránou GP webpay.

4. Stavy platby

Platební brána GP webpay po přijetí požadavku vytvoří objekt nazývaný ORDER. Možnosti další správy platby závisí na stavu, ve kterém se požadavek (ORDER) nachází, viz tabulka a stavový diagram:

Stav platby	Popis stavu platby
Zaplacena	Platba byla zaplacena. Platba bude připsána na účet e-shopu dle smlouvy s bankou pro akceptaci karet na internetu.
Nezaplacena	Platba nebyla zaplacena. Důvodem může být nedokončení platby zákazníkem na platební bráně GP webpay, návrat zákazníka z platební brány GP webpay do e-shopu, zamítnutí platby v systémech GPE, karetní asociace a vydavatelské banky, nebo technický problém.
Vrácena	Platba byla vrácena. Vrácení provedl e-shop prostřednictvím portálu GP webpay (nabídka Platby) nebo s využitím Web Services.
Částečně zaplacena/vrácena	Platba byla částečně zaplacena nebo částečně vrácena. Částečné zaplacení/vrácení provedl e-shop prostřednictvím portálu GP webpay (nabídka Platby) nebo s využitím Web Services.
Povolena	Platba byla povolena vydavatelskou bankou a zaplacená částka byla zablokována na účtu zákazníka. E-shop má možnost provést stržení částky z účtu zákazníka později prostřednictvím portálu GP webpay (nabídka Platby) nebo s využitím Web Services.
Vyřizována	Platba je vyřizována. E-shop vytvořil požadavek na zaplacení a zákazník má možnost zaplatit na platební bráně GP webpay. U standardních plateb je možné zaplatit do konce platnosti časového intervalu pro zaplacení, u PUSH plateb do konce platnosti platebního linku nebo vyčerpání pokusů pro zaplacení.
Zrušena	Platba byla zrušena. Zrušení provedl e-shop prostřednictvím portálu GP webpay (nabídka Platby) nebo s využitím Web Services, nebo platební brána GP webpay po skončení platnosti časového intervalu pro zablokování částky na účtu zákazníka vydavatelskou bankou.



5. Platba kartou

5.1 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 platby** **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
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 platba uhrazena automaticky. Povolené hodnoty: 0 = není požadována okamžitá úhrada 1 = je požadována úhrada
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne	**Číslo platby**. *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. Je použit redirect (metoda GET), nebo formulář (metoda POST). *(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 3D Secure 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

Parametr	Typ	Délka	Povinný	Poznámka
				„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 MPS – MasterPass GPAY – GooglePay
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 GPAY – GooglePay
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 GPAY – GooglePay
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)

Parametr	Typ	Délka	Povinný	Poznámka
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 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.

5.2 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

Parametr	Typ	Délka	Povinný	Poznámka
				(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.**
TOKEN **pole zahrnuto v digest**	znakový	64	ne	Jednoznačný identifikátor platební karty generovaný systémem GP webpay
EXPIRY **pole zahrnuto v digest**	znakový	4	ne	Expirace použité platební karty ve formátu YYMM
ACSRES **pole zahrnuto v digest**	znakový	1	ne	Výsledek autentikace držitele platební karty v systému 3D Možné hodnoty: N = nebyl proveden pokus o ověření – některé karetní asociace neumožňují provedení 3D ověření A = byl proveden pokus o ověření, ale karta není v systému zavedena nebo banka tento systém nevyužívá F = držitel se plně autentikoval – plné ověření D = držitel nebyl úspěšně ověřen – chybně zadané autentikační údaje E = technický problém s autentikací držitele
ACCODE **pole zahrnuto v digest**	znakový	6	ne	Autorizační kód platby přidělený autorizačním centrem
PANPATTERN **pole zahrnuto v digest**	znakový	19	ne	Maskované číslo platební karty použité při platbě ve formátu 6+4 Např. 405607******0016
DAYTOCAPTURE **pole zahrnuto v digest**	znakový	8	ne	Datum kdy lze nejpozději provést stržení požadované částky. Formát: DDMMYYYY.
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.*

6. Ověření karty

Verifikační proces platnosti karty. Nedochází k žádné blokaci finančních prostředků.

