E-Commerce

Manual de Integração

WebService – V.06.7

GETNET – UMA EMPRESA SANTANDER

VALIDADE: MARÇO/2024

COPYRIGHT

CONTROLE DE VERSÕES

Versão	Data	Descrição
1.0	03/2014	Criação do documento
1.0	05/2014	Revisão
1.1	05/2014	Ajuste da Numeração dos Itens
1.2	05/2014	- Revisão do texto nos itens: 3, 5, 5.1, 5.2, 5.3, 5.4, 5.5, 6, 8, 9, 10; - Inclusão dos itens: 7, 7.1, 7.2, 11 e 12.
1.3	09/2014	- Inclusão dos itens 'Regra para UDF (userDefinedField)' e do 'Regra de Preenchimento da Nova Senha'; - Ajuste da Numeração dos Itens; - Retirada a obrigatoriedade do envio do campo CVV2 para o serviço do PurchaseService e AuthorizationService; - Inclusão de novas mensagens de retorno por parte do Webservice;
1.4	11/2014	- Retirada da documentação os campos cardType e cardBrand, já não mais usado no serviço de AuthorizationService; - Inclusão dos itens 'Métodos e suas versões' e do 'Método CardVerificationService'; - Ajuste da Numeração dos Itens; - Ajuste no item 'Processo de Homologação'; - Ajuste nos códigos de Resposta do Emissor do Cartão ou do Sistema de Captura da GETNET.
1.5	03/2015	- Inclusão de novos campos no retorno das chamas para os Métodos PurchaseService/AuthorizationService/CaptureService/CancellationService/Query DataService. Novos campos: ref, amout, currencycode, instType, instNum, tranMCC, softDescriptor e os campos para o Parcelado Emissor (Referente a Carta Circular Nº 3593 - Parcelado MasterCard) que são instIssCet, instIssRate, instIssRqstv, instIssRqstp, instIssChrgv, instIssChrgp, instIssFeev, instIssFeep, instIssTaxv, instIssTaxp, instIssInsv, instIssInsp, instIssOthrv, instIssOthrp, instIssTotv e instIssTotp.
2.0	10/2015	- Nova marca Getnet.
2.1	04/2016	- Incluído no 'Método CardVerificationService' o novo campo Soft Descriptor; - Ajuste nos textos das mensagens de erro CWS.
2.2	05/2016	- Incluído o retorno "SF", que pode ocorrer na chamada dos serviços **CaptureService** / **CancellationService**.
2.3	08/2016	- Incluído os novos TranCategory e AddlReqData.
3.0	05/2017	- Atualização do layout do documento; - Atualização dos textos introdutórios; - Reorganização das sessões; - Revisão geral do texto.
3.1	07/2017	- Inclusão do campo responseMessage na mensagem de retorno da transação.
4.0	10/2017	- Reestruturação do documento para o FULL ADQ das novas Bandeiras ELO, AMEX, HIPER e HIPERCARD; - Inclusão de informações para transacionar com as novas Bandeiras; - Inclusão de indicador de Bandeiras suportadas para cada funcionalidade; - Inclusão de informações de como realizar as novas transações de Pré-Autorização, de acordo com novas regras de Bandeiras (pre-auth./incremental/final);

Versão	Data	Descrição
		- Inclusão de informações de como realizar transações utilizando as carteiras digitais (*e-wallets*) MasterPass e VisaCheckout.
5.0	07/2018	- Inclusão da Bandeira HIPERCARD; - Inclusão de informações de transações de Facilitadores de Pagamento (Gateways e Sub-Adquirentes); - Inclusão dos métodos relacionados a cada funcionalidade; - Inclusão da funcionalidade de Crédito Recorrente; - Exclusão da funcionalidade Crédito Parcelado Emissor BNDES.
5.1	01/2019	- Inclusão dos itens "2.2.14" e "3.4.6.4", descrevendo a nova funcionalidade do "CREDENTIALS ON FILE"; - Inclusão de observação do processo de autenticação, para a bandeira VISA; - Correção da formatação do POSTDATE. Formato DE DDMM PARA MMDD; - Melhoria na tabela de terminais no item "3.4.1 REGRA PARA TERMINALID"; - Inclusão do campo de retorno "result.authorizationDateTime"; - Inclusão da mensagem de retorno "RT".
5.2	07/2019	- Inclusão de informações sobre Recorrência; - Inclusão do retorno "Y" no item 3.5.3
5.3	02/2020	- Inclusão do retorno 63 no item 3.5.3
5.4	04/2020	- Inclusão do Terminal Debito não autenticado
6.0	05/2020	- Exclusão do 3DS 1.0 - Atualização para 3DS 2.01 - Inclusão dos campos – DIRECTORYSERVERTRANSACTIONID (tdsdsxid), SPECIFICATIONVERSION (tdsver) e recurringseqid
6.1	02/2021	- Inclusão de novos itens e regras; - Atualização de textos diversos; - Correção de regras; - Atualização dos códigos de retorno no padrão da ABECS;
6.2	05/2021	- Inclusão do retorno SF para transações de sucesso, para operação de Confirmação e Estorno; - Atualização no texto de Facilitadores, para garantir o envio dos campos; - Atualização no texto do Extrato, para garantir o envio correto das informações; - Inclusão do item de Atenção para fim de versões e migração para a versão estável;
6.3	07/2021	- Melhoria no tratamento da TAG F4042 do envio do Facilitador para CPF/CNPJ. - Dados do extrato, incluindo a formatação.
6.4	02/2022	- Inclusão das regras de SDWO (Staged Digital Wallet Operator) para carteiras digitais contemplando as bandeiras Visa, Mastercard e Elo. - Inclusão do Programa Visa CBPS (Consumer Bill Payment Service) - Inclusão das novas regras para Tokenização Visa e ELO
6.5	06/2022	- Inclusão da bandeira ELO na regra CREDENTIAL ON FILE, página 21: TID da transação original ou de verificação de cartão. Atenção: Este deve ser enviado para as bandeiras VISA e ELO.
6.6	11/2022	-Inclusão dos códigos complementares Mastercard (MAC - Merchant Advice Code); -Inclusão de códigos exclusivos bandeiras; -Ajuste na validade do TID para transações de COF; -Ajuste na informação sobre o valor de estorno;
6.7	03/2023	- Ajuste dos códigos complementares Mastercard (MAC – Merchant Advice Code);

Versão	Data	Descrição
		- Inclusão de novo retorno para determinar se a transação foi executada com um cartão Pré-Pago. - Nova Inclusão de códigos exclusivos bandeiras -Adicionado código T2 na tabela de retornos;

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

Bem-vindo à Getnet!

Este é o manual para que você possa integrar sua empresa à Plataforma de E-Commerce da Getnet e começar a usufruir das melhores soluções do mercado.

Para atendê-lo da melhor maneira, a Getnet oferece diferentes soluções seguras para captura de transações de E-Commerce. Estes serviços permitem aos estabelecimentos credenciados aceitar cartões de crédito e débito como forma de pagamento em suas lojas virtuais através da implementação de processos simples.

Sugerimos que este documento seja lido com atenção, e usado como guia de referência para quaisquer dúvidas não somente no momento da implementação da integração de sua plataforma de comércio eletrônico com a Rede de Adquirência da Getnet, mas para quaisquer mudanças nos sistemas.

Sugerimos também que, periodicamente e sempre que for iniciar um desenvolvimento relacionado à captura de transações, atualize previamente sua documentação utilizando os canais descritos na seção *1.2 – Contatos de Suporte*.

1.1 A QUEM SE DESTINA

O conteúdo deste Manual de Integração se destina a programadores e desenvolvedores de plataformas para comércio eletrônico que desejam realizar a captura e o processamento de suas transações diretamente com a Rede Adquirente da Getnet.

Neste documento o desenvolvedor/analista terá acesso a todos os passos e processos referentes à integração com o sistema de captura e autorização de transações financeiras da Getnet.

1.2 CONTATOS DE SUPORTE

Para suporte técnico durante o desenvolvimento, testes e homologação, a Getnet possui uma equipe treinada para atendê-los, disponível em horário comercial. Após a implantação da integração, o suporte ao ambiente de Produção está disponível 24 horas por dia, 7 dias por semana.

suporte.edigital@getnet.com.br

4020-4009

2 VISÃO GERAL

A seguir são apresentadas as soluções e modelos de E-Commerce e as funcionalidades e serviços disponíveis na Getnet.

Este manual cobre o modelo de E-Commerce WEB via WebService, utilizando protocolo HTTPS, tendo sua chamada através de WebServices em SOAP. Nele são apresentadas as informações técnicas para utilizar cada uma das funcionalidades disponíveis como serviços.

2.1 SOLUÇÕES DE E-COMMERCE NA GETNET

Para atender a todas as demandas de nossos clientes, criamos uma Plataforma de E-Commerce que conta com um conjunto de soluções diversificadas para cada necessidade. Essas soluções estão agrupadas em 3 modelos, de acordo com a forma de captura das transações. São eles:

- E-Commerce WEB via WebService
- E-Commerce WEB via Plug-In
- E-Commerce TEF

Este manual cobre o modelo de **E-Commerce WEB via WebService**, que realiza a conexão com a Getnet utilizando protocolo HTTPS tendo sua chamada através de WebServices em SOAP.

Atualmente (*Agosto de 2018*) nossa plataforma suporta transações das seguintes Bandeiras:

Figura 1 - Bandeiras Suportadas na Plataforma E-Commerce (Agosto de 2018)

2.2 FUNCIONALIDADES E SERVIÇOS SUPORTADOS

Cada uma das funcionalidades é descrita brevemente a seguir, e abordadas em profundidade em sessões específicas do documento que tratam das mesmas tecnicamente.

Como cada Bandeira conectada à Getnet tem um portfólio de funcionalidades e serviços diferente, recomendamos que, antes de se utilizar uma das funcionalidades ou serviços disponibilizados pela Getnet seja consultada a disponibilidade da mesma na bandeira específica que se deseja transacionar.

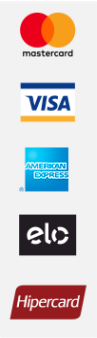
As funcionalidades e serviços suportados pelas Plataforma de E-Commerce da Getnet, de acordo com a disponibilidade em cada Bandeira, são:

Bandeira	Funcionalidades											
	Débito (Autenticado)	Crédito à Vista	Crédito Parcelado Lojista	Crédito Parc. Loj. De Cias. Aéreas	Crédito Parcelado Emissor	Crédito Parc. Emissor do BNDES	Recorrencia	Pré-Autorização	Verificação de Cartão	Autenticação do Portador	MCC Dinâmico	Soft Descriptor
mastercard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VISA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AMERICAN EXPRESS		✓	✓	✓	✓		✓	✓			✓	✓
elo	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Hipercard		✓	✓		✓		✓	✓	✓		✓	✓

Figura 2 – Funcionalidades da Plataforma E-Commerce por Bandeira (Abril 2020)

A seguir são apresentadas todas as funcionalidades e tipos de transações disponíveis. Para cada uma delas é mostrada uma lista das bandeiras suportadas pela Getnet, em cores as que suportam aquela transação ou funcionalidade, e em cinza aquelas que não a suportam.

Por exemplo:



Neste caso todas as Bandeiras suportam a funcionalidade.

Neste caso a funcionalidade é suportada pelas Bandeiras Mastercard, Visa e Elo, mas <u>não</u> é suportada pelas Bandeiras American Express e Hipercard.

2.2.1 Débito

Nesta modalidade, o pagamento é vinculado a uma conta bancária. O valor da transação é debitado da conta bancária associada no ato da compra, mediante disponibilidade de saldo.

De acordo com as regras das Bandeiras para o Brasil, **todas as transações de Débito no E-Commerce devem obrigatoriamente realizar a autenticação do Portador do cartão**, utilizando o protocolo 3D Secure (veja o documento Manual 3DS 2.1).

Para alguns Estabelecimentos específicos as Bandeiras e os Emissores podem abrir exceção para realização de transações de **Débito sem Autenticação**, caso entendam que o processo de autenticação de usuário do EC seja seguro o suficiente para o processo de Débito sem Autenticação. A Getnet está preparada para receber e processar essas transações.

Reforçamos que a aprovação dessas transações sem autenticação depende de acordo firmado pelo EC com as Bandeiras e os Emissores, em processo que não envolve diretamente a Getnet.

2.2.2 Crédito à Vista

Neste tipo de transação o Emissor do Cartão disponibiliza ao Portador um limite de gastos e um prazo para o pagamento da compra. No Brasil, em geral, o prazo para pagamento é de até 27 dias, dependendo das datas da compra e de vencimento do Cartão.

A confirmação (ou captura) da transação deve ser efetuada em até **7** dias. Após este período a transação é desfeita (cancelada) automaticamente pela Getnet. No momento da confirmação o valor pode ser menor (sem limitação) ou igual ao original.

Transações de Crédito também podem ser **autenticadas** utilizando o protocolo 3D Secure (veja o documento Manual 3DS 2.1).

2.2.3 Crédito Parcelado Lojista

Assim como na modalidade "À Vista", neste tipo de transação o Emissor do Cartão disponibiliza ao Portador um limite de gastos e um prazo para o pagamento da primeira parcela. No Brasil, em geral, o prazo para pagamento da primeira parcela é de até 27 dias, dependendo das datas da compra e de vencimento do Cartão.

Nesta modalidade, o parcelamento é ofertado pelo próprio estabelecimento, que divide o valor da compra em até 12 vezes, informando o número de parcelas na transação. O valor total é dividido de acordo com o número de parcelas e cobrado mensalmente do Portador até a quitação de todo o valor. Não são cobrados juros pelo parcelamento.

A confirmação (ou captura) da transação deve ser efetuada em até **7** dias. Após este período a transação é desfeita (cancelada) automaticamente pela Getnet. No momento da confirmação o valor pode ser menor (sem limitação) ou igual ao original.

Transações de Crédito Parcelado Lojista também podem ser **autenticadas** utilizando o protocolo 3D Secure (veja o documento Manual 3DS 2.1).

2.2.4 Crédito Parcelado Lojista de Cias. Aéreas

Esta modalidade é uma especialização do Crédito Parcelado Lojista, e destina-se apenas a Companhias Aéreas e Agências de Viagens que vendem passagens aéreas e ofertam parcelamento sem juros ao Portador.

Esta especialização atende à necessidade desses Estabelecimentos de cobrar a **Taxa de Embarque**, que deve ser repassada à INFRAERO (Empresa Brasileira de Infraestrutura Aeroportuária) e suas contrapartes em aeroportos internacionais, na primeira parcela juntamente com o parcelamento do valor da compra. Também permite que seja cobrado um valor diferenciado na primeira parcela a título de **Valor de Entrada** da transação.

A confirmação (ou captura) da transação deve ser efetuada em até **7** dias. Após este período a transação é desfeita (cancelada) automaticamente pela Getnet. No momento da confirmação o valor pode ser menor (sem limitação) ou igual ao original.

Transações de Crédito Parcelado Lojista de Cias. Aéreas também podem ser **autenticadas** utilizando o protocolo 3D Secure (veja o documento Manual 3DS 2.1).

2.2.5 Crédito Parcelado Emissor

Também como na modalidade “À Vista”, neste tipo de transação o Emissor do Cartão disponibiliza ao Portador um limite de gastos e um prazo para o pagamento da primeira parcela. No Brasil, em geral, o prazo para pagamento da primeira parcela é de até 27 dias, dependendo das datas da compra e de vencimento do Cartão.

Nesta modalidade, o parcelamento é ofertado pelo Emissor do Cartão, que cobra juros pelo financiamento em até 12 parcelas do valor da compra. O estabelecimento deve informar o número de parcelas na transação, e na resposta do Emissor são indicados tanto o valor de cada parcela como todos os encargos da operação. O valor total, acrescido de juros, é dividido de acordo com o número de parcelas e cobrado mensalmente do Portador até a quitação de todo o valor.

A confirmação (ou captura) da transação deve ser efetuada em até **7** dias. Após este período a transação é desfeita (cancelada) automaticamente pela Getnet. No momento da confirmação o valor pode ser menor (sem limitação) ou igual ao original.

Transações de Crédito Parcelado Emissor também podem ser **autenticadas** utilizando o protocolo 3D Secure (veja o documento Manual 3DS 2.1).

2.2.6 Crédito BNDES

Esta modalidade é uma especialização do Crédito Parcelado Emissor e destina-se apenas a Estabelecimentos que tenham convênio com o BNDES (Banco Nacional de Desenvolvimento) para vendas em seu site.

Esta especialização segue as especificações do BNDES, com particularidades como parcelamento em até 48 vezes, e juros subsidiados abaixo do praticado pelo mercado.

A confirmação (ou captura) da transação deve ser efetuada em até **15** dias. Após este período a transação é desfeita (cancelada) automaticamente pela Getnet.

Observação 1: *para utilização desta funcionalidade, o EC (Estabelecimento Comercial) deve estar cadastrado junto ao BNDES, com contrato com este órgão governamental, que é o responsável por enviar as transações para a Getnet em nome do EC.*

Observação 2: *esta funcionalidade está disponível apenas no modelo de conexão WebService. No modelo Plug-In / MPI não é possível realizar a conexão com o BNDES.*

2.2.7 Recorrência

A Recorrência é um serviço de cobrança periódica para estabelecimentos que precisam cobrar regularmente por seus produtos/serviços. É muito utilizado para assinaturas de revistas, mensalidades, licenças de software, entre outros.

No modulo do Webservice, não é feito a gestão de assinaturas (Recorrência), para este gerenciamento deve implementar ou contratar um Gateway que faz a gestão. Esse Gateway deve ser homologado na Getnet e enviará as transações através do Terminal iniciado em R.

O Terminal iniciado em R é o que nos informa que a transação é uma recorrência.

Observação 1: *Toda transação de recorrência, deve estar implementada com as regras do COF, conforme item COF - CREDENTIALS ON FILE: Transações onde o estabelecimento irá gravar as credenciais do Portador, uma transação para armazenamento de cartão do portador no Cofre do Lojista/Gateway deve ser usada.*

2.2.8 Pré-Autorização

Este tipo de transação é utilizado em situações em que a venda do produto ou serviço só será confirmada após algum tempo, porém é necessário reservar o montante junto ao limite do cartão do Portador. Exemplos de utilização são locação de automóvel e reserva de hotel, entre outros. São permitidas as modalidades de Crédito À Vista e Parcelado Lojista. Não é possível realizar uma Pré-Autorização Parcelada Emissor.

Nesta transação é solicitada ao Emissor a reserva do valor junto ao limite do cartão e caso seja aprovada, é fornecido um Código de Autorização da transação.

Para esta modalidade é possível solicitar o ajuste do valor original da transação, tanto a maior (Incremental) quanto a menor (Decremental), utilizando uma **Transação de Ajuste de Pré-Autorização**.

__Não__ é possível realizar transações de __Pré-Autorização__ com características de Cias. Aéreas (enviando o valor da taxa de embarque e/ou primeira parcela).

Ao utilizar uma Transação de Ajuste de Pré-Autorização, seja Incremental ou Decremental, apenas o valor será modificado, o prazo para confirmação seguirá a Transação de Pré-Autorização original, ou seja, será mantido inalterado.

*Transação de Ajuste de Pré-Autorização, seja **Incremental** ou **Decremental**, tem uma limitação da operação. Sendo hoje limitada a 4 operações.*

2.2.8.1 Ajuste de Pré-Autorização Incremental

Ao solicitar um ajuste de valor a maior, é feita uma nova autorização junto ao Emissor. Para tanto é calculada a diferença entre o último valor autorizado e o novo valor enviado, sendo solicitada a aprovação junto ao Emissor apenas da diferença entre os valores.

Por exemplo, a Pré-Autorização foi autorizada com o valor de R$ 1.000,00, e é enviado ajuste (Incremental) de R$ 1.100,00. Será enviado para autorização pelo Emissor o valor de R$ 100,00.

Reforçamos que a aprovação dessas transações está sujeita a todo o processo de Autorização. A transação pode, inclusive, ser negada, por exemplo, por saldo insuficiente ou qualquer outro motivo aferido pelo Emissor.

2.2.8.2 Ajuste de Pré-Autorização Decremental

Ao solicitar um ajuste de valor a menor, é feito o estorno junto ao Emissor da diferença entre a última autorização e o valor de ajuste desejado, sendo restabelecido este valor no saldo do Portador junto ao Emissor.

Seguindo o exemplo anterior, feito o ajuste (Incremental) para R$ 1.100,00, e enviado o ajuste (Decremental) de R$ 900,00. Será enviado o estorno de R$ 200,00 para o Emissor restabelecer o saldo do cliente.

2.2.8.3 Confirmação de Pré-Autorização

Para efetivar a Pré-Autorização, deve ser feita uma nova Transação de Confirmação de Pré-Autorização (Captura da Pré-Autorização), enviando obrigatoriamente o Código da Autorização recebido anteriormente na autorização. A Confirmação deve ser efetuada em até 30 (trinta) dias. Após este período a transação é desfeita automaticamente pela Getnet.

Os requisitos para realizar uma Confirmação de Pré-autorização são:

- Valor igual ou menor (sem limite);
- Pré-Autorização **À Vista** só pode ser confirmada no plano **À Vista**;
- Pré-Autorização no plano Parcelado Lojista só pode ser confirmada no plano Parcelado Lojista, porém é possível alterar o número de parcelas;

2.2.9 Verificação de Cartão

Neste tipo de transação é feita uma verificação se o cartão de crédito ou débito informado pelo portador é um cartão válido.

Este método é muito utilizado para diminuir o risco e o trabalho operacional de revisão de pedidos e solicitações de compras.

Para realizar a verificação, é enviada uma transação com valor zero, que é enviada à Bandeira e aos Emissores identificada como uma transação de verificação. Neste caso, a resposta dos Emissores é se o cartão está apto a realizar transações, sem nenhuma restrição, bloqueio ou suspeita de fraude.

2.2.10 Autenticação do Portador

Neste tipo de transação é usado o protocolo 3D Secure (*3 Domain Secure*) para autenticar o Portador do cartão, garantindo uma transação mais segura. Também, em transações autenticadas, ocorre o *liability shift*, que é a transferência da responsabilidade pelas disputas de *chargeback* do EC para o Emissor que realizou a autenticação.

Vale ressaltar que a Autenticação do Portador é uma etapa separada da Autorização da transação.

Oferecemos as duas versões do processo de autenticação, a versão do 3DS 1.0, que as implementações suportadas pela plataforma são as da Visa e da MasterCard, **Verified by Visa** e **Secure Code**, respectivamente. Esta versão é suportada até a versão do WS 2.0.

Também disponibilizamos a versão mais nova do processo de autenticação 3DS 2.0, com mais segurança e padronização pelas Bandeiras e Emissores. Com a funcionalidade de autenticação silenciosa, trazendo uma experiencia mais confortável para o portador, com toda a segurança do processo do 3DS 2.0. Para utilizar a versão, deve utilizar a versão 3.0 do WS.

O processo de Autenticação é apresentado em detalhes no *Anexo A – Autenticação do Portador*. Também nas sessões que tratam de transações que permitem Autenticação é sempre apresentada a maneira correta de realizá-la, com exemplos.

