3DS GETNET

Manual de Integração

V.01.6

Getnet – Uma empresa Santander

Válido até: 12/2022

COPYRIGHT

CONTROLE DE VERSÕES

Versão	Data	Descrição
1.0	11/2019	- Criação do documento
1.1	02/2020	- Melhorias na apresentação do fluxo de implementação
1.2	05/2020	- Retornos dos serviços - Inclusão de estruturas de dados trocada entre o front-end e back-end do estabelecimento.
1.3	07/2020	- Tópico 2.1.3 – detalhamento sobre Desafios: escolha emissor e número do telefone em caso de SMS; - Tópico 2.2 – Tabela com as bandeiras disponíveis para solicitação de autenticação 3DS v2.1 - Tópicos 3.4.2 e 3.4.3 – Detalhamento nos retornos da tag <status> e StatusCode - Tópico 3.5: Integração com serviços de autorização - Tópico 4.1: Atualização dos cenários e cartões para homologação
1.4	08/2020	- Tópico 3.3.1 e 3.3.4 - Campos de configuração - receberam complementações - XMLs e Json - para colher dados do browser do cliente, se assim indicado. Reduz chance de downgrade para versão 1.0. - Tópico 3.4.2 - Recebeu a tag DeviceInformation com campos para trafegar as informações sobre o browser do cliente. Removido a tag de grupo BuyerInformation. - Tópico 3.4.3 – Complementação para análise no retorno quando indicando falha na autenticação. Campo authenticationStatusMsg adicionado no retorno do XML; - Tópico 4 - Descrição dos retornos do campo veresEnrolled para análise de falhas na autenticação.
1.5		
1.6	03/2021	Melhoria na orientação de campo obrigatórios.

SUMÁRIO

1 INTRODUÇÃO

Bem-vindo à Getnet!

Este é o manual para que você possa adotar a solução “3DS Getnet”. O protocolo de autenticação 3DS poderá ser atendido nas versões 1.0 e 2.1. Neste manual onde mencionarmos “3DS Getnet” sem especificar a versão, nos referimos à ambas as versões.

Com este manual você poderá:

- Avaliar a solução 3DS Getnet;
- Realizar a implantação da solução 3DS Getnet.

Este serviço permite aos estabelecimentos credenciados utilizarem o protocolo de mensagens que promovem a autenticação do consumidor, permitindo a realização de compras de comércio eletrônico com cartão não presente (CNP).

A intenção é buscar uma autenticação de forma transparente, sempre que possível, pois há casos em que a autenticação poderá exigir alguma confirmação ao consumidor.

Sugerimos que este documento seja lido com atenção, e usado como guia de referência para quaisquer dúvidas, não somente no momento da implementação do “3DS 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. O presente manual é um anexo do “Manual de Integração do e-Commerce” (A partir da versão 6.0).

1.1 A QUEM SE DESTINA

O conteúdo deste manual se destina a programadores e desenvolvedores de plataformas para comércio eletrônico que necessitem desta camada de autenticação no protocolo 3DS 1.0/2.1 oferecida pela Getnet.

Neste documento o desenvolvedor/analista terá acesso a todos os passos e processos referentes à integração com o sistema “3DS 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.

Por favor, utilize o contato que lhe forneceu este manual

Com isso, você poderá esclarecer dúvidas quanto à implementação

2 VISÃO GERAL

Este manual cobre o protocolo de comunicação na utilização das funcionalidades disponíveis e nele são apresentadas as informações técnicas para utilizar cada uma delas.

Será apresentada o modo de conexão no 3DS Getnet com sua forma de comunicação para o protocolo 3DS 1.0 e 2.1.

2.1 SOLUÇÃO DE AUTENTICAÇÃO 3DS GETNET

O "3DS Getnet" é um protocolo de mensagens que busca maximizar a autenticação do consumidor sem atrito em transações de compras realizadas em comércio eletrônico com cartão não presente (CNP). Porém, podem haver casos em que serão solicitados desafios ao consumidor.

O objetivo é minimizar o índice de fraude sem prejudicar a taxa de conversão. Isso se tornou possível a partir do momento em que a indústria de meio de pagamento desenvolveu um novo padrão de autenticação, chamado "EMV 3-D Secure" ou "protocolo 3DS".

Este protocolo de mensagens trata-se de uma camada de segurança adicional, que ajuda a identificar se o portador do cartão é ele mesmo, facilitando o aumento das taxas de aprovação e, também, buscando adicionar uma camada adicional de proteção ao comerciante, além do seu processo de antifraude CNP já existente, evitando possíveis *chargebacks*.

Benefícios da solução "3DS Getnet":

- Disponibilização de **API Javascript** que facilita a integração com seu e-commerce;
- Permite a execução de **regras de negócios** próprias em seu ambiente (back-end);
- Com a versão 3DS 2.1, torna-se possível a "**autenticação silenciosa"**, sem a necessidade que um desafio seja solicitado ao portador;
- Diminui a possibilidade de transações **fraudulentas**;

2.1.1 DATA ONLY - NOTIFICAÇÃO

O "Data Only" é uma opção oferecida pela Bandeira Mastercard para os comerciantes que ainda não estejam prontos para atender todo o requisito do protocolo 3DS 2.1, mas que já querem iniciar enviando os campos adicionais através da solução "3DS Getnet", mesmo que este não realize a autenticação por assim dizer, mas que já irá iniciar a contribuição com o processo de amadurecimento do 3DS 2.1 junto a Bandeira e Emissores. A transação nesta categoria deverá ser identificada pelo código 80 enviado através do campo "Categoria da transação" *(vide campo messageCategory no item 3.4.2)*

Este modelo traz o benefício de enriquecer a base de dados dos bancos emissores e da própria Mastercard que, com mais informações sobre os portadores de cada lojista, poderá enriquecer sua análise preditiva e, consequentemente, aprimorar a autenticação silenciosa e, também, o índice de aprovação dos emissores.

Além disto, atualmente o "Data Only" isenta o *fee/*taxa *e* cobrado pela bandeira Mastercard em relação a transações não autenticadas.

Vale ressaltar que o Data Only não realiza uma autenticação do emissor e com isto o risco (liability shift) de chargeback por fraude permanece com o lojista.

2.1.2 API JAVASCRIPT

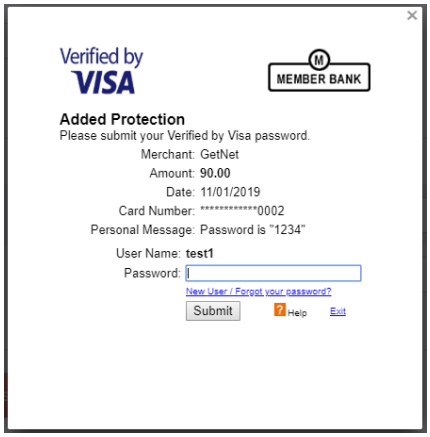
Um dos benefícios da solução "3DS Getnet" é oferecer um componente *javascript* nomeado "**getnet_3DS.js**" que, ao ser incorporado em sua solução de comercio virtual, será responsável por boa parte da integração do processo de autenticação entre sua loja e a Getnet, de forma simplificada.

2.1.3 DESAFIO

Durante o processo de autenticação, quando julgar necessário, o emissor pode solicitar um desafio que é composto por pedir ao portador a confirmação de alguns dados adicionais, informando um código de segurança enviado por SMS/texto, e-mail ou recursos biométricos. **Tipo de desafio**: É o próprio emissor quem define o tipo de desafio levando em consideração o dispositivo (device) utilizado pelo portador para acessar o e-commerce do estabelecimento. **Número de telefone:** Caso o desafio envolva SMS, será utilizado o número de telefone cadastrado na base de dados do emissor e não o número de telefone informado neste processo de solicitação de autenticação.

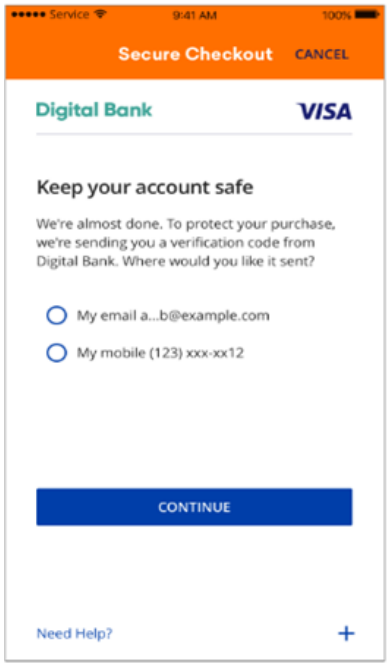
Abaixo exibimos modelos dos desafios que são apresentados ao portador na janela de e-commerce:

3DS 1.0 - Modelo

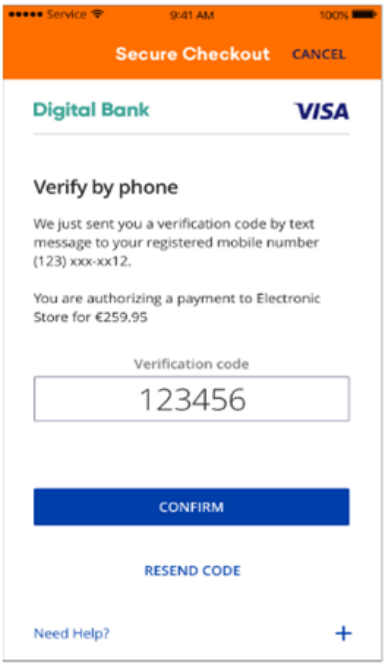


Solicitação da senha do cartão

3DS 2.1 - Modelo



Seleção do canal para recebimento do código de verificação



Digitação do código de verificação recebido

2.2 BANDEIRAS DISPONÍVEIS

Tabela com as bandeiras que estão contempladas para solicitação de autenticação 3DS versão 2.

Bandeiras		Modalidades habilitadas
	**MASTERCARD**	Crédito e Débito.
	**VISA**	Crédito e Débito.
	**AMERICAN EXPRESS**	Crédito em homologação pela bandeira.
	**ELO**	Crédito e Débito.
	**HIPERCARD**	Não disponível.

Em relação aos emissores disponíveis, cada bandeira tem portifólio próprio, recebendo atualização constante. Por favor, caso necessário, **consulte o nosso suporte durante a implementação** para obter esta informação devidamente atualizada.

3 REQUISITOS TÉCNICOS

A integração com a Getnet é realizada pelos 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.

Para implementar a integração com a solução "3DS Getnet", três passos principais deverão ser seguidos:

- O desenvolvedor front-end realizará a integração do *javascript*, disponibilizado pela Getnet, em sua aplicação de pagamento (Checkout);
- O front-end deverá se comunicar com o back-end da loja com a mensageria de comunicação request/response com o **JSON**;
- O desenvolvedor back-end fará a comunicação com o serviço do *CommerceService* para os métodos indicados neste manual.

Já a comunicação entre o front-end e o back-end da loja deverão estar no formato **JSON**.

O objetivo é efetuar a coleta e o tratamento dos dados referente ao portador e à transação e realizar a comunicação entre o estabelecimento e o respectivo emissor do cartão.

Nesta arquitetura, permitimos ao comerciante, realizar regras de negócio em seu back-end, como recuperar dados cadastrais, chamar o antifraude, entre outros.