6.1 Formát požadavku

Parametr	Typ	Délka	Povinný	Poznámka

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 CARD_VERIFICATION**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	**Číslo platby** **Číslo musí být v každém požadavku od obchodníka unikátní.**
MERORDERNUM **pole zahrnuto v digest**	numerický	30	ne	**Číslo platby**. *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. Je použit redirect (metoda GET), nebo formulář (metoda POST). *(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 3D Secure 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.**
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

Parametr	Typ	Délka	Povinný	Poznámka
				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 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.

6.2 Formát odpovědi

Parametr	Typ	Délka	Povinný	Poznámka
OPERATION **pole zahrnuto v digest**	znakový	20	ano	**Hodnota CARD_VERIFICATION**
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*	Hash čísla platební karty. Hash je unikátní hodnota pro každou kartu a každého obchodníka – tj. pokud je platba provedena

Parametr	Typ	Délka	Povinný	Poznámka
			obchodník tuto funkcionalitu zapnutou	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.**
TOKEN **pole zahrnuto v digest**	znakový	64	ne	Jednoznačný identifikátor platební karty generovaný systémem GP webpay
EXPIRY **pole zahrnuto v digest**	znakový	4	ne	Expirace použité platební karty ve formátu YYMM
ACSRES **pole zahrnuto v digest**	znakový	1	ne	Výsledek autentikace držitele platební karty v systému 3D Možné hodnoty: N = nebyl proveden pokus o ověření – některé karetní asociace neumožňují provedení 3D ověření A = byl proveden pokus o ověření, ale karta není v systému zavedena nebo banka tento systém nevyužívá F = držitel se plně autentikoval – plné ověření D = držitel nebyl úspěšně ověřen – chybně zadané autentikační údaje E = technický problém s autentikací držitele
ACCODE **pole zahrnuto v digest**	znakový	6	ne	Autorizační kód platby přidělený autorizačním centrem
PANPATTERN **pole zahrnuto v digest**	znakový	19	ne	Maskované číslo platební karty použité při platbě ve formátu 6+4 Např. 405607******0016
DAYTOCAPTURE **pole zahrnuto v digest**	znakový	8	ne	Datum kdy lze nejpozději provést stržení požadované částky. Formát: DDMMYYYY.
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.*

7. Platba s využitím digitální peněženky

7.1 MasterPass

GP webpay API HTTP nabízí tyto možnosti:

- Vytvoření platby a zaslání nákupního košíku, který je zobrazen v peněžence
- Rozdělení platby do dvou kroků:
    1. Vytvoření platby a získání odpovědi, jakým typem karty bude zaplaceno
    2. Potvrzení platby s možností upravit částku

Pro odeslání košíku se používá parametr ADDINFO. V tomto parametru jsou uložena data ve formátu XML.

Parametry platby jsou stejné jako u standardní platby, je ale 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 platby. 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 platby.

Pro plné využití potenciálu, který MasterPass nabízí, může být služba MasterPass nabídnuta přímo na stránkách e-shopu prostřednictvím tlačítka „Nakupuj s MasterPass“. Možnosti integrace e-shopu s MasterPass popisuje technická specifikace pro vývojáře „GP webpay MasterPass Integracni manual“, který zasílá na vyžádání Aplikační podpora GPE.

7.1.1 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 FINALIZE_ORDER**
ORDERNUMBER **pole zahrnuto v digest**	numerický	15	ano	**Číslo platby – musí odpovídat číslu původní platby**
AMOUNT **pole zahrnuto v digest**	numerický	15	ano	Částka v nejmenších jednotkách dané měny 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. Je použit redirect (metoda GET), nebo formulář (metoda POST).

