E-Commerce

Manual de Integração

WebService – V.04.00

Getnet – Uma empresa Santander

COPYRIGHT

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 atende-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.ecommerce@getnet.com.br

4003-5025

2 VISÃO GERAL

A seguir são apresentadas as soluções e modelos de E-Commerce e as funcionalidade 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 (*Outubro de 2017*) nossa plataforma suporta transações das seguintes Bandeiras:

Figura 1 - Bandeiras Suportadas na Plataforma E-Commerce (Outubro/2017)

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 pela 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	Pré-Autorização	Verificação de Cartão	Autenticação do Portador	MCC Dinâmico	Soft Descriptor
mastercard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VISA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AMERICAN EXPRESS		✓	✓		✓		✓			✓	✓
elo	✓*	✓	✓		✓					✓	✓

Figura 2 – Funcionalidades da Plataforma E-Commerce por Bandeira (Outubro/2017)

* Transações de Débito ELO são apenas sem Autenticação.

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 *Anexo B – Autenticação do Portador*).

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-se o protocolo 3D Secure (veja o *Anexo B – Autenticação do Portador*).

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-se o protocolo 3D Secure (veja o *Anexo B – Autenticação do Portador*).

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 a 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-se o protocolo 3D Secure (veja o *Anexo B – Autenticação do Portador*).

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-se o protocolo 3D Secure (veja o *Anexo B – Autenticação do Portador*).

2.2.6 CRÉDITO PARCELADO EMISSOR DO 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 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**.

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.

2.2.7.1 AJUSTE DE PRÉ-AUTORIZAÇÃO INCREMENTAL

Ao solicitar um ajuste de valor à 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.

2.2.7.2 AJUSTE DE PRÉ-AUTORIZAÇÃO DECREMENTAL

Ao solicitar um ajuste de valor à 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.

2.2.7.3 CONFIRMAÇÃO DE PRÉ-AUTORIZAÇÃO

Para efetivar a Pré-Autorização, deve ser feita uma nova Transação de Confirmação de Pré-Autorização (Captura de 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;

2.2.8 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.

2.2.9 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.

As implementações suportadas pela plataforma são as da Visa e da MasterCard, **Verified by Visa** e **Secure Code**, respectivamente.

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

2.2.10 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.

2.2.11 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
  Os seguintes caracteres especiais:
  % $, . / & ( ) + = = < > - *

- **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)
  Os seguinte caracteres especiais:
  ! ? : ; [ ] { } ' " # _ @ § ^ ~ ¨ \

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.*

2.2.12 CARTEIRAS DIGITAIS

A Getnet disponibiliza integração as 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.

2.2.12.1 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 no campo addlReqData, com o seguinte domínio:

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

Exemplo:

```
<addlReqData>WTYP=01;WID=101;</addlReqData>
```

2.2.12.2 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 campo addlReqData, com o seguinte domínio:

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

Exemplo:

```
<addlReqData>WTYP=02;WID=VCIND;</addlReqData>
```

2.2.13 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
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
Verificação de Cartão	N/A	N/A	N/A	N/A	N/A

Funcionalidades	Especificidades				
	Tempo para Confirmação	Modalidades que podem ser Confirmadas	Valor da Confirmação	Suporta Autenticação	Autenticação Obrigatória
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 3 – 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 4 – 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	Dados de Cartão de Teste
	**CRÉDITO (com ou sem autenticação)** PAN: 5453010000083303 CVV: 123 / VENC.: 04/2018 Portador: Rebecca Sommers SecureCode: secbecky1
	DÉBITO (autenticado) 54326201155166661 CVV: 123 / VENC.: 04/2018 Portador: Terry Roberts SecureCode: secterry1
	**CRÉDITO (sem autenticação)** PAN: 4012001038166662 CVV: 123 / VENC.: 04/2018
	CRÉDITO E DÉBITO (autenticados) PAN: 4012001037141112 CVV: 123 / VENC.: 04/2018

Figura 5 – 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

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

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?
X123456701	Para transações Visa Crédito
X123456702	Para transações MasterCard Crédito
X123456703	Para transações Visa Débito
X123456704	Para transações MasterCard Débito
X123456707	Para transações ELO Crédito
X123456708	Para transações ELO Débito
X123456709	Para transações American Express Crédito

3.1.1 MÉTODOS E VERSÕES

Nessa seção são apresentadas as funcionalidades (métodos) disponíveis em cada versão no serviço CommerceService e AdministrationService.