3.1 POR ONDE COMEÇAR?

Você verá que a solução é composta por três camadas:

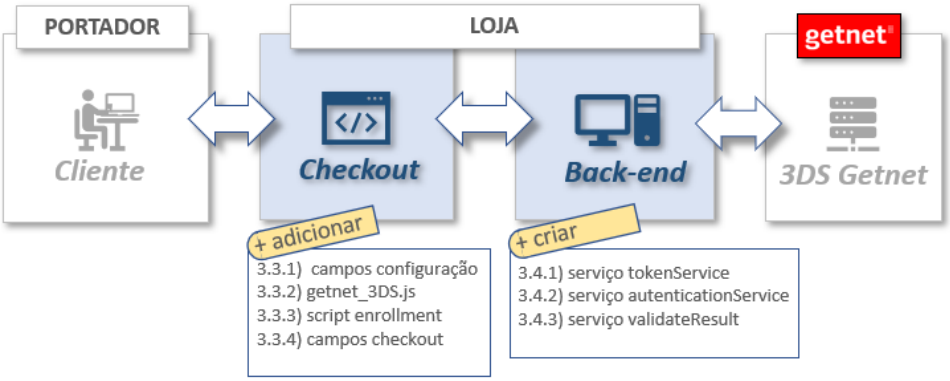
a) **Front-end:** processamento executado junto com a loja no browser do usuário (portador);
b) **Back-end:** camada que recebe os dados do front-end, complementa com dados mantidos no banco de dados e encaminha para a Getnet.
c) **3DS Getnet**: serviços do *CommerceService* disponibilizados pela Getnet para atender as requisições de autenticação 3DS;

Recomendamos que iniciem a análise pelo item (b), ou seja, o Back-end. Em torno desta camada você será capaz de entender e realizar as devidas integrações com as demais camadas (Front-end e 3DS Getnet).

3.2 COMPONENTES PARA A SOLUÇÃO 3DS GETNET

Aqui, apresentamos os componentes necessários para o fluxo da autenticação indicando como configurar e implementar a solução "3DS Getnet" em sua loja.

Premissa: Seu ***checkout*** deve acionar uma camada do seu ***back-end*** e somente esta última deve acionar os métodos/serviços do ***3DS Getnet***.



Para melhor entender os envolvidos em cada etapa da solução (fluxo acima), os descrevemos a seguir:

- **Portador:** Interações do portador do cartão com o checkout da loja;
- **Loja:** Refere-se aos sistemas da loja que devem incorporar a "API Javascript" no *front-end* e, também, implementações que precisam ser feitas em seu *back-end* para interação com os métodos/serviços do 3DS Getnet (webServices);
- **Getnet:** São os serviços disponibilizados pelo *CommerceService*;

3.3 ADICIONAR NO SEU CHECKOUT

O módulo de Checkout (front-end) de sua loja deverá receber alguns componentes para a implementação da solução 3DS Getnet, conforme detalhado abaixo.

3.3.1 CAMPOS CONFIGURAÇÃO

Inserir os campos de configuração abaixo no código HTML do Checkout de sua loja através da tag `<INPUT TYPE=HIDDEN>`.

Campos de Configuração	Descrição
gn3ds_merchantBackEndUrl	Preencher com o *endpoint* do back-end da loja
gn3ds_merchantBackEndTokenBasic	Preencher com as credenciais do *Basic Authentication*, caso tenha
gn3ds_merchantBackEndTokenOauth	Preencher com as credenciais Oauth, caso tenha
gn3ds_environment	**Indicação do ambiente:** **sandbox = SDB,** **produção = PRD**
gn3ds_debug	Caso queira utilizar o modo debug da aplicação. Valores permitidos: true ou false. Requer o "console" aberto. Deve-se preencher com "false" para produção.
gn3ds_debugPrefix	Preencher com "[GN3DS]", caso for utilizar o debug
gn3ds_frameworkModal	Preencher com "default" ou "bootstrap3" (necessário bootstrap versão 3) Este necessário para renderização do desafio.

gn3ds_newApiVersion	Disponibilidade de dados adicionais sobre browser: **false** = sinaliza que não há campos disponíveis para envio de informações adicionais sobre o browser; **true** = sinaliza que podem ser captadas informações sobre o browser do cliente;

Exemplo de como cada campo deve ser inserido na página HTML:

```
<input type="hidden" id="gn3ds_environment" name="gn3ds_environment"
class="gn3ds_environment" value="PRD" />
```

3.3.2 GETNET_3DS.JS

A solução envolve o carregamento do arquivo *javascript* disponibilizado pela Getnet, definido como "API Javascript" e identificado por "**`getnet_3ds.js`**", que deverá ser embutido no front-end da loja responsável pelo checkout de sua aplicação de e-Commerce.

Importante: Para evitar problemas relacionados a cache no browser do cliente, acrescente data e hora (do período de implementação em seu código) ao nome do arquivo original, apenas para diferenciar da versão anterior. Isso garantirá que atualizações futuras deste *javascript*, se necessário for, serão consideradas e carregadas adequadamente no browser do cliente. **Exemplo do formato sugerido:** **`getnet_3ds_1912150842.js`** (data/hora: 15/12/2019 08h42).

Utilize as tags HTML para referenciar o arquivo/script:

```
<script src="http://url_da_loja/getnet_3ds_aammddHHMM.js"
type="text/javascript"></script>
```

3.3.3 SCRIPT ENROLLMENT

O trecho de código (javascript) deve ser adicionado ao final do código do Checkout de sua loja:

```
function enrollment() {

    //Inserir regra de negócio
    GN3DS.init(function(response) { //Inicia o processo 3d

        //Inserir regra de negócio
        if (response != null &&
            response.status >= 200 &&
            response.status <= 299) {

            //Inicia a authenticação do 3ds
            GN3DS.authentication(function(response) {
            //Inserir regra de negócio
                 if (response != null &&
                    response.status >= 200 &&
                    response.status <= 299) {

                  //Tratar o sucesso

                  } else {

             //Tratar o erro
                }
           });
```

```
            } else {
                alert("Página não está pronta.");
            }
        });
    }
```

3.3.4 CAMPOS CHECKOUT

Deve-se inserir campos na página de checkout, descritos na tabela abaixo, para enviar informações ao back-end. São campos definidos através da *tag* <INPUT TYPE=HIDDEN>.

Caso seja mais conveniente, os dados "não obrigatórios" (no front-end) podem ser carregados e encaminhados através da camada de back-end.

Para aumentar a chance de uma autenticação silenciosa (sem aplicação de desafio), o envio de informações sobre o portador e sobre a compra é muito importante.

FRONT-END Campo Tela - Checkout <input text>	Obriga-tório	Muito Recomen-dado	Tipo	Tam.	Descrição
gn3ds_personalId	Não	**Sim**	string	26	Documento do portador do cartão, a falta do envio dessa informação pode ocasionar uma autenticação com desafio ou até mesmo uma falha na autenticação.
gn3ds_personalType	Não	**Sim**	string	14	O tipo de documento que será enviado, a falta do envio dessa informação pode ocasionar uma autenticação com desafio ou até mesmo uma falha na autenticação. - CPF - CPNJ (cnpj)
gn3ds_currency	**Sim**	**Sim**	string	3	Moeda na qual o valor da compra é expresso, , a falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_totalAmount	**Sim**	**Sim**	string	19	Valor da compra na menor unidade monetária sem nenhuma pontuação, a falta do envio dessa informação vai ocasionar uma falha na autenticação. Formato: 9999999999999999.99 **Importante:** Apenas o "ponto" do decimal é aceito. Não deve ser enviada "vírgula" indicando milhar.
gn3ds_shipToAddress1	Não	Não	string	60	Ambos os campos são destinados ao endereço de entrega do portador associado ao cartão utilizado na compra. **Importante**: Deve-se iniciar pelo logradouro, respeitando o formato de endereço, ou pode causar falha na autenticação.
gn3ds_shipToAddress2	Não	Não	string	60	
gn3ds_shipToAdministrativeArea	Não	Não	string	2	Estado (UF) do endereço de entrega do portador associado ao cartão utilizado na compra.
gn3ds_shipToCountry	Não	Não	string	2	País do endereço de entrega do portador associado ao cartão utilizado na compra.
gn3ds_shipToLocality	Não	Não	string	50	Cidade do endereço de entrega. Não incluir informações adicionais sob risco de falhar a autenticação. Ex: São Paulo (capital) – a informação "capital" não deve ser incluída.
gn3ds_shipToFirstName	Não	Não	string	60	Primeiro nome da pessoa que recebe a mercadoria
gn3ds_shipToLastName	Não	Não	string	60	Último sobrenome da pessoa que recebe a mercadoria
gn3ds_shipToPostalCode	Não	Não	string	10	CEP do endereço de cobrança do portador associado ao cartão utilizado na compra (sem traço e ponto)
gn3ds_shipToDestinationCode	Não	Não	string	2	Local de entrega. Conteúdos possíveis:

					01- Enviar para o endereço de cobrança do titular do cartão; 02- Enviar para outro endereço confirmado pela loja 03- Enviar para endereço diferente do endereço de cobrança 04- Enviar para a loja (o endereço da loja deve ser preenchido no pedido) 05- Bens digitais (ex: e-Books), 06- Bilhetes de viagens e eventos, que não serão enviados. 07- Outro
FRONT-END Campo Tela - Checkout <input text>	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
gn3ds_shipToMethod	Não	Não	string	8	Método de envio da mercadoria. Conteúdo possíveis: - **lowcost**: serviço de menor custo - **sameday**: Courier ou serviço no mesmo dia - **oneday**: serviço no dia seguinte ou durante a noite - **twoday**: serviço de dois dias - **threeday**: serviço de três dias - **pickup**: Retirada na loja - **other**: Ourto método de envio - **none**: nenhum método de envio, porque o produto é um serviço ou assinatura Necessário para o American Express SafeKey (EUA).
gn3ds_item_#_totalAmount *	Não	Não	string	19	Valor da compra do item sem nenhuma pontuação. * O caracter # deve ser substituído pelo número de ordem do item apresentado. Devem ser repetidas estas TAGs para cada item do pedido.
gn3ds_item_#_unitPrice *	Não	Não	string	15	Valor unitário do item
gn3ds_item_#_quantity *	Não	Não	integer	10	Quantidade deste produto
gn3ds_item_#_sku *	Não	Não	string	255	Código do produto
gn3ds_item_#_description *	Não	Não	string	255	Descrição do produto
gn3ds_item_#_name *	Não	Não	string	255	Nome que identifique o produto
gn3ds_billToAddress1	Não	**Sim**	string	60	Ambos os campos são destinados ao endereço de cobrança do portador associado ao cartão utilizado na compra. **Importante:** Deve-se iniciar pelo logradouro, respeitando o formato de endereço, ou pode causar falha na autenticação.
gn3ds_billToAddress2	Não	**Sim**	string	60	
gn3ds_billToAdministrativeArea	Não	**Sim**	string	2	Estado (UF) do endereço de cobrança do portador associado ao cartão utilizado na compra.
gn3ds_billToCountry	Não	**Sim**	string	2	País do endereço de cobrança do portador associado ao cartão utilizado na compra.
gn3ds_billToLocality	Não	**Sim**	string	50	Cidade do endereço de cobrança do portador. Não incluir informações adicionais sob risco de falhar a autenticação. Ex: São Paulo (capital) – a informação “capital” não deve ser incluída.
gn3ds_billToHomePhone	Não	**Sim**	string	15	Número de telefone residencial fornecido pelo portador, enviar apenas números, sem espaços ou outros caracteres. **Exemplo:**1125660089
gn3ds_billToEmail	**Sim**	**Sim**	string	255	Endereço de e-mail do portador. Deve-se enviar um formato válido de e-mail, a falta do envio dessa informação vai ocasionar uma falha na autenticação. **Exemplo**: meucontato@empresa.com.br,

gn3ds_billToPostalCode	**Sim**	**Sim**	string	10	CEP do endereço de cobrança do portador associado ao cartão utilizado na compra, a falta do envio dessa informação pode ocasionar uma falha na autenticação.
gn3ds_billToMobilePhone	**Sim**	**Sim**	string	15	Número de celular fornecido pelo portador, enviar apenas números, sem espaços ou outros caracteres, a falta do envio dessa informação vai ocasionar falha na autenticação. **Exemplo:**11995660089
gn3ds_cardType	**Sim**	**Sim**	string	3	Tipo de cartão, a falta do envio dessa informação pode ocasionar uma autenticação com desafio ou até mesmo uma falha na autenticação.
gn3ds_cardExpirationMonth	**Sim**	**Sim**	string	2	Mês da Validade do cartão – MM A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_cardExpirationYear	**Sim**	**Sim**	string	4	Ano da Validade do cartão – AAAA A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_cardNumber	**Sim**	**Sim**	string	20	Número de conta que será utilizado na requisição de autorização para transações de pagamento. Pode ser representado por um PAN ou token. A falta do envio dessa informação vai ocasionar uma falha na autenticação.
FRONT-END Campo Tela - Checkout <input text>	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
gn3ds_cardHolderName	**Sim**	**Sim**	string	26/28	Nome do portador. Como impresso no cartão do portador. Importante: É nome completo do portador do cartão (ex: nome referente a fatura do cartão), a falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_installmentTotalCount	Não	Não	integer	4	Indica o número máximo de autorizações (parcelas) permitidas para um pagamento parcelado.
gn3ds_overridePaymentMethod	**Sim**	**Sim**	string	2	Indica o tipo de conta. Por exemplo, para um cartão multiconta como os cartões combo (crédito e débito) brasileiros, a falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_additionalData	Não	Não	string	2000	Este campo é opcional, e pode ser utilizado para transitar alguma informação, que deseje, entre seu front-end e seu back-end.
gn3ds_additionalObject	Não	Não	Object		Este campo é opcional, e pode ser utilizado para transitar alguma um objeto, se necessário, entre seu front-end e seu back-end. Por exemplo: Json
gn3ds_httpBrowserColorDepth	**Sim**	**Sim**	String	2	O valor representa a profundidade de bits da paleta de cores para exibir imagens, em bits por pixel. **Exemplo**: 24 A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserJavaEnabled	**Sim**	**Sim**	String	1	Valor que representa a habilidade do navegador do titular do cartão para execute Java, **valores possíveis: Y ou N** A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserJavaScriptEnabled	**Sim**	**Sim**	String	1	Valor que representa a habilidade do navegador do titular do cartão para execute JavaScript, **valores possíveis: Y ou N**