Parametr	Typ	Délka	Povinný	Poznámka
				(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.*

7.1.2 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 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

Parametr	Typ	Délka	Povinný	Poznámka
				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.*

8. Platba s využitím platebního tlačítka

8.1 PLATBA 24

PLATBA 24 může být nabídnuta přímo na stránkách e-shopu prostřednictvím tlačítka „PLATBA 24“. Pro integraci e-shopu pro tento případ použití se v požadavku použije parametr „PAYMETHOD“ s hodnotou „BTNCS“:

Parametr	Typ	Délka	Povinný	Poznámka
PAYMETHOD **pole zahrnuto v digest**	znakový	255	ne	Hodnota určující preferovanou platební metodu. Podporované hodnoty: CRD – platební karta MCM – MasterCard Mobile MPS – MasterPass **BTNCS – PLATBA 24 – platební tlačítko České spořitelny**

9. Funkce usnadňující platby

9.1 Opakovaná platba

9.1.1 Registrační platba

První tzv. registrační platba probíhá jako standardní platba 3D Secure a musí při ní dojít k ověření držitele platební karty a k zaplacení. Poté lze vytvořit opakovanou platbu.

Registrační platba se označuje přidáním parametru „USERPARAM1“ do požadavku:

Parametr	Typ	Délka	Povinný	Poznámka
USERPARAM1 **pole zahrnuto v digest**	znakový	255	ano/ne *povinné pro registraci „master“ platby, jinak nepovinné*	Uživatelské pole. Nyní použito pro předávání parametru „R“ – informace o požadavku registrace „master“ opakované platby.

Tento parametr je řazen za parametr MD.

Formát odpovědi je identický se standardním formátem.

9.1.2 Opakovaná platba

Opakovaná platba probíhá s využitím API WS (Web Services) bez přesměrování prohlížeče zákazníka na platební stránku pro zadání údajů o platební kartě (viz technická specifikace pro vývojáře „GP webpay API WS“).

9.2 Uložená karta (card on file [COF] platby)

9.2.1 Registrační platba

První tzv. registrační platba probíhá jako standardní platba 3D Secure a musí při ní dojít k ověření držitele platební karty a k zaplacení. Poté lze vytvořit další platby.

Registrační platba se označuje přidáním parametru „USERPARAM1“ do požadavku:

Parametr	Typ	Délka	Povinný	Poznámka
USERPARAM1 **pole zahrnuto v digest**	znakový	255	ano/ne *povinné pro uložení platebních dat pro COF platby, jinak nepovinné*	Uživatelské pole. Nyní použito pro předávání parametru „**T**“ – informace o požadavku na uložení platebních dat.

Tento parametr je řazen za parametr MD (viz seznam/pořadí parametrů).

Formát odpovědi je identický se standardním formátem + je vrácen TOKEN platební karty.

9.2.2 Platba pomocí uložených platebních údajů

Další platba probíhá s využitím API WS (Web Services) bez přesměrování prohlížeče zákazníka na platební stránku pro zadání údajů o platební kartě (viz technická specifikace pro vývojáře „GP webpay API WS“).

9.3 Fastpay

Funkce Fastpay umožňuje obchodníkovi zobrazit přihlášenému zákazníkovi na platební stránce poslední 4 číslice a platnost karty, kterou zákazník zaplatil předchozí platbu. Pro integraci e-shopu pro tento případ použití se v požadavku použije parametr „FASTPAYID“ s hodnotou „ORDERNUMBER“ z předchozí platby:

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

Pokud se patřičná platba nenajde, k zobrazení údajů nedojde.

Tento parametr je řazen za parametr MD.

Formát odpovědi je identický se standardním formátem.

9.4 Ověření správnosti platební karty

Systém GP webpay umožňuje ověření zadané platební karty vůči dodanému vzoru (pole PANPATTERN) nebo tokenu (pole TOKEN). Hodnota tokenu je vypočtena po prvním použití platební karty a je vrácena v návratovém parametru odpovědi. V kombinaci s parametrem VRCODE je možné ověřit provázanost držitele platební karty a bankovního účtu.

Současně je rozšířena sada výstupních parametrů.