Todas as operações mantêm as mesmas características das versões anteriores.

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

Figura 6 – Tabela Métodos vs Versões

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	19	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.
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	

TAG	Tipo	Obrig.	Tam.	Descrição
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*.

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>
      </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.
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	19	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	

TAG	Tipo	Obrig.	Tam.	Descrição
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*.

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>
      </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 pode ser maior (desde que não ultrapasse 15% do valor original), igual ou menor (sem limitação).

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	19	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 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>
      </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.

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*.
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	19	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 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>
         </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 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 AUTHENTICATEDPURCHASESERVICE

Destinado a transações Autenticadas (3D Secure) de Crédito ou Débito.

Esta operação é muito semelhante ao processo do PurchaseService, na qual o desejo é que em uma única chamada, uma Autorização seguida de uma Confirmação (Captura), sejam realizadas.

A diferença é que neste processo temos um passo a mais. Na primeira parte da operação, se o cartão do portador for participante do processo 3DS, no retorno da chamada estarão os dados que a Loja deve utilizar para carregar a página web de autenticação do portador com seu Banco Emissor. Após o Portador finalizar o processo de Autenticação, a Loja deve enviar os dados da Autenticação para o E-Commerce Web, utilizando o método FinalizeAuthenticationService, para concluir toda a operação, desde que toda a operação tenha sido concluída com sucesso.

Com este modelo, a transação se torna mais segura tanto para o Lojista como para o Portador do cartão.

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.
authenticatedPurchase	n/a	R	1	Elemento da transação.
authenticatedPurchase.terminalID	AN	R	10	Ver *Regra para TerminalID*.
authenticatedPurchase.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
authenticatedPurchase.amount	N	R	19	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
authenticatedPurchase.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
authenticatedPurchase.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
authenticatedPurchase.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
authenticatedPurchase.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*.
authenticatedPurchase.card	n/a	R	1	Elemento com os dados do cartão.
authenticatedPurchase.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
authenticatedPurchase.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.

TAG	Tipo	Obrig.	Tam.	Descrição
authenticatedPurchase.card.expiryMonth	N	R	2	Mês de expiração do cartão.
authenticatedPurchase.card.expiryYear	N	R	4	Ano de expiração do cartão.
authenticatedPurchase.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authenticatedPurchase.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
authenticatedPurchase.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).
authenticatedPurchase.userDefinedField.udf2	AN	O	255	
authenticatedPurchase.userDefinedField.udf3	AN	O	255	
authenticatedPurchase.userDefinedField.udf4	AN	O	255	
authenticatedPurchase.userDefinedField.udf5	AN	O	255	
authenticatedPurchase.xid	AN	O	40	Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authenticatedPurchase.ucaf	AN	O	40	Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authenticatedPurchase.eci	N	O	2	Código ECI da transação Autenticada 3D Secure. Gerado por um MPI Externo. Ver processo.
authenticatedPurchase.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authenticatedPurchase.softDescriptor	AN	O	22	Ver *Regra para Soft-Descriptor*.
authenticatedPurchase.addlReqData	AN	O	255	Ver *Regras para AddlReqData*.
authenticatedPurchase.tranType	AN	R	6	Identifica o tipo de pagamento a ser efetuado: **CREDIT** – Crédito **DEBIT** – Débito
authenticatedPurchase.brazilAccountType	N	O	2	**Usado pelo Verified by Visa Brasil** Tipo de modalidade de compra selecionado pelo Portador do cartão. **Valor** – Descrição **00** – NOT APPLICABLE **01** – CREDIT **02** – DEBIT
authenticatedPurchase.brazilMobileNumber	N	O	25	**Usado pelo Verified by Visa Brasil** Identifica o número de telefone do Portador do Cartão.
authenticatedPurchase.brazilTranType	N	O	2	**Usado pelo Verified by Visa Brasil** Indica o tipo de transação informado pela Loja. **Valor** – Descrição **00** – Os bens/serviços de Compra **03** – Verificar aceitação