Observação: *para transações autenticadas VISA, solicitamos que sempre sejam enviados os campos referentes ao "Brazil Market Extensions" (brazilaccounttype, brazilmobilenumber e braziltransactiontype). Mesmo sendo opcionais, muitos dos emissores utilizam este campo para o processo de Autenticação.*

2.2.11 MCC Dinâmico

A funcionalidade de MCC Dinâmico permite que o EC utilize um MCC (*Merchant Category Code* – Código de Categoria do Estabelecimento) específico para cada transação, de acordo com o produto sendo vendido, ou no caso de Subadquirentes, de acordo com o EC da venda, identificando corretamente o ramo de atividade para a transação.

Como esta informação é utilizada para classificação (que influencia na taxa de aprovação) e cobrança da transação pelas Bandeiras, é de suma importância que ela seja exata. O MCC também é de suma importância para controles de Prevenção a Fraude e comportamento de compra.

Caso seja informado um MCC Dinâmico inválido, o mesmo será substituído pelo MCC que consta no Cadastro do EC para envio na autorização da transação.

2.2.12 Soft Descriptor

A funcionalidade de Soft Descriptor permite que o EC envie um texto alternativo de até 22 caracteres ao Nome Fantasia cadastrado na Getnet para demonstração da transação na fatura do Portador.

Como exemplo, pode-se ter o nome do Estabelecimento Comercial que está no cadastro da Adquirência mais o nome do intermediador que está recebendo o pagamento, ou a identificação do departamento da loja, sempre usando como delimitador o caractere asterisco (*).

Caso não seja informado um Soft Descriptor, será utilizado o Nome Fantasia do cadastro do EC.

	1				5					10					15					20		22
Exemplo 1	S	U	B	A	D	Q	U	I	R	E	N	T	E	*	L	O	J	A				
Exemplo 2	L	O	J	A	*	D	E	P	A	R	T	A	M	E	N	T	O					
Exemplo 3	L	O	J	A	*	S	U	B	L	O	J	A										
Exemplo 4	A	I	R	L	I	N	E	*	0	1	2	3	4	5	6	7	8	9	0			
Exemplo 5	A	I	R	L	I	N	E	*	Y	C	7	3	T	U								

As regras para utilização do Soft Descriptor são:

- Possuir no máximo 22 caracteres. **Caracteres além deste limite serão desprezados**.
- Utilizar apenas os seguintes caracteres:

  A-Z (todas as letras maiúsculas)
  0123456789
  caracteres especiais permitidos:
  % $, . / ( ) + = = - *

- **Não** utilizar os seguintes caracteres (a transação será **negada** se um desses caracteres for enviado no Soft Descriptor):

  a-z (todas as letras minúsculas)
  acentuações (qualquer caractere acentuado, maiúsculo ou minúsculo)
  ç (c cedilha)
  qualquer caracteres especiais, como estes:
  ! ? : ; [ ] { } ' " # _ @ § ^ ~ ¨ \ < > & ¹ ² ³ ª º £ ¢ ¬

Observação 1: *Diferente de outras Adquirentes, na Getnet não há cadastro prévio de nome do EC a ser utilizado no Soft Descriptor. O texto enviado pelo EC é* ***exatamente*** *o texto que será apresentado na fatura do Portador (limitado a 22 caracteres).*

Observação 2: *Caso seja informado um Soft Descriptor inválido, o mesmo será substituído pelo Nome Fantasia que consta no Cadastro do EC para envio na autorização da transação.*

2.2.13 Carteiras Digitais

A Getnet disponibiliza integração às principais Carteiras Digitais (*e-wallets*) do mercado de transações digitais. A seguir são apresentadas as carteiras disponíveis e indicadas as especificidades de cada uma a serem observadas no envio das transações que as envolvam.

2.2.13.1 MasterPass

MasterPass é uma solução de pagamento gratuita da MasterCard que permite fazer compras on-line com um único cadastro. Através de uma única conta, o portador registra seus dados de entrega e pagamento em um único ambiente digital seguro e não precisa preencher todos os seus dados a cada nova compra online. Basta criar uma conta e registrar seus cartões de crédito, débito e pré-pagos de diversas bandeiras.

Além de funcionar como uma carteira digital, o MasterPass também permite a integração de outras carteiras digitais, funcionando como um agregador, no qual o portador pode escolher qual carteira e cartão irá utilizar.

Para aceitação do MasterPass é preciso que o EC faça uma integração com a bandeira MasterCard para receber as informações do portador. Esta integração é feita diretamente, e não tem envolvimento da Getnet. Após este desenvolvimento, o EC oferece o botão do MasterPass como uma nova forma de pagamento, e ao ser utilizado, envia os dados específicos indicando a utilização do mesmo na transação para a Getnet.

Os dados devem ser informados na tag Wallet:

- type=01 (Domínio interno da Getnet para identificar a carteira)
- id=101,102, etc. (Domínio de acordo com a carteira escolhida, retornado pelo MasterPass)

Exemplo:

```
<wallet>
   <!--Optional:-->
   <type>01</type>
   <!--Optional:-->
   <id>102</id>
</wallet>
```

2.2.13.2 Visa Checkout

Visa Checkout é uma solução de pagamento gratuita da Visa que permite fazer compras on-line com um único cadastro. Através de uma única conta, o portador registra seus dados de entrega e pagamento em um único ambiente digital seguro e não precisa preencher todos os seus dados a cada nova compra online. Basta criar uma conta e registrar seus cartões de crédito e débito Visa, MasterCard, American Express ou Discover.

Para aceitação do Visa Checkout é preciso que o EC faça uma integração com a bandeira Visa para receber as informações do portador. Esta integração é feita diretamente, e não tem envolvimento da Getnet. Após este desenvolvimento, o EC oferece o botão do Visa Checkout como uma nova forma de pagamento, e ao ser utilizado, envia os dados específicos indicando a utilização do mesmo na transação para a Getnet.

Os dados devem ser informados no tag:

- type=02 (Domínio interno da Getnet para identificar a carteira)
- id=VCIND (Domínio de acordo com retorno do Visa Checkout, atualmente apenas VCIND)

Exemplo:

```
<wallet>
   <!--Optional:-->
   <type>02</type>
   <!--Optional:-->
   <id>VCIND</id>
</wallet>
```

2.2.14 Transações de Facilitadores de Pagamento

Um **Facilitador de Pagamento** é uma entidade que fornece soluções de pagamento para clientes finais (subcomércios), que podem ser estabelecimentos comerciais, prestadores de serviços, autônomos, etc., comercializarem seus produtos e/ou serviços, capturando, processando e liquidando diretamente aos subcomércios, tornando-se um credor do Adquirente.

De maneira geral, as Bandeiras e/ou Arranjos do mercado solicitam às Adquirentes o envio das informações dos subcomércios recebedores contratantes dos serviços dos Facilitadores de Pagamento (estabelecimentos comerciais, prestadores de serviços, autônomos, etc.).

No mercado atual podemos identificar dois tipos de Facilitadores de Pagamento:

- **Subadquirente**: é uma entidade jurídica que intermedia as transações de pagamento em nome dos subcomércios (lojas físicas ou e-commerce) e realiza a liquidação dos recebíveis destes em suas respectivas contas bancárias.
- **Marketplace**: é um site ou plataforma que vende produtos ou serviços, próprios e de terceiros (subcomércios), que intermedia as transações de pagamento e realiza a liquidação dos recebíveis destes em suas respectivas contas bancárias.

Figura 3 – Esquematização do modelo de operação de Facilitadores de Pagamento com a Getnet

Importante: Para que a Getnet possa cumprir com as regras das Bandeiras e Arranjos, as Leis Federais e determinações do BACEN (Banco Central do Brasil) para **identificação das entidades finais (subcomércios)** que fazem as transações financeiras, os **Facilitadores de Pagamento** devem enviar os dados de identificação de seus clientes **a cada transação** enviada à Getnet.

Os Facilitadores de Pagamento (Subadquirentes e Marketplaces) devem fornecer à Getnet as seguintes informações de seus clientes (subcomércios) em cada transação:

- ID DO SUBCOMERCIO
- CNPJ ou CPF
- LOGRADOURO
- CIDADE
- ESTADO
- CÓDIGO POSTAL (CEP)
- MCC (Enviado no campo do MCC DINÂMICO)
- SOFT DESCRIPTOR

*O papel do **Facilitador é enviar todos os dados do subcomercio para a Getnet**, a falta de campos e valores ou formatação incorreta, **pode acarretar transação negada ou penalidade pela Bandeira**.*

*Além desses campos, o Facilitador deve entrar em contato com a Getnet para a **atualização cadastral da identificação do Facilitador de Pagamento junto à Bandeira** (ID do Facilitador). Mesmo enviando todos os campos, se o cadastro não for atualizado as transações serão enviadas sem a característica de Facilitador de Pagamento.*

Os dados de MCC Dinâmico e Soft Descriptor devem ser informados de acordo com as regras específicas de envio relatadas nas seções *2.2.11 - MCC Dinâmico* e *2.2.12 Soft Descriptor*. Ainda para o Soft Descriptor, para o caso específico de Facilitadores de Pagamento, deve-se seguir as seguintes regras adicionais das Bandeiras:

- Identificação do Facilitador de Pagamentos, com 3, 7 ou 12 caracteres;
- Caractere de separação "*" (asterisco);
- Identificação do subcomercio;

Exemplo:

	1				5					10					15					20		22
Exemplo 1	F	A	C	*	S	U	B	C	O	M	E	R	C	I	O							

	1				5					10					15					20		22
Exemplo 2	F	A	C	I	L	I	T	*	S	U	B	C	O	M	E	R	C	I	O			

	1				5					10					15					20		22
Exemplo 3	F	A	C	I	L	I	T	A	D	O	R	1	*	S	U	B	C	O	M	E	R	C

Não seguir as regras de preenchimento do Soft Descriptor é de total responsabilidade do Facilitador de Pagamento. A falta de preenchimento do campo e / ou formatação incorreta, ***pode acarretar transação negada ou penalidade pela Bandeira.***

Os demais dados devem ser informados no campo addlReqData, com o seguinte domínio:

TAG	TIPO	TAMANHO	DESCRIÇÃO
F4538	AN	15	ID do Subcomércio Deve ser formatado à esquerda e complementado com ' ' (espaços) à direita, caso o ID do subcomércio seja menor que o tamanho. Ex.: 'F4538=AB123456 ;' 'F4538=1234567890 ;' Exemplo de pattern: ^[A-Z0-9\s]{15}$
F4539	A	13	Cidade do Subcomércio Se comprimento for maior, será desprezado (Truncado) o excedente. Caso menor, poderá ser complementado com ' ' (espaço) a direita. Não são aceitos caracteres especiais, incluindo letra com acento. Exemplo de pattern: ^[A-Z0-9\s]{13}$
F4540	A	2	Estado do Subcomércio Sigla do Estado conforme padrão Exemplo de pattern: ^[A-Z]{2}$
F4541	N	8	Código Postal (CEP) do Subcomércio Somente números, sem hífen. Exemplo de pattern: ^[0-9]{8}$
F4542	AN	15	CNPJ ou CPF do Subcomércio Deve ser enviado com o tipo do documento, J = Pessoa Jurídica (CNPJ) ou F = Pessoa Física (CPF). Somente números, sem pontos e/ou hífen. Exemplo de pattern: ^([JF]{1}[0-9]{14})$

F4543	A	40	Logradouro do Subcomércio Se comprimento for maior, será desprezado o excedente. Caso seja menor, poderá ser complementado com ' ' (espaços) à direita. Não são aceitos caracteres especiais, incluindo letra com acento. Exemplo de pattern: ^[A-Z0-9\s]{40}$

Todos os domínios devem ser finalizados com o caractere ";" (ponto-e-vírgula).

Deve ser observado a regra de preenchimento de cada domínio a ser enviado. Considerando a regra de preenchimento (Pattern). Seguindo os tipos e caracteres aceitos para cada domínio.

- *Utilizar **apenas** os seguintes caracteres:*

  A-Z (todas as letras maiúsculas)
  0123456789
  caracteres especiais permitidos:
  *% $, . / ( ) + = = - **

- ***Não** utilizar os seguintes caracteres:*

  a-z (todas as letras minúsculas)
  acentuações (qualquer caractere acentuado, maiúsculo ou minúsculo)
  ç (c cedilha)
  qualquer caracteres especiais, como estes:
  ! ? : ; [ ] { } ' " # _ @ § ^ ~ ¨ \ < > & ¹ ² ³ ª º £ ¢ ¬

Exemplos:

```
// se o subcomércio é Pessoa Jurídica (empresa)
<addlReqData>F4538=0012346        ;F4539=CIDADE;F4540=SP;F4541=12345678;
F4542=J12345678901234;F4543=LOGRADOURO;</addlReqData>

// se o subcomércio é Pessoa Física
<addlReqData>F4538=0012346        ;F4539=CIDADE;F4540=SP;F4541=12345678;
F4542=F12345678901;F4543=LOGRADOURO;</addlReqData>
```

2.2.15 SDWO - Staged Digital Wallet Operator

O modelo de **SDWO** (Staged Digital Wallet Operator) se trata de carteiras digitais (Wallets) que credenciam estabelecimentos para aceite de seu meio de pagamento, similar ao modelo de Facilitadores de Pagamento.

Se tratando da liquidação, os valores provenientes de pagamentos através das Wallets são enviados para o EC Wallet e, em segundo momento, ela realiza o repasse aos seus subcomercios finais. Hoje o modelo está estruturado para Visa, Mastercard e Elo.

Necessário separar o modelo de wallets SDWO de Pass-Through Digital Wallets. Onde neste caso, a carteira só tem o papel de ser um substituto do cartão físico, não participando da transação. Portanto as transações de QR Code gerados nos POS's Getnet ou de Carteiras por NFC (Samsung Pay, Google Pay e Apple Pay) não são aderentes ao modelo de SDWO e sim de Pass-Trough Digital Wallets. Todas as bandeiras solicitam certificação PCI-DSS para aceite das Wallets em seus arranjos.

As SDWO's podem estar no meio físico (QR Code proprietário) ou no meio digital (Checkout Integrado / Direcionamento para ambiente do App).

As transações de uma Carteira Digital Escalonada (SDWO) possuem basicamente dois Modelos:

- **Cash-In: transação bandeirada não vinculada a uma compra:**
  - Abastecimento de Fundos na Carteira utilizando Cartão. Ex.: recarga de saldo na carteira através de cartão
  - Transferência para saldo de outra pessoa utilizando cartão
- **Compra (também conhecida como back-to-back):**
  - Pagamento de QR Code impresso / proprietário da carteira utilizando cartão. Ex.: QR Code da carteira digital impresso no balcão e pago através de cartão
  - Pagamento online através de área logada da carteira utilizando cartão

Importante: Para que a Getnet possa cumprir com as regras das bandeiras, arranjos e as determinações do BACEN (Banco Central do Brasil) para identificação de transações de SDWO, **faz-se necessário aos clientes da Genet que se enquadram como carteiras digitais o envio de alguns campos, de acordo com a respectiva bandeira e caso de uso SDWO, como descrito abaixo:**

Visa Cash-in

- Tipo de Financiamento = FT (Funding Transfer)
- Identificação da carteira: [1]MVV (Merchant Value Verification) = 6 posições (referente ao número de registro da carteira digital junto a Visa)
- CPF/CNPJ do destinatário da transferência
- [2]MCC 6051
- [3]Soft Descriptor com o nome da respectiva carteira digital

Visa Back-to-back

- Tipo de Financiamento = FP (Funding and Purchase)
- Identificação da carteira: [1]MVV (Merchant Value Verification) = 6 posições (referente ao número de registro da carteira digital junto a Visa)
- [4] Dados do subcomercio da carteira digital
- [2]MCC Dinâmico
- [3]Soft Descriptor

Mastercard Cash-in

- Tipo de Financiamento = FT (Funding Transfer)
- Identificação da carteira: [1]WID (Wallet ID) = 3 posições referente ao número de registro da carteira digital junto a Mastercard)
- CPF/CNPJ do destinatário da transferência
- Nome do destinatário da transação
- Sobrenome do destinatário da transação
- País do destinatário da transação
- Account Type = 00
- Account Number = "#NA" ou "9999999999999995"
- [2] MCC 6051
- [3]Soft Descriptor com o nome da respectiva carteira digital

Mastercard Back-to-back

- Tipo de Financiamento = FP (Funding and Purchase)
- Identificação da carteira: [1]WID (Wallet ID) = 3 posições referente ao número de registro da carteira digital junto a Mastercard)
- [4] Dados do subcomercio da carteira digital
- [2]MCC Dinâmico
- [3]Soft Descriptor

Elo Cash-in

- Tipo de Financiamento = FT (Funding Transfer)
- Identificação da carteira: [1]WID (Wallet ID) = 11 posições referente ao número de registro da carteira digital junto a Elo)
- [2]MCC 6540
- [3]Soft Descriptor com o nome da respectiva carteira digital

Elo Back-to-back

- Tipo de Financiamento = FP (Funding and Purchase)
- Identificação da carteira: [1]WID (Wallet ID) = 11 posições referente ao número de registro da carteira digital junto a Elo)
  [4] Dados do subcomercio da carteira digital
- [2]MCC Dinâmico
- [3]Soft Descriptor

Importante: Os dados de [2]MCC Dinâmico e [3]Soft Descriptor devem ser informados de acordo com as regras específicas de envio relatadas nas seções *2.2.11 - MCC Dinâmico*, *2.2.12 Soft Descriptor*. Ainda para o Soft Descriptor e [4]Dados do Subcomercio, para o caso em particular de SDWO Back-to-back, deve seguir as mesmas regras dos Facilitadores de Pagamento descritas na seção *2.2.14 – Facilitadores de Pagamentos* deste manual, sendo a "identificação do Facilitador de Pagamentos" no campo do soft descriptor, o nome da respectiva carteira digital.

[1]Além do envio desses campos, as carteiras digitais que operam com as bandeiras Visa, Mastercard e Elo, devem entrar em contato com as bandeiras para ***realizar seu devido cadastro e gerar seu número de identificação (MVV para a Visa e Wallet ID para***

***Mastercard e Elo)**, como também, realizar o envio dessa informação no campo solicitado.*

O papel das carteiras digitais que se enquadram no arranjo SDWO é enviar todos os dados solicitados para a Getnet, a falta de campos e valores ou formatação incorreta, pode acarretar transação negada ou penalidade pelas Bandeiras.

NOTA: Essa é a primeira versão da regra do arranjo SDWO (Staged Digital Wallet Operator), dessa forma as especificações desse item podem sofrer alterações recorrentes. Em caso de dúvidas sobre a implementação contate: suporte.edigital@getnet.com.br

Os demais dados devem ser informados nos campos wallet.id, wallet.type, wallet.merchantId e wallet.fundTransfer com seus subdomínios descritos nas seções *3.2.1 – Método PurchaseService* e *3.2.2 – Método AuthorizationService*.

Exemplo:

```
<wallet>
        <!--Optional:-->
        <type>55</type>
        <!--Optional:-->
        <id>BRL</id>
        <!--Optional:-->
        <merchantId>12300000000</merchantId>
        <!--Optional:-->
        <fundTransfer>
                <!--Optional:-->
                <payAction>FT</payAction>
                <!--Optional:-->
                <receiver>
                        <!--Optional:-->
                        <accountNumber>9999999999999995</accountNumber>
                        <!--Optional:-->
                        <accountType>00</accountType>
                        <!--Optional:-->
                        <firstName>Pedro</firstName>
                        <!--Optional:-->
                        <middleName>I</middleName>
                        <!--Optional:-->
                        <lastName>do Brasil</lastName>
                        <!--Optional:-->
                        <addrStreet>Rua Juscelino</addrStreet>
                        <!--Optional:-->
                        <addrCity>SAO PAULO</addrCity>
                        <!--Optional:-->
                        <addrState>SP</addrState>
                        <!--Optional:-->
                        <addrCountry>BRA</addrCountry>
                        <!--Optional:-->
                        <addrPostalCode>01408000</addrPostalCode>
                        <!--Optional:-->
                        <nationality>BRA</nationality>
                        <!--Optional:-->
                        <phone>5511977778888</phone>
                        <!--Optional: Format YYYYMMDD -->
                        <dateOfBirth>20221231</dateOfBirth>
```

```
                            <!--Optional:-->
                            <idType>03</idType>
                            <!--Optional:-->
                            <idNum>12345678900000</idNum>
                        </receiver>
                    </fundTransfer>
            </wallet>
```

2.2.16 Programa Visa CBPS - Consumer Bill Payment Service

O Serviço de Pagamento de Contas para Consumidores **CBPS** (Consumer Bill Payment Service), é um serviço opcional para empresas terceiras especializadas em pagamento de contas para consumidores. O CBPS fornece mais visibilidade e precisão nas transações de terceiros que oferecem serviços consolidados de pagamento de contas aos portadores de cartão.

Os usuários típicos do CBPS são empresas que possuem aplicativos ou sites de comércio eletrônico onde os portadores de cartão podem gerenciar e pagar suas contas. Após o pagamento, a empresa fornecedora do aplicativo ou site realiza os pagamentos das contas cadastradas, em nome dos portadores de cartão, por meio de uma câmara de compensação automática (ACH) ou outros métodos de pagamento.

As entidades do Serviço de Pagamento de Contas para Consumidores (CBPS) diferem de outros terceiros (como facilitadores de pagamento e agentes), pois não têm acordos ou contratos com cobradores subjacentes. Os facilitadores de pagamentos precisam ter acordos com os cobradores para que possam oferecer aceitação direta, e os agentes têm acordos com os cobradores para que possam cobrar os pagamentos em nome desse cobrador;

Principais vantagens do CBPS:

- Permitir que os provedores classifiquem suas transações pelos códigos de categoria de comerciante (MCC) das empresas emissoras das contas;
- Fee de Intercâmbio incentivado;
- Isentar os provedores da exigência de que um terceiro precise ter um contrato com das empresas emissoras das contas;

*Para participar do CBPS primeiramente é necessário entrar em contato com a Getnet para realizar o devido cadastro do estabelecimento junto Visa no programa. Após a conclusão do cadastro e aprovação é necessário realizar os envios dos campos abaixo:

- MCC Dinâmico: com o MCC que melhor descreve o emissor da conta que está sendo paga
- Marcação BP: sigla para Bill Pay (pagamento de conta)

***Abaixo a lista de MCCs elegíveis para a classificação no programa CBPS no Brasil:**

- 4814 (Serviços de Telecomunicação)
- 4899 (TV à cabo, Satélite e outros Serviços de Televisão/Rádio)
- 4900 (Serviços Públicos – Eletricidade, Gás, Água, Esgoto)
- 6300 (Vendas de Seguros, Subscrição e Prêmios)
- 6513 (Agentes e Gerentes de Imóveis – Aluguéis)
- 8211 (Escolas de 1º e 2º Graus)
- 8220 (Faculdades, Universidades, Escolas Profissionais e Faculdades de Curta Duração)

- 8241 (Escolas por Correspondência)
- 8244 (Escolas de Negócios e Secretariado)
- 8249 (Ensino Profissionalizante/Formação Profissional)
- 8299 (Serviços Escolares e Educacionais [Não Classificados em Nenhum Outro Lugar])
- 9311 (Pagamento de Impostos)

Importante: Os dados de MCC Dinâmico deve ser informado de acordo com as regras específicas de envio relatadas nas seções *2.2.11 - MCC Dinâmico* deste manual.

**Para o estabelecimento poder fazer parte do programa CBPS, é necessário entrar em contato com a Getnet para realização do devido cadastro junto a bandeira Visa. Caso o cadastro não seja realizado, apenas o envio dos campos não caracteriza a elegibilidade nem a participação no programa.*

**Os MCCs válidos aqui descritos são até a data da última atualização deste manual e podem ocorrer atualizações. Em caso de dúvidas contate: suporte.edigital@getnet.com.br*

Os demais dados devem ser informados no campo addlReqData com o domínio abaixo exemplificado, que só está disponível nos métodos *3.2.1 – Método PurchaseService* e *3.2.2 – Método AuthorizationService*.