9.4.1 Vstupní parametry

Parametr	Typ	Délka	Povinný	Poznámka
VRCODE **pole zahrnuto v digest**	znakový	48	ano/ne *pole povinné pro zaslání ověřovacího kódu prostřednictvím názvu obchodníka do AC*	Pole pro kontrolní kód zasílaný do autorizačního centra a propagovaný do internetového bankovnictví. Znakové pole o max. délce 22 **PŘED** zašifrováním. Šifrování probíhá pomocí AES algoritmu v CBC módu s „0000000000000000“ (16x byte 0) inicializačním vektorem a PKCS5 paddingem. Výsledek je převeden pomocí konverze bin dat do hex soustavy na text – tj. každý byte je reprezentován dvěma znaky v rozsahu 00-FF.

Parametr	Typ	Délka	Povinný	Poznámka
PANPATTERN **pole zahrnuto v digest**	znakový	255	ne	Pro účely ověření zadaného čísla platební karty (PAN) do formuláře na platební bráně, je možné zaslat až 10 různých „masek“ platebních karet. Hodnoty jsou odděleny čárkou „,“. Kontrola je prováděna při standardním zadání PAN na bráně, tak i při využití funkce Fastpay.

Parametr	Typ	Délka	Povinný	Poznámka
				Maska může obsahovat následující varianty hodnot: {6}*{4} – prvních 6 čísel z PAN, následováno **jedním znakem** „*“, poslední 4 čísla PAN. Délka PAN se nekontroluje. {6}******{4} – prvních 6 čísel z PAN, následováno **více znaky** „*“, poslední 4 čísla PAN. Délka PAN se kontroluje. {6}* – prvních 6 čísel z PAN, následováno **jedním znakem** „*“. Délka PAN se nekontroluje. *{4} – **jeden znak** „*“, poslední 4 čísla PAN. Délka PAN se nekontroluje.
TOKEN **pole zahrnuto v digest**	znakový	64	ne	Jednoznačný identifikátor platební karty generovaný systémem GP webpay.

Parametry jsou řazeny za pole ADDINFO.

Formát odpovědi je identický se standardním formátem.

9.4.2 Výstupní parametry

Parametr	Typ	Délka	Povinný	Poznámka
TOKEN **pole zahrnuto v digest**	znakový	64	ne	Jednoznačný identifikátor platební karty generovaný systémem GP webpay
EXPIRY **pole zahrnuto v digest**	znakový	4	ne	Expirace použité platební karty ve formátu YYMM
ACSRES **pole zahrnuto v digest**	znakový	1	ne	Výsledek autentikace držitele platební karty v systému 3D Možné hodnoty: N = nebyl proveden pokus o ověření – některé karetní asociace neumožňují provedení 3D ověření A = byl proveden pokus o ověření, ale karta není v systému zavedena nebo banka tento systém nevyužívá F = držitel se plně autentikoval – plné ověření D = držitel nebyl úspěšně ověřen – chybně zadané autentikační údaje E = technický problém s autentikací držitele
ACCODE **pole zahrnuto v digest**	znakový	6	ne	Autorizační kód platby přidělený autorizačním centrem
PANPATTERN **pole zahrnuto v digest**	znakový	20	ne	Maskované číslo použité platební karty ve formátu: 6{***}4
DAYTOCAPTURE **pole zahrnuto v digest**	znakový	8	ne	Datum, do kterého lze provést úhradu platby (pro objednávky založené s DEPOSITFLAG=0) Formát: DDMMYYYY

Parametry jsou řazeny za pole ADDINFO.

Formát odpovědi je identický se standardním formátem.

10. Přílohy a dodatky

10.1 Příloha č. 1 – Podepisování zpráv

10.1.1 Podepisování požadavku

GP webpay API HTTP přijme pouze ty požadavky, u kterých lze doložit, že původcem požadavku byl oprávněný subjekt, tedy obchodník, se kterým poskytovatel uzavřel smlouvu.