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

```
<authenticatedPurchaseService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <authenticatedPurchase>
      <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:-->
      <tranType>string</tranType>
      <!--Optional:-->
      <brazilAccountType>string</brazilAccountType>
      <!--Optional:-->
      <brazilMobileNumber>string</brazilMobileNumber>
      <!--Optional:-->
```

```
      <brazilTranType>string</brazilTranType>
    </authenticatedPurchase>
  </arg0>
</authenticatedPurchaseService>
```

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

```
<authenticatedPurchaseServiceResponse>
   <!--Optional:-->
   <authenticatedPurchaseResponse>
      <result>
     "Os retornos são sempre no objeto Result. Veja a Relação de TAGs de retorno de operações Autenticadas (3D Secure)"
      </result>
   </authenticatedPurchaseResponse>
</authenticatedPurchaseServiceResponse>
```

3.2.8 MÉTODO AUTHENTICATEDAUTHORIZATIONSERVICE

Executa uma Autorização autenticada 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.
authenticatedAuthorization	n/a	R	1	Elemento da transação.
authenticatedAuthorization.terminalID	AN	R	10	Ver *Regra para TerminalID*.
authenticatedAuthorization.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
authenticatedAuthorization.amount	N	R	19	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
authenticatedAuthorization.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
authenticatedAuthorization.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor

TAG	Tipo	Obrig.	Tam.	Descrição
authenticatedAuthorization.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
authenticatedAuthorization.tranCategory	AN	R	4	Identifica a categoria da transação a ser efetuado: **DFLT** – Todas **IATA** – Transações Cias Aéreas Ver *Regra para TranCategory*.
authenticatedAuthorization.card	n/a	R	1	Elemento com os dados do cartão.
authenticatedAuthorization.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
authenticatedAuthorization.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
authenticatedAuthorization.card.expiryMonth	N	R	2	Mês de expiração do cartão.
authenticatedAuthorization.card.expiryYear	N	R	4	Ano de expiração do cartão.
authenticatedAuthorization.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authenticatedAuthorization.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
authenticatedAuthorization.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).
authenticatedAuthorization.userDefinedField.udf2	AN	O	255	
authenticatedAuthorization.userDefinedField.udf3	AN	O	255	
authenticatedAuthorization.userDefinedField.udf4	AN	O	255	
authenticatedAuthorization.userDefinedField.udf5	AN	O	255	
authenticatedAuthorization.xid	AN	O	40	Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authenticatedAuthorization.ucaf	AN	O	40	Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authenticatedAuthorization.eci	N	O	2	Código ECI da transação Autenticada 3D Secure. Gerado por um MPI Externo. Ver processo.
authenticatedAuthorization.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authenticatedAuthorization.softDescriptor	AN	O	22	Ver *Regra para Soft-Descriptor*.
authenticatedAuthorization.addlReqData	AN	O	255	Ver *Regras para AddlReqData*.
authenticatedAuthorization.tranType	AN	R	6	Identifica o tipo de pagamento a ser efetuado: **CREDIT** – Crédito **DEBIT** – Débito
authenticatedAuthorization.brazilAccountType	N	O	2	**Usado pelo Verified by Visa Brasil** Tipo de modalidade de compra selecionado pelo Portador do cartão. **Valor** – Descrição **00 –** NOT APPLICABLE **01** – CREDIT **02** – DEBIT
authenticatedAuthorization.brazilMobileNumber	N	O	25	**Usado pelo Verified by Visa Brasil** Identifica o número de telefone do Portador do Cartão.