					A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserLanguage	**Sim**	**Sim**	String	8	O valor representa o idioma do navegador conforme definido em IETF BCP47. **Exemplo**: pt-BR A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserScreenHeight	**Sim**	**Sim**	String	6	Altura total da tela do titular do cartão em pixels; **Exemplo**: 657 A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserScreenWidth	**Sim**	**Sim**	String	6	Largura total da tela do titular do cartão em pixels; **Exemplo**: 1366 A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_httpBrowserTimeDifference	**Sim**	**Sim**	String	5	Diferença horária entre o horário UTC e o horário local do titular do cartão, em minutos. **Exemplo**: 180 A falta do envio dessa informação vai ocasionar uma falha na autenticação.
gn3ds_userAgentBrowserValue	**Sim**	**Sim**	String	2048	O conteúdo exato do cabeçalho do “HTTP agent user”. **Exemplo**: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36` A falta do envio dessa informação vai ocasionar uma falha na autenticação.

3.4 CRIAR NA CAMADA BACK-END

Deve-se implementar os métodos do CommerceService 3.0, em sua camada de Back-end conforme os métodos abaixo.

3.4.1 SERVIÇO TOKENSERVICE

Deve-se implementar um webService com nome sugerido de "generateToken" que será acionado automaticamente pelo front-end enviando informações em formato JSON.

Objetivo: Abrir uma sessão de autenticação 3DS junto à Getnet.

Local: Deve ser hospedado no back-end da loja conforme parametrizado através do campo gn3ds_merchantBackEndUrl (tópico 3.3.1).

End-point* Sandbox: https://cgws-hti.getnet.com.br:443/eCommerceWS/3.0/CommerceService
End-point* Produção: https://cgws.getnet.com.br/eCommerceWS/3.0/CommerceService

*O webservice é "Soap padrão" e sempre retornará HTTPS 200/201. Para verificar o status do retorno (sucesso ou erro), verifique as respectivas tags contidas no XML de retorno.

Identificação: Deverão ser enviados dados que identifiquem o estabelecimento (Merchant) e a compra que está sendo efetuada (Order).

BACK-END - TAG	Obriga-tório	Muito Recomen-dado	Tipo	Tam.	Descrição
<AUTHENTICATION>					
Username	**Sim**	**Sim**	string	20	Usuário para autenticação do serviço
Password	**Sim**	**Sim**	string	40	Senha para autenticação do serviço
merchantID	**Sim**	**Sim**	string	15	Código de identificação do estabelecimento junto à Getnet
</AUTHENTICATION>					
<TOKEN>					
orderNumber	Não	Não	string	40	Número do pedido
merchantTrackID	**Sim**	**Sim**	string	40	Identificador único da transação. Este identificador deverá ser o mesmo que será utilizado no tópico 3.4.2 AuthenticationService.
merchantId	**Sim**	**Sim**	string	15	Código de identificação do estabelecimento junto à Getnet
merchantName	**Sim**	**Sim**	string	40	Nome da empresa da forma que deverá ser apresentada ao cliente no formulário de autenticação do banco emissor. Este valor substitui o valor especificado pelo seu banco comercial.
overridePaymentMethod	**Sim**	**Sim**	string	10	Indica o tipo de transação Valores possíveis: - CREDIT = Transação de crédito - DEBIT = Transação de débito
currency	**Sim**	**Sim**	string	3	Moeda na qual o valor da compra é expresso. Exemplo: BRL
totalAmount	**Sim**	**Sim**	string	19	Valor total da compra
jsVersion	Não	Não	string	10	Versão do JS Core informada pela Getnet. Por exemplo: 1.0.6

BACK-END - TAG	Obriga-tório	Muito Recomen-dado	Tipo	Tam.	Descrição
clientCode	**Sim**	**Sim**	string	13	Referência do pedido gerado pelo cliente ou número de rastreamento. Para garantir unicidade deste código, ao receber seu clientCode, iremos adicionar mais 36 posições a ele com uma chave única gerada na solução 3DS Getnet.
<ITEMS>					
<ITEMS>					
totalAmount	Não	Não	string	15	Valor da compra na menor unidade monetária
unitPrice	Não	Não	string	10	Valor unitário
quantity	Não	Não	string	255	Quantidade deste produto
productSKU	Não	Não	string	255	Código do produto
productDescription	Não	Não	string	255	Descrição do produto
productName	Não	Não	string	60	Nome que identifique o produto
</ITEMS>					
</ITEMS>					
</TOKEN>					

a) **Estrutura JSON – Front-end > Backend:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser enviado do front-end para o back-end do **estabelecimento**:

```
{
 "orderNumber": ?,
 "merchantTrackID": ?,
 "merchantId": ?,
 "merchantName": ?,
 "overridePaymentMethod": ?,
 "currency": ?,
 "totalAmount": ?,
 "jsVersion": ?,
 "clientCode": ?,
  "items":[
     {
        "name": ?,
        "description": ?,
        "sku": ?,
        "quantity": ?,
        "unitPrice": ?,
        "totalAmount": ?
     },{
        "name": ?,
        "description": ?,
        "sku": ?,
        "quantity": ?,
        "unitPrice": ?,
        "totalAmount": ?
     }
  ],
```

```
  "additionalData":null,
  "additionalObject":null
}
```

b) **Estrutura XML – Backend > 3DS Getnet:** O quadro a seguir demonstra as TAGs XML do "Service Request" do TokenService:

```
      <tokenService>
            <authentication>
               <username>?</username>
               <password>?</password>
               <merchantID>?</merchantID>
            </authentication>
            <token>
               <orderNumber>?</orderNumber>
               <merchantTrackID>?</merchantTrackID>
               <merchantId>?</merchantId>
               <merchantName>?</merchantName>
               <overridePaymentMethod>CREDIT</overridePaymentMethod>
               <currency>?</currency>
               <totalAmount>?</totalAmount>
               <jsVersion>?</jsVersion>
               <clientCode>?</clientCode>
               <items>
                  <!--Zero or more repetitions:-->
                  <items>
                     <totalAmount>?</totalAmount>
                     <unitPrice>?</unitPrice>
                     <quantity>?</quantity>
                     <productSKU>?</productSKU>
                     <productDescription>?</productDescription>
                     <productName>?</productName>
                  </items>
               </items>
            </token>
```

c) **Estrutura XML – Resposta – 3DS Getnet > Back-end:** O quadro a seguir demonstra as TAGs XML do "Service Response" do 3DS Getnet:

```
<authorizationServiceResponse>
   <authorizationResponse>
      <result>
         <!--Zero or more repetitions:-->
         <result>
            "Os retornos são sempre no objeto Result."
         </result>
      </result>
   </authorizationResponse>
</authorizationServiceResponse>
```

d) **Estrutura JSON – Resposta Sucesso – Back-end > Front-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser retornado do back-end para front-end do **estabelecimento** em caso de sucesso:

```
{
  "status":200,
  "message":"SUCCESSFUL",
  "data":[
     {
        "accessToken": (retorno da tag <accessToken></accessToken>),
        "expirationDate":(retorno da tag <expirationDate></expirationDate>),
        "paymentId":(retorno da tag <merchantTrackID></merchantTrackID>),
        "tokenType":(retorno da tag <token_type></token_type>)
     }
  ],
  "error":[{}]
}
```

e) **Estrutura JSON – Resposta Erro – Back-end > Front-end:** O quadro a seguir demonstra exemplo de estrutura JSON a ser retornado do back-end para front-end do **estabelecimento** em caso de erro:

```
{
  "status":500, //400 a 500
  "message":"ERROR", // Exemplo
  "data":[{}],
  "error":[{
             "reason": "Internal Server Error", // Exemplo
             "description": "Internal Server Error" // Exemplo
  }]
}
```

3.4.2 SERVIÇO AUTHENTICATIONSERVICE

Deve-se implementar um webService com nome sugerido “authentications” para receber informações em formato JSON. Este serviço é responsável efetivamente pela solicitação de autenticação da transação junto à solução 3DS Getnet.

Objetivo: Acionar o webservice de autenticação “3DS Getnet” chamado “enrollmentService” enviando informações compostas por dados do pedido/pagamento recebidos a partir do front-end e complementados com a partir de sua base de dados obtidas no back-end da loja.

Local: Deve ser hospedado no back-end da loja conforme parametrizado através do campo gn3ds_merchantBackEndUrl (tópico 3.3.1).

End-point* Sandbox: https://cgws-hti.getnet.com.br:443/eCommerceWS/3.0/CommerceService
End-point* Produção: https://cgws.getnet.com.br/eCommerceWS/3.0/CommerceService

*O webservice é “Soap padrão” e sempre retornará HTTPS 200/201. Para verificar o status do retorno (sucesso ou erro), verifique as respectivas tags contidas no XML de retorno.

Importante: Antes de acionar o webservice de autenticação, pode-se aplicar “regras de negócio”.

Deverão ser enviados dados que identifiquem o estabelecimento (Merchant) e a compra que está sendo efetuada (Order).