TAG	TIPO	TAM	DESCRIÇÃO
payAction	A	2	BP - Bill Pay (Pagamento de Conta)

Exemplo:

```
<fundTransfer>
        // marcação de pagamento de conta no programa Visa CBPS
        <payAction>BP</payAction>
</fundTransfer>
```

2.2.17COF - CREDENTIALS ON FILE

Requisito mandatório das Bandeiras para enviar mais informações na autorização, quando o portador do cartão quiser armazenar um número de conta ou token através de um estabelecimento, um facilitador de pagamentos ou uma carteira digital para processa transações futuras.

Este documento descreve como enviar os novos dados para uma transação que o cartão será salvo ou foi salvo em um Cofre do Lojista.

Lembrando que um cartão só é salvo no Cofre do Lojista se na transação de Verificação de Cartão ou na Autorização de uma transação, o retorno for "Cartão Valido" (VERIFIED) para o método de Verificação de Cartão e "Aprovado" (APPROVED) para Autorização.

Neste quadro descreve os domínios permitidos:

TAG	TIPO	TAM	DESCRIÇÃO
addlReqData [credentialsonfile]	A	1	F – Solicitação para que as credenciais sejam armazenadas S – Usar as credenciais armazenadas para pagamento.
addlReqData [initiationreason]	A	1	"A" - Nova autorização "C" - Pagamento não agendado "D" - atrasos de cobrança "I" - Incremental "O" - Outro motivo "R" - Recorrente agendado "S" - reenvio "X" - No-show (para uma reserva de hotel)
transactionID	N	18	TID da transação original ou de verificação de cartão. Atenção: Este deve ser enviado para as bandeiras VISA e ELO. **OBS:** O TID da transação original ou verificação de cartão tem validade de um ano, após esse período deve ser gerado um novo TID.

Todos os domínios devem ser finalizados com o caractere ";" (ponto-e-vírgula).

Exemplos:

```
        // solicitar a guarda do cartão no COFRE do EC
        <addlReqData>credentialsonfile=F;</addlReqData>
        <transactionID/>

        // solicitando uma autorização com a indicação de cartão armazenado no COFRE do EC para
Bandeira VISA
        <addlReqData>credentialsonfile=S;initiationreason=S;</addlReqData>
        <transactionID>123456789012345678</transactionID>

        // solicitando uma autorização com a indicação de cartão armazenado no COFRE do EC
        <addlReqData>credentialsonfile=S;initiationreason=S;</addlReqData>
        <transactionID/>


        // solicitando da segunda chamada de autorização de uma Recorrência
        <addlReqData>credentialsonfile=S;initiationreason=R;</addlReqData>
        <transactionID>123456789012345678</transactionID>
```

2.2.18 Transação de Valor Final

Requisito mandatório das Bandeiras para enviar mais informações na autorização de confirmação tardia, quando a venda sendo realizada tem a possibilidade de alteração do seu valor no processo de confirmação. O estabelecimento deve indicar no processo de autorização de confirmação tardia, se a venda é de um valor estimado, a qual ela poderá ser confirmada com valor menor da autorização.

Este atributo faz necessário quando o Lojista decide realizar uma transação de confirmação tardia. Para transações com a operação de purchase ou PreAuth, não faz necessário a indicação.

Por default, toda a transação é marcada como Valor Final, onde o estabelecimento indica que não terá alteração de valor, então para as transações que o estabelecimento sabe que poderá alterar o valor, deve enviar a marcação.

Neste quadro descreve o domínio a ser usado:

TAG	TIPO	TAM	DESCRIÇÃO
addlReqData [initiationreason]	A	1	"F" – Autorização de valor estimado

O domínio deve ser finalizado com o caractere ";" (ponto-e-vírgula).

Exemplos:

```
<addlReqData>initiationreason=F;</addlReqData>
```

2.2.19 Dados para Extrato

Para atender a melhorias de integração das vendas na Getnet com os seus conciliadores, disponibilizamos aos clientes opção de informar os dados que serão utilizados para realizar a conciliação entre o Extrato Getnet e a ferramenta de conciliação adotada. Para isto o estabelecimento deve enviar os dados que deseja, seguindo os domínios preestabelecidos, no campo [*].userDefinedField.udf5, a qual estes dados serão incorporados no arquivo de Extrato disponibilizados.

Estes dados podem ser enviados nas operações de Purchase, Authorization e Capture.
Enviando os dados nas operações de Purchase e Authorization, estes dados subiram para o Extrato.
Se enviar novos dados na operação de Captura, estes dados irão substituir os dados enviados nas operações anteriores.

O uso desta opção está vinculado a contratação do serviço e uso da versão disponível para o produto do Extrato Getnet V9.

Os dados devem ser informados no campo UDF5, seguido o formato EXTRATO=ORDER_ID:XXX;CHARGER_ID:XXX;CONSOLIDA_ID:XXX;IDEMP_KEY:XXX, tendo o seguinte domínio:

Neste quadro descreve os domínios permitidos:

TAG	TIPO	TAMANHO	DESCRIÇÃO
ORDER_ID	AN	36	Campo Order Id do cliente ou seu TID transacional. Exemplo de pattenr: ^[a-zA-Z0-9\-]{36}$
CHARGE_ID	AN	36	Campo Charge ID do cliente. Exemplo de pattern: ^[a-zA-Z0-9]{36}$
CONSOLIDA_ID	AN	70	Campo livre do cliente. Exemplo de pattern: ^[A-Z]{70}$
IDEMP_KEY	AN	64	Campo Idempotence Key do cliente. Exemplo de pattern: ^[a-zA-Z0-9\-]{64}$

Todos os domínios devem ser finalizados com o caractere “;” (ponto-e-vírgula).

Exemplos:

```
<udf5>EXTRATO=ORDER_ID:1234567890;</udf5>

<udf5>EXTRATO=ORDER_ID:ae673c74-bb52-2m7c-9c12-319b0b6843a6;</udf5>

<udf5>EXTRATO=ORDER_ID:1234567890;CHARGE_ID:;CONSOLIDA_ID:;IDEMP_KEY:;</udf5>

<udf5>EXTRATO=ORDER_ID:12345678901234567890123456789012345 6;</udf5>

<udf5>EXTRATO=ORDER_ID:ae673c74-bb52-2m7c-9c12-319b0b6843a6;CHARGE_ID:ae987c74-bb52-
4a62-9b12-309b0b9993a6;CONSOLIDA_ID:;IDEMP_KEY:;</udf5>

<udf5>EXTRATO=CHARGE_ID:1234567890;</udf5>

<udf5>EXTRATO=CHARGE_ID:ae987c74-bb52-4a62-9b12-309b0b9993a6;</udf5>
```

2.2.20 MAC - Merchant Advice Code Mastercard

Com o intuito de evitar que o motivo específico de uma negativa de autorização seja exposto a potenciais fraudadores, a bandeira Mastercard criou três códigos de resposta exclusivos:

79 (Ciclo de vida)

82 (Política)

83 (Fraude/ Segurança)

Quando o emissor nega uma autorização e envia um código de resposta sensível, a Mastercard converte o código original do emissor em um dos três novos códigos criados; a credenciadora e o estabelecimento recebem apenas o código exclusivo Mastercard na resposta da autorização.

Sem o motivo específico da negativa, passa a ser necessária alguma informação adicional para que o estabelecimento saiba se a negativa é reversível ou não – ou seja, se deve ou não tentar novamente aquela autorização. Para esta finalidade, a Mastercard criou um novo código denominado MAC – Merchant Advice Code (Código de Aconselhamento do Estabelecimento).

O código MAC informa se o estabelecimento deve ou não tentar novamente e, em caso positivo, se alguma ação deve ser executada antes da nova tentativa.

Os valores do código MAC podem ser:

- **1 -** Informações atualizadas/adicionais necessárias (Updated/additional information needed)
- **2 -** Tente novamente mais tarde (Try Again Later)
- **3 -** Não Tente Novamente (Do Not Try Again)
- **4 -** Requisitos de token não atendidos para este tipo de token (Token requirements not fulfilled for this token type)
- **U -** Cancelamento de Pagamento – Não reenvie a transação (Payment Cancellation – Do not resubmit transaction)

Quando o código de resposta for igual a 51 (Saldo / Limite Insuficiente), a Mastercard também poderá enviar no campo disponível para o código MAC um aconselhamento com o tempo após o qual é possível retentar uma transação. O número inicial do retorno quando igual a 1 significa “horas” e quando igual a 2 significa “dias”, conforme exposto abaixo:

- **101** = 1 hora
- **124** = 24 horas
- **202** = 2 dias
- **204** = 4 dias
- **206** = 6 dias
- **208** = 8 dias
- **210** = 10 dias

OBS: A Getnet realiza um DE PARA dos códigos originas recebidos pela bandeira Mastercard para melhor agrupar os retornos em caso de regras semelhantes para as demais bandeiras, dessa forma, no quadro abaixo é possível encontrar o DE PARA realizado:

DE PARA MASTERCARD X GETNET			
MAC Mastercard	DE PARA MAC Getnet	Descrição	Classificação
01	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Reversível
02	2	Tente novamente mais tarde (Try Again Later)	Reversível
03	3	Não Tente Novamente (Do Not Try Again)	Irreversível
04	4	Requisitos de token não atendidos para este tipo de token (Token requirements not fulfilled for this token type)	Reversível
21	U	Cancelamento de Pagamento – Não reenvie a transação (Payment Cancellation – Do not resubmit transaction)	Irreversível
24	101	Tente após 1 hora	Reversível
25	124	Tente após 24 horas	Reversível
26	202	Tente após 2 dias	Reversível
27	204	Tente após 4 dias	Reversível
28	206	Tente após 6 dias	Reversível
29	208	Tente após 8 dias	Reversível
30	210	Tente após 10 dias	Reversível

O quadro abaixo descreve as combinações possíveis dos códigos MAC junto aos códigos de resposta que podem ser enviados pela Mastercard e descreve os aconselhamentos que os comércios podem ter a partir delas:

Exemplos de Combinações do Reponse Code com o Código Complementar MAC				
Response Code	MAC	Descrição	Aconselhamento	Classificação
79 ou 82	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Informações atualizadas disponíveis no banco de dados Mastercard ABU - cheque as novas informações antes de tentar novamente	Reversível
79 ou 82	3	Não Tente Novamente (Do Not Try Again)	Não foram encontradas credenciais atualizadas no banco de dados Mastercard ABU – não tente novamente	Irreversível
83	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Verifique se as informações do cartão estão corretas. A autenticação pode melhorar a probabilidade de aprovação - tente novamente usando autenticação (Ex: 3DS)	Reversível
83	3	Não Tente Novamente (Do Not Try Again)	Suspeita de fraude. Não tente novamente	Irreversível
79, 82, 83	2	Tente novamente mais tarde (Try Again Later)	Tente novamente mais tarde	Reversível
51	101	Tente após 1 hora	Tente após 1 hora	Reversível
51	124	Tente após 24 horas	Tente após 24 horas	Reversível
51	202	Tente após 2 dias	Tente após 2 dias	Reversível
51	204	Tente após 4 dias	Tente após 4 dias	Reversível
51	206	Tente após 6 dias	Tente após 6 dias	Reversível
51	208	Tente após 8 dias	Tente após 8 dias	Reversível
51	210	Tente após 10 dias	Tente após 10 dias	Reversível

NOTA: Os códigos MAC 101, 124, 202, 204, 206, 208 e 2010 são de uso exclusivo Mastercard. Os demais códigos MAC (1, 2, 3, 4 e U) podem também ser enviados pelos emissores para aconselhamento junto aos demais códigos ABECS e, caso isso aconteça, para verificar se a transação pode ou não ser retentada, verifique a classificação do MAC recebido que está descrita na tabela: *DE PARA MASTERCARD X GETNET*: se o MAC for reversível, a transação pode ser retentada, se o MAC for irreversível a transação não pode ser retentatada.

2.2.21 Resumo das Funcionalidades

A seguir é apresentado um quadro-resumo com as funcionalidades de acordo com o tempo e valor para confirmação, autenticação e outras especificidades.

Funcionalidades	Especificidades				
	Tempo para Confirmação	Modalidades que podem ser Confirmadas	Valor da Confirmação	Suporta Autenticação	Autenticação Obrigatória
Débito	0 dias	Débito	Igual ao original	SIM	SIM
Crédito à Vista	7 dias	Crédito à Vista	Menor ou igual ao original	SIM	NÃO
Crédito Parcelado Lojista	7 dias	Crédito à Vista ou Parcelado Lojista	Menor ou igual ao original	SIM	NÃO
Crédito Parc. Loj. De Cias. Aéreas	7 dias	Crédito à Vista ou Parcelado Lojista	Menor ou igual ao original	SIM	NÃO
Crédito Parcelado Emissor	7 dias	Parcelado Emissor	Igual ao original	SIM	NÃO
Recorrência	Captura Online	Crédito à Vista	Igual ao original	SIM (Apenas credito)	NÃO
Crédito Parc. Emissor do BNDES	15 dias	Parcelado Emissor	Igual ao original	NÃO	NÃO
Pré-Autorização	30 dias	Crédito à Vista = Crédito à Vista Parcelado Lojista = Parcelado Lojista	Menor ou igual ao original	SIM	NÃO

Funcionalidades	Especificidades				
	Tempo para Confirmação	Modalidades que podem ser Confirmadas	Valor da Confirmação	Suporta Autenticação	Autenticação Obrigatória
Verificação de Cartão	N/A	N/A	N/A	N/A	N/A
Autenticação do Portador	N/A	N/A	N/A	SIM	N/A
MCC Dinâmico	N/A	N/A	N/A	N/A	N/A
Soft Descriptor	N/A	N/A	N/A	N/A	N/A

Figura 4 – Quadro-resumo das funcionalidades e suas especificidades

2.3 Como se Conectar à Getnet?

2.3.1 Requisitos Técnicos

A integração com a GetNet é feita através de chamadas de WebServices em SOAP em HTTPS, que tem por objetivo efetuar a coleta e o tratamento dos dados referente à transação de E-Commerce e realizar a comunicação entre o EC e os Emissores de cartão.

*Para segurança das transações, a Indústria de Pagamentos com Cartões segue o padrão indicado pelo PCI-DSS (*Payment Card Industry – Data Security Standard*). De acordo com estes padrões, toda comunicação em HTTPS deve ser realizada com o protocolo **TLS 1.2** ou superior. Não serão aceitas conexões em versões anteriores.*

2.3.2 Homologação e Certificação

Para que possa ocorrer a integração entre o EC e a Plataforma de E-Commerce da GetNet, é necessário que a plataforma de comércio on-line ou Loja Virtual passe por uma Homologação para garantir a segurança e a qualidade do produto assim como a estabilidade e minimização de riscos de erro.

Para tanto, é realizada uma série de testes para verificar o sistema nos quesitos de segurança das informações e comportamento em situações pré-determinadas como timeout, transações rejeitadas, parâmetros inválidos, inserção de dados inesperados e uma extensa rotina de testes.

O EC deverá solicitar à Getnet a criação de **usuário** e **senha** para acesso ao ambiente de homologação. E deve criar o seu cliente a partir da versão desejada (URL) do serviço disponível (*2.3.2.3 – Endereços de Conexão para Homologação*).

Será então disponibilizado um ambiente para realizar o roteiro de testes junto à Getnet. O processo de integração, ajustes e demais testes acontecerão nesse ambiente. O desenvolvedor da Loja Virtual realiza o processo de integração em seu ambiente sem necessidade de deslocamentos. Todo processo é online e acompanhado por uma equipe disponível para responder dúvidas e auxiliar em casos de dificuldade.

Através do pacote disponibilizado para desenvolvimento é possível simular todos os comportamentos que serão utilizados em Produção (ambiente real).

Depois de finalizados os testes com sucesso o EC receberá um comunicado informando o término da Homologação e liberado para entrada em Produção e início da realização de transações.

Para o processo de homologação devem ser usados alguns valores pré-fixados para alguns dados da transação. Isto faz-se necessário pois são usados simuladores para fazer os papeis das Bandeiras e dos Emissores, e alguns dados só são permitidos com estes valores. Estes valores são apresentados nas duas próximas sessões.

2.3.2.1 Regras para Testes de Transações Parceladas

Para realizar transações Parcelado Lojista ou Emissor, os valores e número de parcelas seguem as regras descritas nas tabelas a seguir.

Parcelado Lojista MasterCard / VISA			
Categoria	Tipo	N.Parc.	Valor
Geral	Lojista	02	nnn02,02
Geral	Lojista	03	nnn03,03
Geral	Lojista	04	nnn04,04
Geral	Lojista	05	nnn05,05
Geral	Lojista	06	nnn06,06
Assim até 36			
Geral	Lojista	35	nnn35,35
Geral	Lojista	36	nnn36,36

Parcelado Emissor Visa			
Exclusivo	Tipo	N.Parc	Valor
Visa	Emissor	02	202,21
Visa	Emissor	03	302,21
Visa	Emissor	04	402,21
Visa	Emissor	05	502,21

Parcelado Emissor MasterCard			
Categoria	Tipo	N.Parc	Valor
Geral	Emissor	02	202,21
Geral	Emissor	03	302,21
Geral	Emissor	04	402,21
Geral	Emissor	05	502,21
Geral	Emissor	06	602,21
Geral	Emissor	07	702,21
Geral	Emissor	08	802,21
Geral	Emissor	09	902,21
Geral	Emissor	10	1002,21
Geral	Emissor	11	1102,21
Assim até 48			
Geral	Emissor	47	4702,21
Geral	Emissor	48	4802,21

Figura 5 – Regras para Testes de Transações Parceladas Lojista e Emissor

Caso a transação seja negada ou o retorno seja diferente de um parcelado, favor entrar em contato para verificar se possivelmente alguma regra foi alterada.

2.3.2.2 Dados de Cartões de Teste

Para realizar as transações de teste, em qualquer modalidade, utilize os seguintes cartões:

BANDEIRA	CARTÕES DE TESTE	CRÉDITO	DÉBITO	AUTENTICAÇÃO
mastercard	PAN: 5447318879391031 CVV: 528 / VENC.: 02/2024	✓		✓
	PAN: 5201328232183740 CVV: 989 / VENC.: 12/2023	✓	✓	✓
VISA	PAN: 4220612154786956 CVV: 083 / VENC.: 12/2023	✓		✓
	PAN: 4220619003385567 CVV: 473 / VENC.: 10/2023	✓	✓	✓
AMERICAN EXPRESS	PAN: 376442058032004 CVV: 1589 / VENC.: 07/2023	✓		
	PAN: 374245001771004 CVV: 123 / VENC.: 03/2021	✓		
elo	PAN: 5067230000009011 CVV: 568 / VENC.: 10/2021	✓	✓	
	PAN: 5067410010100070 CVV: 568 / VENC.: 10/2021	✓	✓	
Hipercard	PAN: 6370950924782803 CVV: 832 / VENC.: 10/2023	✓	✓	
	PAN: 6370950926873000 CVV: 979 / VENC.: 07/2024	✓	✓	

Figura 6 – Dados de Cartões de Testes

2.3.2.3 Endereços de Conexão para Homologação

Versão 2.0

https://cgws-hti.getnet.com.br/eCommerceWS/2.0/AdministrationService?wsdl
https://cgws-hti.getnet.com.br/eCommerceWS/2.0/CommerceService?wsdl

Versão 3.0

https://cgws-hti.getnet.com.br/eCommerceWS/3.0/AdministrationService?wsdl
https://cgws-hti.getnet.com.br/eCommerceWS/3.0/CommerceService?wsdl

Caso os servidores de origem que irão acessar o ambiente da Getnet (Homologação ou Produção) estejam fora do Brasil, é preciso pedir o cadastro prévio de todos os IPs de origem junto ao Firewall da Getnet para que a conexão seja efetivada.

*Os IPs do ambiente de Produção devem ser enviados com, no mínimo, **uma semana de antecedência** do início da operação para cadastro no Firewall da Getnet.*

3 E-COMMERCE WEB VIA WEBSERVICE

Para realização das chamadas aos serviços disponíveis, o EC deve incluir no sistema da Loja Virtual ou do Gateway de Pagamentos responsável pela conexão com a Getnet as chamadas aos mesmos, de acordo com a funcionalidade desejada.

A seguir apresentamos o fluxo macro do processo transacional e nas sessões seguintes os detalhes para uso de cada funcionalidade disponível.

Processo Transacional Macro

1. Cliente da Loja Virtual (Portador) finaliza sua compra e encerra o pedido.
2. É direcionado ao formulário de coleta dos dados onde insere as informações do seu cartão no site da Loja Virtual para iniciar o processo de pagamento.
3. Loja Virtual aciona a URL do serviço para realizar a transação.
4. O serviço solicita uma transação à Plataforma de E-Commerce Getnet.
5. Após análise cadastral e consistência dos dados da transação feitas com sucesso a Plataforma de E-Commerce Getnet encaminha a transação para a Bandeira, e em caso de insucesso retorna um código e descritivo referente ao erro encontrado.
6. No caso de sucesso, a Bandeira retorna com a resposta do Emissor e a mesma é enviada para o EC.
7. O serviço devolve o retorno para a Loja Virtual, onde é realizada a interação com o portador.

O formulário de coleta dos dados fica no ambiente da Loja Virtual. O estabelecimento é responsável pelo desenvolvimento da página respeitando as políticas de segurança para manipulação dos dados do cartão do Portador estabelecidas pelas Bandeiras.

3.1 INTEGRAÇÃO

Nesta seção é descrito como o sistema da Loja Virtual deve interagir com o portador e a Plataforma de E-Commerce da Getnet.

Primeiramente, o EC deverá solicitar à Getnet a criação de **usuário** e **senha** para acesso ao ambiente de homologação. A seguir, deve criar o seu sistema cliente a partir da versão desejada (URL) do serviço disponível (*2.3.2.3 – Endereços de Conexão para Homologação*).

Para a integração, são necessárias as informações de número de EC e Terminal, que são fornecidas juntamente com o usuário e senha requisitados.

O número de Terminal é utilizado para identificação do estabelecimento durante uma transação. Esta informação é recebida após o Credenciamento e vinculação do meio de captura E-Commerce e é composto de 8 dígitos, por exemplo: **X1234567**.

A letra inicial do código de Terminal indica o meio de captura (WEB ou TEF) e o modo de autenticação do portador. Deve-se utilizar os terminais corretamente de acordo com o meio de captura e forma de autenticação para cada transação.

Letra Inicial	Meio de Captura
D	E-Commerce WEB Não Autenticado
E	E-Commerce WEB Autenticado
F	E-Commerce TEF Não Autenticado
G	E-Commerce TEF Autenticado
R	E-Commerce Recorrente

Existe um mapeamento 1:1 entre o Terminal e o seu perfil para cada Bandeira com a adição de um sufixo de dois dígitos no Terminal para indicá-lo no momento da transação. Este código composto é o **TerminalID**. Assim, o TerminalID é um campo alfanumérico de 10 posições, por exemplo: **X123456799**.

Cada sufixo está mapeado para um único perfil de Terminal que define as moedas, transações, opções de processamento e instrumentos de pagamento válidos para ele.