K prokázání původu požadavku slouží parametr DIGEST. Jeho obsah je vypočten na základě:

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

Při zahájení integrace obchodník vygeneruje s využitím portálu GP webpay soukromý klíč, který si obchodník bezpečně uloží a poskytne ho vývojáři pro integraci. Veřejný klíč obchodníka je během tohoto procesu automaticky uložen na server GP webpay a před přijetím požadavku od obchodníka se pomocí něj bude kontrolovat, zda obchodník podepsal požadavek svým soukromým klíčem.

Parametr DIGEST, obsažené v předávaných požadavcích, obsahuje elektronický podpis všech ostatních polí požadavku. Tento podpis zajišťuje integritu a nepopiratelnost předávaného požadavku.

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

- PRCODE=5 SRCODE=34 “Chybi povinne pole, DIGEST” nebo
- PRCODE =31 “Chybny podpis”.

Pro výpočet i ověření elektronického podpisu slouží jako datová zpráva řetězec sestavený jako součet (concatenation) textové interpretace hodnot všech parametrů (definovaných v API HTTP, ostatní parametry se ignorují) v zasílaném požadavku s výjimkou parametru DIGEST. Při sestavení vstupní zprávy je nutné dodržet stejné pořadí parametrů (viz tabulka v kapitole 3.1 Požadavek), jako v definici příkazu a oddělovat jednotlivé parametry 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 parametru DIGEST stane hodnota, která vznikne zřetězením obsahů parametrů v tomto pořadí:

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

V případě, že v požadavku není obsažen některý z nepovinných parametrů, parametr se přeskočí. Jestliže je zasílán parametr prázdný, 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

10.1.2 Ověření odpovědi

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

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

Při zahájení integrace si obchodník v portálu GP webpay stáhne veřejný klíč GPE, který mu slouží k ověření obsahu pole DIGEST.

Tímto způsobem se obchodník může přesvědčit, že:

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

Dále odpověď obsahuje také parametr DIGEST1, který dále zvyšuje bezpečnost odpovědi. Parametr DIGEST1 je tvořen stejně jako parametr 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 parametru DIGEST1 vypadá takto:

<řetězec pro parametr DIGEST> + | + MERCHANTNUMBER

10.1.3 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

10.1.4 Ověření elektronického podpisu

Vstupy:

- datová zpráva
- elektronický podpis (BASE64 kódovaný)
- veřejný RSA klíč

Výstupy:

- logická hodnota „ano“ – podpis je platný
- logická hodnota „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;