BACK-END – TAG	Obriga-tório	Muito Recomen-dado	Tipo	Tam.	Descrição
<AUTHENTICATION>					
username	**Sim**	**Sim**	string	20	Usuário para autenticação do serviço
password	**Sim**	**Sim**	string	40	Senha para autenticação do serviço
merchantID	**Sim**	**Sim**	string	15	Código de identificação do estabelecimento junto à Getnet
</AUTHENTICATION>					
<ENROLLMENT>					
merchantTrackID	**Sim**	**Sim**	string	40	Identificador único da transação. Este identificador deverá ser o mesmo que foi utilizado no tópico 3.4.1- TokenService.
<PERSONALIDENTIFICATION>					
id	Não	**Sim**	string	26	Documento de identificação do proprietário do cartão, o envio desse campo aumenta a possibilidade de uma autenticação silenciosa.
type	Não	**Sim**	string	14	O tipo de documento que será enviado, o envio desse campo aumenta a possibilidade de uma autenticação silenciosa. -CPF -CPNJ (cnpj)
</PERSONALIDENTIFICATION>					
<ORDERINFORMATION>					
<AMOUNTDETAILS>					
currency	**Sim**	**Sim**	string	3	Moeda na qual o valor da compra é expresso.

totalAmount	**Sim**	**Sim**	string	19	Valor da compra na menor unidade monetária sem nenhuma pontuação.
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
</AMOUNTDETAILS>					
<SHIPTO>					
address1	Não	Não	string	60	Ambos os campos são destinados ao endereço de entrega do portador associado ao cartão utilizado na compra. **Importante**: Deve-se iniciar pelo logradouro, respeitando o formato de endereço, ou pode causar falha na autenticação.
address2	Não	Não	string	60	
administrativeArea	Não	Não	string	2	Estado (UF) do endereço de entrega do portador.
country	Não	Não	string	2	País do endereço de entrega do portador associado ao cartão utilizado na compra.
locality	Não	Não	string	50	Cidade do endereço de entrega. Não incluir informações adicionais sob risco de falhar a autenticação. Ex: São Paulo (capital) – a informação "capital" não deve ser incluída.
firstName	Não	Não	string	60	Primeiro nome da pessoa que recebe a mercadoria
lastName	Não	Não	string	60	Último sobrenome da pessoa que recebe a mercadoria
phoneNumber	Não	Não	string	15	Número do telefone, enviar apenas números, sem espaços ou outros caracteres. **Exemplo**:1125660089
postalCode	Não	Não	string	10	CEP do endereço de cobrança do portador associado ao cartão utilizado na compra (sem traço e ponto)
destinationCode	Não	Não	string	2	Local de entrega. Conteúdos possíveis: 01- Enviar para o endereço de cobrança do titular do cartão; 02- Enviar para outro endereço confirmado pela loja 03- Enviar para endereço diferente do endereço de cobrança 04- Enviar para a loja (endereço da loja deve ser preenchido no pedido) 05- Bens digitais (ex: e-Books), 06- Bilhetes de viagens e eventos, que não serão enviados. 07- Outro
Method	Não	Não	string	8	Método de envio da mercadoria. Conteúdo possíveis: - lowcost: serviço de menor custo - sameday: Courier ou serviço no mesmo dia - oneday: serviço no dia seguinte ou durante a noite - twoday: serviço de dois dias - threeday: serviço de três dias - pickup: Retirada na loja - other: Ourto método de envio - none: nenhum método de envio, porque o produto é um serviço ou assinatura Necessário para o American Express SafeKey (EUA).
</SHIPTO>					
<LINEITEMS>					
<LINEITEMS>					
totalAmount	Não	Não	string	19	Valor da compra na menor unidade monetária sem nenhuma pontuação.
unitPrice	Não	Não	string	15	Valor unitário
Quantity	Não	Não	integer	10	Quantidade deste produto

productSKU	Não	Não	string	255	Código do produto
productDescription	Não	Não	string	255	Descrição do produto
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
productName	Não	Não	string	255	Nome que identifique o produto
</LINEITEMS>					
</LINEITEMS>					
<BILLTO>					
address1	Não	**Sim**	string	60	Ambos os campos são destinados ao endereço de cobrança do portador associado ao cartão utilizado na compra. **Importante**: Deve-se iniciar pelo logradouro, respeitando o formato de endereço, ou pode causar falha na autenticação.
address2	Não	**Sim**	string	60	
administrativeArea	Não	**Sim**	string	2	Estado (UF) do endereço de cobrança do portador associado ao cartão utilizado na compra.
country	Não	**Sim**	string	2	País do endereço de cobrança do portador associado ao cartão utilizado na compra.
locality	Não	**Sim**	string	50	Cidade do endereço de cobrança. Não incluir informações adicionais sob risco de falhar a autenticação. Ex: São Paulo (capital) – a informação "capital" não deve ser incluída.
firstName	Não	Não	string	60	Primeiro nome da pessoa que recebe a mercadoria
lastName	Não	Não	string	60	Último sobrenome da pessoa que recebe a mercadoria
homePhone	Não	**Sim**	string	15	Número de telefone residencial fornecido pelo portador, enviar apenas números, sem espaços ou outros caracteres. **Exemplo**:1125660089
email	**Sim**	**Sim**	string	255	Endereço de e-mail associado a conta que foi informado pelo portador ou já estava armazenado em cadastro prévio pelo 3DS Requestor. Deve-se enviar um formato válido de e-mail. **Exemplo**: meucontato@empresa.com.br. OBS: O envio correto desse campo aumenta a possibilidade de uma autenticação silenciosa.
postalCode	**Sim**	**Sim**	string	10	CEP do endereço de cobrança do portador associado ao cartão utilizado na compra (sem traço e ponto), , o envio desse campo aumenta a possibilidade de uma autenticação silenciosa.
mobilePhone	**Sim**	**Sim**	string	15	Número de celular fornecido pelo portador, enviar apenas números, sem espaços ou outros caracteres. **Exemplo**:11995660089 OBS: O envio correto desse campo aumenta a possibilidade de uma autenticação silenciosa.
</BILLTO>					
</ORDERINFORMATION> **<PAYMENTINFORMATION>**					
<CARD>					
type	**Sim**	**Sim**	string	3	Tipo de cartão. Valores possíveis: 001 - VISA 002 - Mastercard 003 - American Express 024 - Maestro (UK Domestic)

					042 - Maestro (International) 054 - ELO
expirationMonth	**Sim**	**Sim**	string	2	Mês da Validade do cartão - MM
expirationYear	**Sim**	**Sim**	string	4	Ano da Validade do cartão - AAAA
number	**Sim**	**Sim**	string	20	Número de conta que será utilizado na requisição de autorização para transações de pagamento. Pode ser representado por um PAN ou token.
holderName	**Sim**	**Sim**	string	26/28	Nome do portador. Como impresso no cartão do portador. * Nome completo do portador do cartão (ex: nome referente a fatura do cartão)
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
</CARD>					
</PAYMENTINFORMATION>					
<DEVICEINFORMATION>					
httpBrowserColorDepth	**Sim**	**Sim**	String	2	O valor representa a profundidade de bits da paleta de cores para exibir imagens, em bits por pixel. **Exemplo**: 24
httpBrowserJavaEnabled	**Sim**	**Sim**	String	1	Valor que representa a habilidade do navegador do titular do cartão para execute Java, valores possíveis: **Y** ou **N**
httpBrowserJavaScriptEnabled	**Sim**	**Sim**	String	1	Valor que representa a habilidade do navegador do titular do cartão para execute JavaScript, valores possíveis: **Y** ou **N**
httpBrowserLanguage	**Sim**	**Sim**	String	8	O valor representa o idioma do navegador conforme definido em IETF BCP47. **Exemplo**: pt-BR
httpBrowserScreenHeight	**Sim**	**Sim**	String	6	Altura total da tela do titular do cartão em pixels; **Exemplo**: 657
httpBrowserScreenWidth	**Sim**	**Sim**	String	6	Largura total da tela do titular do cartão em pixels; **Exemplo**: 1366
httpBrowserTimeDifference	**Sim**	**Sim**	String	5	Diferença horária entre o horário UTC e o horário local do titular do cartão, em minutos. **Exemplo**: 180
userAgentBrowserValue	**Sim**	**Sim**	String	2048	O conteúdo exato do cabeçalho do “HTTP agent user”.
httpAcceptBrowserValue	**Sim**	**Sim**	String	2048	O conteúdo do cabeçalho “Http accept content”. **Exemplo**: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
httpAcceptContent	**Sim**	**Sim**	String	2048	O conteúdo do cabeçalho “Http accept content”. **Exemplo**: text/html
ipAddress	**Sim**	**Sim**	String	45	Endereço I.P. do cliente. **Exemplo**: 1.12.123..255 OBS: O envio correto desse campo aumenta a possibilidade de uma autenticação silenciosa
</DEVICEINFORMATION>					
<MERCHANTINFORMATION>					
merchantName	Não	Não	string	25	O nome da sua empresa como você deseja que apareça no formulário de autenticação do banco emissor. Este valor substitui o valor especificado pelo seu banco comercial.
</MERCHANTINFORMATION>					
<RECURRINGPAYMENTINFORMATION>					

endDate	Não	Recorrencia	string	10	Data limite para autorização adicional. Formato: AAAAMMDD
frequency	Não	Recorrencia	integer	3	Indica o número mínimo de dias entre pedidos de autorização subsequentes.
originalPurchaseDate	Não	Recorrencia	string	17	Data da compra original (inicial). Necessário para transações recorrentes. Formato: AAAAMMDD:HH:MM:SS **OBS**: Se este campo estiver vazio, a data atual (hoje) será utilizada.
</RECURRINGPAYMENTINFORMATION>					
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
<CONSUMERAUTHENTICATIONINFORMATION>					
alternateAuthenticationMethod	Não	Não	string	2	Mecanismo usado pelo titular do cartão para autenticar no solicitante do 3D Secure. Valores possíveis: 01:Nenhuma autenticação ocorreu 02:Login usando credenciais do sistema comercial 03: Login usando ID Federado 04: Faça login usando o FIDO Authenticator
challengeCode	Não	**Sim**	string	2	Indica se um desafio é requerido pelo solicitante para essa transação. Por **exemplo**: **01** : Sem preferência. **02** : Nenhum pedido de contestação **03** : Desafio solicitado (preferência do solicitante do 3D Secure) **04** : Desafio solicitado (mandatório), mas neste caso competirá ao emissor decidir se desafiará ou se possui elementos suficientes para autenticar silenciosamente.
defaultCard	Não	Não	boolean	-	true ou false : indica que o cartão em uso é o designado como o cartão de pagamento principal para compra.
installmentTotalCount	Não	Não	integer	4	Indica o número máximo de autorizações (parcelas) permitidas para um pagamento parcelado.
marketingOptIn	Não	Não	boolean	-	true ou false : Indica se o cliente optou por receber ofertas de marketing.
marketingSource	Não	Não	string	50	
mcc	**Sim**	**Sim**	string	4	Código definido pelo DS descrevendo o tipo de negócio, produto ou serviço pertinente ao comércio.
messageCategory	**Não**	**Sim**	string	2	Categoria da mensagem para um caso específico. Valores possíveis: • **01** = PA (Transação de pagamento/compra) • **02** = NPA (Não é transação de pagamento/compra) • **80**: Apenas para Mastercard, para indicar que deseja enviar DATAONLY.
npaCode	Não	**Sim**	string	2	Recomendamos indicar “01”. Opções disponíveis: **01**: Adiciona um cartão. **02**: Mantém informação do cartão **03**: Verificação do portador do cartão para EMV token;
overridePaymentMethod	**Sim**	**Sim**	string	2	Indica o tipo de conta. Por exemplo, para um cartão multi-conta como os cartões combo (crédito e débito) brasileiros.
productCode	**Sim**	**Sim**	string	2	Identifica o tipo de transação que está sendo autenticada. Recomendamos indicar “01”. Opções disponíveis: **01**: Compra de bens / serviços

					03: Verifica Aceitação **10**: Financiamento da Conta **11**: Transação Cash **28**: Ativação e Carga Pré-Paga
requestorId	Não	Não	string	35	Identificador atribuído pelo DS ao 3DS Requestor. Cada DS atribuirá um ID único e individual para cada 3DS Requestor.
requestorName	Não	Não	string	40	Nome do solicitante da autenticação 3DS
transactionMode	Não	**Sim**	string	1	Identificador do modo de transação. Identifica o canal do qual a transação se origina. Valores possíveis: **M** - Mail Order/Telephone Order **P** - Dispositivo móvel (Celular) **R** - Varejo (loja física), **S** – Computador/PC, **T** - Tablet
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
alternateAuthenticationData	Não	Não	string	2048	Dados de documentos e suporte para um processo de autenticação específico.
deviceChannel	**Sim**	**Sim**	string	10	Valor possíveis: **SDK/Browser/3RI** **SDK** – Enviar se estiver usando SDK. **Browser** – Enviar se estiver usando uma aplicação pelo Browser. **3RI** – Enviar quando a autenticação é iniciada pelo 3DS.
acsWindowSize	Não	Não	string	2	Indicação do tamanho desejado (pixels) da tela de desafio, quando for o caso. Valores possíveis: **01**: (250x400), **02**: (390x400), **03**: (500x600), **04**: (600x400) ou **05**: (Full page)
</CONSUMERAUTHENTICATIONINFORMATION>					
<RISKINFORMATION>					
<BUYERHISTORY>					
<CUSTOMERACCOUNT>					
lastChangeDate	Não	Não	string	10	Data de quando os dados da conta do titular do cartão foram alterados pela última vez com o 3DS Requestor, incluindo endereço de cobrança ou entrega, nova conta de pagamento ou novos usuários adicionados.
creationHistory	Não	Não	string	16	Data de quando os dados da conta do titular do cartão foram alterados pela última vez com o 3DS Requestor, incluindo endereço de cobrança ou entrega, nova conta de pagamento ou novos usuários adicionados.
modificationHistory	Não	Não	string	18	Data de quando os dados da conta do titular do cartão com o 3DS Requestor teve alteração de senha ou redefinição de conta (reset).
passwordHistory	Não	Não	string	19	Indica a quanto tempo a conta do titular do cartão com o 3DS Requestor teve uma alteração de senha ou redefinição de conta (reset).
createDate	Não	Não	string	10	Quando o titular do cartão teve a conta criada no 3DS Requestor.