É necessário usar o TerminalID correto para a operação que está sendo feita. Por exemplo, se o Terminal é **'X1234567'**, e a transação é VISA Crédito, o estabelecimento deve usar **'X123456701'** para essa transação.

TerminalID	Quando usar?
X123456**701**	Para transações Visa Crédito
X123456**702**	Para transações MasterCard Crédito
X123456**703**	Para transações Visa Débito
X123456**704**	Para transações MasterCard Débito
X123456**707**	Para transações ELO Crédito
X123456**708**	Para transações ELO Débito autenticado ou Não autenticado
X123456**709**	Para transações American Express Crédito
X123456**710**	Para transações Hipercard Débito (ainda não utilizado)
X123456**712**	Para transações Hipercard Crédito

3.1.1 Métodos e Versões

Nessa seção são apresentadas as funcionalidades (métodos) disponíveis em cada versão nos serviços CommerceService e AdministrationService.

Todas as operações mantêm as mesmas características das versões anteriores.

MÉTODO	DISPONÍVEL NA VERSÃO			
	1.0	1.1	2.0	3.0
PurchaseService	√	√	√	√
AuthorizationService	√	√	√	√
CaptureService	√	√	√	√
CancellationService	√	√	√	√
QueryDataService	√	√	√	√
CardVerificationService		√	√	√
ChangeAuthenticationService	√	√	√	√
ChangeKeysService	√	√	√	√
AuthenticatedPurchaseService			√	×
AuthenticatedAuthorizationService			√	×
AuthenticationOnlyService			√	×
FinalizeAuthenticationService			√	×
PreAuthorizationService			√	√
CapturePreAuthService			√	√
AdjustmentPreAuthService			√	√
CancellationPreAuthService			√	√
authenticationEnrollmentService				√
tokenService				√
validateAuthenticationService				√

Figura 7 – Tabela Métodos vs Versões

***Atenção**: As versões 1.0 e 1.1, não mais serão comercializadas. Favor programar a migração das versões para versão 3.0, recomendada.*

***Atenção**: A versão 2.0, irá entrar no processo de desativação de novas funcionalidades (Sunset). Favor programar a migração das versões para versão 3.0.*

3.2 INTERFACES DE INTEGRAÇÃO DOS SERVIÇOS TRANSACIONAIS

Nessa seção são detalhadas as funcionalidades (métodos) disponíveis nos serviços transacionais (*CommerceService*) para que o desenvolvedor realize a integração da loja virtual com o sistema de captura de transações da GetNet, utilizando a tecnologia WebService com SOAP.

O modelo empregado é bastante simples: há uma única URL que recebe os POSTS via HTTPS e, dependendo das informações do XML enviado, uma determinada operação é realizada.

Cada uma das operações disponíveis é apresentada nas sessões seguintes.

3.2.1 MÉTODO PURCHASESERVICE

Executa, em uma única chamada, uma Autorização seguida de uma Confirmação (Captura), caso a autorização tenha sido aprovada.

A tabela a seguir detalha cada uma das TAGs do XML a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual
authentication.username	AN	R	20	Usuário de acesso
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GetNet.
purchases	ARRAY	R	1..n	Elemento raiz com as N transações.
purchase	n/a	R	1	Elemento de cada transação.
purchase.terminalID	AN	R	10	Ver *Regra para TerminalID*.
purchase.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
purchase.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
purchase.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
purchase.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
purchase.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
purchase.tranCategory	AN	R	4	Campo disponível a partir da **versão 2.0.** Identifica a categoria da transação a ser efetuado: **DFLT** – Todas **IATA** – Transações Cias Aéreas Ver *Regra para TranCategory*.
purchase.card	n/a	R	1	Elemento com os dados do cartão.

TAG	Tipo	Obrig.	Tam.	Descrição
purchase.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
purchase.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
purchase.card.expiryMonth	N	R	2	Mês de expiração do cartão.
purchase.card.expiryYear	N	R	4	Ano de expiração do cartão.
purchase.card.holderName	AN	R	26	Nome do portador impresso no cartão.
purchase.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
purchase.userDefinedField.udf1	AN	O	255	Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis. Ver *Regra para UDF (userDefinedField)*.
purchase.userDefinedField.udf2	AN	O	255	
purchase.userDefinedField.udf3	AN	O	255	
purchase.userDefinedField.udf4	AN	O	255	
purchase.userDefinedField.udf5	AN	O	255	
purchase.xid	AN	O	40	Campo disponível a partir da **versão 2.0.** Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
purchase.ucaf	AN	O	40	Campo disponível a partir da **versão 2.0.** Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
purchase.eci	N	O	2	Campo disponível a partir da **versão 2.0.** Código ECI da transação Autenticada 3D Secure.
purchase.tranType	AN	R	8	Campo disponível a partir da **versão 2.0.** Identifica o tipo de transação a ser efetuado: **CREDIT** – Crédito **DEBIT** – Débito não autenticado. Modalidade disponível para determinado contrato. Para maiores informações, entrar em contato.
purchase.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
purchase.softDescriptor	AN	O	22	Ver *Regra para Soft Descriptor*.
purchase.addlReqData	AN	O	255	Campo disponível a partir da **versão 2.0.** Ver *Regras para AddlReqData*.
purchase.recurringseqid	N	O		Campo utilizado para informar o número da recorrência (parcela) vai de 1 até 999
purchase.tdsver	N	O		Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização.
purchase.tdsdsxid	AN	O		Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.
purchase.wallet	n/a	O	1	Dados para a Carteira Digital
purchase.wallet.type	N	O	2	Tipo de Carteira (Wallet Type): 01: MasterPass Wallet 02: Visa Checkout 10: Generic Tokenized Wallet 55: Local Brazil Wallet (SDWO)

TAG	Tipo	Obrig.	Tam.	Descrição
purchase.wallet.id	AN	O	5	Identificação da Carteira (Wallet Identification) - MasterPass: 101 = Wallet Remote 102 = Wallet Remote NFC Payment - Visa Checkout VCIND - Generic Tokenized Wallet 000 = Unspecified 101 = Wallet Remote 102 = Wallet Remote NFC Payment 103 = Apple Pay 216 = Android Pay 217 = Samsung Pay 327 = MDES for merchants (M4M) - Local Brazil Wallet BRL = Valor default
purchase.wallet.merchantId	AN	O	12	Número de identificação da Carteira Digital registrado juntos as bandeiras **Visa** = MVV (Merchant Value Verification) com 6 posições **Mastercard** = WID (Wallet ID) com 3 posições **Elo** = WID (Wallet ID) com 11 posições
purchase.wallet.fundTransfer	n/a	O	1	Dados para transações do arranjo SDWO (Staged Digital Wallet Operator)
purchase.wallet.fundTransfer.payAction	A	O	2	Tipo de Financiamento **FT**: Funding Transfer – Que deve ser marcado em transações de Cash-in SDWO para todas as bandeiras. **FP**: Funding and Purchase – Que deve ser marcado em transações de Back-to-Back SDWO para todas as bandeiras. **BP**: Billpay – CBPS VISA
purchase.wallet.fundTransfer.receiver	n/a	O	1	Dados complementares Usados pela Mastercard.
purchase.wallet.fundTransfer.receiver.accountNumber	AN	O	20	Receiver Account Number que pode ser preenchido com um dos valores a seguir: “#NA” ou “9999999999999995”. Necessário o preenchimento apenas para a bandeira Mastercard, para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.wallet.fundTransfer.receiver.accountType	N	O	2	Receiver Account Type que deve ser preenchido com 00. **00 – Outros (Default, currently only allowed value)** 01 — RTN + Conta Bancária 02 — IBAN 03 — Conta de Cartão (for getnet currently only available type) 04 — E-mail 05 — Número de Telefone 06 — Número da conta bancária (BAN) + Código de Identificação do Banco (BIC) 07 — ID da Carteira 08 — ID da Rede Social Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional

TAG	Tipo	Obrig.	Tam.	Descrição
purchase.wallet.fundTransfer.receiver.firstName	AN	O	35	Receiver First Name que deve ser preenchido com o primeiro nome do destinatário da transferência. Ex: Jane Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.wallet.fundTransfer.receiver.middleName	AN	O	1	Receiver Middle Name que deve ser preenchido com a abreviação do nome do meio do destinatário da transferência. Ex: T O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.lastName	AN	O	35	Receiver Last Name que deve ser preenchido com último nome (sobrenome) do destinatário da transferência. Ex: Smith Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.wallet.fundTransfer.receiver.addrStreet	AN	O	50	Receiver Addr Street que deve ser preenchido com o endereço do destinatário da transferência (rua e número). Ex: 1 Main St O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.addrCity	AN	O	25	Receiver Addr City que deve ser preenchido com a cidade do destinatário da transferência. Ex: SAO PAULO O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.addrState	A	O	3	Receiver Addr State que deve ser preenchido com o estado do destinatário da transferência. Ex: SP O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.addrCountry	A	O	3	Receiver Addr Country que deve ser preenchido com o país do destinatário da transferência. Seguindo o padrão ISO 3166-1 alfa 3. Ex: BRA Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.wallet.fundTransfer.receiver.addrPostalCode	AN	O	10	Receiver Addr Postal Code que deve ser preenchido com o código postal (CEP) do destinatário da transferência. Ex: 01408000 O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.nationality	A	O	3	Receiver Nationality que deve ser preenchido com a nacionalidade do destinatário da transferência. Seguindo o padrão ISO 3166-1 alfa 3. Ex: BRA O preenchimento é opcional para todas as bandeiras.

TAG	Tipo	Obrig.	Tam.	Descrição
purchase.wallet.fundTransfer.receiver.phone	N	O	20	Receiver Phone que deve ser preenchido com o número de telefone do destinatário da transferência, incluindo o código do país. Ex: 5511977778888 O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.dateOfBirth	N	O	8	Receiver Date Of Birth que deve ser preenchido com a data de nascimento do destinatário da transferência com o formato: YYYYMMDD. Ex: 19901230 O preenchimento é opcional para todas as bandeiras.
purchase.wallet.fundTransfer.receiver.idType	N	O	2	Receiver Id Type que deve ser preenchido com o tipo do documento utilizado pelo destinatário da transferência **(CPF ou CNPJ)**. Nesse caso preenchido com 03. **Ex: 03** 00 = Passaporte 01 = Carteira de Identificação Nacional 02 = Carteira de Motorista **03 = Emitida pelo Governo** 04 = Outros Necessário o preenchimento para as bandeiras Mastercard e Visa para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.wallet.fundTransfer.receiver.idNum	AN	O	25	Receiver Id Number que deve ser preenchido com o número do **CPF ou CNPJ** do destinatário da transferência. Ex: 12345678900000 Necessário o preenchimento para as bandeiras Mastercard e Visa para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
purchase.tokenization	n/a	O	1	Tokenização + DSRP
purchase.tokenization.type	A	O	5	UCAF – Mastercard TAVV – VISA / ELO
purchase.tokenization.cryptogram	NA	O	36	Criptograma (UCAF/TAVV) gerado no processo do DSRP / Token Requestor. Sendo o criptograma codificado em Base64 e com até 32 caracteres.
purchase.tokenization.eci	N	O	2	Indicador do ECI (Electronic Commerce Indicator) - Mastercard 02 – Dados gerados no DSRP com criptograma gerado por carteira In-App; 06 – Dados gerados no DSRP com criptograma 07 – Para transações de pagamentos recorrentes, deve enviar a marcação do CoF. - VISA 05 - Quando usando tokens de dispositivo pelo VTS - ELO 04 – Transações com criptograma gerado em tokens de dispositivo (In-App). * Verificar item Reclassificação de ECI

TAG	Tipo	Obrig.	Tam.	Descrição
purchase.tokenization.requestorId	AN	O	11	ID do Token Requestor. A entidade provedora dos dados, normalmente a carteira digital. (Mastercard)

O quadro a seguir demonstra as TAGs XML do “Service Request” do PurchaseService:

```
<purchaseService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <purchases>
      <!--Zero or more repetitions:-->
      <purchase>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <amount>string</amount>
        <currencycode>string</currencycode>
        <instType>string</instType>
        <!--Optional:-->
        <instNum>string</instNum>
        <tranCategory>string</tranCategory>
        <card>
          <number>string</number>
          <!--Optional:-->
          <cvv2>string</cvv2>
          <expiryMonth>string</expiryMonth>
          <expiryYear>string</expiryYear>
          <holderName>string</holderName>
        </card>
        <!--Optional:-->
        <userDefinedField>
          <!--Optional:-->
          <udf1>string</udf1>
          <!--Optional:-->
          <udf2>string</udf2>
          <!--Optional:-->
          <udf3>string</udf3>
          <!--Optional:-->
          <udf4>string</udf4>
          <!--Optional:-->
          <udf5>string</udf5>
        </userDefinedField>
        <!--Optional:-->
        <xid>string</xid>
        <!--Optional:-->
        <ucaf>string</ucaf>
        <!--Optional:-->
        <eci>string</eci>
        <!--Optional:-->
```

```
<tranType>string</tranType>
<!--Optional:-->
<tranMCC>string</tranMCC>
<!--Optional:-->
<softDescriptor>string</softDescriptor>
<!--Optional:-->
<addlReqData>string</addlReqData>
 <!--Optional:-->
<recurringseqid>string</recurringseqid>
 <!--Optional:-->
<tdsver>string</tdsver>
 <!--Optional:-->
<tdsdsxid>string</tdsdsxid>
<!--Optional:-->
<wallet>
  <!--Optional:-->
  <type>string</type>
  <!--Optional:-->
  <id>string</id>
  <!--Optional:-->
  <merchantId>string</merchantId>
  <!--Optional:-->
  <fundTransfer>
      <!--Optional:-->
      <payAction>string</payAction>
      <!--Optional:-->
      <receiver>
             <!--Optional:-->
             <accountNumber>9999999999999995</accountNumber>
             <!--Optional:-->
             <accountType>00</accountType>
             <!--Optional:-->
             <firstName>Pedro</firstName>
             <!--Optional:-->
             <middleName>I</middleName>
             <!--Optional:-->
             <lastName>do Brasil</lastName>
             <!--Optional:-->
             <addrStreet>Rua Juscelino</addrStreet>
             <!--Optional:-->
             <addrCity>SAO PAULO</addrCity>
             <!--Optional:-->
             <addrState>SP</addrState>
             <!--Optional:-->
             <addrCountry>BRA</addrCountry>
             <!--Optional:-->
             <addrPostalCode>01408000</addrPostalCode>
             <!--Optional:-->
             <nationality>BRA</nationality>
             <!--Optional:-->
             <phone>5511977778888</phone>
             <!--Optional: Format YYYYMMDD -->
             <dateOfBirth>20221231</dateOfBirth>
             <!--Optional:-->
             <idType>03</idType>
             <!--Optional:-->
             <idNum>12345678900000</idNum>
      </receiver>
  </fundTransfer>
</wallet>
```

```
            <!--Optional:-->
            <tokenization>
              <!--Optional:-->
              <type>string</type>
              <!--Optional:-->
              <cryptogram>string</cryptogram>
              <!--Optional:-->
              <eci>string</eci>
              <!--Optional:-->
              <requestorId>string</requestorId>
            </tokenization>
          </purchase>
        </purchases>
      </arg0>
    </purchaseService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do PurchaseResponse:

```
    <purchaseServiceResponse>
       <!--Optional:-->
       <purchaseResponse>
          <!--Optional:-->
          <result>
             <!--Zero or more repetitions:-->
             <result>
                “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
             </result>
          </result>
       </purchaseResponse>
    </purchaseServiceResponse>
```

3.2.2 MÉTODO AUTHORIZATIONSERVICE

Executa uma Autorização, **sem a Confirmação (Captura)**. A transação, se autorizada, se mantêm pendente de Confirmação.

A tabela a seguir detalha cada uma das TAGs do XML a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual
authentication.username	AN	R	20	Usuário de acesso
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
authorizations	ARRAY	R	1..n	Elemento raiz com as N transações.

TAG	Tipo	Obrig.	Tam.	Descrição
authorization	n/a	R	1	Elemento de cada transação.
authorization.terminalID	AN	R	10	Ver *Regra para TerminalID*.
authorization.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
authorization.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
authorization.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
authorization.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
authorization.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
authorization.tranCategory	AN	R	4	Campo disponível a partir da **versão 2.0.** Identifica a categoria da transação a ser efetuado: **DFLT** – Todas **IATA** – Transações destinadas a Cias Aéreas Ver *Regra para TranCategory*.
authorization.card	n/a	R	1	Elemento com os dados do cartão.
authorization.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
authorization.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
authorization.card.expiryMonth	N	R	2	Mês de expiração do cartão.
authorization.card.expiryYear	N	R	4	Ano de expiração do cartão.
authorization.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authorization.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
authorization.userDefinedField.udf1	AN	O	255	Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis. Ver *Regra para UDF (userDefinedField)*.
authorization.userDefinedField.udf2	AN	O	255	
authorization.userDefinedField.udf3	AN	O	255	
authorization.userDefinedField.udf4	AN	O	255	
authorization.userDefinedField.udf5	AN	O	255	
authorization.xid	AN	O	40	Campo disponível a partir da **versão 2.0.** Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authorization.ucaf	AN	O	40	Campo disponível a partir da **versão 2.0.** Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authorization.eci	N	O	2	Campo disponível a partir da **versão 2.0.** Código ECI da transação Autenticada 3D Secure. Gerado por um MPI Externo.
authorization.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authorization.softDescriptor	AN	O	22	Ver *Regra para Soft Descriptor*.
authorization.addlReqData	AN	O	255	Campo disponível a partir da **versão 2.0.** Ver *Regras para AddlReqData*.

TAG	Tipo	Obrig.	Tam.	Descrição
authorization.tdsver	N	O		Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização.
authorization.tdsdsxid	AN	O		Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.
authorization.wallet	n/a	O	1	Dados para a Carteira Digital
authorization.wallet.type	N	O	2	Tipo de Carteira (Wallet Type): 01: MasterPass Wallet 02: Visa Checkout 10: Generic Tokenized Wallet 55: Local Brazil Wallet (SDWO)
authorization.wallet.id	N	O	5	Identificação da Carteira (Wallet Identification) - MasterPass: 101 = Wallet Remote 102 = Wallet Remote NFC Payment - Visa Checkout VCIND - Generic Tokenized Wallet 000 = Unspecified 101 = Wallet Remote 102 = Wallet Remote NFC Payment 103 = Apple Pay 216 = Android Pay 217 = Samsung Pay 327 = MDES for merchants (M4M) - Local Brazil Wallet BRL = Valor default
authorization.wallet.merchantId	AN	O	12	Número de identificação da Carteira Digital registrado juntos as bandeiras **Visa** = MVV (Merchant Value Verification) com 6 posições **Mastercard** = WID (Wallet ID) com 3 posições **Elo** = WID (Wallet ID) com 11 posições
authorization.wallet.fundTransfer	n/a	O	1	Dados para transações do arranjo SDWO (Staged Digital Wallet Operator)
authorization.wallet.fundTransfer.payAction	A	O	2	Tipo de Financiamento **FT**: Funding Transfer – Que deve ser marcado em transações de Cash-in SDWO para todas as bandeiras. **FP**: Funding and Purchase – Que deve ser marcado em transações de Back-to-Back SDWO para todas as bandeiras. **BP**: Billpay – CBPS VISA
authorization.wallet.fundTransfer.receiver	n/a	O	1	Dados complementares Usados pela Mastercard.
authorization.wallet.fundTransfer.receiver.accountNumber	AN	O	20	Receiver Account Number que pode ser preenchido com um dos valores a seguir: “#NA” ou “9999999999999995”. Necessário o preenchimento apenas para a bandeira Mastercard, para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.accountType	N	O	2	Receiver Account Type que deve ser preenchido com 00. **00 – Outros (Default, currently only allowed value)** 01 — RTN + Conta Bancária 02 — IBAN

TAG	Tipo	Obrig.	Tam.	Descrição
				03 — Conta de Cartão (for getnet currently only available type) 04 — E-mail 05 — Número de Telefone 06 — Número da conta bancária (BAN) + Código de Identificação do Banco (BIC) 07 — ID da Carteira 08 — ID da Rede Social Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.firstName	AN	O	35	Receiver First Name que deve ser preenchido com o primeiro nome do destinatário da transferência. Ex: Jane Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.middleName	AN	O	1	Receiver Middle Name que deve ser preenchido com a abreviação do nome do meio do destinatário da transferência. Ex: T O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.lastName	AN	O	35	Receiver Last Name que deve ser preenchido com último nome (sobrenome) do destinatário da transferência. Ex: Smith Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.addrStreet	AN	O	50	Receiver Addr Street que deve ser preenchido com o endereço do destinatário da transferência (rua e número). Ex: 1 Main St O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.addrCity	AN	O	25	Receiver Addr City que deve ser preenchido com a cidade do destinatário da transferência. Ex: SAO PAULO O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.addrState	A	O	3	Receiver Addr State que deve ser preenchido com o estado do destinatário da transferência. Ex: SP O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.addrCountry	A	O	3	Receiver Addr Country que deve ser preenchido com o país do destinatário da transferência. Seguindo o padrão ISO 3166-1 alfa 3. Ex: BRA Necessário o preenchimento apenas para a bandeira Mastercard para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.addrPostalCode	AN	O	10	Receiver Addr Postal Code que deve ser preenchido com o código postal (CEP) do destinatário da transferência. Ex: 01408000

TAG	Tipo	Obrig.	Tam.	Descrição
				O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.nationality	A	O	3	Receiver Nationality que deve ser preenchido com a nacionalidade do destinatário da transferência. Seguindo o padrão ISO 3166-1 alfa 3. Ex: BRA O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.phone	N	O	20	Receiver Phone que deve ser preenchido com o número de telefone do destinatário da transferência, incluindo o código do país. Ex: 5511977778888 O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.dateOfBirth	N	O	8	Receiver Date Of Birth que deve ser preenchido com a data de nascimento do destinatário da transferência com o formato: YYYYMMDD. Ex: 19901230 O preenchimento é opcional para todas as bandeiras.
authorization.wallet.fundTransfer.receiver.idType	N	O	2	Receiver Id Type que deve ser preenchido com o tipo do documento utilizado pelo destinatário da transferência **(CPF ou CNPJ)**. Nesse caso preenchido com 03. **Ex: 03** 00 = Passaporte 01 = Carteira de Identificação Nacional 02 = Carteira de Motorista **03 = Emitida pelo Governo** 04 = Outros Necessário o preenchimento para as bandeiras Mastercard e Visa para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.wallet.fundTransfer.receiver.idNum	AN	O	25	Receiver Id Number que deve ser preenchido com o número do **CPF ou CNPJ** do destinatário da transferência. Ex: 12345678900000 Necessário o preenchimento para as bandeiras Mastercard e Visa para transações de SDWO de Cash-in, para as demais bandeiras o preenchimento é opcional
authorization.tokenization	n/a	O	1	Tokenização + DSRP
authorization.tokenization.type	A	O	5	UCAF – Mastercard TAVV – VISA
authorization.tokenization.cryptogram	NA	O	36	Criptograma (UCAF/TAVV) gerado no processo do DSRP / Token Requestor. Sendo o criptograma codificado em Base64 e com até 32 caracteres.
authorization.tokenization.eci	N	O	2	Indicador do ECI (Electronic Commerce Indicator) - Mastercard 02 – Dados gerados no DSRP com criptograma gerado por carteira In-App; 06 – Dados gerados no DSRP com criptograma

TAG	Tipo	Obrig.	Tam.	Descrição
				07 – Para transações de pagamentos recorrentes, deve enviar a marcação do CoF. - VISA 05 - Quando usando tokens de dispositivo pelo VTS - ELO 04 – Transações com criptograma gerado em tokens de dispositivo (In-App). * Verificar item Reclassificação de ECI
authorization.tokenization.requestor Id	AN	O	11	ID do Token Requestor. A entidade provedora dos dados, normalmente a carteira digital. (Mastercard)

O quadro a seguir demonstra as TAGs XML do “Service Request” do AuthorizationService:

```
<authorizationService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <authorizations>
      <!--Zero or more repetitions:-->
      <authorization>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <amount>string</amount>
        <currencycode>string</currencycode>
        <instType>string</instType>
        <!--Optional:-->
        <instNum>string</instNum>
        <tranCategory>string</tranCategory>
        <card>
          <number>string</number>
          <!--Optional:-->
          <cvv2>string</cvv2>
          <expiryMonth>string</expiryMonth>
          <expiryYear>string</expiryYear>
          <holderName>string</holderName>
        </card>
        <!--Optional:-->
        <userDefinedField>
          <!--Optional:-->
          <udf1>string</udf1>
          <!--Optional:-->
          <udf2>string</udf2>
          <!--Optional:-->
          <udf3>string</udf3>
          <!--Optional:-->
          <udf4>string</udf4>
          <!--Optional:-->
```

```
  <udf5>string</udf5>
</userDefinedField>
<!--Optional:-->
<xid>string</xid>
<!--Optional:-->
<ucaf>string</ucaf>
<!--Optional:-->
<eci>string</eci>
<!--Optional:-->
<tranMCC>string</tranMCC>
<!--Optional:-->
<softDescriptor>string</softDescriptor>
<!--Optional:-->
<addlReqData>string</addlReqData>
 <!--Optional:-->
<recurringseqid>string</recurringseqid>
 <!--Optional:-->
<tdsver>string</tdsver>
 <!--Optional:-->
<tdsdsxid>string</tdsdsxid>
 <!--Optional:-->
<wallet>
  <!--Optional:-->
  <type>string</type>
  <!--Optional:-->
  <id>string</id>
  <!--Optional:-->
  <merchantId>string</merchantId>
  <!--Optional:-->
  <fundTransfer>
      <!--Optional:-->
      <payAction>string</payAction>
      <!--Optional:-->
      <receiver>
              <!--Optional:-->
              <accountNumber>9999999999999995</accountNumber>
              <!--Optional:-->
              <accountType>00</accountType>
              <!--Optional:-->
              <firstName>Pedro</firstName>
              <!--Optional:-->
              <middleName>I</middleName>
              <!--Optional:-->
              <lastName>do Brasil</lastName>
              <!--Optional:-->
              <addrStreet>Rua Juscelino</addrStreet>
              <!--Optional:-->
              <addrCity>SAO PAULO</addrCity>
              <!--Optional:-->
              <addrState>SP</addrState>
              <!--Optional:-->
              <addrCountry>BRA</addrCountry>
              <!--Optional:-->
              <addrPostalCode>01408000</addrPostalCode>
              <!--Optional:-->
              <nationality>BRA</nationality>
              <!--Optional:-->
              <phone>5511977778888</phone>
              <!--Optional: Format YYYYMMDD -->
              <dateOfBirth>20221231</dateOfBirth>
```

```
                            <!--Optional:-->
                            <idType>03</idType>
                            <!--Optional:-->
                            <idNum>12345678900000</idNum>
                        </receiver>
                    </fundTransfer>
                </wallet>
                <!--Optional:-->
                <tokenization>
                  <!--Optional:-->
                  <type>string</type>
                  <!--Optional:-->
                  <cryptogram>string</cryptogram>
                  <!--Optional:-->
                  <eci>string</eci>
                  <!--Optional:-->
                  <requestorId>string</requestorId>
              </authorization>
            </authorizations>
          </arg0>
        </authorizationService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do AuthorizationResponse:

```
        <authorizationServiceResponse>
           <!--Optional:-->
           <authorizationResponse>
              <!--Optional:-->
              <result>
                 <!--Zero or more repetitions:-->
                 <result>
                    “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
                 </result>
              </result>
           </authorizationResponse>
        </authorizationServiceResponse>
```

3.2.3 MÉTODO CAPTURESERVICE

Executa a Captura da Autorização (Confirmação). O valor da transação a ser capturado pode ser igual ou menor (sem limitação) ao valor original autorizado.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
capture	ARRAY	R	1..n	Elemento raiz com as N transações.
capture	n/a	R	n/a	Elemento de cada transação.
capture.terminalID	AN	R	10	Ver *Regra para TerminalID*.
capture.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo de autorização.
capture.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
capture.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
capture.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
capture.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
capture.transactionID	N	R	18	Id da transação gerado pela Plataforma de E-Commerce e retornado no processo de autorização.
capture.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
capture.userDefinedField.udf1	AN	O	255	Campo disponível a partir da **versão 3.0.** Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis. Ver *Regra para UDF (userDefinedField)*.
capture.userDefinedField.udf2	AN	O	255	
capture.userDefinedField.udf3	AN	O	255	
capture.userDefinedField.udf4	AN	O	255	
capture.userDefinedField.udf5	AN	O	255	

O quadro a seguir demonstra as TAGs XML do “Service Request” do CaptureService:

```
<captureService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <capture>
      <!--Zero or more repetitions:-->
      <capture>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <amount>string</amount>
        <currencycode>string</currencycode>
        <instType>string</instType>
        <!--Optional:-->
```

```
                <instNum>string</instNum>
                <transactionID>string</transactionID>
                <!--Optional:-->
                <userDefinedField>
                  <!--Optional:-->
                  <udf1>string</udf1>
                  <!--Optional:-->
                  <udf2>string</udf2>
                  <!--Optional:-->
                  <udf3>string</udf3>
                  <!--Optional:-->
                  <udf4>string</udf4>
                  <!--Optional:-->
                  <udf5>string</udf5>
                </userDefinedField>
              </capture>
            </capture>
          </arg0>
        </captureService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do CaptureResponse:

```
        <captureServiceResponse>
           <!--Optional:-->
           <captureResponse>
              <!--Optional:-->
              <result>
                 <!--Zero or more repetitions:-->
                 <result>
                    “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
                 </result>
              </result>
           </captureResponse>
        </captureServiceResponse>
```

3.2.4 MÉTODO CANCELLATIONSERVICE

Executa o estorno de uma transação Autorizada ou Confirmada. Somente é possível estornar uma transação Confirmada (Capturada) no dia corrente. Se a transação ainda não foi confirmada, o prazo é de 7 dias corridos para o estorno e só é possível estonar transações com o valor total da autorização ou captura.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.

TAG	Tipo	Obrig.	Tam.	Descrição
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
cancel	ARRAY	R	1..n	Elemento raiz com as N transações.
cancel	n/a	R	n/a	Elemento de cada transação.
cancel.terminalID	AN	R	10	Ver *Regra para TerminalID*.
cancel.transactionID	N	R	18	Id da transação gerado pela Plataforma de E-Commerce e retornando no processo de Purchase/Autorização/Captura. Importante: Para estornar transações realizadas com a Action 1 ou 4 (Purchase ou Captura respectivamente), devemos utilizar o ID da transação original, ou seja, result.originalTransactionID que nada mais é que o ID da Autorização, pois o estorno só é realizado com o ID da Autorização e não da Confirmação (Captura).
cancel.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo anterior.
cancel.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
cancel.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
cancel.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
cancel.userDefinedField.udf1	AN	O	255	Campo disponível a partir da **versão 3.0.** Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis. Ver *Regra para UDF (userDefinedField)*.
cancel.userDefinedField.udf2	AN	O	255	
cancel.userDefinedField.udf3	AN	O	255	
cancel.userDefinedField.udf4	AN	O	255	
cancel.userDefinedField.udf5	AN	O	255	

O quadro a seguir demonstra as TAGs XML do “Service Request” do CancellationService:

```
<cancellationService>
   <!--Optional: -->
   <arg0>
      <authentication>
         <username>string</username>
         <password>string</password>
         <merchantID>string</merchantID>
      </authentication>
      <cancel>
         <!--Zero or more repetitions: -->
         <cancel>
            <terminalID>string</terminalID>
            <transactionID>string</transactionID>
            <merchantTrackID>string</merchantTrackID>
            <amount>string</amount>
            <currencycode>string</currencycode>
            <!--Optional:-->
            <userDefinedField>
               <!--Optional:-->
               <udf1>string</udf1>
               <!--Optional:-->
               <udf2>string</udf2>
```

```
                    <!--Optional:-->
                    <udf3>string</udf3>
                    <!--Optional:-->
                    <udf4>string</udf4>
                    <!--Optional:-->
                    <udf5>string</udf5>
                 </userDefinedField>
              </cancel>
           </cancel>
        </arg0>
     </cancellationService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do CancellationResponse:

```
     <cancellationServiceResponse>
        <!--Optional:-->
        <cancellationResponse>
           <!--Optional:-->
           <result>
              <!--Zero or more repetitions:-->
              <result>
                 “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
              </result>
           </result>
        </cancellationResponse>
     </cancellationServiceResponse>
```

3.2.5 MÉTODO QUERYDATASERVICE

Executa uma operação de Consulta do status da transação.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
query	ARRAY	R	1..n	Elemento raiz com as N transações.
query	n/a	R	n/a	Elemento de cada transação.
query.terminalID	AN	R	10	Ver *Regra para TerminalID*.
query.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo anterior.

O quadro a seguir demonstra as TAGs XML do “Service Request” do QueryDataService:

```
<queryDataService>
   <!--Optional:-->
   <arg0>
      <authentication>
         <username>string</username>
         <password>string</password>
         <merchantID>string</merchantID>
      </authentication>
      <query>
         <!--Zero or more repetitions:-->
         <query>
            <terminalID>string</terminalID>
            <merchantTrackID>string</merchantTrackID>
         </query>
      </query>
   </arg0>
</queryDataService>
```

O quadro a seguir demostra o XML do “Service Response” do QueryResponse:

```
<queryDataServiceResponse>
   <queryResponse>
      <!--Optional:-->
      <result>
         <!--Zero or more repetitions:-->
         <result>
           "Os retornos são sempre no objeto Result. Veja a Relação de TAGs de retorno"
         </result>
      </result>
   </queryResponse>
</queryDataServiceResponse>
```

3.2.6 MÉTODO CARDVERIFICATIONSERVICE

O objetivo da transação de verificação de cartão de crédito é verificar se o cartão de crédito informado pelo portador é um cartão válido.

Entende-se como um cartão crédito válido um cartão que não está cancelado, bloqueado ou com restrições.

Este método é muito utilizado para diminuir o risco e o trabalho operacional de revisão de pedidos/solicitações de compras.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
cardVerification	ARRAY	R	1..10	Elemento raiz com as N transações. **Este processo é limitado a 10 números de cartão.**
cardVerification	n/a	R	n/a	Elemento de cada transação.
cardVerification.terminalID	AN	R	10	Ver *Regra para TerminalID*.
cardVerification.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
cardVerification.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
cardVerification.card	n/a	R	1	Elemento com os dados do cartão.
cardVerification.card.number	N	R	0..19	Número do cartão do portador que será utilizado na verificação.
cardVerification.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
cardVerification.card.expiryMonth	N	R	2	Mês de expiração do cartão.
cardVerification.card.expiryYear	N	R	4	Ano de expiração do cartão.
cardVerification.card.holderName	AN	R	26	Nome do portador impresso no cartão.
cardVerification.softDescriptor	AN	O	22	Ver *Regra para Soft Descriptor*.

O quadro a seguir demonstra as TAGs XML do “Service Request” do CardVerificationService:

```
<cardVerificationService>
   <!--Optional: -->
   <arg0>
      <authentication>
         <username>string</username>
         <password>string</password>
         <merchantID>string</merchantID>
      </authentication>
      <cardVerification>
         <!--Zero or more repetitions: -->
         <cardVerification>
            <terminalID>string</terminalID>
            <merchantTrackID>string</merchantTrackID>
            <currencycode>string</currencycode>
            <card>
               <number>string</number>
               <!--Optional:-->
               <cvv2>string</cvv2>
               <expiryMonth>string</expiryMonth>
               <expiryYear>string</expiryYear>
               <holderName>string</holderName>
            </card>
            <!--Optional:-->
            <softDescriptor>string</softDescriptor>
         </cardVerification>
      </cardVerification>
   </arg0>
</cardVerificationService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do CardVerificationResponse:

```
<cardVerificationServiceResponse>
   <!--Optional:-->
   <cardVerificationResponse>
      <!--Optional:-->
      <result>
         <!--Zero or more repetitions:-->
         <result>
            “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
         </result>
      </result>
   </cardVerificationResponse>
</cardVerificationServiceResponse>
```

3.2.7 MÉTODO PREAUTHORIZATIONSERVICE

Executa uma Pré-Autorização, sem a Confirmação (Captura). A transação, se autorizada, se mantêm pendente de Confirmação.

Esta transação tem o mesmo processo de autorização e confirmação de uma Autorização, diferenciando apenas na classificação da transação no Base I e Base II. E também nos prazos de confirmação, que hoje, para uma Pré-Autorização, são 30 dias, enquanto para uma Autorização são 7 dias.

A tabela a seguir detalha cada uma das TAGs do XML a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual
authentication.username	AN	R	20	Usuário de acesso
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
authorizations	ARRAY	R	1..n	Elemento raiz com as N transações.
authorization	n/a	R	1	Elemento de cada transação.
authorization.terminalID	AN	R	10	Ver *Regra para TerminalID*.
authorization.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
authorization.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
authorization.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
authorization.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
authorization.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
authorization.tranCategory	AN	R	4	Campo disponível a partir da **versão 2.0.** Identifica a categoria da transação a ser efetuado: **DFLT** – Todas **IATA** – Transações destinadas a Cias Aéreas Ver *Regra para TranCategory*.
authorization.card	n/a	R	1	Elemento com os dados do cartão.
authorization.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
authorization.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
authorization.card.expiryMonth	N	R	2	Mês de expiração do cartão.
authorization.card.expiryYear	N	R	4	Ano de expiração do cartão.
authorization.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authorization.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
authorization.userDefinedField.udf1	AN	O	255	Campos de apoio e alternativos na transação, qualquer conteúdo pode ser
authorization.userDefinedField.udf2	AN	O	255	

TAG	Tipo	Obrig.	Tam.	Descrição
authorization.userDefinedField.udf3	AN	O	255	informado e recuperado nestas variáveis. Ver *Regra para UDF (userDefinedField)*.
authorization.userDefinedField.udf4	AN	O	255	
authorization.userDefinedField.udf5	AN	O	255	
authorization.xid	AN	O	40	Campo disponível a partir da **versão 2.0.** Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authorization.ucaf	AN	O	40	Campo disponível a partir da **versão 2.0.** Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authorization.eci	N	O	2	Campo disponível a partir da **versão 2.0.** Código ECI da transação Autenticada 3D Secure. Gerado por um MPI Externo. Ver processo.
authorization.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authorization.softDescriptor	AN	O	22	Ver *Regra para Soft Descriptor*.
authorization.addlReqData	AN	O	255	Campo disponível a partir da **versão 2.0.** Ver *Regras para AddlReqData*.
purchase. tdsver	N	O		Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização.
purchase. tdsdsxid	AN	O		Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.

O quadro a seguir demonstra as TAGs XML do “Service Request” do PreAuthorizationService:

```
<preAuthorizationService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <authorizations>
      <!--Zero or more repetitions:-->
      <authorization>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <amount>string</amount>
        <currencycode>string</currencycode>
        <instType>string</instType>
        <!--Optional:-->
        <instNum>string</instNum>
        <tranCategory>string</tranCategory>
        <card>
          <number>string</number>
          <!--Optional:-->
```

```
                <cvv2>string</cvv2>
                <expiryMonth>string</expiryMonth>
                <expiryYear>string</expiryYear>
                <holderName>string</holderName>
              </card>
              <!--Optional:-->
              <userDefinedField>
                <!--Optional:-->
                <udf1>string</udf1>
                <!--Optional:-->
                <udf2>string</udf2>
                <!--Optional:-->
                <udf3>string</udf3>
                <!--Optional:-->
                <udf4>string</udf4>
                <!--Optional:-->
                <udf5>string</udf5>
              </userDefinedField>
              <!--Optional:-->
              <xid>string</xid>
              <!--Optional:-->
              <ucaf>string</ucaf>
              <!--Optional:-->
              <eci>string</eci>
              <!--Optional:-->
              <tranMCC>string</tranMCC>
              <!--Optional:-->
              <softDescriptor>string</softDescriptor>
              <!--Optional:-->
              <addlReqData>string</addlReqData>
               <!--Optional:-->
              <recurringseqid>string</recurringseqid>
               <!--Optional:-->
              <tdsver>string</tdsver>
               <!--Optional:-->
              <tdsdsxid>string</tdsdsxid>
            </authorization>
          </authorizations>
        </arg0>
      </preAuthorizationService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do AuthorizationResponse:

```
      <preAuthorizationServiceResponse>
         <!--Optional:-->
         <authorizationResponse>
            <!--Optional:-->
            <result>
               <!--Zero or more repetitions:-->
               <result>
                  “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
               </result>
```

```
            </result>
        </authorizationResponse>
    </preAuthorizationServiceResponse>
```

3.2.8 MÉTODO CAPTUREPREAUTHSERVICE

Executa a Captura da Pré-Autorização (Confirmação). O valor da confirmação pode ser igual ou menor (sem limitação) ao valor original.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
capture	ARRAY	R	1..n	Elemento raiz com as N transações.
capture	n/a	R	n/a	Elemento de cada transação.
capture.terminalID	AN	R	10	Ver *Regra para TerminalID*.
capture.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo de autorização.
capture.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
capture.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
capture.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
capture.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
capture.transactionID	N	R	18	Id da transação gerado pela Plataforma de E-Commerce e retornado no processo de autorização.

O quadro a seguir demonstra as TAGs XML do “Service Request” do CapturePreAuthService:

```
<capturePreAuthService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <capture>
      <!--Zero or more repetitions:-->
      <capture>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <amount>string</amount>
```

```
                <currencycode>string</currencycode>
                <instType>string</instType>
                <!--Optional:-->
                <instNum>string</instNum>
                <transactionID>string</transactionID>
              </capture>
            </capture>
          </arg0>
        </capturePreAuthService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do CapturePreAuthServiceResponse:

```
        <capturePreAuthServiceResponse>
           <!--Optional:-->
           <captureResponse>
              <!--Optional:-->
              <result>
                 <!--Zero or more repetitions:-->
                 <result>
                    “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
                 </result>
              </result>
           </captureResponse>
        </capturePreAuthServiceResponse>
```

3.2.9 MÉTODO ADJUSTMENTPREAUTHSERVICE

Executa um ajuste (Incremento/Decremento) no valor previamente reservado no saldo do Portador por uma Transação de Pré-Autorização. O valor da Transação de Ajuste de Pré-Autorização pode ser maior ou menor que o valor original. Na chamada do processo de ajuste sempre deve ser enviado o valor final desejado no campo de valor.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
adjustmentsPreAuth	ARRAY	R	1..n	Elemento raiz com as N transações.
adjustmentsPreAuth	n/a	R	n/a	Elemento de cada transação.
adjustmentsPreAuth.terminalID	AN	R	10	Ver *Regra para TerminalID*.

TAG	Tipo	Obrig.	Tam.	Descrição
adjustmentsPreAuth.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo de autorização.
adjustmentsPreAuth.transactionID	N	R	18	Id da transação gerado pela Plataforma de E-Commerce e retornado no processo de autorização.
adjustmentsPreAuth.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
adjustmentsPreAuth.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
adjustmentsPreAuth.card	n/a	R	1	Elemento com os dados do cartão.
adjustmentsPreAuth.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
adjustmentsPreAuth.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
adjustmentsPreAuth.card.expiryMonth	N	R	2	Mês de expiração do cartão.
adjustmentsPreAuth.card.expiryYear	N	R	4	Ano de expiração do cartão.
adjustmentsPreAuth.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authorization.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authorization.softDescriptor	AN	O	22	Ver *Regra para Soft Descriptor*.

O quadro a seguir demonstra as TAGs XML do “Service Request” do CapturePreAuthService:

```
<adjustmentPreAuthService >
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    < adjustmentsPreAuth>
      <!--Zero or more repetitions:-->
      <adjustmentsPreAuth>
        <terminalID>string</terminalID>
        <merchantTrackID>string</merchantTrackID>
        <transactionID>string</transactionID>
        <amount>string</amount>
        <currencycode>string</currencycode>
        <card>
          <number>string</number>
          <!--Optional:-->
          <cvv2>string</cvv2>
          <expiryMonth>string</expiryMonth>
          <expiryYear>string</expiryYear>
          <holderName>string</holderName>
        </card>
        <!--Optional:-->
        <tranMCC>string</tranMCC>
        <!--Optional:-->
        <softDescriptor>string</softDescriptor>
```

```
            </adjustmentsPreAuth >
          </adjustmentsPreAuth >
        </arg0>
      </adjustmentPreAuthService >
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do CapturePreAuthServiceResponse:

```
      <capturePreAuthServiceResponse>
         <!--Optional:-->
         <captureResponse>
            <!--Optional:-->
            <result>
               <!--Zero or more repetitions:-->
               <result>
                  “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno”
               </result>
            </result>
         </captureResponse>
      </capturePreAuthServiceResponse>
```

3.2.10 MÉTODO CANCELLATIONPREAUTHSERVICE

Executa o estorno de uma transação de Pré-Autorização ou Confirmada.

Somente é possível estornar uma transação confirmada (Capturada) **no dia corrente**.

A tabela a seguir detalha cada uma das TAGs do XML, a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
authentication	n/a	R	n/a	Elemento raiz para identificação da Loja Virtual.
authentication.username	AN	R	20	Usuário de acesso.
authentication.password	AN	R	40	Senha de acesso. Ver *Regra para Caracteres Especiais*.
authentication.merchantID	N	R	10	Código de EC cadastrado na GETNET.
cancel	ARRAY	R	1..n	Elemento raiz com as N transações.
cancel	n/a	R	n/a	Elemento de cada transação.
cancel.terminalID	AN	R	10	Ver *Regra para TerminalID*.

TAG	Tipo	Obrig.	Tam.	Descrição
cancel.transactionID	N	R	18	Id da transação gerado pela Plataforma de E-Commerce e retornado no processo de Purchase/Autorização/Captura. Importante: Para estornar transações realizadas com a Action 1 ou 4 (Purchase ou Captura respectivamente), devemos utilizar o ID da transação original, ou seja, result.originalTransactionID que nada mais é que o ID da Autorização, pois o estorno só é realizado com o ID da Autorização e não da Confirmação (Captura).
cancel.merchantTrackID	AN	R	40	ID da transação que foi gerado pela loja virtual e informado no processo anterior.
cancel.amount	N	R	12	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
cancel.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.