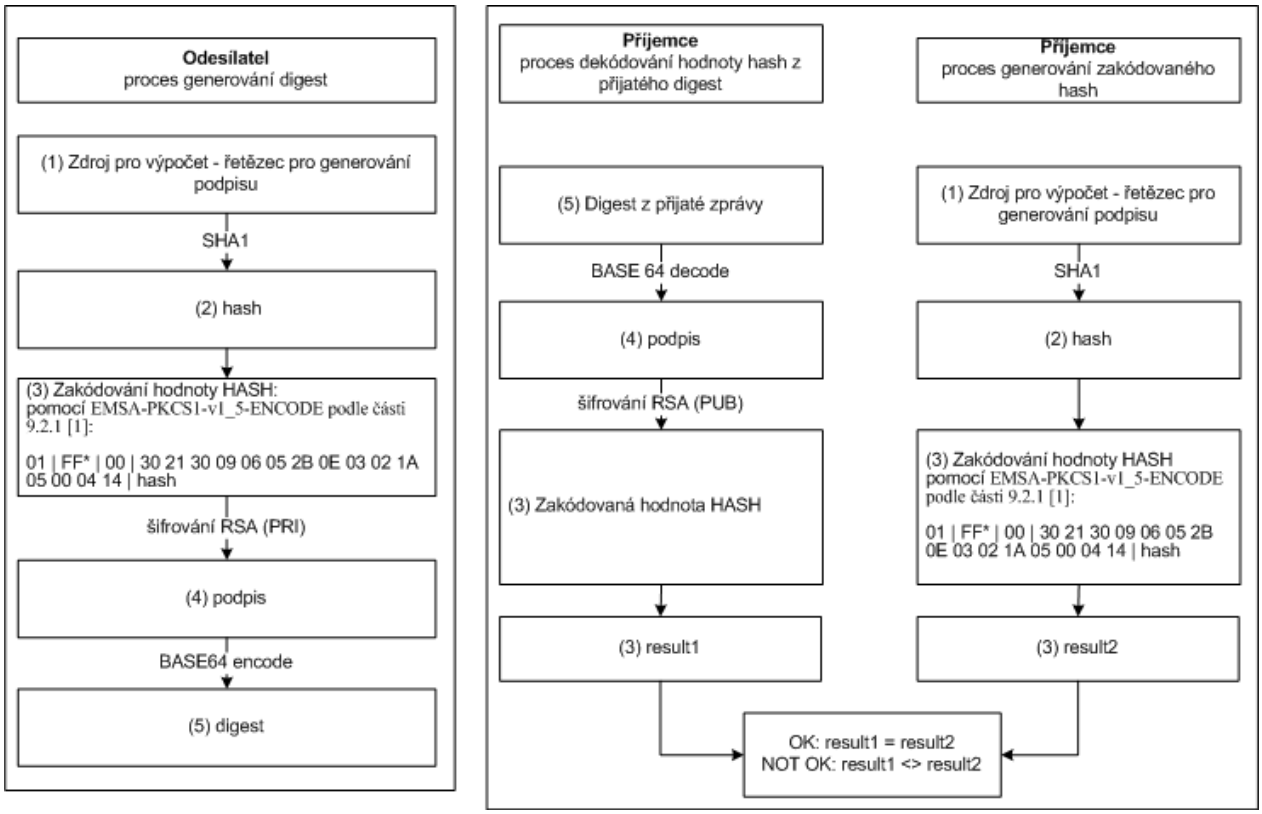
d) d) ze zprávy je vypočtena miniatura (hash) a zakódována v souladu s předchozí částí “Výpočet elektronického podpisu“ body a) b);

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).

10.1.5 Grafické znázornění generování a ověření



10.1.6 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

Funkce pro vytvoření soukromého klíče je součástí aplikace portál GP webpay. Lze použít i komerčně vydávané klíče, ale jejich platnost je omezena 1-2 roky (na rozdíl od klíče vytvořeného aplikací portál GP webpay, kde je platnost delší).

10.1.7 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.

10.1.8 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.

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

10.2 Příloha č. 2 – Seznam návratových kódů

Výsledek platby 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 byl parametr DEPOSITFLAG příliš dlouhý. RESULTTEXT, vrácený v tomto případě má hodnotu “Parametr příliš dlouhý, DEPOSITFLAG“.

10.2.1 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 platby	Duplicate order number
15	Objekt nenalezen	Object not found
17	Částka k zaplacení překročila povolenou (autorizovanou) částku	Amount to deposit exceeds approved amount
18	Součet vracených částek překročil zaplacenou částku	Total sum of credited amounts exceeded deposited amount
20	Objekt není ve stavu odpovídajícím této operaci *Info: Pokud v případě vytváření platby (CREATE_ORDER) obdrží obchodník tento návratový kód, vytvoření platby již proběhlo a platby 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 platby	Incorrect payment 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

10.2.2 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 platby.*	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**[1] *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).

[1] 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.