passwordChangeDate	Não	Não	string	10	Quando a conta do titular do cartão com o 3DS Requestor teve uma alteração de senha ou redefinição de conta (reset).
</CUSTOMERACCOUNT>					
<ACCOUNTHISTORY>					
firstUseOfShippingAddress	Não	Não	boolean	-	true ou false : Aplicável quando esta não é uma conta de convidado
shippingAddressUsageDate	Não	Não	string	10	Data em que o endereço de entrega para esta transação foi usado pela primeira vez. Recomendado para "Discover ProtectBuy". Se o campo firstUseOfShippingAddress for falso e não uma conta de convidado, essa data informada será inserida. Formato: AAAA-MM-DD
</ACCOUNTHISTORY>					
accountPurchases	Não	Não	integer	4	Número de compras com esta conta do titular do cartão durante os últimos seis meses.
BACK-END – TAG	**Obriga-tório**	**Muito Recomen-dado**	**Tipo**	**Tam.**	**Descrição**
addCardAttempts	Não	Não	integer	3	Número de tentativas de adicionar cartão nas últimas 24 horas. Exemplo de valores: • 02 • 002
priorSuspiciousActivity	Não	Não	boolean	-	true ou false : Indica se o comerciante teve atividade suspeita (incluindo fraude anterior) na conta. Recomendado para Discover ProtectComprar.
paymentAccountHistory	Não	Não	string	23	Isso indica sobre Novas Contas e Contas Existentes no creationHistory. Os valores possíveis são: PAYMENTACCOUNTEXISTS, PAYMENTACCOUNTADDED_NOW
paymentAccountDate	Não	Não	string	8	Data aplicável somente para PAYMENTACCOUNTEXISTS in paymentAccountHistory
transactionCountDay	Não	Não	integer	3	Número de transações (com sucesso e abandonadas) deste cartão com 3DS Requestor em todas as contas de pagamento nas últimas 24 horas. Exemplo de valores: • 02 • 002
transactionCountYear	Não	Não	integer	3	Número de transações (com sucesso e abandonadas) deste cartão com 3DS Requestor em todas as contas de pagamento no último ano. Exemplo de valores: • 2 • 002
</BUYERHISTORY>					
</RISKINFORMATION>					
Token	**Sim**	**sim**	string	2000	Token JWT - obtido nos serviços TokenService
</ENROLLMENT>					

a) **Estrutura JSON – Front-end > Back-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser enviado do front-end para o back-end do **estabelecimento**:

```
{
   "token": ?,
   "orderInformation": {
       "amountDetails": {
           "currency": ?,
           "totalAmount": ?
       },
       "shipTo": {
           "firstName": ?,
           "lastName": ?,
           "locality": ?,
           "administrativeArea": ?,
           "country": ?,
           "address1": ?,
           "address2": ?,
           "postalCode": ?,
           "method": ?,
           "destinationCode": ?
       },
       "billTo": {
           "firstName": ?,
           "lastName": ?,
           "email": ?,
           "locality": ?,
           "administrativeArea": ?,
           "country": ?,
           "address1": ?,
           "address2": ?,
           "postalCode": ?,
           "homePhone": ?,
           "mobilePhone": ?
       },
       "items": [{
           "name": ?,
           "description": ?,
           "sku": ?,
           "quantity": ?,
           "unitPrice": ?,
           "totalAmount": ?
       }, {
           "name": ?,
           "description": ?,
           "sku": ?,
           "quantity": ?
           "unitPrice": ?,
           "totalAmount": ?
       }]
   },
   "paymentInformation": {
       "card": {
           "number": ?,
           "expirationMonth": ?,
           "expirationYear": ?,
           "holderName": ?,
           "type": ?
       }
   },
```

```
   "personalIdentification": {
       "id": ?,
       "type": ?
   },
   "consumerAuthenticationInformation": {
      "challengeCode": ?,
      "mcc": ?,
      "messageCategory": ?,
     "npaCode": ?,
      "productCode": ?,
     "transactionMode": ?,
     "installmentTotalCount": ?,
     "overridePaymentMethod": ?
   },
  "deviceInformation": {
       "httpBrowserColorDepth": ?,
       "httpBrowserJavaEnabled": ?,
      "httpBrowserJavaScriptEnabled": ?,
      "httpBrowserLanguage":  ?,
      "httpBrowserScreenHeight": ?,
      "httpBrowserScreenWidth": ?,
      "httpBrowserTimeDifference":  ?,
      "userAgentBrowserValue": ?
    },
   "additionalData": null,
   "additionalObject": null,
}
```

b) **Estrutura XML – Back-end > 3DS Getnet:** O quadro a seguir demonstra as TAGs XML do “Service Request” do EnrollmentService:

```
      <enrollmentService>
            <authentication>
               <username>?</username>
               <password>?</password>
               <merchantID>?</merchantID>
            </authentication>
            <enrollment>
               <merchantTrackID>?</merchantTrackID>
               <personalIdentification>
                  <id>?</id>
                  <type>?</type>
               </personalIdentification>
               <orderInformation>
                  <amountDetails>
                     <currency>?</currency>
                     <totalAmount>?</totalAmount>
                  </amountDetails>
                  <shipTo>
                     <address1>?</address1>
                     <address2>?</address2>
                     <administrativeArea>?</administrativeArea>
                     <country>?</country>
                     <locality>?</locality>
                     <firstName>?</firstName>
                     <lastName>?</lastName>
                     <phoneNumber>?</phoneNumber>
                     <postalCode>?</postalCode>
```

```
            <destinationCode>?</destinationCode>
            <method>?</method>
         </shipTo>
         <lineItems>
            <!--Zero or more repetitions:-->
            <lineItems>
               <totalAmount>?</totalAmount>
               <unitPrice>?</unitPrice>
               <quantity>?</quantity>
               <productSKU>?</productSKU>
               <productDescription>?</productDescription>
               <productName>?</productName>
            </lineItems>
         </lineItems>
         <billTo>
            <address1>?</address1>
            <address2>?</address2>
            <administrativeArea>?</administrativeArea>
            <country>?</country>
            <locality>?</locality>
            <homePhone>?</homePhone>
            <email>?</email>
            <postalCode>?</postalCode>
            <mobilePhone>?</mobilePhone>
         </billTo>
      </orderInformation>
      <paymentInformation>
         <card>
            <type>?</type>
            <expirationMonth>?</expirationMonth>
            <expirationYear>?</expirationYear>
            <number>?</number>
            <holderName>?</holderName>
         </card>
      </paymentInformation>
      <deviceInformation>
         <httpBrowserColorDepth>?</httpBrowserColorDepth>
         <httpAcceptBrowserValue>?</httpAcceptBrowserValue>
         <httpAcceptContent>?</httpAcceptContent>
         <httpBrowserJavaEnabled>?</httpBrowserJavaEnabled>
         <httpBrowserJavaScriptEnabled>?</httpBrowserJavaScriptEnabled>
         <httpBrowserLanguage>?</httpBrowserLanguage>
         <httpBrowserScreenHeight>?</httpBrowserScreenHeight>
         <httpBrowserScreenWidth>?</httpBrowserScreenWidth>
         <httpBrowserTimeDifference>?</httpBrowserTimeDifference>
         <ipAddress>?</ipAddress>
         <userAgentBrowserValue>?</userAgentBrowserValue>
      </deviceInformation>
      <merchantInformation>
         <merchantName>?</merchantName>
      </merchantInformation>
      <recurringPaymentInformation>
         <endDate>?</endDate>
         <frequency>?</frequency>
         <originalPurchaseDate>?</originalPurchaseDate>
      </recurringPaymentInformation>
      <consumerAuthenticationInformation>
         <alternateAuthenticationMethod>?</alternateAuthenticationMethod>
         <challengeCode>?</challengeCode>
         <defaultCard>?</defaultCard>
```

```
            <installmentTotalCount>?</installmentTotalCount>
            <marketingOptIn>?</marketingOptIn>
            <marketingSource>?</marketingSource>
            <mcc>?</mcc>
            <messageCategory>?</messageCategory>
            <npaCode>?</npaCode>
            <overridePaymentMethod>CREDIT</overridePaymentMethod>
            <productCode>?</productCode>
            <requestorId>?</requestorId>
            <requestorName>?</requestorName>
            <transactionMode>?</transactionMode>
            <alternateAuthenticationData>?</alternateAuthenticationData>
            <deviceChannel>?</deviceChannel>
            <acsWindowSize>?</acsWindowSize>
         </consumerAuthenticationInformation>
         <riskInformation>
            <buyerHistory>
               <customerAccount>
                  <lastChangeDate>?</lastChangeDate>
                  <creationHistory>?</creationHistory>
                  <modificationHistory>?</modificationHistory>
                  <passwordHistory>?</passwordHistory>
                  <createDate>?</createDate>
                  <passwordChangeDate>?</passwordChangeDate>
               </customerAccount>
               <accountHistory>
                  <firstUseOfShippingAddress>?</firstUseOfShippingAddress>
                  <shippingAddressUsageDate>?</shippingAddressUsageDate>
               </accountHistory>
               <accountPurchases>?</accountPurchases>
               <addCardAttempts>?</addCardAttempts>
               <priorSuspiciousActivity>?</priorSuspiciousActivity>
               <paymentAccountHistory>?</paymentAccountHistory>
               <paymentAccountDate>?</paymentAccountDate>
               <transactionCountDay>?</transactionCountDay>
               <transactionCountYear>?</transactionCountYear>
            </buyerHistory>
         </riskInformation>
         <token>?</token>
      </enrollment>
```

c) **Estrutura XML – Resposta - 3DS Getnet > Back-end:** O quadro a seguir demonstra as TAGs XML do "Service Response" do EnrollmentService.

IMPORTANTE: A tag <status> pode retornar uma das seguintes indicações abaixo. Mais detalhes em relação a risco estabelecimento ou risco emissor par os retornos ECI, observe no tópico 4.