O quadro a seguir demonstra as TAGs XML do “Service Request” do CancellationPreAuthService:

```
<cancellationPreAuthService>
   <!--Optional: -->
   <arg0>
      <authentication>
         <username>string</username>
         <password>string</password>
         <merchantID>string</merchantID>
      </authentication>
      <cancel>
         <!--Zero or more repetitions: -->
         <cancel>
            <terminalID>string</terminalID>
            <transactionID>string</transactionID>
            <merchantTrackID>string</merchantTrackID>
            <amount>string</amount>
            <currencycode>string</currencycode>
         </cancel>
      </cancel>
   </arg0>
</cancellationPreAuthService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do AuthorizationResponse:

```
      <authorizationServiceResponse>
         <!--Optional:-->
         <authorizationResponse>
            <!--Optional:-->
            <result>
               <!--Zero or more repetitions:-->
               <result>
                  "Os retornos são sempre no objeto Result. Veja a Relação de TAGs de
retorno"
               </result>
            </result>
         </authorizationResponse>
      </authorizationServiceResponse>
```

3.2.11 Método tokenService

Método que gera um Token para iniciar o processo de autenticação. Obrigatório processo para abrir sessão (15 min) com a Bandeira/Emissor. (veja o documento Manual 3DS 2.1).

3.2.12 Método authenticationEnrollmentService

Método que solicita a autenticação para o 3DS Requestor. (veja o documento Manual 3DS 2.1).

3.2.13 Método validateAuthenticationService

Método que será executado se tiver desafio. Valia se o desafio foi completado com sucesso. (veja o documento Manual 3DS 2.1).

3.2.14 Relação de TAGs de retorno

A tabela a seguir representa as TAGs do XML de retorno:

TAG	Tipo	Descrição
result	n/a	Elemento com os dados de todas as transações do mesmo pedido.
result	ARRAY	Elemento com os dados de cada transação realizada.
result.transactionID	N	Id da transação gerado pela Plataforma de E-Commerce. Este parâmetro é único para cada transação processada.
result.originalTransactionID	N	Retorna o Id da transação associada a transação sendo realizada.
result.merchantTrackID	AN	ID da transação que foi gerado pela loja virtual e informado na autorização.

<table>
<tr><th>TAG</th><th>Tipo</th><th>Descrição</th></tr>
<tr><td>result.descriptionResponse</td><td>A</td><td>Representação do resultado junto à operadora.
Possíveis retornos:
APPROVED (Aprovado)
NOT APPROVED (Não Aprovada)
CAPTURED (Confirmada)
NOT CAPTURED (Não Confirmada)
VOIDED (Cancelada)
NOT VOIDED (Não Cancelada)
VERIFIED (Cartão válido)
NOT VERIFIED (Cartão inválido)</td></tr>
<tr><td>result.responseCode</td><td>N</td><td>Códigos de Resposta do Emissor do Cartão e do Sistema de Captura da GETNET.
(Veja os Códigos de Retorno do Emissor / Getnet)</td></tr>
<tr><td>result.responseMessage</td><td>AN</td><td>Descrição do motivo do Código de Resposta.
(A descrição é a mesma que consta na listagem de Códigos de Retorno do Emissor / Getnet)</td></tr>
<tr><td>result.errorCodeTag</td><td>AN</td><td>Código de erro gerado pela Plataforma de E-Commerce.
(Veja os Códigos de Retorno da Plataforma de E-Commerce)</td></tr>
<tr><td>result.descriptionError</td><td>NA</td><td>Descrição da mensagem de erro gerado pela Plataforma de E-Commerce.
(Veja os Códigos de Retorno da Plataforma de E-Commerce)</td></tr>
<tr><td>result.cvv2response</td><td>AN</td><td>Valor retornado referente a validação do campo CVV2</td></tr>
<tr><td>result.eci</td><td></td><td>Campo disponível a partir da versão 3DS 2.0, mas reflete na versão anterior, autenticação 3DS 1.0
Código indicando se a transação foi processada com Autenticação do Portador. *00, 01 e 02 para Mastercard e 05, 06 e 07 para Visa e demais bandeiras.
<table>
<tr><th>VISA</th><th>MASTERCARD</th><th>Descrição</th></tr>
<tr><td>05</td><td>02</td><td>Risco emissor: Sucesso na autenticação 3DS;</td></tr>
<tr><td>06</td><td>01</td><td>Risco emissor: Solicitação de autenticação recebida, mas não pode ser completada;</td></tr>
<tr><td>07</td><td>00</td><td>Risco estabelecimento: Autenticação falhou por motivos variados relacionados ao cartão, emissor ou mesmo problemas técnicos ou configuração.</td></tr>
</table></td></tr>
<tr><td>result.xid</td><td></td><td>Campo disponível a partir da versão 2.0.
Quando de uma transação 3DS o seu retorno é o identificador do MPI da transação Autenticada.
O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.</td></tr>
<tr><td>result.ucaf</td><td></td><td>Campo disponível a partir da versão 2.0.
Quando de uma transação 3DS o seu retorno é o código de autenticação criptografado pela Bandeira.
O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.</td></tr>
<tr><td>result.paymentid</td><td></td><td>Campo disponível a partir da versão 2.0.
ID exclusivo gerada no momento da solicitação à Plataforma de E-Commerce, para identificar a operação de Autenticação.</td></tr>
<tr><td>result.auth</td><td>N</td><td>Código de Autorização gerado pelo Emissor quando a transação é realizada com sucesso.</td></tr>
<tr><td>result.ref</td><td>N</td><td>Valor referente ao NSU da transação da GETNET. Este campo é o número do Comprovante de Venda (CV) da Autorização. Campos este para identificação das transações em outros canais da GETNET.
Considerar as 9 últimas posições.</td></tr>
<tr><td>result.postdate</td><td>A</td><td>Data (MMDD) realização da transação</td></tr>
</table>

TAG	Tipo	Descrição
result.authorizationDateTime	AN	Campo disponível a partir da **versão 2.0.** Retorna a data do pedido de autorização. Padrão de formatação "dd/MM/yyyyThh:mm:ss.SSS"
result.udf1	A	Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis.
result.udf2	A	
result.udf3	A	
result.udf4	A	
result.udf5	A	
result.instAmt1	N	Para as transações parceladas, este contém o valor da primeira parcela a ser paga.
result.instAmtN	N	Para as transações parceladas, este contém o valor das demais parcelas a serem pagas.
result.instAmtT	N	Para as transações parceladas, este contém o valor total a ser pago (valor acrescido dos juros, impostos, taxas, etc).
result.amout	N	Retorna o valor da transação da transação que foi realizada.
result.currencycode	N	Retorna o código da moeda da transação que foi realizada.
result.instType	N	Identifica o tipo de pagamento efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
result.instNum	N	Retorna o número de parcelas da transação que foi realizada.
result.tranMCC	N	Retorna o tranMCC da transação que foi realizada.
result.softDescriptor	AN	Retorna o SoftDescriptor da transação que foi realizada.
result.addlResData	AN	Campo disponível a partir da **versão 2.0.** Retorna informações adicionais para o Lojista, podendo ser: ***MCC Dinâmico*** **TranMCC** – Quando o valor enviado para o MCC Dinâmico não estiver de acordo com a Regra de utilização, o Adquirente irá utilizar o valor corretor e informará neste campo o valor usado; ***Soft Descriptor*** **TranSD** – Quando o valor enviado para o Soft Descriptor não estiver de acordo com a Regra de utilização, o Adquirente irá utilizar o valor corretor e informará neste campo o valor usado; ***Ajustes de Pré-Autorização*** **4352** – Quando é feito um ajuste no valor da transação de Pré-Autorização, neste campo é informado o valor anterior ao ajuste; **4353** – Quando é feito um ajuste no valor da transação, neste campo é informado o valor do REF da transação Original;
result.instIssCet	N	Para as transações parceladas emissor, indica a taxa de juros anual da instituição financeira.
result.instIssRate	N	Para as transações parceladas emissor, indica os encargos mensais da instituição financeira.
result.instIssRqstv	N	Para as transações parceladas emissor, indica o valor liberado.
result.instIssRqstp	N	Para as transações parceladas emissor, indica a porcentagem do valor liberado.
result.instIssChrgv	N	Para as transações parceladas emissor, indica o valor das despesas vinculadas.
result.instIssChrgp	N	Para as transações parceladas emissor, indica a porcentagem das despesas vinculadas.
result.instIssFeev	N	Para as transações parceladas emissor, indica o valor das tarifas.
result.instIssFeep	N	Para as transações parceladas emissor, indica a porcentagem das tarifas.
result.instIssTaxv	N	Para as transações parceladas emissor, indica o valor dos tributos.
result.instIssTaxp	N	Para as transações parceladas emissor, indica a porcentagem dos tributos.
result.instIssInsv	N	Para as transações parceladas emissor, indica o valor do seguro.
result.instIssInsp	N	Para as transações parceladas emissor, indica a porcentagem do seguro.
result.instIssOthrv	N	Para as transações parceladas emissor, indica o valor de outras despesas.

TAG	Tipo	Descrição
result.instIssOthrp	N	Para as transações parceladas emissor, indica a porcentagem de outras despesas.
result.instIssTotv	N	Para as transações parceladas emissor, indica o valor total emprestado.
result.instIssTotp	N	Para as transações parceladas emissor, indica a porcentagem do valor total emprestado.
result.wsErrorCode	AN	Código de erro gerado no Webservice. (Veja os *Códigos de Retorno do WebService*)
result.wsErrorText	AN	Descrição do erro gerado no Webservice. (Veja os *Códigos de Retorno do WebService*)
result.brand	AN	Retorna a Bandeira da transação.
result.brandType	AN	Retorno para informar se a transação executada foi através de um cartão Pré-Pago. Caso esse retorno seja recebido, a liquidação dessa transação será realizada em D+2. Exemplo pattern: (^(..)(-PP)$). Consulte o anexo
result.eciStatus	N	Retorna o ECI que foi acatado no processo de autorização/autenticação. Caso o ECI seja diferente do enviado na requisição de autorização, significa que o ECI foi reclassificado.
result.tokenStatus	AN	Para transações Tokenizada Visa - TAVV, será retornado o Status da operação, onde: U: Qualificação indefinido Y: Qualificado para Token Visa N: Não Qualificado para Serviço de Token Visa
result.mrchAdviceMsg	AN	MAC - Merchant Advice Code Mastercard – Código complementar ao responseCode exclusivo para a bandeira Mastercard. Sua combinação com o responseCode sugere se a transação pode ser retentada ou não. (Veja os *Códigos MAC – Merchant Advice Code Mastercard)*

O quadro a seguir demostra o XML do “Service Response”:

```
<...ServiceResponse>
   <!--Optional:-->
   <...Response>
      <!--Optional:-->
      <result>
         <!--Zero or more repetitions:-->
         <result>
            <!--Optional:-->
            <transactionID>string</transactionID>
            <!--Optional:-->
            <originalTransactionID>string</originalTransactionID>
            <!--Optional:-->
            <merchantTrackID>string</merchantTrackID>
            <!--Optional:-->
            <descriptionResponse>string</descriptionResponse>
            <!--Optional:-->
            <responseCode>string</responseCode>
            <!--Optional:-->
            <errorCodeTag>string</errorCodeTag>
            <!--Optional:-->
            <descriptionError>string</descriptionError>
            <!--Optional:-->
            <cvv2response>string</cvv2response>
```

```
<!--Optional:-->
<eci>?</eci>
<!--Optional:-->
<xid>?</xid>
<!--Optional:-->
<ucaf>?</ucaf>
<!--Optional:-->
<paymentid>?</paymentid>
<!--Optional:-->
<auth>string</auth>
<!--Optional:-->
<ref>string</ref>
<!--Optional:-->
<postdate>string</postdate>
<!--Optional:-->
<authorizationDateTime>string</authorizationDateTime>
<!--Optional:-->
<udf1>string</udf1>
<!--Optional:-->
<udf2>string</udf2>
<!--Optional:-->
<udf3>string</udf3>
<!--Optional:-->
<udf4>string</udf4>
<!--Optional:-->
<udf5>string</udf5>
<!--Optional:-->
<instAmt1>string</instAmt1>
<!--Optional:-->
<instAmtN>string</instAmtN>
<!--Optional:-->
<instAmtT>string</instAmtT>
<!--Optional:-->
<instRate>string</instRate>
<!--Optional:-->
<instCET>string</instCET>
<!--Optional:-->
<amout>string</amout>
<!--Optional:-->
<currencycode>string</currencycode>
<!--Optional:-->
< instType>string</instType>
<!--Optional:-->
<instNum>string</instNum>
<!--Optional:-->
<tranMCC>string</tranMCC>
<!--Optional:-->
< softDescriptor>string</softDescriptor>
<!--Optional:-->
<addlResData>string</addlResData>
<!--Optional:-->
<instIssCet>string</instIssCet>
<!--Optional:-->
<instIssRate>string</instIssRate>
<!--Optional:-->
<instIssRqstv>string</instIssRqstv>
<!--Optional:-->
<instIssRqstp>string</instIssRqstp>
<!--Optional:-->
<instIssChrgv>string</instIssChrgv>
```

```
                <!--Optional:-->
                <instIssChrgp>string</instIssChrgp>
                <!--Optional:-->
                <instIssFeev>string</instIssFeev>
                <!--Optional:-->
                <instIssFeep>string</instIssFeep>
                <!--Optional:-->
                <instIssTaxv>string</instIssTaxv>
                <!--Optional:-->
                <instIssTaxp>string</instIssTaxp>
                <!--Optional:-->
                <instIssInsv>string</instIssInsv>
                <!--Optional:-->
                <instIssInsp>string</instIssInsp>
                <!--Optional:-->
                <instIssOthrv>string</instIssOthrv>
                <!--Optional:-->
                <instIssOthrp>string</instIssOthrp>
                <!--Optional:-->
                <instIssTotv>string</instIssTotv>
                <!--Optional:-->
                <instIssTotp>string</instIssTotp>
                <!--Optional:-->
                <wsErrorCode>string</wsErrorCode>
                <!--Optional:-->
                <wsErrorText>string</wsErrorText>
                <!--Optional:-->
                <brand>string</brand>
                <!--Optional:-->
                <brandType>string</brandType>
                <!--Optional:-->
                <eciStatus>string</eciStatus>
                <!--Optional:-->
                <tokenStatus>string</tokenStatus>
                <!--Optional:-->
                <mrchAdviceMsg>string</mrchAdviceMsg>
            </result>
        </result>
    </...Response>
</...ServiceResponse>
```

3.2.15 Relação de TAGs de retorno de operações Autenticadas (3D Secure)

A tabela a seguir apresenta as TAGs do XML de retorno para operações de Autenticação (3D Secure):

TAG	Tipo	Descrição
result	n/a	Elemento com os dados do pedido.
result.transactionID	N	Id da transação gerado pela Plataforma de E-Commerce. Este parâmetro é único para cada transação processada.

TAG	Tipo	Descrição
result.merchantTrackID	AN	ID da transação que foi gerado pela loja virtual e informado na autorização.
result.descriptionResponse	A	Representação do resultado junto à operadora. Possíveis retornos: **ENROLLED** (Participante) **NOT ENROLLED** (Não Participante)
result.errorCodeTag	AN	Código de erro gerado pela Plataforma de E-Commerce. (Veja os *Códigos de Retorno da Plataforma de E-Commerce*)
result.descriptionError	NA	Descrição da mensagem de erro gerado pela Plataforma de E-Commerce. (Veja os *Códigos de Retorno da Plataforma de E-Commerce*)
result.PAReq	AN	Campo a ser enviado para o Emissor, onde contém as informações previamente validadas pela Plataforma de E-Commerce com o Emissor. Este campo deve ser enviado para o endereço (URL) retornado.
result.url	AN	URL com o endereço do site do Emissor para que o Portador informe os dados necessários para a Autenticação.
result.paymentid	AN	ID exclusivo gerada no momento da solicitação à Plataforma de E-Commerce, para identificar a operação de Autenticação. Este campo deve ser enviado para o endereço (URL) retornado.
result.eci	N	Código indicando se a transação foi processada com Autenticação do Portador. VISA / MASTERCARD: 05 / 02 — Status da Autentição: Sim — Descrição: Autenticada VISA / MASTERCARD: 06 / 01 — Status da Autentição: Não — Descrição: Emissor/portador não participa do 3DSecure VISA / MASTERCARD: 07 / 00 — Status da Autentição: Não — Descrição: Não autenticada
result.wsErrorCode	AN	Código de erro gerado no Webservice. (Veja os *Códigos de Retorno do WebService*)
result.wsErrorText	AN	Descrição do erro gerado no Webservice. (Veja os *Códigos de Retorno do WebService*)

O quadro a seguir demostra o XML do “Service Response”:

```
<...ServiceResponse>
   <!--Optional:-->
   <...Response>
      <!--Optional:-->
      result>
        <!--Optional:-->
        <transactionID>string</transactionID>
        <!--Optional:-->
        <merchantTrackID>string</merchantTrackID>
        <!--Optional:-->
        <descriptionResponse>string</descriptionResponse>
        <!--Optional:-->
        <responseCode>string</responseCode>
        <!--Optional:-->
        <errorCodeTag>string</errorCodeTag>
        <!--Optional:-->
        <descriptionError>string</descriptionError>
        <!--Optional:-->
        <PARreq>string</PARreq>
```

```
            <!--Optional:-->
            <url>string</url>
            <!--Optional:-->
            <paymentid>string</paymentid>
            <!--Optional:-->
            <eci>string</eci>
            <!--Optional:-->
            <wsErrorCode>string</wsErrorCode>
            <!--Optional:-->
            <wsErrorText>string</wsErrorText>
         </result>
      </...Response>
   </...ServiceResponse>
```

3.3 Interfaces de Integração dos Serviços Administrativos

Nessa seção serão detalhadas as funcionalidades (métodos) disponíveis nos serviços Administrativos (AdministrationService) para o desenvolvedor realizar a integração da loja virtual com o sistema de Gerenciamento de Segurança da GetNet.

O modelo empregado é bastante simples: há uma única URL que recebe os POSTS via HTTPS e, dependendo das informações do XML enviado uma determinada operação é realizada.

Cada uma das operações disponíveis é apresentada nas sessões seguintes.

3.3.1 Método ChangeAuthenticationService

Por segurança ao cadastrar uma nova Loja Virtual, a GetNet obriga a Loja Virtual a alterar seu código de acesso antes de iniciar o fluxo transacional.

A tabela a seguir detalha cada uma das TAGs do XML a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
username	AN	R	20	Usuário de acesso
merchantID	N	R	10	Código de EC cadastrado na GetNet.
currentPassword	AN	R	40	Senha atual de acesso. Veja a *Regra para Caracteres Especiais*.
newPassword	AN	R	40	Nova senha de acesso. Veja a *Regra de Preenchimento da Nova Senha*.

O quadro a seguir demonstra as TAGs XML do “Service Request” do changeAuthenticationService:

```
<changeAuthenticationService>
  <arg0>
      <username>string</username>
      <merchantID>string</merchantID>
      <currentPassword>string</currentPassword>
      <newPassword>string</newPassword>
  </arg0>
</changeAuthenticationService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do changeAuthenticationResponse:

```
<changeAuthenticationServiceResponse>
   <changeAuthenticationResponse>
      <result>string</result>
      <description>string</description>
      <wsErrorCode>string</wsErrorCode>
      <wsErrorText>string</wsErrorText>
   </changeAuthenticationResponse>
</changeAuthenticationServiceResponse>
```

3.3.2 MÉTODO CHANGEKEYSSERVICE

Por segurança a Loja Virtual pode optar por enviar os dados sensíveis criptografados no fluxo transacional. Para isto a Loja Virtual deve ter optado por este processo no momento da sua habilitação.

Tendo optado, a Loja Virtual dispõe do serviço de alteração das chaves de criptografia, tornando o processo mais seguro.

A tabela a seguir detalha cada uma das TAGs do XML a serem enviadas na chamada da transação:

TAG	Tipo	Obrig.	Tam.	Descrição
username	AN	R	20	Usuário de acesso
password	AN	R	40	Senha de acesso
merchantID	N	R	10	Código de EC cadastrado na GetNet.
key	AN	R		Chave de criptografia. Veja a *Regra de Preenchimento da Chave de* Segurança.
Iv	AN	R		Vetor de inicialização (IV). Veja a *Regra de Preenchimento da Chave de* Segurança.

O quadro a seguir demonstra as TAGs XML do “Service Request” do changeKeysService:

```
<changeKeysService>
  <arg0>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
      <key>string</key>
      <iv>string</iv>
  </arg0>
</changeKeysService>
```

O quadro a seguir demonstra as TAGs XML do “Service Response” do changeKeysServiceResponse:

```
<changeKeysServiceResponse>
   <changeKeysResponse>
      <result>string</result>
      <description>string</description>
      <wsErrorCode>string</wsErrorCode>
      <wsErrorText>string</wsErrorText>
   </changeKeysResponse>
</changeKeysServiceResponse>
```

3.4 Regras Gerais

Nesta seção são apresentadas as regras gerais, comuns a todos os métodos.

3.4.1 Regra para TerminalID

O TerminalID é utilizado como parte da chave que identifica uma transação.

Ele é composto por um campo Alfanumérico de **8** posições e **2** dígitos adicionais que identificam o produto e a Bandeira.

Exemplo: **D123456799** / **E123456799**

Campo	Descritivo
D	E-Commerce WEB Não Autenticado
E	E-Commerce WEB Autenticado e não autenticado
R	E-Commerce WEB Recorrência Não Autenticado
1234567	Identificação do Terminal
99	Identificação do Produto e da Bandeira

Existe um mapeamento 1:1 entre o Terminal e o seu perfil (Bandeira). Assim, cada sufixo de 2 dígitos está mapeado para um único perfil de Terminal que vai definir as moedas, transações, opções de processamento e instrumentos de pagamento válidos para aquele terminal.

Devido esta relação entre Terminal e perfil, é necessário usar o **TerminalID** correto para a operação que está sendo feita, ou a transação será negada. Por exemplo, se o Terminal é '**D1234567**', e pretende-se fazer uma transação de Crédito da Visa, o estabelecimento deve usar '**D12345670 1**' como TerminalID da transação.

A seguir são apresentados os possíveis sufixos (identificações de Produto e Bandeira) que devem ser utilizados na formação do TerminalID.

Quando usar?	Prefixo	Sufixo	TerminalID
Para as transações de Visa Crédito não autenticado	D	01	D12345670 1
Para as transações de MasterCard Crédito não autenticado	D	02	D12345670 2
Para as transações de Visa Electron Débito não autenticado (se disponível)	D	03	D12345670 3
Para as transações de Maestro Débito não autenticado (se disponível)	D	04	D12345670 4
Para transações ELO Crédito não autenticado	D	07	D12345670 7
Para transações ELO Débito não autenticado	D	08	D12345670 8
Para transações American Express Crédito não autenticado	D	09	D12345670 9
Para transações Hipercard Crédito não autenticado	D	12	D12345671 2
Para as transações de Visa Crédito Autenticado e não autenticado	E	01	E12345670 1
Para as transações de MasterCard Crédito Autenticado e não autenticado	E	02	E12345670 2
Para as transações de Visa Electron Débito Autenticado e não autenticado (se disponível)	E	03	E12345670 3
Para as transações de Maestro Débito Autenticado e não autenticado (se disponível)	E	04	E12345670 4
Para transações ELO Crédito Autenticado e não autenticado	E	07	E12345670 7
Para transações ELO Débito Autenticado e não autenticado (se disponível)	E	08	E12345670 8
Para transações American Express Crédito não autenticado	E	09	E12345670 9
Para transações Hipercard Crédito não autenticado	E	12	E12345671 2
Para as transações de Visa Crédito Recorrência	R	01	R12345670 1
Para as transações de MasterCard Recorrência	R	02	R12345670 2
Para transações ELO Crédito Recorrência	R	07	R12345670 7
Para transações American Express Recorrência	R	09	R12345670 9
Para transações Hipercard Recorrência	R	12	R12345671 2

3.4.2 Regra para Soft Descriptor

O Soft Descriptor possibilita que seja enviada nas transações a informação de identificação que deseja que apareça no campo nome fantasia. Como exemplo, pode-se ter o nome do Estabelecimento Comercial que está no cadastro da Adquirência mais o nome do intermediador que está recebendo o pagamento.