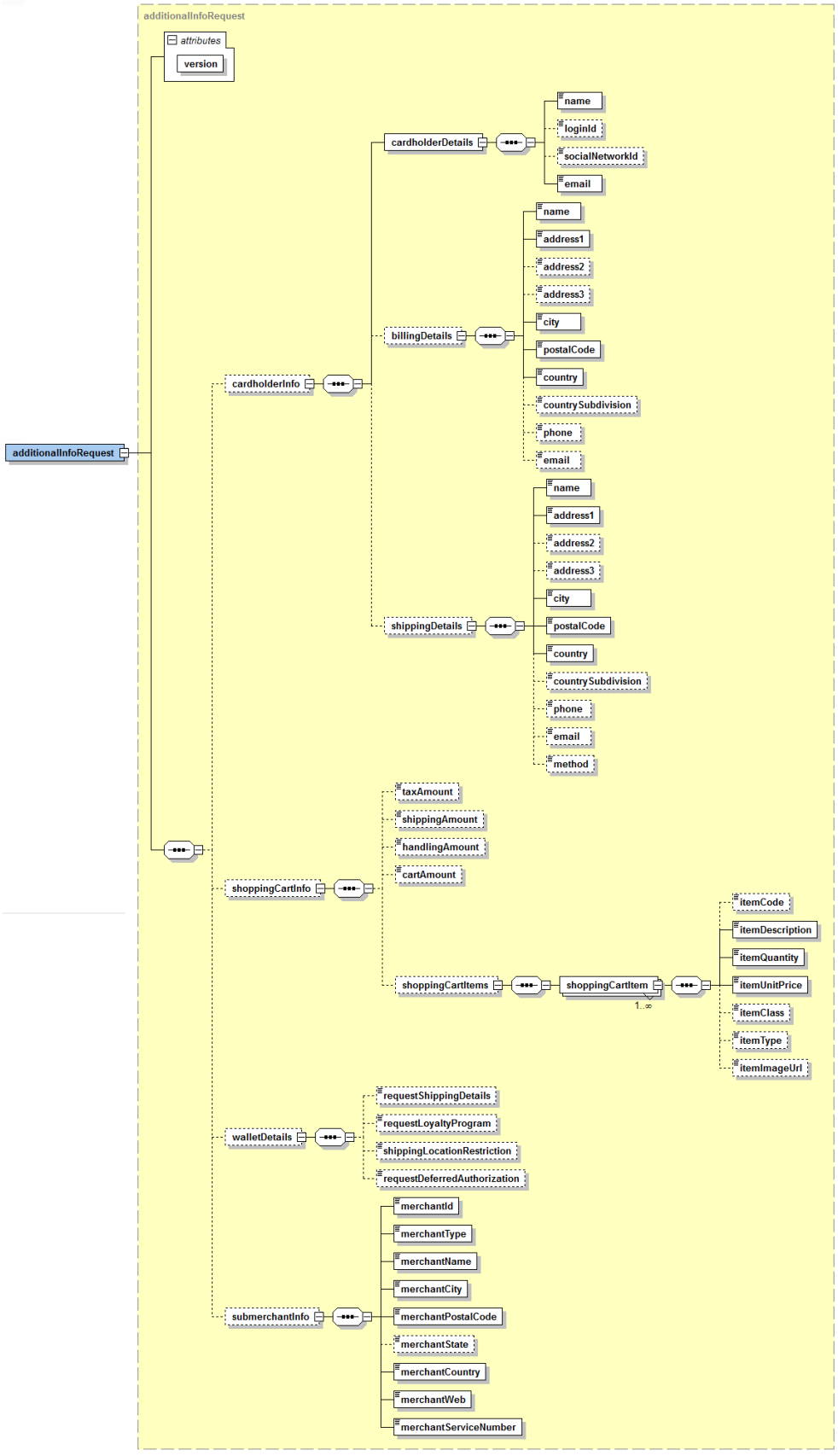
10.3Příloha č. 3 – formát polí ADDINFO

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

10.3.1 Vstupní parametr „ADDINFO“

10.3.1.1 Popis elementů



Název elementu	Popis	P/N[2]	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