- **AUTHENTICATION_SUCESSFULL**: Indica que foi possível realizar a comunicação com a bandeira para autenticação, mas deve observar o campo ECI que indicará se a transação foi ou não autenticada:
  - **ECI = 02 ou 05**: Sucesso na autenticação 3DS pelo Banco Emissor;
  - **ECI = 01 ou 06**: Sucesso na autenticação 3DS pela Bandeira;
  - **ECI = 00 ou 07**: Autenticação falhou por motivos variados relacionados ao cartão, emissor ou mesmo problemas técnicos ou configuração;
  - **ECI = 04** : Para solicitações de autenticação "Data Only" (apenas Mastercard).
- **AUTHENTICATION_FAILED**: O fluxo de autenticação falhou e não foi possível concluir a solicitação de autenticação.
  - Quando <status> apresentar este retorno, deve-se analisar as informações vindas nas *tags* contidas no grupo <**errorinformation**>. As tags <**paresStatus**> e <**veresEnrolled**> também podem ajudar na orientação para entendimento da falha na autenticação. Detalhes sobre estas 2 últimas *tags* podem ser obtidas no **item 4** (Homologação).

```
<enrollmentServiceResponse>
   <enrollmentResponse>
      <result>
          <wsErrorCode></wsErrorCode>
          <wsErrorText></wsErrorText>
          <merchantTrackID></merchantTrackID>
          <links>
             <self>
                <href></href>
                <method></method>
             </self>
          </links>
          <id></id>
          <submitTimeUtc></submitTimeUtc>
          <submitTimeLocal></submitTimeLocal>
          <status></status>
          <reason></reason>
          <message></message>
          <referenceId></referenceId>
          <orgUnitId></orgUnitId>
          <clientReferenceInformation>
             <code></code>
          </clientReferenceInformation>
          <orderInformation>
             <amountDetails>
                <currency></currency>
             </amountDetails>
          </orderInformation>
          <consumerAuthenticationInformation>
             <acsUrl></acsUrl>
             <authenticationPath></authenticationPath>
             <authenticationTransactionId></authenticationTransactionId>
             <ucaf></ucaf>
             <cavvAlgorithm></cavvAlgorithm>
```

```
            <challengeRequired></challengeRequired>
            <ecommerceIndicator></ecommerceIndicator>
            <eci></eci>
            <eciRaw></eciRaw>
            <pareq></pareq>
            <paresStatus></paresStatus>
            <proofXml></proofXml>
            <proxyPan></proxyPan>
            <specificationVersion></specificationVersion>
            <ucafAuthenticationData></ucafAuthenticationData>
            <ucafCollectionIndicator></ucafCollectionIndicator>
            <veresEnrolled></veresEnrolled>
            <xid></xid>
            <token></token>
            <directoryServerTransactionId></directoryServerTransactionId>
            <threeDSServerTransactionId></threeDSServerTransactionId>
            <acsTransactionId></acsTransactionId>
         </consumerAuthenticationInformation>
         <errorInformation>
            <reason></reason>
            <message></message>
         </errorInformation>
         <threeDSTransactionError>
            <statusCode></statusCode>
            <reason></reason>
            <errors>
               <!--Zero or more repetitions:-->
                 <errors>
                     <reason></reason>
                     <description></description>
                 </errors>
            </errors>
         </threeDSTransactionError>
      </result>
   </enrollmentResponse>
</enrollmentServiceResponse>
```

STATUS CODE: Em caso de inconsistência/erro, o 3DS Getnet poderá retornar os seguintes códigos de erro HTTP na tag <StatusCode>:

- 400 – erro encontrado em validação dos campos enviados;
- 403 – problemas relacionados com token durante autenticação 3DS ou desafio;
- 500 – quando for detectado erro na aplicação/fluxo 3DS Getnet;
- 504 – timeout no fluxo de serviço de autenticação 3DS;

d) **Estrutura JSON – Resposta Sucesso – Back-end > Front-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser retornado do back-end para front-end do **estabelecimento** em caso de sucesso:

```
{   "status": 200,
   "message": "SUCCESSFUL",
   "data": [{
       "id": (retorno da tag <id></id>),
       "submitTimeUtc": (retorno da tag <submitTimeUtc></submitTimeUtc>),
       "submitTimeLocal": (retorno da tag <submitTimeLocal></submitTimeLocal>),
       "status": (retorno da tag <status></status>),
       "clientReferenceInformation": {
```

```
            "code": (retorno da tag <code></code>)
        },
        "consumerAuthenticationInformation": {
            "acsUrl": (retorno da tag <acsUrl></acsUrl>),
            "authenticationPath": (tag <authenticationPath></authenticationPath>),
            "authenticationTransactionId": (tag <authenticationTransactionId>),
            "ucaf": (retorno da tag <ucaf></ucaf>),
            "cavvAlgorithm": (retorno da tag <cavvAlgorithm></cavvAlgorithm>),
            "challengeRequired": (tag <challengeRequired></challengeRequired>),
            "ecommerceIndicator": (tag <ecommerceIndicator></ecommerceIndicator>),
            "eci": (retorno da tag <eci></eci>),
            "eciRaw": (retorno da tag <eciRaw></eciRaw>),
            "pareq": (retorno da tag <pareq></pareq>),
            "paresStatus": (retorno da tag <paresStatus></paresStatus>),
            "proofXml": (retorno da tag <proofXml></proofXml>),
            "proxyPan": (retorno da tag <proxyPan></proxyPan>),
            "specificationVersion": (tag <specificationVersion></specificationVersion>),
            "ucafAuthenticationData": (tag <ucafAuthenticationData>),
            "ucafCollectionIndicator": (tag <ucafCollectionIndicator>),
            "veresEnrolled": (retorno da tag <veresEnrolled></veresEnrolled>),
            "xid": (retorno da tag <xid></xid>),
            "token": (retorno da tag <token></token>)
             "directoryServerTransactionId": (tag <directoryServerTransactionId>)
            "threeDSServerTransactionId": (tag <threeDSServerTransactionId>)
            "acsTransactionId": (tag <acsTransactionId>)
        },
        "referenceId": (retorno da tag <referenceId></referenceId>),
        "orgUnitId": (retorno da tag <orgUnitId></orgUnitId>),
        "orderInformation": {}
    }],
    "error": [{}]
}
```

e) **Estrutura JSON – Resposta Erro – Back-end > Front-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser retornado do back-end para front-end do **estabelecimento** em caso de erro:

```
{
  "status":500, //400 a 500
  "message":"ERROR", // Exemplo
  "data":[{}],
  "error":[{
             "reason": "Internal Server Error", // Exemplo
             "description": "Internal Server Error" // Exemplo
  }]
}
```

3.4.3 SERVIÇO VALIDATERESULT

Deve-se implementar um webService com nome sugerido “authentication-results” para confirmação do desafio, quando ocorrer.

Objetivo: Validar um desafio requisito pelo 3DS.

Local: Deve ser hospedado no back-end da loja conforme parametrizado através do campo gn3ds_merchantBackEndUrl (tópico 3.3.1).

End-point* Sandbox: https://cgws-hti.getnet.com.br:443/eCommerceWS/3.0/CommerceService
End-point* Produção: https://cgws.getnet.com.br/eCommerceWS/3.0/CommerceService

*O webservice é “Soap padrão” e sempre retornará HTTPS 200/201. Para verificar o status do retorno (sucesso ou erro), verifique as respectivas tags contidas no XML de retorno.

Ações: Este método acionará o webservice Getnet “validateService” para confirmação e validação do desafio.

BACK-END - TAG	Obriga-tório	Muito Recomen-dado	Tipo	Tam.	Descrição
<authentication>					
username	**Sim**	**Sim**	string	20	Usuário para autenticação do serviço
password	**Sim**	**Sim**	string	40	Senha para autenticação do serviço
merchantID	**Sim**	**Sim**	string	15	Código de identificação do estabelecimento junto à Getnet
</authentication>					
<validate>					
merchantTrackID	**Sim**	**Sim**	string	2	Identificador único da transação
<clientReferenceInformation>					
code	Não	Não			
</clientReferenceInformation>					
<paymentInformation>					
<card>					
type	**Sim**	**Sim**	string	3	Tipo de cartão. Valores possíveis: **001** - VISA **002** - Mastercard **003** - American Express **024** - Maestro (UK Domestic) **042** - Maestro (International) **054** - ELO
expirationMonth	**Sim**	**Sim**	string	2	Mês da Validade do cartão – MM
expirationYear	**Sim**	**Sim**	string	4	Ano da Validade do cartão – AAAA
number	**Sim**	**Sim**	string	20	Número de conta que será utilizado na requisição de autorização para transações de pagamento. Pode ser representado por um PAN ou token.
holderName	Não	Não	string	26	Nome do portador. Como impresso no cartão do portador. * Nome completo do portador do cartão (ex: nome referente a fatura do cartão)
</card>					

</paymentInformation>					
<amountDetails>					
currency	**Sim**	**Sim**	string	3	Moeda na qual o valor da compra é expresso. Exemplo: BRL
totalAmount	**Sim**	**Sim**	string	15	Valor total da compra
</amountDetails>					
tokenChallenge	**Sim**	**Sim**			Token do desafio, se houver
token	**Sim**	**Sim**			Token
overridePaymentMethod	**Sim**	**Sim**	string	60	Indica o tipo de conta. Exemplo: CREDIT ou DEBIT

a) **Estrutura JSON – Front-end > Back-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser enviado do front-end para o back-end do **estabelecimento**:

```
{
"token": ?,
"tokenChallenge": ?,
  "orderInformation":{
     "amountDetails":{
        "currency": ?,
        "totalAmount": ?
     }
  },
  "consumerAuthenticationInformation":{
     "overridePaymentMethod": ?
  },
  "paymentInformation":{
     "card":{
        "number": ?,
        "expirationMonth": ?,
        "expirationYear": ?,
        "holderName": ?,
        "type": ?
     }
  },
  "additionalData":null,
  "additionalObject":null
}
```

b) **Estrutura XML – Back-end > 3DS Getnet:** O quadro a seguir demonstra as TAGs XML do "Service Request" do ValidateService:

```
     <validateService>
           <authentication>
              <username>?</username>
              <password>?</password>
              <merchantID>?</merchantID>
           </authentication>
           <validate>
              <merchantTrackID>?</merchantTrackID>
              <clientReferenceInformation>
                 <code>?</code>
              </clientReferenceInformation>
```

```
            <paymentInformation>
               <card>
                  <type>?</type>
                  <expirationMonth>?</expirationMonth>
                  <expirationYear>?</expirationYear>
                  <number>?</number>
                  <holderName>?</holderName>
               </card>
            </paymentInformation>
            <amountDetails>
               <currency>?</currency>
               <totalAmount>?</totalAmount>
            </amountDetails>
            <tokenChallenge>?</tokenChallenge>
            <token>?</token>
            <overridePaymentMethod>CREDIT</overridePaymentMethod>
         </validate>
      </validateService>
```

c) **Estrutura XML – Resposta – 3DS Getnet > Back-end:** O quadro a seguir demonstra as TAGs XML do "Service Response" do ValidateService.

IMPORTANTE: A tag <status> pode retornar uma das seguintes indicações abaixo. Mais detalhes em relação a risco estabelecimento ou risco emissor par os retornos ECI, observe no tópico 4.

- **AUTHENTICATION_SUCESSFULL**: Indica que foi possível realizar a comunicação com a bandeira para autenticação, mas deve observar o campo ECI que indicará se a transação foi ou não autenticada:
  - **ECI = 02 ou 05**: Sucesso na autenticação 3DS pelo Banco Emissor;
  - **ECI = 01 ou 06**: Sucesso na autenticação 3DS pela Bandeira;
  - **ECI = 00 ou 07**: Autenticação falhou por motivos variados relacionados ao cartão, emissor ou mesmo problemas técnicos ou configuração;
  - **ECI = 04** : Para solicitações de autenticação "Data Only" (apenas Mastercard).
- **AUTHENTICATION_FAILED**: O fluxo de autenticação falhou e não foi possível concluir a solicitação de autenticação.
  Para analisar o motivo da falha, observe o conteúdo dos campos abaixo, ambos localizados no grupo **consumerAuthenticationInformation**:
  - **AuthenticationStatusMsg**
  - **ParesStatus** (detalhes no item 4-Homologação).

```
<validateServiceResponse>
   <validateResponse>
      <result>
         <wsErrorCode></wsErrorCode>
         <wsErrorText></wsErrorText>
         <merchantTrackID></merchantTrackID>
         <links>
            <self>
               <href></href>
               <method></method>
            </self>
         </links>
         <id></id>
         <submitTimeUtc></submitTimeUtc>
```

```
            <submitTimeLocal></submitTimeLocal>
            <status></status>
            <reason></reason>
            <message></message>
            <referenceId></referenceId>
            <orgUnitId></orgUnitId>
            <clientReferenceInformation>
               <code></code>
            </clientReferenceInformation>
            <orderInformation>
               <amountDetails>
                  <currency></currency>
               </amountDetails>
            </orderInformation>
            <consumerAuthenticationInformation>
               <acsUrl></acsUrl>
               <authenticationPath></authenticationPath>
               <authenticationTransactionId></authenticationTransactionId>
               <ucaf></ucaf>
               <cavvAlgorithm></cavvAlgorithm>
               <challengeRequired></challengeRequired>
               <ecommerceIndicator></ecommerceIndicator>
               <eci></eci>
               <eciRaw></eciRaw>
               <pareq></pareq>
               <paresStatus></paresStatus>
               <proofXml></proofXml>
               <proxyPan></proxyPan>
               <specificationVersion></specificationVersion>
               <ucafAuthenticationData></ucafAuthenticationData>
               <ucafCollectionIndicator></ucafCollectionIndicator>
               <veresEnrolled></veresEnrolled>
               <xid></xid>
               <token></token>
               <directoryServerTransactionId></directoryServerTransactionId>
               <threeDSServerTransactionId></threeDSServerTransactionId>
               <acsTransactionId></acsTransactionId>
               <authenticationStatusMsg></authenticationStatusMsg>
            </consumerAuthenticationInformation>
            <threeDSTransactionError>
               <statusCode></statusCode>
               <reason></reason>
               <errors>
                   <!--Zero or more repetitions:-->
                   <errors>
                      <reason></reason>
                      <description></description>
                   </errors>
               </errors>
            </threeDSTransactionError>
         </result>
      </validateResponse>
</validateServiceResponse>
```