Ex: GatewayPagto*Loja. Ou a identificação do departamento da loja. Ex: Loja*Departamento ou Loja*SubLoja. Esta informação é a que será informada na fatura do portador do cartão.

Caso não seja informado um Soft Descriptor, será utilizado o nome fantasia do Cadastro do Estabelecimento Comercial.

Seguem os caracteres cujo uso é permitido ou não no Soft Descriptor:

- **Caracteres permitidos**
  - A-Z (letras maiúsculas);
  - 0123456789;
  - Exclusivamente estes caracteres especiais:
    % $, . / ( ) + = - * (Veja a *Regra para Caracteres Especiais*)
- **Caracteres não permitidos**
  - a-z (letras minúsculas);
  - acentuações (qualquer caractere acentuado, maiúsculo ou minúsculo);
  - c cedilha (ç);
  - caracteres especiais:
    ! ? : ; [ ] { } ' " # _ @ § ^ ~ ¨ \ & < >

3.4.3 Regra para UDF (userDefinedField)

O *userDefinedField* (Campo definido pelo Cliente) possibilita que sejam enviadas nas transações as informações que a Loja deseja identificar a transação. Este pode ser enviado até 5 campos, definidos como udf1, udf2, udf3, udf4 e udf5. Como exemplo, pode-se ter o nome do Cliente, o número do Pedido, o e-mail do cliente, ou outros dados desejados. Estes dados não são enviados para Bandeira/Emissor, ficando apenas gravados na Base do eCommerce da GetNet.

Seguem os caracteres cujo uso é permitido ou não no userDefinedField:

- **Caracteres permitidos**
  - a-zA-Z (letras minúsculas/maiúsculas);
  - 0123456789;
  - caracteres especiais:
  - @ : % $ & , . + = < > - (Veja a *Regra para Caracteres Especiais*)
- **Caracteres não permitidos**
  - acentuações (qualquer caractere acentuado, maiúsculo ou minúsculo);
  - c cedilha (ç);
  - caracteres especiais:
    ~ ` ! # ^ | \ ' " /

3.4.4 Regra para MCC Dinâmico

O MCC permite que o Estabelecimento Comercial realize a venda de diversos tipos de produtos/serviços de segmentos diferentes, possibilitando a identificação do correto ramo de atividade para cada transação efetuada.

Dessa forma uma loja pode identificar ao Adquirente o MCC de cada compra, seja uma compra de eletroeletrônico, seja uma compra de livros, etc., facilitando controles como perfil de fraude e comportamento de compras.

- **Caracteres permitidos**
  0123456789

3.4.5 Regra para TranCategory

Indica a categoria que a transação faz parte.

Este campo é usado para diferenciar tipos específicos de transações, como Cias Aéreas, categorizando corretamente a transação.

Valores Aceitos

DFLT – Para todas as transações.

IATA – Para transações Parceladas Lojistas que são derivadas de transações de Cias Aéreas.

3.4.6 Regras para AddlReqData

O campo AddlReqData é utilizado para informar dados adicionais para tipos específicos de transações (de Cias. Aéreas, por exemplo). Para tanto, são utilizadas TAGs para cada dado. As TAGs são separadas pelo caractere de ponto-e-vírgula (;), que também deve finalizar o campo.

3.4.6.1 Transações de Cias. Aéreas – TAGs I4116 e I4117

São TAGs usadas para informar os dados de transações de Cias Aéreas.

Estes dados são lidos apenas se informados corretos e se a categoria da transação for IATA.

Valores Aceitos

- **I4116** – Valor da taxa de embarque.
  - Numérico indicando o valor, com os centavos separados pelo caractere de ponto (.)
- **I4117** – Valor de entrada.
  - Numérico indicando o valor, com os centavos separados pelo caractere de ponto (.)

Exemplo de preenchimento

```
<addlReqData>I4116=10.45;</addlReqData>
<addlReqData>I4116=10.45;I4117=20.45;</addlReqData>
```

3.4.6.2 Transações de Facilitador de Pagamento – TAGs F4538 a F4543

Para que a Getnet possa cumprir com as regras das Bandeiras e Arranjos, as Leis Federais e determinações do BACEN (Banco Central do Brasil) para identificação das entidades finais (subcomércios) que fazem as transações financeiras, os Facilitadores de Pagamento devem enviar os dados de identificação de seus clientes a cada transação enviada à Getnet.

Valores Aceitos

TAG	TIPO	TAMANHO	DESCRIÇÃO
F4538	AN	15	ID do Subcomércio Deve ser formatado à esquerda e complementado com ' ' (espaços) à direita, caso o ID do subcomércio seja menor que o tamanho. Ex.: 'F4538=AB123456 ;' 'F4538=1234567890 ;' Exemplo de pattern: ^[A-Z0-9\s]{15}$
F4539	A	13	Cidade do Subcomércio Se comprimento for maior, será desprezado (Truncado) o excedente. Caso menor, poderá ser complementado com ' ' (espaço) a direita. Não são aceitos caracteres especiais, incluindo letra com acento. Exemplo de pattern: ^[A-Z0-9\s]{13}$
F4540	A	2	Estado do Subcomércio Sigla do Estado conforme padrão Exemplo de pattern: ^[A-Z]{2}$
F4541	N	8	Código Postal (CEP) do Subcomércio Somente números, sem hífen. Exemplo de pattern: ^[0-9]{8}$
F4542	AN	15	CNPJ ou CPF do Subcomércio Deve ser enviado com o tipo do documento, J = Pessoa Jurídica (CNPJ) ou F = Pessoa Física (CPF). Somente números, sem pontos e/ou hífen. Exemplo de pattern: ^([JF]{1}[0-9]{14})$
F4543	A	40	Logradouro do Subcomércio Se comprimento for maior, será desprezado o excedente. Caso seja menor, poderá ser complementado com ' ' (espaços) à direita. Não são aceitos caracteres especiais, incluindo letra com acento. Exemplo de pattern: ^[A-Z0-9\s]{40}$

3.4.6.3 COF - Credentials on file

Transações em que o EC não irá gravar as credenciais do Portador para usar em futuras transações, não precisam enviar dados do COF, devem ser chamadas como hoje já são chamadas.

Transações em que o EC irá gravar as credenciais do Portador, uma transação para armazenamento de cartão do portado no Cofre do Lojista/Gateway deve ser usada.

Para este, podem partir de dois tipos de transações, Verificação de Cartão (Bandeiras Visa e Mastercard) e Autorização (Bandeiras Visa, Mastercard e Elo). Mastercard sugere que a primeira transação para solicitação de armazenamento de cartão, seja pelo produto **Verificação de Cartão**, assim convertendo a taxa de aprovação maior que nas transações de autorização**.**

Neste quadro descreve-se os novos valores e seus domínios:

TAG	TIPO	TAM	DESCRIÇÃO
addlReqData [credentialsonfile]	A	1	F – Solicita o armazenamento das credenciais S – Usar as credenciais armazenadas para pagamento.
addlReqData [initiationreason]	A	1	"A" - Nova autorização "C" - Pagamento não agendado "D" - atrasos de cobrança "I" - Incremental "O" - Outro motivo "R" - Recorrente agendado "S" - reenvio "X" - No-show (para uma reserva de hotel)
transactionID	N	18	TID da transação original ou de verificação de cartão. Atenção: Este deve ser enviado para as bandeiras VISA e ELO. **OBS:** O TID da transação original ou verificação de cartão tem validade de um ano, após esse período deve ser gerado um novo TID.

3.4.7 Regra de Preenchimento da Nova Senha

Para a nova senha, é obrigatório informar no mínimo oito caracteres, sendo:

- **Caracteres permitidos:**
  - a-zA-Z (letras minúsculas/maiúsculas);
  - 0123456789;
  - caracteres especiais:
    @ # $ % & + = (Veja a *Regra para Caracteres Especiais*)

3.4.8 Regra de Preenchimento da Chave de Segurança

Existem dois algoritmos de criptografia utilizados pela GetNet, o AES e o 3DES. Com isto, o preenchimento dos campos deve seguir a regra:

- **AES**
  - Key deve conter 16 bytes;

- IV deve conter 16 bytes;

- **3DES**
  - Key deve conter 24 bytes;
  - IV deve conter 8 bytes.

- **Caracteres permitidos:**
  - a-zA-Z (letras minúsculas/maiúsculas);
  - 0123456789;
  - caracteres especiais:
    % $, . / ( ) + = - * (Veja a *Regra para Caracteres Especiais*)

3.4.9 Regra para Caracteres Especiais

No parser do XML, existem os caracteres que são estritamente ilegais. Para isto devemos usar o mecanismo de CDATA ou as referências de entidade.

Há 5 referências de entidade pré-definidas no XML que devemos substituir por:

Descrição	Caractere	Substituir por
E comercial	&	**&**
Menor do que	<	**<**
Maior do que	>	**>**
Apóstrofo	'	**'**
Aspas	"	**"**

Observação: Somente os caracteres "<" e "&" são estritamente ilegais na XML. Apóstrofes, aspas e sinais de maior do que são legais, mas é um bom hábito substitui-los.

Ou podemos usar o CDATA, onde tudo que estiver dentro de uma seção CDATA será ignorado pelo parser.

Uma seção CDATA começa com "**<![CDATA[**" e termina com "**]]>**".

3.5 Códigos de Retorno

3.5.1 Códigos de Retorno do WebService

Códigos de mensagens gerados pelo WebService	
Código	**Retorno**
CWS000000	Operação efetuada com sucesso
CWS000001	Alteração efetuada com sucesso
CWS100000	Ocorreu erro de conexão, tente novamente. Caso persista favor contatar a GetNet.
CWS100001	O Estabelecimento {0} não cadastro ou erro de cadastro.
CWS100002	Erro na leitura do arquivo de configuração para o Estabelecimento {0}.
CWS100003	Ocorreu erro de conexão nos nossos servidores, tente novamente. Caso persista favor contatar a GetNet.
CWS100004	Erro na autenticação do usuário.
CWS100005	Identificamos que este é o seu primeiro acesso. É obrigatório alterar a sua senha provisória.
CWS100006	Tente novamente, tivemos uma falha interna. Caso persista favor contatar a GetNet.
CWS100007	Problema no processamento do retorno, favor realizar uma operação de consulta para verificar status da transação.
CWS100008	Documento WSDL não formatado corretamente, favor revisar. Caso a mensagem persista favor contatar a GetNet.
CWS100009	Ocorreu erro no processamento da solicitação. Caso a mensagem persista favor contatar a GetNet.
CWS110000	Erro não identificado de Banco de Dados.
CWS110001	Erro de acesso ao Banco de Dados.
CWS110002	Falha para consultar o EC.
CWS110003	Falha para atualizar os dados do usuário.
CWS120001	Problema no cadastro de criptografia do EC.
CWS120002	{0} a codificação não é suportada. Favor entrar em contato.
CWS120003	{0} não definido. Favor entrar em contato.
CWS120004	Chave inválida (codificação inválida, comprimento errado, não inicializado, etc.)
CWS120005	Erro na geração da chave, sendo a chave com codificação inválida.
CWS120006	Erro no mecanismo de preenchimento, o mesmo não encontra-se disponível no ambiente. Favor entrar em contato e informar o mecanismo {0}.
CWS120007	{0} - Parâmetros do algoritmo inválidos ou inapropriados.
CWS120008	Essa exceção é lançada quando o comprimento dos dados fornecidos para uma cifra de bloco está incorreto, ou seja, não coincide com o tamanho do bloco da cifra.
CWS120009	Essa exceção é lançada quando é esperado um mecanismo de preenchimento específico para os dados de entrada, mas os dados não são preenchidos corretamente.
CWS200014	Terminal {0} desabilitado para o estabelecimento

Códigos de mensagens gerados pelo WebService	
Código	**Retorno**
CWS200000	O terminal {0} não cadastrado para o estabelecimento.
CWS200001	Parâmetro inválido.
CWS200002	Parâmetro obrigatório. O campo {0} não foi preenchido.
CWS200003	Parâmetro inválido. O campo {0} não contém o tamanho mínimo de caracteres. Deve conter no mínimo {1} caracteres.
CWS200004	Parâmetro inválido. O campo {0} contém mais caracteres do que o permitido. Deve conter no máximo {1} caracteres.
CWS200005	Parâmetro inválido. O campo {0} deve conter apenas caracteres do tipo {1}.
CWS200006	Parâmetro inválido. O campo {0} contém caracteres inválidos ou não foi formatado corretamente.
CWS200007	Parâmetro inválido. O campo {0} não contém caracteres válidos.
CWS200008	A senha deve conter no mínimo {0} caracteres, entre maiúsculas e minúsculas, números e caracteres especiais {1}.
CWS200009	A senha deve ser diferente das três últimas.
CWS200010	O EC não habilitou a criptografia dos dados seguros.
CWS200011	Comprimento inválido da chave (Key). Deve conter {0} caracteres.
CWS200012	Comprimento inválido do vetor de inicialização (IV). Deve conter {0} caracteres.
CWS200013	Número máximo de ocorrências alcançado.

* Todo conteúdo entre {} (chaves) representa um valor dinâmico.

** O código de retorno tem a seguinte formatação:

```
## CWS000000
## Onde os três primeiros dígitos:
##      CWS - Commerce WebService
## 4o. dígito
##  0 - Informativo
##  1 - Erro
##  2 - Alerta
## 5o. dígito
##  0 - Aplicação
##  1 - Banco de Dados
##  2 - Criptografia
## Últimos dígitos sequenciais das mensagens.
```

3.5.2 Códigos de Retorno da Plataforma de E-Commerce

Códigos de Erros gerados na Plataforma de E-Commerce		
Código	**Retorno**	**Descrição**
CGW000006	Tran Action Invalid	Parâmetro 'Action' informado não está na tabela de parâmetros.
CGW000013	Brand ID Invalid	Perfil não existe dentro do Resource.CGN Transação com cartão MasterCard, mas perfil é Visa (vice-versa)
CGW000018	Payment Instrument List Invalid	Bandeira informada na transação não é compatível com TerminalAlias.
CGW000021	Card Expiration Flag Invalid	Data de vencimento inválida.
CGW000024	Currency Code Invalid	Código de pais inválido
CGW000029	Card Number Invalid	Número de cartão inválido
CGW000242	Track ID Not Unique	Informar um NSU de transação diferente, ver ***trackid*** na tabela de parâmetros.
CGW000126	Payment Instrument Invalid	Perfil existe no Resource.CGN mas não tem no cadastro na Plataforma de E-Commerce GETNET
CGW000184	Payment ID Invalid	Bandeira informada não existe no TerminalAlias
CGW000186	Tran Amount Invalid	Valor inválido para esta transação
CGW000216	Capture Amount Invalid	Valor capturado é diferente do valor autorizado

3.5.3 Códigos de Retorno do Emissor / Getnet

Com o objetivo de apoiar os estabelecimentos comerciais na clareza da negativa das transações, a ABECS (Associação Brasileira das Empresas de Cartões de Crédito e Serviços) atualizou os códigos de retorno. A Getnet está preparada para retornar a todos os clientes os códigos informados na tabela abaixo.

Tipo de código **Irreversível (I)**: deverá ser solicitado outro meio de pagamento.

Tipo de código **Reversível (R)**: poderá reenviar a transação de acordo com as orientações descritas na planilha

Cód.: Campo *response_code*
Bandeira: Campo *brand*
Descrição: Campo *responseMessage*

Códigos de Resposta gerados pelo Emissor do Cartão (ABECS)			
Cód.	Bandeira	Descrição	I/R
00	TODAS	TRANSACAO EXECUTADA COM SUCESSO	
SF	TODAS	TRANSACAO EXECUTADA COM SUCESSO	
1	HIPERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-01]	I
1	MASTERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-01]	I
12	HIPERCARD	PARCELAMENTO INVALIDO - NAO TENTE NOVAMENTE [ECOM-12]	I

12	MASTERCARD	PARCELAMENTO INVALIDO - NAO TENTE NOVAMENTE [ECOM-12]	I
12	ELO	VERIFIQUE OS DADOS DO CARTAO [ECOM-12]	I
64	ELO	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-64]	I
76	ELO	CONTA DESTINO INVALIDA - NAO TENTE NOVAMENTE [ECOM-76]	I
912	AMEX	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-912]	R
911	AMEX	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-911]	R
4	ELO	REFAZER A TRANSACAO [ECOM-04]	R
6	ELO	LOJISTA CONTATE O ADQUIRENTE [ECOM-06]	R
R1	VISA	SUSPENSAO DE PAGAMENTO RECORRENTE PARA SERVICO - NAO TENTE NOVAMENTE [ECOM-R1]	I
4	VISA	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-04]	I
100	AMEX	CONTATE A CENTRAL DO SEU CARTAO [ECOM-100]	R
101	AMEX	VERIFIQUE OS DADOS DO CARTAO [ECOM-101]	I
106	AMEX	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-106]	R
109	AMEX	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-109]	I
110	AMEX	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-110]	I
115	AMEX	VERIFIQUE OS DADOS DO CARTAO [ECOM-115]	I
116	AMEX	NAO AUTORIZADA [ECOM-116]	R
117	AMEX	SENHA INVALIDA [ECOM-117]	R
122	AMEX	VERIFIQUE OS DADOS DO CARTAO [ECOM-122]	I
3	HIPERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-03]	I
43	HIPERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-43]	I
43	VISA	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-43]	I
4	MASTERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-04]	I
4	HIPERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-04]	I
5	ELO	CONTATE A CENTRAL DO SEU CARTAO [ECOM-05]	R
5	VISA	CONTATE A CENTRAL DO SEU CARTAO [ECOM-05]	R
5	MASTERCARD	CONTATE A CENTRAL DO SEU CARTAO [ECOM-05]	R
5	HIPERCARD	CONTATE A CENTRAL DO SEU CARTAO [ECOM-05]	R
6	VISA	VERIFIQUE OS DADOS DO CARTAO [ECOM-06]	I
7	VISA	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-07]	I
12	VISA	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-12]	I
13	ELO	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-13]	I
13	HIPERCARD	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-13]	I
13	MASTERCARD	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-13]	I
13	VISA	VALOR DA TRANSACAO NAO PERMITIDO - NAO TENTE NOVAMENTE [ECOM-13]	I
14	ELO	VERIFIQUE OS DADOS DO CARTAO [ECOM-14]	I
14	HIPERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-14]	I
14	MASTERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-14]	I
14	VISA	VERIFIQUE OS DADOS DO CARTAO [ECOM-14]	R
15	HIPERCARD	DADOS DO CARTAO INVALIDO - NAO TENTE NOVAMENTE [ECOM-15]	I
15	VISA	DADOS DO CARTAO INVALIDO - NAO TENTE NOVAMENTE [ECOM-15]	I
15	MASTERCARD	DADOS DO CARTAO INVALIDO - NAO TENTE NOVAMENTE [ECOM-15]	I
19	ELO	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-19]	I
19	VISA	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-19]	I
23	ELO	PARCELAMENTO INVALIDO - NAO TENTE NOVAMENTE [ECOM-23]	I
30	ELO	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-30]	I
30	MASTERCARD	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-30]	I
30	HIPERCARD	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-30]	I
38	ELO	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-38]	R

39	VISA	UTILIZE FUNCAO DEBITO [ECOM-39]	I
41	HIPERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-41]	I
41	MASTERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-41]	I
41	ELO	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-41]	I
41	VISA	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-41]	I
43	MASTERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-43]	I
43	ELO	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-43]	I
53	VISA	UTILIZE FUNCAO CREDITO [ECOM-53]	I
56	ELO	VERIFIQUE OS DADOS DO CARTAO [ECOM-56]	I
51	VISA	NAO AUTORIZADA [ECOM-51]	R
51	MASTERCARD	NAO AUTORIZADA [ECOM-51]	R
51	HIPERCARD	NAO AUTORIZADA [ECOM-51]	R
51	ELO	NAO AUTORIZADA [ECOM-51]	R
52	VISA	UTILIZE FUNCAO CREDITO [ECOM-52]	I
61	VISA	VALOR EXCEDIDO. CONTATE A CENTRAL DO SEU CARTAO [ECOM-61]	R
54	HIPERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-54]	I
54	MASTERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-54]	I
54	ELO	VERIFIQUE OS DADOS DO CARTAO [ECOM-54]	I
55	VISA	SENHA INVALIDA [ECOM-55]	R
55	HIPERCARD	SENHA INVALIDA [ECOM-55]	R
55	ELO	SENHA INVALIDA [ECOM-55]	R
55	MASTERCARD	SENHA INVALIDA [ECOM-55]	R
61	ELO	VALOR EXCEDIDO. CONTATE A CENTRAL DO SEU CARTAO [ECOM-61]	R
57	MASTERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-57]	I
57	HIPERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-57]	I
57	VISA	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-57]	I
57	ELO	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-57]	I
58	HIPERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-58]	I
58	ELO	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-58]	I
58	MASTERCARD	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-58]	I
58	VISA	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-58]	I
59	VISA	CONTATE A CENTRAL DO SEU CARTAO [ECOM-59]	R
59	ELO	CONTATE A CENTRAL DO SEU CARTAO [ECOM-59]	R
61	MASTERCARD	VALOR EXCEDIDO. CONTATE A CENTRAL DO SEU CARTAO [ECOM-61]	R
61	HIPERCARD	VALOR EXCEDIDO.CONT ATE A CENTRAL DO SEU CARTAO [ECOM-61]	R
76	VISA	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-76]	I
77	ELO	CONTA ORIGEM INVALIDA - NAO TENTE NOVAMENTE [ECOM-77]	I
62	ELO	CARTAO NAO PERMITE TRANSACAO INTERNACIONAL [ECOM-62]	I
62	VISA	CARTAO NAO PERMITE TRANSACAO INTERNACIONAL [ECOM-62]	I
62	MASTERCARD	CARTAO NAO PERMITE TRANSACAO INTERNACIONAL [ECOM-62]	I
62	HIPERCARD	CARTAO NAO PERMITE TRANSACAO INTERNACIONAL [ECOM-62]	I
63	ELO	VERIFIQUE OS DADOS DO CARTAO [ECOM-63]	I
63	VISA	VERIFIQUE OS DADOS DO CARTAO [ECOM-63]	R
63	HIPERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-63]	R
63	MASTERCARD	VERIFIQUE OS DADOS DO CARTAO [ECOM-63]	R
64	VISA	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-64]	I
65	VISA	QTDADE DE SAQUES EXCEDIDA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-65]	R