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

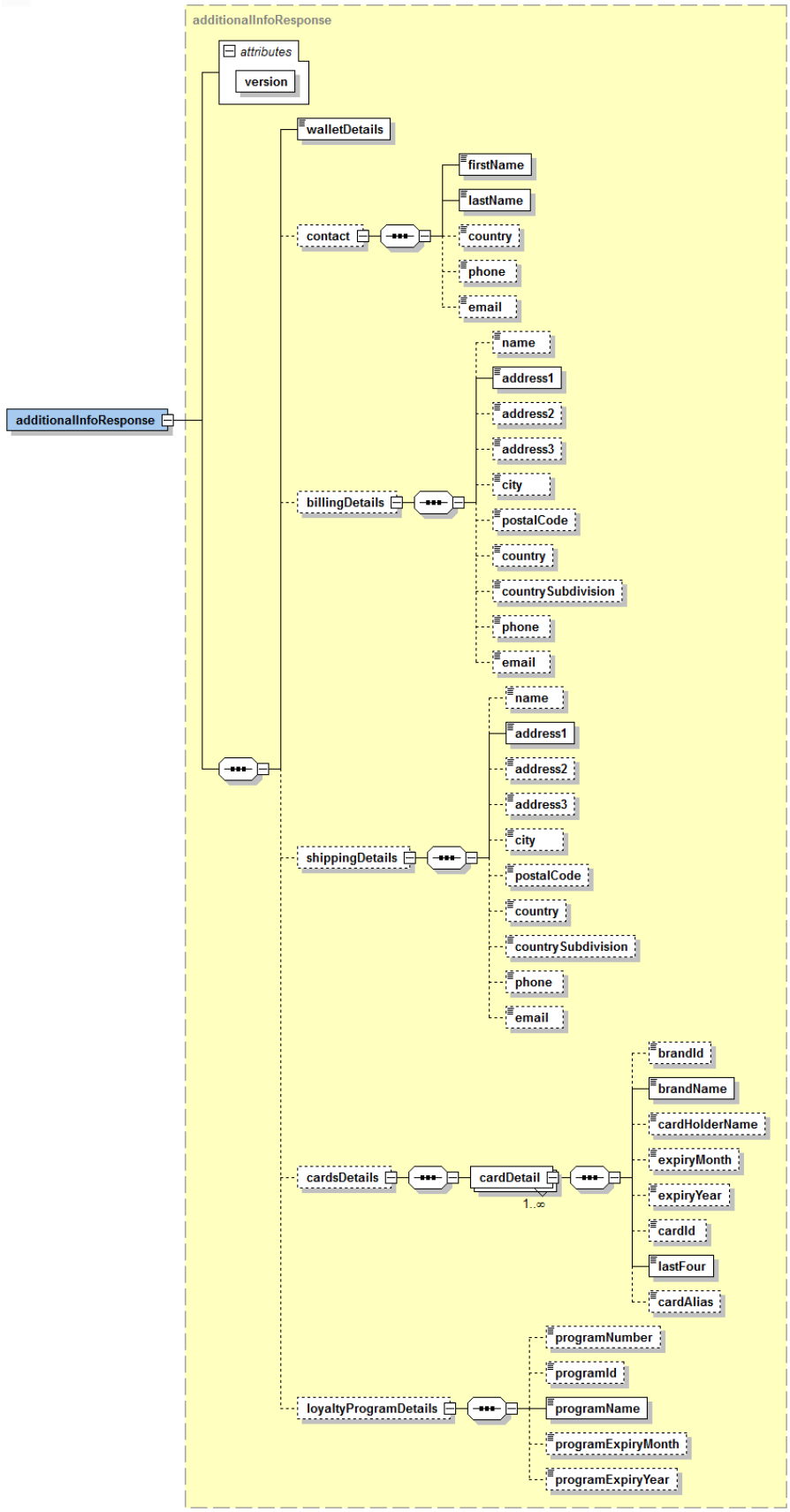
cartAmount	Čistá hodnota nákupního košíku bez DPH. Hodnota se vypočítá takto: `(shoppingCartItem1[itemQuantity] * shoppingCartItem1[itemUnitPrice]) + (shoppingCartItem2[itemQuantity] * shoppingCartItem2[itemUnitPrice]) + …`	N	Částka
shoppingCartItems	Jednotlivé položky nákupního košíku. Je možné uvést 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 platby 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

10.3.1.2 Schéma parametru

10.3.2 Návratový parametr „ADDINFO“

10.3.2.1 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

10.3.2.2 Schéma parametru

10.4Dodatek 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 nebezpečí, 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.

10.5Dodatek 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

10.6Dodatek 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	