STATUS CODE: Em caso de inconsistência/erro, o 3DS Getnet poderá retornar os seguintes códigos de erro HTTP na tag <StatusCode>:

- 400 – erro encontrado em validação dos campos enviados;
- 403 – problemas relacionados com token durante autenticação 3DS ou desafio;
- 500 – quando for detectado erro na aplicação/fluxo 3DS Getnet;
- 504 – timeout no fluxo de serviço de autenticação 3DS;

d) **Estrutura JSON – Resposta Sucesso – Back-end > Front-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser retornado do back-end para front-end do **estabelecimento** em caso de sucesso:

```
{
   "status": 200,
   "message": "SUCCESSFUL",
   "data": [{
       "id": (retorno da tag <id></id>),
       "submitTimeUtc": (retorno da tag <submitTimeUtc></submitTimeUtc>),
       "status": (retorno da tag <status></status>),
       "clientReferenceInformation": {
           "code": (retorno da tag <code></code>)
       },
       "consumerAuthenticationInformation": {
           "acsUrl": (retorno da tag <acsUrl></acsUrl>),
           "authenticationPath": (tag <authenticationPath></authenticationPath>),
           "authenticationTransactionId": (tag <authenticationTransactionId>),
           "ucaf": (retorno da tag <ucaf></ucaf>),
           "cavvAlgorithm": (retorno da tag <cavvAlgorithm></cavvAlgorithm>),
           "challengeRequired": (tag <challengeRequired></challengeRequired>),
           "ecommerceIndicator": (tag <ecommerceIndicator></ecommerceIndicator>),
           "eci": (retorno da tag <eci></eci>),
           "eciRaw": (retorno da tag <eciRaw></eciRaw>),
           "pareq": (retorno da tag <pareq></pareq>),
           "paresStatus": (retorno da tag <paresStatus></paresStatus>),
           "proofXml": (retorno da tag <proofXml></proofXml>),
           "proxyPan": (retorno da tag <proxyPan></proxyPan>),
           "specificationVersion": (tag <specificationVersion></specificationVersion>),
           "ucafAuthenticationData": (tag <ucafAuthenticationData>),
           "ucafCollectionIndicator": (tag <ucafCollectionIndicator>),
           "veresEnrolled": (retorno da tag <veresEnrolled></veresEnrolled>),
           "xid": (retorno da tag <xid></xid>),
           "token": (retorno da tag <token></token>)
            "directoryServerTransactionId": (tag <directoryServerTransactionId>)
           "threeDSServerTransactionId": (tag <threeDSServerTransactionId>)
           "acsTransactionId": (tag <acsTransactionId>)
       }
   }],
   "error": [{}]
}
```

e) **Estrutura JSON – Resposta Erro – Back-end > Front-end:** O quadro a seguir demonstra um exemplo de estrutura JSON que deve ser retornado do back-end para front-end do **estabelecimento** em caso de erro:

```
{
  "status":500, //400 a 500
  "message":"ERROR", // Exemplo
  "data":[{}],
  "error":[{
             "reason": "Internal Server Error", // Exemplo
             "description": "Internal Server Error" // Exemplo
```

```
    }]
}
```

3.5 CAPTURA COM INDICAÇÃO DE AUTENTICAÇÃO 3DS

Após realizar a autenticação 3DS da transação, alguns dados devem ser enviados na captura da transação para indicar que se trata de uma transação autenticada.

IMPORTANTE: O envio correto destas informações de autenticação junto à solicitação de autorização busca facilitar o aumento das taxas de aprovação.

São estes campos:

Campo	Obrigatório para indicar que foi autenticado?	Tipo	Tam.	Descrição
eci	**SIM,** enviar sempre	String	02	Indicador de retorno de uma solicitação de autenticação 3DS
ucaf	**SIM,** enviar sempre. Quando for usado **Data Only** não teremos essa informação.	String	40	Código de autenticação criptografado pela bandeira.
xid	**NÃO,** mas sempre que receber retorno da autenticação, deve ser enviado	string	40	Identificador do MPI para cada transação autenticada.
tdsver	**SIM,** enviar sempre	integer	1	Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização. Deve ser informado 1 ou 2, conforme a versão retornada na autenticação.
tdsdsxid	**NÃO,** mas sempre que receber retorno da autenticação, deve ser enviado	string	36	Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.

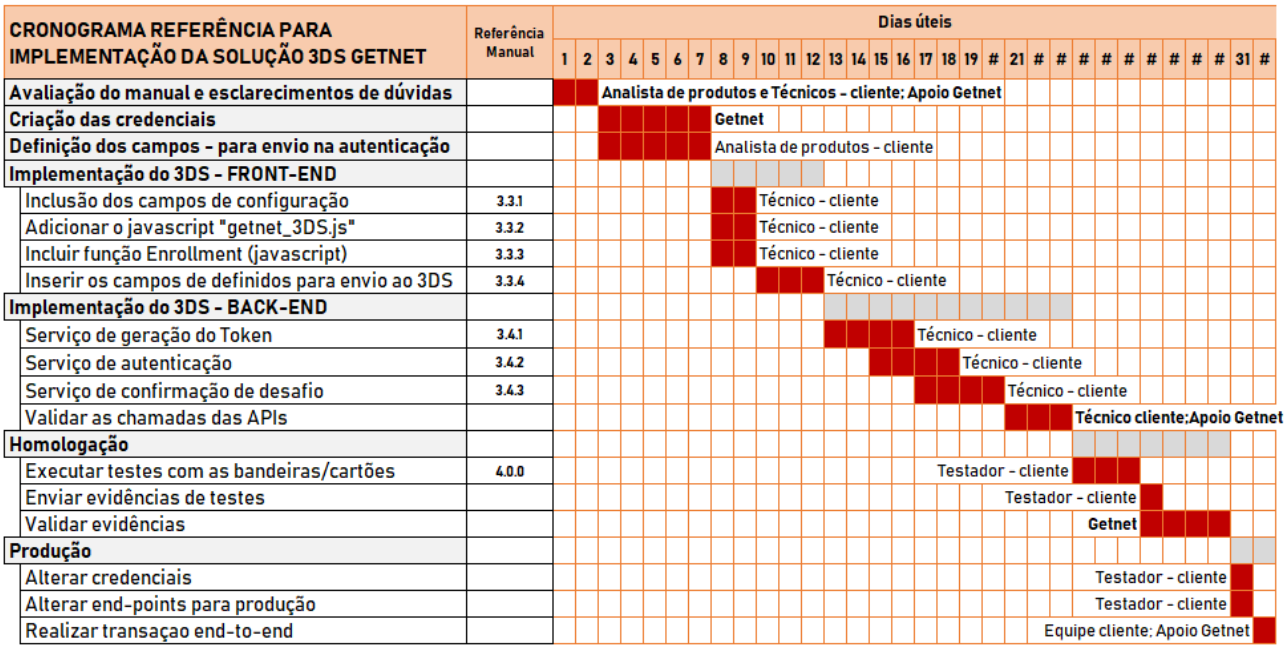
Considere o envio destes campos sempre que utilizar um dos métodos abaixo:

- PurchaseService
- AuthorizationService (captura sem confirmação/captura)
- PreAuthorizationService (pré-autorização sem confirmação/captura)

Detalhes sobre a utilização destes métodos de autorização de transações podem ser obtidos no **"E-Commerce - WebService - Manual de Integração – v6.0.pdf"**.

3.6 CRONOGRAMA DO PROJETO

Abaixo, apresentamos um cronograma de referência com estimativa do tempo para implementar a solução 3DS 2.1 Getnet. Estimamos 32 dias úteis com base em histórico de projetos anteriores relacionados a esta solução. Logo no início do planejamento da implementação, adequaremos os prazos em conjunto com as equipes do Cliente e da Getnet.



Devem participar do projeto os seguintes perfis profissionais:

- **Analista de produtos** (colaborador do cliente)
  Será responsável por definir o escopo do projeto (incluindo possíveis regras do negócio)

- **Desenvolvedor** (colaborador do cliente)
  Será responsável pela codificação e integração entre Front-end, Back-end e as APIs da Getnet.

- **Testador** (colaborador do cliente)
  Será responsável pela qualidade da integração realizando os devidos cenários de teste.

- **Apoio Getnet**
  A área de Captura Digital da Getnet disponibilizará um colaborador Técnico com os conhecimentos necessário para apoia o Desenvolvedor (cliente).

4 HOMOLOGAÇÃO

Este tópico oferece cenários para homologar sua aplicação com as bandeiras habilitados para o protocolo de autenticação 3DS e contém números de cartões de teste para os mais variados comportamentos.

Nos retornos de autenticação, há as seguintes possibilidades:

ParesStatus	Descrição
Y	**O cliente foi autenticado com sucesso**
A	Prova de tentativa de autenticação foi gerada
B	Autenticação ignorada
N	O cliente falhou ou cancelou a autenticação. Transação negada.
R	Autenticação rejeitada (utilizada apenas em 3DS 2.0)
U	Autenticação não concluída, independente do motivo.

VeresEnrolled	Descrição
Y	Cartão inscrito ou pode ser inscrito; você deve autenticar. Mudança de responsabilidade.
N	Cartão não inscrito; prossiga com a autorização. Mudança de responsabilidade
U	Incapaz de autenticar independentemente do motivo. Responsabilidade continua com estabelecimento.
B	Ique a autenticação foi ignorada.

Definição para alguns campos retornados na autenticação que devem ser usados no processo de autorização:

Campo	Descrição
XID	Identificador único de transação. Gerado automaticamente e tem tipicamente 28 bytes de tamanho é codificado em Base64, deve ser enviado na autorização sempre que for retornado.
UCAF	Identificador exclusivo gerado pelo banco emissor do cartão, nesse campo retornaremos os valores CAVV, AVV e UCAF de acordo com suas bandeiras, é codificado em Base64, deve ser sempre enviado na autorização, **quando estiver usando Data Only, não teremos essa informação**.
ECI	Indica o resultado da autenticação do cartão do portador no processo 3DS. Deve-se avaliar o resultado ECI e decidir se seguirá para autenticação levando em consideração os riscos apontados (emissor ou estabelecimento). Valores possíveis*: **02 ou 05** - Sucesso na autenticação 3DS pelo Emissor; **Risco emissor**. **01 ou 06** - : Sucesso na autenticação 3DS pela Bandeira; **Risco emissor** quando for indicado autenticação 3DS versão 2 e **Risco estabelecimento** quando 3DS versão 1 (downgrade). **00 ou 07** - Autenticação falhou por motivos variados relacionados ao cartão, emissor ou mesmo problemas técnicos ou configuração. **Risco estabelecimento.** **04** – Quando for informado, em solicitações de autenticação Mastercard, que se trata de “Data Only”, este será o ECI retornado. **Risco estabelecimento.**

	**00, 01 e 02 para Mastercard e 05, 06 e 07 para Visa e demais bandeiras.*
DIRECTORYSERVERTRANSACTIONID (tdsdsxid)	Identificador da transação do servidor 3 DS versão 2, deve ser enviado na autorização sempre que for retornado.
SPECIFICATIONVERSION (tdsver)	Indica a versão 3 DS utilizada na autenticação, deve ser sempre enviado na autorização.