TAG	Tipo	Obrig.	Tam.	Descrição
authenticatedAuthorization.brazilTranType	N	O	2	**Usado pelo Verified by Visa Brasil** Indica o tipo de transação informado pela Loja. **Valor** – Descrição **00** – Os bens/serviços de Compra **03** – Verificar aceitação

O quadro a seguir demonstra as TAGs XML do "Service Request" do AuthenticatedAuthorizationService:

```
<authenticatedAuthorizationService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <authenticatedAuthorization>
      <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:-->
      <tranType>string</tranType>
      <!--Optional:-->
      <brazilAccountType>string</brazilAccountType>
      <!--Optional:-->
      <brazilMobileNumber>string</brazilMobileNumber>
      <!--Optional:-->
      <brazilTranType>string</brazilTranType>
    </authenticatedAuthorization>
  </arg0>
</authenticatedAuthorizationService>
```

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

```
<authenticatedAuthorizationServiceResponse>
   <!--Optional:-->
   <authenticatedAuthorizationResponse>
      <result>
     "Os retornos são sempre no objeto Result. Veja a Relação de TAGs de retorno de operações Autenticadas (3D Secure)"
      </result>
   </authenticatedAuthorizationResponse>
</authenticatedAuthorizationServiceResponse>
```

3.2.9 MÉTODO AUTHENTICATIONONLYSERVICE

Executa apenas o processo de Autenticação, sem realizar a Autorização da transação (sem sensibilizar o saldo do Portador do Cartão). Este método gera apenas as chaves de Autenticação, podendo utilizar estes dados para realizar a operação de Crédito pelos métodos *Método* PurchaseService ou *Método* AuthorizationService.

Método tem o objetivo de quando o desejo é realizar uma Autorização Externa, por exemplo com uma Integradora de TEF. Onde após obter os dados de retorno da Autenticação, os mesmos podem ser inseridos na Autorização de uma transação TEF Dedicado.

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.
authenticationOnly	n/a	R	1	Elemento da transação.
authenticationOnly.terminalID	AN	R	10	Ver *Regra para TerminalID*.
authenticationOnly.merchantTrackID	AN	R	40	ID da transação, que deverá ser gerado pela Loja Virtual. Este deve ser único por transação.
authenticationOnly.amount	N	R	19	Valor da transação. O formato deve ser o valor inteiro com ponto e 2 casas decimais. Ex.: "10000.00"
authenticationOnly.currencycode	N	R	3	Código da moeda. Segue o padrão ISO 4217. O valor padrão é 986 – Real.
authenticationOnly.instType	N	R	3	Identifica o tipo de pagamento a ser efetuado: **SGL** - À vista **ACQ** - Parcelado Lojista **ISS** - Parcelado Emissor
authenticationOnly.instNum	N	O	2	Para transações parceladas indica o número de parcelas. Para transações à vista não deve ser preenchido.
authenticationOnly.tranCategory	AN	R	4	Identifica a categoria da transação a ser efetuado: **DFLT** – Todas **IATA** – Transações Cias Aéreas Ver *Regra para TranCategory*.
authenticationOnly.card	n/a	R	1	Elemento com os dados do cartão.
authenticationOnly.card.number	N	R	0..19	Número do cartão do portador que será utilizado na transação.
authenticationOnly.card.cvv2	N	O	0..5	O código de segurança, encontrado no verso do cartão do portador.
authenticationOnly.card.expiryMonth	N	R	2	Mês de expiração do cartão.
authenticationOnly.card.expiryYear	N	R	4	Ano de expiração do cartão.
authenticationOnly.card.holderName	AN	R	26	Nome do portador impresso no cartão.
authenticationOnly.userDefinedField	n/a	O	1	Elemento com os campos livres de preenchimento.
authenticationOnly.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).
authenticationOnly.userDefinedField.udf2	AN	O	255	
authenticationOnly.userDefinedField.udf3	AN	O	255	
authenticationOnly.userDefinedField.udf4	AN	O	255	
authenticationOnly.userDefinedField.udf5	AN	O	255	
authenticationOnly.xid	AN	O	40	Identificador do MPI para cada transação autenticada. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.
authenticationOnly.ucaf	AN	O	40	Código de autenticação criptografado pela Bandeira. O conteúdo do campo pode ser um valor HEXA ou Base64, de acordo com o MPI utilizado.