65	ELO	QTDADE DE SAQUES EXCEDIDA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-65]	R
65	MASTERCARD	QTDADE DE SAQUES EXCEDIDA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-65]	R
65	HIPERCARD	QTDADE DE SAQUES EXCEDIDA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-65]	R
74	VISA	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-74]	I
74	ELO	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-74]	I
75	HIPERCARD	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-75]	R
75	ELO	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-75]	R
75	MASTERCARD	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-75]	R
75	VISA	EXCEDIDAS TENTATIVAS DE SENHA. CONTATE A CENTRAL DO SEU CARTAO [ECOM-75]	R
78	ELO	DESBLOQUEIE O CARTAO [ECOM-78]	R
78	VISA	DESBLOQUEIE O CARTAO [ECOM-78]	R
81	VISA	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-81]	I
88	HIPERCARD	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-88]	I
88	MASTERCARD	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-88]	I
82	ELO	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-82]	I
82	VISA	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-82]	I
86	HIPERCARD	SENHA INVALIDA [ECOM-86]	R
86	VISA	SENHA INVALIDA [ECOM-86]	R
86	MASTERCARD	SENHA INVALIDA [ECOM-86]	R
P6	ELO	SENHA INVALIDA UTILIZE A NOVA SENHA [ECOM-P6]	R
3	VISA	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-03]	I
91	HIPERCARD	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-91]	R
91	VISA	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-91]	R
91	ELO	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-91]	R
91	MASTERCARD	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-91]	R
92	VISA	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-92]	I
92	MASTERCARD	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-92]	I
92	HIPERCARD	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-92]	I
93	VISA	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-93]	I
94	VISA	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-94]	I
94	MASTERCARD	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-94]	I
94	HIPERCARD	CONTATE A CENTRAL DO SEU CARTAO - NAO TENTE NOVAMENTE [ECOM-94]	I
96	MASTERCARD	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-96]	R
96	HIPERCARD	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-96]	R
96	VISA	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-96]	R
96	ELO	FALHA DE COMUNICACAO - TENTE MAIS TARDE [ECOM-96]	R
99	ELO	VALOR DIFERENTE DA PRE AUTORIZACAO - NAO TENTE NOVAMENTE [ECOM-99]	I
AB	ELO	UTILIZE FUNCAO CREDITO [ECOM-AB]	I
AC	ELO	UTILIZE FUNCAO DEBITO [ECOM-AC]	I
B1	VISA	CONTATE A CENTRAL DO SEU CARTAO [ECOM-B1]	R
B2	VISA	CONTATE A CENTRAL DO SEU CARTAO [ECOM-B2]	R
G3	GETNET	ESTABELECIMENTO NAO CADASTRADO LIGUE GETNET [ECOM-G3]	R
G4	GETNET	CARTAO INVALIDO [ECOM-G4]	I
G5	GETNET	PRODUTO NAO HABILITADO [ECOM-G5]	R
T2	GETNET	ERRO NOS DADOS INFORMADOS. TENTE NOVAMENTE [ECOM - T2]	R
N0	VISA	CONTATE A CENTRAL DO SEU CARTAO [ECOM-N0]	R
N3	VISA	SAQUE NAO DISPONÍVEL - NAO TENTE NOVAMENTE [ECOM-N3]	I
N4	VISA	VALOR EXCEDIDO. CONTATE A CENTRAL DO SEU CARTAO [ECOM-N4]	R

N8	VISA	VALOR DIFERENTE DA PRE AUTORIZACAO - NAO TENTE NOVAMENTE [ECOM-N8]	I
P5	ELO	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-P5]	I
03	MASTERCARD	TRANSACAO NAO PERMITIDA - NAO TENTE NOVAMENTE [ECOM-03]	I
R0	VISA	SUSPENSAO DE PAGAMENTO RECORRENTE PARA SERVICO - NAO TENTE NOVAMENTE [ECOM-R0]	I
R2	VISA	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-R2]	I
R3	VISA	SUSPENSAO DE PAGAMENTO RECORRENTE PARA SERVICO - NAO TENTE NOVAMENTE [ECOM-R3]	I
180	AMEX	SENHA INVALIDA - NAO TENTE NOVAMENTE [ECOM-180]	I
181	AMEX	ERRO NO CARTAO – NAO TENTE NOVAMENTE [ECOM-181]	I
200	AMEX	TRANSACAO NAO PERMITIDA PARA O CARTAO - NAO TENTE NOVAMENTE [ECOM-200]	I

Outros Retornos

Os retornos abaixo são de uso exclusivo das bandeiras e não fazem parte do normativo 21 ABECS.

Cód.	Bandeira	Descrição	I/R/A
79	MASTERCARD	ERRO NO CARTAO - NAO TENTE NOVAMENTE [ECOM-79]	A
82	MASTERCARD	ERRO NO CARTAO - NAO TENTE NOVAMENTE [ECOM-82]	A
83	MASTERCARD	ERRO NO CARTAO - NAO TENTE NOVAMENTE [ECOM-83]	A
79	VISA	VERIFIQUE OS DADOS DO CARTAO [ECOM - 70]	R
111	AMEX	DESBLOQUEIE O CARTAO [ECOM - 111]	I

Para a bandeira Mastercard existe a possibilidade do envio de um código complementar de aconselhamento – Merchant Advice Code (MAC). Dessa forma, para códigos que estão passíveis do recebimento do código complementar Mastercard, estarão descritos com o Tipo de código **Advice (A)**, onde é necessário realizar a leitura do MAC para identificar se é possível ou não realizar uma retentativa daquela transação.

OBS: A Getnet realiza um DE PARA dos códigos MAC originas recebidos pela bandeira Mastercard para melhor agrupar os retornos em caso de regras semelhantes para as demais bandeiras, dessa forma, no quadro abaixo é possível encontrar o DE PARA realizado:

DE PARA MASTERCARD X GETNET			
MAC Mastercard	**DE PARA MAC Getnet**	**Descrição**	**Classificação**
01	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Reversível
02	2	Tente novamente mais tarde (Try Again Later)	Reversível
03	3	Não Tente Novamente (Do Not Try Again)	Irreversível
04	4	Requisitos de token não atendidos para este tipo de token (Token requirements not fulfilled for this token type)	Reversível
21	U	Cancelamento de Pagamento – Não reenvie a transação (Payment Cancellation – Do not resubmit transaction)	Irreversível
24	101	Tente após 1 hora	Reversível
25	124	Tente após 24 horas	Reversível
26	202	Tente após 2 dias	Reversível
27	204	Tente após 4 dias	Reversível
28	206	Tente após 6 dias	Reversível
29	208	Tente após 8 dias	Reversível
30	210	Tente após 10 dias	Reversível

O quadro abaixo descreve as combinações possíveis dos códigos MAC junto aos códigos de resposta que podem ser enviados pela Mastercard e descreve os aconselhamentos que os comércios podem ter a partir delas:

Exemplos de Combinações do Reponse Code com o Código Complementar MAC				
Response Code	**MAC**	**Descrição**	**Aconselhamento**	**Classificação**
79 ou 82	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Informações atualizadas disponíveis no banco de dados Mastercard ABU - cheque as novas informações antes de tentar novamente	Reversível
79 ou 82	3	Não Tente Novamente (Do Not Try Again)	Não foram encontradas credenciais atualizadas no banco de dados Mastercard ABU – não tente novamente	Irreversível
83	1	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Verifique se as informações do cartão estão corretas. A autenticação pode melhorar a probabilidade de aprovação - tente novamente usando autenticação (Ex: 3DS)	Reversível
83	3	Não Tente Novamente (Do Not Try Again)	Suspeita de fraude. Não tente novamente	Irreversível
79, 82, 83	2	Tente novamente mais tarde (Try Again Later)	Tente novamente mais tarde	Reversível
51	101	Tente após 1 hora	Tente após 1 hora	Reversível
51	124	Tente após 24 horas	Tente após 24 horas	Reversível
51	202	Tente após 2 dias	Tente após 2 dias	Reversível
51	204	Tente após 4 dias	Tente após 4 dias	Reversível
51	206	Tente após 6 dias	Tente após 6 dias	Reversível
51	208	Tente após 8 dias	Tente após 8 dias	Reversível
51	210	Tente após 10 dias	Tente após 10 dias	Reversível

NOTA: Os códigos MAC 101, 124, 202, 204, 206, 208 e 2010 são de uso exclusivo Mastercard. Os demais códigos MAC (1, 2, 3, 4 e U) podem também ser enviados pelos emissores para aconselhamento junto aos demais códigos ABECS e, caso isso aconteça, para verificar se a transação pode ou não ser retentada, verifique a classificação do MAC recebido que está descrita na tabela: *DE PARA MASTERCARD X GETNET*: se o MAC for reversível, a transação pode ser retentada, se o MAC for irreversível a transação não pode ser retentatada.

4 GLOSSÁRIO

TERMO	DEFINIÇÃO
3D Secure	***3 Domain Secure*** 3D Secure é um protocolo de E-Commerce baseado em XML desenvolvido para ser uma camada adicional de segurança para transações online de crédito e débito, que permite que um portador autentique-se durante a transação. Ele permite que três domínios - do ***Adquirente***, de ***Interoperabilidade*** e do ***Emissor*** - trabalhem em conjunto com segurança (daí o nome do protocolo): - O Portador tem a percepção de que seu cartão não é usado sem sua autorização; - Lojistas são protegidos de fraudes; - Bancos (Emissores de cartões), ao terem autenticado a transação, têm mais segurança para aprovar a transação. O protocolo foi desenvolvido pela Visa, mas cada bandeira implementou serviços baseados no mesmo como um produto próprio: - Visa: ***Verified by Visa (VbV)***; - Mastercard: ***Mastercard SecureCode***; - JCB International: J/Secure; - American Express: ***SafeKey***; - Diners Club: ProtectBuy**.**
AAV	Ver ***Accountholder Authentication Value***
Access Control Server	Componente que opera no Domínio do Emissor (Bancos), verifica se a autenticação está disponível para um determinado número de cartão e a autentica quando possível.
Accountholder Authentication Value	Implementação da Mastercard para o UCAF. Ver ***UCAF / Universal Cardholder Authentication Field***
ACS	Ver ***Access Control Server***
Adquirente	Instituição que estabelece um contrato de serviço com um Lojista para aceitação de cartões. Também determina se o Lojista é elegível a participar do 3D Secure. Faz o papel tradicional de receber e enviar mensagens de autorização e liquidação.
AHS	Ver ***Authentication History Server***
American Express	Uma das principais Bandeiras internacionais. Ver ***Bandeira***
ATN	Ver ***Authentication Tracking Number***
Autenticação	Processo de verificar se o **Portador** realizando a compra via E-Commerce está habilitado a usar o cartão de pagamento informado.

TERMO	DEFINIÇÃO
Authentication History Server	Componente que opera no ***Domínio de Interoperabilidade***, arquiva a atividade de autenticação para uso dos ***Adquirentes*** e ***Emissores*** para resolução de disputas e outros propósitos.
Authentication Tracking Number	Número de 16 dígitos gerado pelo ***ACS*** para identificar a transação, e usado na criação do ***UCAF*** (***CAVV/AAV***).
Autorização	Processo pelo qual o ***Emissor*** ou um ***Processador***, em nome do ***Emissor***, aprova uma transação para pagamento.
Bandeira	É a empresa proprietária dos sistemas que permitem a emissão do cartão e utilização dos mesmos nos ***ECs***. É também a empresa responsável pela comunicação da transação entre o ***Adquirente*** e o ***Emissor*** do cartão. As principais bandeiras presentes no mercado brasileiro são ***Visa, MasterCard, American Express, Hipercard*** e ***Elo***.
BIN	*Bank Identification Number* (Número de Identificação Bancária). Número que identifica o ***Emissor*** do ***Cartão***, representado pelos 6 primeiros dígitos do ***PAN*** (número do cartão). O primeiro dígito do BIN é chamado de MII *Major Industry Identifier*, que identifica a categoria da entidade que emitiu o cartão.
Cardholder Authentication Verification Value	Implementação da Visa para o UCAF. Ver ***UCAF / Universal Cardholder Authentication Field***
Cartão	É o cartão de Crédito e/ou Débito emitido e administrado pelo ***Emissor***, de titularidade e responsabilidade do ***Portador***, para uso pessoal e intransferível do mesmo.
CAVV	Ver ***Cardholder Authentication Verification Value***
CRReq	***Card Range Request***
CRRes	***Card Range Response***
Directory Server	Entidade de hardware/software operada no ***Domínio de Interoperabilidade***. Mantém uma lista de *ranges* de cartões para os quais a autenticação pode estar disponível e coordena a comunicação entre o ***MPI*** e o ***ACS*** para determinar se a autenticação está disponível para um determinado número de cartão.
Domínio de Interoperabilidade	Facilita a transferência de informações entre o ***Domínio do Emissor*** e o ***Domínio do Adquirente***.
Domínio do Adquirente	Contém os sistemas e funções do Adquirente e seus clientes (***Lojistas***).
Domínio do Emissor	Contém os sistemas e funções do Emissor e seus clientes (***Portadores***).
EC (Estabelecimento Comercial)	Entidade que contrata o ***Adquirente*** para aceitar cartões de Crédito e/ou Débito para pagamento de seus produtos e/ou serviços.

TERMO	DEFINIÇÃO
ECI	Ver ***Electronic Commerce Indicator***
Electronic Commerce Indicator	Valor que é retornado pelo Directory Server (Visa ou Mastercard) para indicar o resultado da autenticação do cartão do portador no 3D Secure.
ELO	Uma das principais Bandeiras nacionais. Ver ***Bandeira***
Emissor	Instituição financeira que emite cartões de pagamento, mantém contrato com o Portador para prestar esses serviços, determina a eligibilidade do Portador para participar do ***3D Secure***, e identifica para o ***Directory Server*** os *ranges* de números de cartões eligíveis a participar do 3D Secure. Para identificar qual é o ***Emissor*** do cartão, usam-se os 6 primeiros números do cartão, chamados de ***BIN***.
Gateway de Pagamento	Terceiro que provê uma interface entre o ***Lojista*** e o sistema de pagamento do ***Adquirente***.
Hipercard	Uma das principais Bandeiras nacionais. Ver ***Bandeira***
IIN	*Issuer Identification Number* (Número de Identificação do Emissor). O mesmo que **BIN**.
Lojista	Ver ***EC (Estabelecimento Comercial)***.
Mastercard	Uma das principais Bandeiras internacionais. Ver ***Bandeira***
MasterCard SecureCode	Implementação da Mastercard do protocolo 3D Secure. Ver ***3D Secure***
Merchant Server Plug In	Componente que opera no Domínio do Adquirente, o MPI é um módulo de software que provê uma interface de comunicação entre o lojista e os Directory Servers das Bandeiras. Ele pode ser integrado ao website do lojista ou hospedado em um provedor de serviços (como um Gateway de Pagamento) ou no Adquirente. As principais funções do MPI são verificar a assinatura digital dos Emissores usada no processo de autenticação, validar as mensagens de resposta de registro e autenticação, criptografar e armazenar senhas e certificados, e recuperar registros de transações para resolução de disputas de *chargeback*.
MPI	Ver ***Merchant Server Plug In***
DIRECTORYSERVERTRANSACTIONID	Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.
SPECIFICATIONVERSION	Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização.

TERMO	DEFINIÇÃO
Payer Authentication Request	Mensagem enviada pelo ***MPI*** para o ***ACS*** via equipamento do Portador. Pede ao ***Emissor*** que autentique o portador e contém as informações necessárias do ***Portador***, ***Lojista*** e específicas da transação necessárias para realizar a autenticação.
Payer Authentication Response	Mensagem formatada, assinada digitalmente e enviada pelo ***ACS*** para o ***MPI***, via equipamento do ***Portador***, informando os resultados da autenticação ***3D Secure*** do Portador pelo ***Emissor***.
Portador	Aquele que tem um cartão de pagamento (Débito e/ou Crédito), realiza a compra, provê o número do cartão e compromete-se com o pagamento do valor.
SafeKey	Implementação da American Express do protocolo 3D Secure. Ver ***3D Secure***
SecureCode	O mesmo que ***Mastercard SecureCode***. Implementação da Mastercard do protocolo 3D Secure. Ver ***3D Secure***
TEF	TEF (Transferência Eletrônica de Fundos), são sistemas computacionais que executam transações financeiras de forma eletrónica, no Brasil, em especial, refere-se ao Meio de Captura que é integrado com a Automação Comercial do **EC**. A comunicação das transações eletrônicas entre os servidores e as operadoras de cartão são feitas, em geral, através de linhas ***X.25***, mas podem ser feitas por MPLS ou IP. Existem ***Gateways de Pagamento*** que utilizam a Internet, através de VPN, para comunicar com as pontas clientes e a partir deles a comunicação acontece através de linhas X.25 (E-Commerce via TEF). As principais ferramentas para as transações eletrônicas utilizadas atualmente utilizam comunicação via IP entre clientes e ***Gateways*** e X.25 entre ***Gateways*** e ***Adquirentes***.
UCAF	Ver ***Universal Cardholder Authentication Field***

TERMO	DEFINIÇÃO
Universal Cardholder Authentication Field	Valor criptografado gerado pelo ***ACS*** para prover uma maneira de, durante o processo de autorização, o sistema de autorização validar rapidamente a integridade de certos valores copiados da ***Payer Authentication Response*** para o pedido de autorização e para provar que a autenticação ocorreu. É usado como evidência de autenticação do pagamento durante a compra online para qualificação de proteção do *chargeback*. Na implementação da ***Visa*** é chamado de ***CAVV***, na implementação da ***Mastercard*** é chamado de ***AAV***. Ao submeter uma transação, o CAVV ou AAV deve ser incluído para demonstrar que o portador foi autenticado. O **UCAF** é um campo binário de 32 bytes com uma estrutura de dados variável Exemplo: jMoRyYgNSt0ZAREBBu8LHI+3oZo= O CAVV é uma *string* de caracteres que contém um valor de 20 bytes que são codificados na Base64 em 28 bytes.
VbV	O mesmo que ***Verified by Visa***. Implementação da Visa do protocolo 3D Secure. Ver ***3D Secure***
VEReq	Ver ***Verify Enrollment Request***
VERes	Ver ***Verify Enrollment Response***
Verified by Visa	Implementação da Visa do protocolo 3D Secure. Ver ***3D Secure***
Verify Enrollment Request	Mensagem do ***MPI*** para o ***Directory Server*** ou do Directory Server para o ***ACS*** perguntando se a autenticação está disponível para um número de cartão específico.
Verify Enrollment Response	Mensagem do ***ACS*** ou ***Directory Server*** dizendo ao ***MPI*** se a autenticação está disponível ou não.
Visa	Uma das principais Bandeiras internacionais. Ver ***Bandeira***
X.25	Protocolo de comunicação em rede dedicada, com garantia de entrega e segurança de mensagens. É utilizado na comunicação com **TEFs Dedicados**.
XID	***Unique Transaction Identifier*** É gerado automaticamente pelo MPI. Tem tipicamente 28 bytes de tamanho e é codificado em Base64. Exemplo: CBKJB289V1PZL4TDXXWF

A. AUTENTICAÇÃO DO PORTADOR

3D Secure ajuda a proteger as informações de pagamento dos portadores que efetuam compras on-line com cartões de crédito ou débito.

O portador cadastra uma senha para seu cartão junto ao Emissor e em transações online é preciso informá-la para ser aprovado.

VISA *https://usa.visa.com/personal/security/vbv/index.html*

MasterCard *http://www.mastercard.us/support/securecode.html*

ENTENDENDO OS PASSOS

1. Portador finaliza sua compra e informa os dados de seu cartão.
2. MPI solicita verificação de inscrição ao Gateway GetNet.
3. Se participar encaminha transação a Bandeira.
4. Se a Bandeira indicar que o Emissor participa do programa direciona ao Emissor para verificar o portador.
5. O Emissor responde informando se o portador do cartão está cadastrado no programa.
6. A Bandeira encaminha a resposta a GetNet que devolve o resultado para a loja.
    a. Em caso **POSITIVO**, é retornado **ENROLLED**, e são enviados os seguintes dados para prosseguir com a Autenticação: o endereço da URL de acesso ao ACS (Access Control Server) para autenticação, o PARes e o PaymentID.
    b. Se a autenticação for **NEGADA**, é retornado **NOT ENROLLED**, e a transação deve ser finalizada.
7. Com os dados que indicam que o portador está cadastrado, a Loja deve fazer a chamada com a URL fornecida, que irá carregar a página de autenticação do Emissor. A loja deve montar o formulário HTTPS e enviar os campos com os seguintes parâmetros obrigatórios:
    a. Form action: URL (Access Control Server);
    b. PaReq: PaReq;
    c. PaymentID: MD;
    d. URL de retorno: TermUrl; Esta URL é para o ACS redirecionar o resultado após o usuário realizar a autenticação.
8. O Portador preenche as informações solicitadas pelo Emissor na página de autenticação.
9. O browser do portador encaminha o pedido de autenticação para o ACS.
10. Emissor recebe a mensagem do Internet Banking e retorna para a URL informada pela Loja os dados da Autenticação pelas informações fornecidas pelo Portador.
11. ACS valida os dados informados pelo portador, cria e assina digitalmente a mensagem de resposta de autenticação do portador, contendo: **ECI**, **XID** e **UCAF**.
    O ACS envia para Bandeira uma solicitação de registro da autenticação gerada.
12. Mensagem de 'AUTENTICADO' via SecureCode / VerifiedbyVISA.
    Sua transação pode ser submetida para autorização.

*Mesmo que uma transação tenha sua **AUTENTICAÇÃO NEGADA**, ela ainda pode ser enviada para **AUTORIZAÇÃO**. Porém a responsabilidade é do EC assumir o risco em caso de* chargeback *desta venda. A identificação deste status é feita pelo valor do campo ECI (verificar na tabela parâmetros).*

B. Tabela brandType Pré-Prago

Na tabela abaixo constam os valores válidos par ao campo brandType que podem ser recebidos no retorno quando a transação for executada com um cartão pré-pago. Caso esse retorno seja recebido, essa transação será liquidada em D+2.

Brandeira (brand)	Iss-Type	Acc Type (PrePago)	IT-AT (brandType)	Emissor	Tipo
Mastercard	M	PP	**M -PP**	Estrangeiro	FOREIGN Credit
Mastercard	MN	PP	**MN-PP**	Doméstico	DOMESTIC Credit
Maestro	MF	PP	**MF-PP**	Estrangeiro	FOREIGN Debit
Maestro	ML	PP	**ML-PP**	Doméstico	DOMESTIC Debit
Mastercard	MD	PP	**MD-PP**	Doméstico	DOMESTIC Debit
Visa Crédito	V	PP	**V -PP**	Estrangeiro	FOREIGN Credit
Visa	VN	PP	**VN-PP**	Doméstico	DOMESTIC Credit
Visa Electron	VF	PP	**VF-PP**	Estrangeiro	FOREIGN Debit
Visa Electron	VL	PP	**VL-PP**	Doméstico	DOMESTIC Debit
ELO	EL	PP	**EL-PP**	Doméstico	DOMESTIC Debit
ELO	EN	PP	**EN-PP**	Doméstico	DOMESTIC Credit
Hipercard	HI	PP	**HI-PP**	Doméstico	DOMESTIC Credit
Amex	A	PP	**A -PP**	Estrangeiro	DOMESTIC Credit
Amex	AN	PP	**NA-PP**	Doméstico	DOMESTIC Credit

ESTAMOS CONECTADOS 24 HORAS, 7 DIAS POR SEMANA

APP
GETNET

GETNET
.COM.BR

CENTRAL DE RELACIONAMENTO GETNET
4002 4000
(Regiões Metropolitanas)
0800 648 8000
(Demais localidades)
24h por dia, todos os dias.

/GetnetBrasil
@GetnetBrasil
/GetnetBrasil
@GetnetBrasil
/GetnetBrasil

OUVIDORIA
Se não ficar satisfeito
com a solução apresentada.
0800 646 3404
De segunda a sexta-feira,
das 8h30 às 17h30, exceto feriados.
Avenida Pernambuco, 1483
São Geraldo – Porto Alegre/RS
CEP 90240-005

PORTAL DO CLIENTE
www.santandergetnet.com.br
PORTAL DE RECARGAS
portal.getnet.com.br