Importante: Não é recomendado que os campos de XID e UCAF sejam armazenados, ou seja, devem ser utilizados apenas para concluir as etapas de autenticação e autorização, sendo descartados logo em seguida.

4.1 HOMOLOGAÇÃO– 3DS 2.1

Este tópico apresenta cenários para homologar sua aplicação com emissor VISA, MASTERCARD, ELO e AMERICAN EXPRESS.

Para data de validade do cartão utilize: 01/yyyy, sendo yyyy=ano corrente+3; por exemplo: se o ano corrente é 2020, a data de validade deverá ser 01/2023.

Cenário	Bandeira	PAN / Cartão	Retorno esperado
01-Autenticação COM sucesso (sem desafio)	VISA	4000/0000/0000/1000	**ECI=05** (Visa, Elo e American Express) **ECI=02** (Mastercard) Enrolled = Y PAResStatus = Y Xid=<valor do Xid> **Ação:** O estabelecimento deve anexar os valores Xid e Eci à mensagem de autorização
	MASTERCARD	5200/0000/0000/1005	
	ELO	6505/0500/0000/1000	
	AMERICAN EXPRESS	3400/0000/000/1007	
02-Autenticação SEM sucesso (sem desafio)	VISA	4000/0000/0000/1018	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = Y PAResStatus = Y Xid=<valor do Xid> **Ação:** O estabelecimento ainda pode autorizar um 3DS com falha como uma transação não autenticada.
	MASTERCARD	5200/0000/0000/1015	
	ELO	6505/0500/0000/1018	
	AMERICAN EXPRESS	3400/0000/000/1015	
03-Tentativa de Autenticação SEM sucesso (sem desafio)	VISA	4000/0000/0000/1026	**ECI=06** (Visa, Elo e American Express) **ECI=01** (Mastercard) Enrolled = Y PAResStatus = A Xid=<valor do Xid> **Ação:** O estabelecimento deve anexar Xid e Eci à mensagem de autorização.
	MASTERCARD	5200/0000/0000/1021	
	ELO	6505/0500/0000/1026	
	AMERICAN EXPRESS	3400/0000/000/1023	
	VISA	4000/0000/0000/1034	**ECI=07** (Visa, Elo e American Express)

04-Autenticação indisponível com Emissor	MASTERCARD	5200/0000/0000/3035	**ECI=00** (Mastercard) Enrolled = Y PAResStatus = U Xid=<valor do Xid> **Ação:** O estabelecimento deve continuar com a mensagem de autorização.
	ELO	6505/0500/0000/1034	
	AMERICAN EXPRESS	3400/0000/000/1031	
05-Autenticação rejeitada pelo emissor (sem desafio)	VISA	4000/0000/0000/1042	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = Y PAResStatus = R Xid=<valor do Xid> **Ação:** O estabelecimento NÃO deve continuar com a autorização. Deve solicitar outro pagamento e não tem permissão para enviar esta transação para autorização.
	MASTERCARD	5200/0000/0000/3043	
	ELO	6505/0500/0000/1042	
	AMERICAN EXPRESS	3400/0000/000/1049	
06-Autenticação não disponível na pesquisa	VISA	4000/0000/0000/1059	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = U PAResStatus = <vazio> Xid=<valor do Xid> **Ação:** O estabelecimento deve continuar com a mensagem de autorização.
	MASTERCARD	5200/0000/0000/3054	
	ELO	6505/0500/0000/1059	
	AMERICAN EXPRESS	3400/0000/000/1056	
07-Erro na tentativa de autenticação	VISA	4000/0000/0000/1067	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = U PAResStatus = <vazio> Xid=<valor do Xid> **Ação:** O estabelecimento deve continuar com a mensagem de autorização.
	MASTERCARD	5200/0000/0000/1062	
	ELO	6505/0500/0000/1067	
	AMERICAN EXPRESS	3400/0000/000/1064	
08-Timeout na tentativa de autenticação	VISA	4000/0000/0000/1075	**ECI=<vazio>** Enrolled = U PAResStatus = <vazio> Xid=<valor do Xid> **Ação:** O estabelecimento deve continuar com a mensagem de autorização.
	MASTERCARD	5200/0000/0000/1070	
	ELO	6505/0500/0000/1075	
	AMERICAN EXPRESS	3400/0000/000/1072	
09-Autenticação ignorada	VISA	4000/0000/0000/1083	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard)
	MASTERCARD	5200/0000/0000/1088	

	ELO	6505/0500/0000/1083	
	AMERICAN EXPRESS	3400/0000/000/1080	Enrolled = B PAResStatus = <vazio> Xid=<vazio> **Ação:** O estabelecimento deve continuar com a mensagem de autorização.
10-Autenticação COM sucesso (COM desafio)	VISA	4000/0000/0000/1091	**ECI=05** (Visa, Elo e American Express) **ECI=02** (Mastercard) Enrolled = Y PAResStatus = C Xid=<vazio> ****DESAFIO - deverá retornar:** PAResStatus = Y Xid=<valor do Xid> **Ação:** O estabelecimento deve anexar Xid e Eci à mensagem de autorização.
	MASTERCARD	5200/0000/0000/1096	
	ELO	6505/0500/0000/1091	
	AMERICAN EXPRESS	3400/0000/000/1098	
11- Autenticação SEM sucesso (COM desafio)	VISA	4000/0000/0000/1109	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = Y PAResStatus = C Xid=<vazio> ****DESAFIO - deverá retornar:** PAResStatus = N Xid=<vazio> **Ação:** O estabelecimento NÃO deve continuar com a autorização. O estabelecimento deve solicitar outro pagamento e não tem permissão para enviar esta transação para autorização
	MASTERCARD	5200/0000/0000/1104	
	ELO	6505/0500/0000/1109	
	AMERICAN EXPRESS	3400/0000/000/1106	
12-Desafio não disponível	VISA	4000/0000/0000/1117	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = Y PAResStatus = C Xid=<vazio> ****DESAFIO - deverá retornar:**
	MASTERCARD	5200/0000/0000/1112	
	ELO	6505/0500/0000/1117	
	AMERICAN EXPRESS	3400/0000/000/1114	

			PAResStatus = U Xid=<vazio> **Ação:** O estabelecimento pode tentar novamente a autenticação ou processar a autorização como responsabilidade/risco do comerciante
13-Autenticação com erro	VISA	4000/0000/0000/1125	**ECI=07** (Visa, Elo e American Express) **ECI=00** (Mastercard) Enrolled = Y PAResStatus = C Xid=<vazio> ****DESAFIO - deverá retornar:** PAResStatus = U Xid=<vazio> **Ação:** Os estabelecimentos têm a opção de reter a responsabilidade/risco e enviar a transação como não autenticada. Uma ação alternativa seria solicitar outra forma de pagamento.
	MASTERCARD	5200/0000/0000/1120	
	ELO	6505/0500/0000/1125	
	AMERICAN EXPRESS	3400/0000/0000/1122	
	MASTERCARD	5200/0000/0000/2011	
	ELO	Não disponível	
	AMERICAN EXPRESS	3400/0000/000/2013	

4.2 HOMOLOGAÇÃO– 3DS 1.0

Este tópico apresenta cenários para homologar sua aplicação com emissor VISA.

Cenário	Bandeira	PAN / Cartão	Retorno esperado
01-Autenticação COM sucesso	VISA	4000/0000/0000/0002	**ECI=05** (Visa, Elo e American Express) **ECI=02** (Mastercard) paresStatus : Y SignatureVerification = Y
	MASTERCARD	Não disponível	
	ELO	Não disponível	
	AMERICAN EXPRESS	Não disponível	
02- Autenticação COM sucesso, mas com parRes inválido	VISA	4000/0000/0000/0010	veresEnrolled : Y authenticationResult : -1
	MASTERCARD	Não disponível	
	ELO	Não disponível	
	AMERICAN EXPRESS	Não disponível	

5 LAYTOUT PARA IMPLEMENTAÇÃO

5.1 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 "**]]>**".

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.**

TERMO	DEFINIÇÃO
AAV	Ver ***Accountholder Authentication Value***
Access Control Server	Componente que opera no Domínio do Emissor (Bancos), verifica se a autenticação está disponível para um determinado número de cartão e a autentica quando possível.
Accountholder Authentication Value	Implementação da Mastercard para o UCAF. Ver ***UCAF / Universal Cardholder Authentication Field***
ACS	Ver ***Access Control Server***
Adquirente	Instituição que estabelece um contrato de serviço com um Lojista para aceitação de cartões. Também determina se o Lojista é elegível a participar do 3D Secure. Faz o papel tradicional de receber e enviar mensagens de autorização e liquidação.
AHS	Ver ***Authentication History Server***
ATN	Ver ***Authentication Tracking Number***

TERMO	DEFINIÇÃO
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).
EMV	***Europay, MasterCard e Visa***. O EMV é um padrão de especificações para pagamentos com cartões inteligentes e em dispositivos de aceitação. O seu objetivo é dificultar as atividades fraudulentas com os cartões bancários.
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.
ABECS	***Associação Brasileira das Empresas de Cartões de Crédito e Serviços*** apoia e atua no mercado de cartões desde 1971 para um desenvolvimento sustentável do setor.

TERMO	DEFINIÇÃO
BIN	*Bank Identification Number* (Número de Identificação Bancária). Número que identifica o **Emissor** do **Cartão**, representado pelos 6 primeiros dígitos do **PAN** (número do cartão). O primeiro dígito do BIN é chamado de MII *Major Industry Identifier*, que identifica a categoria da entidade que emitiu o cartão.
Cardholder Authentication Verification Value	Implementação da Visa para o UCAF. Ver ***UCAF / Universal Cardholder Authentication Field***
Cartão	É o cartão de Crédito e/ou Débito emitido e administrado pelo Emissor, de titularidade e responsabilidade do **Portador**, para uso pessoal e intransferível do mesmo.
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.
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 (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.

TERMO	DEFINIÇÃO
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.
Mastercard SecureCode	Implementação da Mastercard do protocolo 3D Secure. Ver **3D Secure**
MasterCard	Uma das principais Bandeiras internacionais. Ver **Bandeira**
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***

TERMO	DEFINIÇÃO
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.
SecureCode	O mesmo que ***Mastercard SecureCode***. Implementação da Mastercard do protocolo 3D Secure. Ver ***3D Secure***
Universal Cardholder Authentication Field	Valor criptografado gerado pelo ACS para prover uma maneira de, durante o processo de autorização, o sistema de autorização validar rapidamente a integridade de certos valores copiados da Payer Authentication Response para o pedido de autorização e para provar que a autenticação ocorreu. É usado como evidência de autenticação do pagamento durante a compra online para qualificação de proteção do *chargeback*. Na implementação da Visa é chamado de **CAVV**, na implementação da Mastercard é chamado de **AAV**. Ao submeter uma transação, o CAVV ou AAV deve ser incluído para demonstrar que o portador foi autenticado. O UCAF é um campo binário de 32 bytes com uma estrutura de dados variável Exemplo: jMoRyYgNSt0ZAREBBu8LHI+3oZo= O CAVV é uma string de caracteres que contém um valor de 20 bytes que são codificados na Base64 em 28 bytes.
VbV	O mesmo que ***Verified by Visa***. Implementação da Visa do protocolo 3D Secure. Ver ***3D Secure***
VEReq	Ver ***Verify Enrollment Request***
VERes	Ver ***Verify Enrollment Response***

TERMO	DEFINIÇÃO
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**
XID	***Unique Transaction Identifier*** É gerado automaticamente pelo MPI. Tem tipicamente 28 bytes de tamanho e é codificado em Base64. Exemplo: CBKJB289V1PZL4TDXXWF