TAG	Tipo	Obrig.	Tam.	Descrição
authenticationOnly.eci	N	O	2	Código ECI da transação Autenticada 3D Secure. Gerado por um MPI Externo. Ver processo.
authenticationOnly.tranMCC	N	O	4	Ver *Regra para MCC Dinâmico*.
authenticationOnly.softDescriptor	AN	O	22	Ver *Regra para Soft-Descriptor*.
authenticationOnly.addlReqData	AN	O	255	Ver *Regras para AddlReqData*.
authenticationOnly.tranType	AN	R	6	Identifica o tipo de pagamento a ser efetuado: **CREDIT** – Crédito **DEBIT** – Débito
authenticationOnly.brazilAccountType	N	R	2	Length1–2, Numeric digits **00** – NOT APPLICABLE **01** – CREDIT **02** – DEBIT
authenticationOnly.brazilMobileNumber	N	R	8	Identifica a modalidade do pagamento a ser efetuado: **CREDIT** - Crédito **DEBIT** – Débito
authenticationOnly.brazilTranType	N	R	2	Usado para o Verified by Visa Brasil. Indica o tipo de transação informado pelo comerciante. Os valores válidos são: 00 - Os bens / serviços de Compra 03 - Verificar aceitação 10 - Financiamento 11 - Operação Quasi-Cash 28 - Pré-pago Ativação e carga

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

```
<authenticationOnlyService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <authenticationOnly>
      <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:-->
      <tranType>string</tranType>
      <!--Optional:-->
      <brazilAccountType>string</brazilAccountType>
      <!--Optional:-->
      <brazilMobileNumber>string</brazilMobileNumber>
      <!--Optional:-->
      <brazilTranType>string</brazilTranType>
    </authenticationOnly>
  </arg0>
</authenticationOnlyService>
```

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

```
<authenticationOnlyServiceResponse>
   <!--Optional:-->
   <authenticationOnlyResponse>
      <result>
     “Os retornos são sempre no objeto Result. Veja a Relação de TAGs de retorno de operações Autenticadas (3D Secure)”
      </result>
   </authenticationOnlyResponse>
</authenticationOnlyServiceResponse>
```

3.2.10 MÉTODO FINALIZEAUTHENTICATIONSERVICE

Finaliza o processo de Autenticação 3DS.

Se utilizada a operação AuthenticatedPurchaseService, realiza a Autorização e Captura da transação, se a Autorização for aprovada.

Se utilizada a operação AuthenticatedAuthorizationService, realiza a Autorização da transação, ficando pendente de Confirmação, se a Autorização for aprovada.

Se utilizada a operação AuthenticationOnlyService, apenas retorna os dados da Autenticação para realizar a operação desejada.

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.
finalizeAuthentication	n/a	R	1	Elemento da transação.
finalizeAuthentication.terminalID	AN			Ver *Regra para TerminalID*.
finalizeAuthentication.PARes	AN	R	40	Assinada digitalmente e informando os resultados da autenticação 3D Secure do Portador pelo Emissor.
finalizeAuthentication.paymentid	N	R	20	Identificador único gerado e usado para identificar pagamentos

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

```
<finalizeAuthenticationService>
  <!--Optional:-->
  <arg0>
    <authentication>
      <username>string</username>
      <password>string</password>
      <merchantID>string</merchantID>
    </authentication>
    <finalizeAuthentication>
      <terminalID>string</terminalID>
      <PARes>string</PARes>
      <paymentid>string</paymentid>
    </finalizeAuthentication>
  </arg0>
</finalizeAuthenticationService>
```

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

```
<finalizeAuthenticationServiceResponse>
   <!--Optional:-->
   <authorizationResponse>
     <result>
   "Os retornos são sempre no objeto Result. Veja a Relação de TAGs de retorno de operações Autenticadas (3D Secure)"
     </result>
   </authorizationResponse>
</finalizeAuthenticationServiceResponse>
```

3.2.11 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	19	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.

TAG	Tipo	Obrig.	Tam.	Descrição
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. 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*.

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>
      </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>
```

3.2.12 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	19	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>
```

3.2.13 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*.
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	19	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>
```

3.2.14 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*.
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	19	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>
```

3.2.15 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.
result.descriptionResponse	A	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)
result.responseCode	N	Códigos de Resposta do Emissor do Cartão e do Sistema de Captura da GETNET. (Veja os *Códigos de Retorno do Emissor / Getnet*)
result.responseMessage	AN	Descrição do motivo do Código de Resposta. (A descrição é a mesma que consta na listagem de *Códigos de Retorno do Emissor / Getnet*)
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.cvv2response	AN	Valor retornado referente a validação do campo CVV2

<table>
<tr><th>TAG</th><th>Tipo</th><th>Descrição</th></tr>
<tr><td>result.eci</td><td></td><td>Campo disponível a partir da versão 2.0.
Código indicando se a transação foi processada com Autenticação do Portador.
<table>
<tr><th>VISA / MASTERCARD</th><th>Status da Autentição</th><th>Descrição</th></tr>
<tr><td>05 / 02</td><td>Sim</td><td>Autenticada</td></tr>
<tr><td>06 / 01</td><td>Não</td><td>Emissor/portador não participa do 3DSecure</td></tr>
<tr><td>07 / 00</td><td>Não</td><td>Não autenticada/</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 (DDMM) realização da transação</td></tr>
<tr><td>result.udf1</td><td>A</td><td rowspan="5">Campos de apoio e alternativos na transação, qualquer conteúdo pode ser informado e recuperado nestas variáveis.</td></tr>
<tr><td>result.udf2</td><td>A</td></tr>
<tr><td>result.udf3</td><td>A</td></tr>
<tr><td>result.udf4</td><td>A</td></tr>
<tr><td>result.udf5</td><td>A</td></tr>
<tr><td>result.instAmt1</td><td>N</td><td>Para as transações parceladas, este contém o valor da primeira parcela a ser paga.</td></tr>
<tr><td>result.instAmtN</td><td>N</td><td>Para as transações parceladas, este contém o valor das demais parcelas a serem pagas.</td></tr>
<tr><td>result.instAmtT</td><td>N</td><td>Para as transações parceladas, este contém o valor total a ser pago (valor acrescido dos juros, impostos, taxas, etc).</td></tr>
<tr><td>result.amout</td><td>N</td><td>Retorna o valor da transação da transação que foi realizada.</td></tr>
<tr><td>result.currencycode</td><td>N</td><td>Retorna o código da moeda da transação que foi realizada.</td></tr>
<tr><td>result.instType</td><td>N</td><td>Identifica o tipo de pagamento efetuado:
SGL - À vista
ACQ - Parcelado Lojista
ISS - Parcelado Emissor</td></tr>
<tr><td>result.instNum</td><td>N</td><td>Retorna o número de parcelas da transação que foi realizada.</td></tr>
<tr><td>result.tranMCC</td><td>N</td><td>Retorna o tranMCC da transação que foi realizada.</td></tr>
<tr><td>result.softDescriptor</td><td>AN</td><td>Retorna o SoftDescriptor da transação que foi realizada.</td></tr>
</table>

TAG	Tipo	Descrição
result.addlResData		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.
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*)

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:-->
            <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>
         </result>
      </result>
   </.../...Response>
</.../...ServiceResponse>
```

3.2.16 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.
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.
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*)

VISA / MASTERCARD	Status da Autentição	Descrição
05 / 02	Sim	Autenticada
06 / 01	Não	Emissor/portador não participa do 3DSecure
07 / 00	Não	Não autenticada/

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
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 '**D123456701**' 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	D	01	D123456701
Para as transações de MasterCard Crédito	D	02	D123456702
Para as transações de Visa Crédito e Crédito Autenticado	E	01	E123456701
Para as transações de MasterCard Crédito e Crédito Autenticado	E	02	E123456702
Para as transações de Visa Electron Débito Autenticado	E	03	E123456703
Para as transações de Maestro Débito Autenticado	E	04	E123456704
Para as transações de Visa Crédito BNDES	D	05	D123456705
Para as transações de MasterCard Crédito BNDES	D	06	D123456706
Para transações ELO Crédito	D	07	D123456707
Para transações ELO Débito	D	08	D123456708
Para transações American Express Crédito	D	09	D123456709

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

Para aceitação do MasterPass e do Visa Checkout é preciso que o EC faça uma integração com as bandeiras MasterCard e Visa, respectivamente, para receber as informações do portador. Esta integração é feita diretamente, e não tem envolvimento da Getnet. Após este desenvolvimento, o EC oferece os botões do MasterPass e/ou Visa Checkout como novas formas de pagamento, e ao ser utilizado um deles, envia os dados específicos indicando a utilização do mesmo na transação para a Getnet.

Valores Aceitos

- MasterPass
  - WTYP=01 (Domínio interno da Getnet para identificar a carteira)
  - WID=101,102, etc. (Domínio de acordo com a carteira escolhida, retornado pelo MasterPass)
- Visa Checkout
  - WTYP=02 (Domínio interno da Getnet para identificar a carteira)
  - WID=VCIND (Domínio de acordo com retorno do Visa Checkout, atualmente apenas VCIND)

Exemplo de preenchimento

```
// se foi utilizado o MasterPass
<addlReqData>WTYP=01;WID=101;</addlReqData>

// se foi utilizado o Visa Checkout
<addlReqData>WTYP=02;WID=VCIND;</addlReqData>
```

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.

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

Códigos de Resposta gerados pelo Emissor do Cartão	
Código	**Descrição**
00	APROVADA. TRANSACAO EXECUTADA COM SUCESSO
SF	TRANSACAO EXECUTADA COM SUCESSO
01	TRANSACAO REFERIDA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
02	TRANSACAO REFERIDA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
03	ESTABELECIMENTO INVALIDO
04	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
05	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
06	ERRO NO PROCESSAMENTO
08	TRANSACAO APROVADA SOB IDENTIFICACAO
10	TRANSACAO NAO AUTORIZADA
12	TRANSACAO INVALIDA
13	VALOR DA TRANSACAO INVALIDO
14	CARTAO INVALIDO
15	CARTAO NAO PERTENCE A REDE GETNET
19	EMISSOR TEMPORARIAMENTE FORA DE OPERACAO
23	CARTAO EXCEDEU O LIMITE PARA PARCELAMENTO

Códigos de Resposta gerados pelo Emissor do Cartão	
Código	**Descrição**
27	TRANSACAO NAO PERMITIDA P/ PRODUTO. LIGUE GETNET
28	QUANTIDADE DE PARCELAS NAO PERMITIDA P/ PRODUTO. LIGUE GETNET
30	ERRO DE FORMATO. TENTE NOVAMENTE
31	INSTITUICAO NAO PERTENCE A REDE GETNET
33	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
36	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
38	EXCEDIDO NUMERO DE TENTATIVAS DO PIN
41	CARTAO EXTRAVIADO
43	TRANSACAO NAO AUTORIZADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
51	TRANSACAO NAO AUTORIZADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
54	CARTAO VENCIDO
55	SENHA INCORRETA
56	ERRO NOS DADOS INFORMADOS
57	TRANSACAO NAO PERMITIDA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
58	TRANSACAO NAO PERMITIDA. ENTRE EM CONTATO COM A GETNET
61	LIMITE DE RETIRADA EXCEDIDO
62	CARTAO RESTRITO
64	PARCELADO NAO PERMITIDO PARA CARTAO
65	QUANTIDADE DE SAQUES EXCEDIDA
68	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE (TIME OUT)
75	SENHA BLOQUEADA
76	CARTAO BLOQUEADO
78	TRANSACAO NAO AUTORIZADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
82	CVV INVALIDO.
84	NUMERO DO CARTAO INVALIDO
85	SISTEMA DO EMISSOR INDISPONIVEL. TENTE NOVAMENTE
86	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE
87	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE
88	SISTEMA DO EMISSOR INDISPONIVEL. TENTE NOVAMENTE
89	BANDEIRA NAO PERTENCE A REDE GETNET
94	TRANSMISSAO DUPLICADA. TENTE NOVAMENTE
N0	SISTEMA DO EMISSOR INDISPONIVEL. LIGUE EMISSOR
N1	NUMERO DO CARTAO INVALIDO
N2	LIMITE DE SAQUE EXCEDIDO
N3	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
N4	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
N5	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
N6	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
N7	CVV2 INVALIDO
N8	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
N9	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
O0	SISTEMA DO EMISSOR INDISPONIVEL. TENTE NOVAMENTE
O1	SISTEMA DO EMISSOR INDISPONIVEL. TENTE NOVAMENTE
O2	VALOR INVALIDO. TENTE NOVAMENTE
O3	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
O4	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
O5	SENHA INVALIDA. TENTE NOVAMENTE
O6	NUMERO DO CARTAO INVALIDO

Códigos de Resposta gerados pelo Emissor do Cartão	
Código	**Descrição**
O7	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
O8	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
O9	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P0	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P1	LIMITE DE SAQUE EXCEDIDO
P2	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P3	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P4	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P5	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P6	SOLICITE AO CLIENTE CONTATAR O EMISSOR
P7	VALOR INVALIDO. TENTE NOVAMENTE
P8	NUMERO DO CARTAO INVALIDO
P9	LIMITE DE SAQUE EXCEDIDO
Q0	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE
Q1	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE
Q2	TRANSACAO NAO COMPLETADA. TENTE NOVAMENTE
Q3	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q4	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q5	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q6	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q7	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q8	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
Q9	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
R6	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
R7	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
R8	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
S4	SOLICITE AO CLIENTE CONTATAR O EMISSOR
S8	SOLICITE AO CLIENTE CONTATAR O EMISSOR
S9	SOLICITE AO CLIENTE CONTATAR O EMISSOR
T0	PRODUTO NÃO HABILITADO
T1	VALOR INVALIDO. TENTE NOVAMENTE
T2	ERRO NOS DADOS INFORMADOS. TENTE NOVAMENTE
T3	CARTAO NAO PERTENCE A REDE GETNET
T4	SOLICITE AO CLIENTE CONTATAR O EMISSOR
T5	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
T6	SOLICITE AO CLIENTE CONTATAR O EMISSOR
T7	TRANSACAO NAO APROVADA. SOLICITE AO CLIENTE CONTATAR O EMISSOR
T8	CARTAO INVALIDO

A. 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** (apenas para o Reino Unido e Singapura); - 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***

TERMO	DEFINIÇÃO
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***
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.
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 **EC**s. 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, Diners, Hiper, Elo e Aura.
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.

TERMO	DEFINIÇÃO
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. Também é responsável pelo gerenciamento da experiência de compra online do ***Portador***.
ECI	Ver ***Electronic Commerce Indicator***

TERMO	DEFINIÇÃO
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.
Emissor	Instituição financeira que emite cartões de pagamento (Débito e/ou Crédito) e mantém contrato com o Portador para prestar os serviços de cartão. Para identificar qual é o Emissor do cartão, usam-se os 6 primeiros números do cartão, chamados de **BIN**. Também 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.
Gateway de Pagamento	Terceiro que provê uma interface entre o ***Lojista*** e o sistema de pagamento do ***Adquirente***.
IIN	*Issuer Identification Number* (Número de Identificação do Emissor). O mesmo que **BIN**.
Lojista	Ver **EC (Estabelecimento Comercial)**.
Mastercard SecureCode	Implementação da Mastercard do protocolo 3D Secure. Ver **3D Secure**
MasterCard	Uma das principais Bandeiras internacionais. Ver **Bandeira**
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*.

TERMO	DEFINIÇÃO
MPI	Ver ***Merchant Server Plug In***
PAN	***Primary Account Number*** (Número de Conta Primário). O número do cartão de Crédito e/ou Débito, criado de acordo com a norma ISO/IEC 7812. O PAN tem geralmente 16 dígitos, mas pode conter até 19, na seguinte estrutura: - 6 dígitos representando o **IIN**/**BIN**; - 7 a 12 dígitos (geralmente 9), que identificam o **Portador**; - 1 dígito verificador, calculado usando-se o Algoritmo de Luhn.
PAReq	Ver ***Payer Authentication Request***
PARes	Ver ***Payer Authentication Response***
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.
ProtectBuy	Implementação da Diners Club do protocolo 3D Secure. Ver ***3D Secure***
SafeKey	Implementação da American Express do protocolo 3D Secure. Ver ***3D Secure***

TERMO	DEFINIÇÃO
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***
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***

TERMO	DEFINIÇÃO
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

B. 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-lo 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).*

getnet
Uma empresa Santander

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