

O objetivo deste manual é auxiliar o desenvolvedor a integrar sua aplicação com o e.Red, listando as funcionalidades e métodos, com exemplos de mensagens a serem enviadas e recebidas.

🔗 [English Documentation](#)

Sobre

Atualizado em: 21/01/2026

O e.Red é uma solução de pagamentos on-line prática e segura para realizar vendas pela internet com toda tranquilidade.

Com diferentes tipos de integração, a solução realiza a captura e processamento de transações financeiras diretamente pela Rede, ou seja, sem necessidade de um intermediador, oferecendo pagamentos com cartões de crédito e débito das principais bandeiras do mercado. Estão disponíveis no crédito as bandeiras Mastercard, Visa, Hiper, Elo, Diners, Sorocred, American Express, Hipercard, JCB, Banescard, Cabal, Mais, Credz; e no débito Mastercard, Visa e Elo.

Além disso, o e.Red oferece uma série de funcionalidades para agregar ainda mais valor aos negócios de seus clientes, com maior foco na conversão de vendas e maior controle de gestão.

O objetivo deste manual é auxiliar o desenvolvedor a integrar sua aplicação com o e.Red, listando as funcionalidades e métodos, com exemplos de mensagens a serem enviadas e recebidas.

A solução e.Red foi desenvolvida pensando na facilidade para o estabelecimento que deseja utilizar a API sem a necessidade de instalar novos sistemas. As principais vantagens de se utilizar uma API são: interoperabilidade entre aplicações distintas e fisicamente distantes, portabilidade entre diferentes plataformas, facilidade de integração, redução de custos para transporte de dados e formato universal.

Glossário

Para facilitar o entendimento criamos um glossário com os termos mais utilizados relacionados a e-commerce, aquisição e cartões.

- **Autorização:** processo que sensibiliza o limite de crédito do portador do cartão junto ao banco emissor, geralmente utilizado para análise de prevenção, análise de limite de crédito e da validação dos dados de cartão utilizado. A autorização não gera cobrança na fatura do comprador.
- **Captura:** processo que confirma uma transação autorizada. Após a captura o valor é debitado dos créditos do portador do cartão gerando a cobrança na fatura do mesmo.
- **Cancelamento:** processo que devolve ao comprador o valor autorizado ou capturado no cartão.
- **PV (número de filiação):** código identificador gerado pela Rede para os estabelecimentos filiados. O PV (ponto de venda) é único para cada estabelecimento.
- **Chave de integração:** código de segurança gerado pela Rede utilizado para garantir a integridade da transação. Faz parte, junto com o PV, das credenciais de autenticação da API.
- **Emissor:** é a instituição financeira que emite o cartão de crédito ou débito.
- **Portador:** é o proprietário do cartão, comprador do produto.
- **Estabelecimento:** é a entidade responsável pelo e-commerce (loja ou serviço virtual).
- **TID:** é o identificador único de uma transação composto por 20 caracteres gerados pela Rede. Esse identificador não se repete.
- **MPI:** sistema responsável em autenticar junto ao emissor as transações de crédito e débito.
- **SecureCode:** é o sistema de compra protegida da MasterCard que certifica junto ao emissor o portador do cartão, validando dados que apenas ele e o banco possuem. Segue o padrão universal 3D Secure.
- **Verified by Visa (VBV):** é o sistema de compra protegida da Visa que certifica junto ao emissor o portador do cartão, validando dados que apenas ele e o banco possuem. Segue o padrão universal 3D Secure.
- **Tokenização:** Um processo pelo qual o número do cartão é substituído por um valor chamado token estático que será usado em todas as transações de pagamento.
- **Ciclo de vida:** Uma vez que um token do cartão é gerado, ele passará por diferentes estágios ao longo da sua existência. O Emissor também poderá solicitar a substituição dos dados cadastrais do cartão físico atrelado a àquele token, por exemplo, por motivos de vencimento, fraude, danificação do plástico etc.

- **Criptograma:** é um valor criptografado único que é gerado dinamicamente pela Bandeira a cada transação, juntamente com os dados do token.
- **Data de validade do token:** é gerado e mantido na Bandeira, é aprovada durante o processamento do token. A data de validade do token geralmente não é a mesma que a data de validade do Cartão e pode ser antes ou depois da data de validade informada.
- **TokenizationId:** Identificador único da Rede para a solicitação de tokenização do número do cartão realizada pelo portador.
- **ProvisionedTokenId:** Um ID único associado a um token. O ID é criado após o provisionamento inicial de um token pela Bandeira.
- **Postback:** Retorno **síncrono** da API, por exemplo, no fluxo de autenticação 3DS.
- **Callback:** Retorno **assíncrono** da API, por exemplo, na API de cancelamento.

Bibliotecas

Módulos

Confira o módulo disponível para integração com e.Redde. Fique atento a data de atualização.



Primeiros Passos

Autenticação e autorização

Para gerenciar o acesso aos serviços é utilizado o protocolo de autorização **OAuth 2.0**. Ele foi projetado para fornecer segurança e controle granular sobre o acesso as aplicações.

Mudança para protocolo OAuth 2.0

Nosso protocolo de autenticação e autorização será alterado para **OAuth 2.0**. Todos os clientes que usam o **e.Redde** devem ajustar o padrão de integração com a API até **05/01/2026**. A atualização visa trazer mais segurança e evitar ataques direcionados a suas transações. Caso não seja realizada, suas transações podem ser impactadas. Confira o que muda.

Autenticação da Rede via APIs

As APIs da Rede utilizam o protocolo de autenticação **OAuth 2.0**, um padrão da indústria para autorização e autenticação de aplicações. Esse protocolo foi projetado para simplificar o desenvolvimento de fluxos de autorização para aplicações web, desktop, smartphones, outros.

Passo a passo para integração OAuth 2.0

1. Obtenha as credenciais de acesso PV e Chave de Integração no [Portal Use Rede](#).

Com a utilização do protocolo **OAuth 2.0**, essas credenciais foram renomeadas para o novo padrão, conforme a tabela. Confira todas credenciais usadas em ambiente de desenvolvimento:

Portal Use Rede	Credencial para OAuth 2.0
PV	clientId
Chave de Integração	clientSecret
Token de acesso dinâmico	access_token

2. Com essas credenciais, faça uma chamada ao endpoint de autenticação: <https://api.userede.com.br/redelabs/oauth2/token>

3. Essa chamada gera uma **access_token**, que será usado para transacionar com a Rede

4. O **access_token** deve ser armazenado de forma segura, evitando exposição ou uso indevido

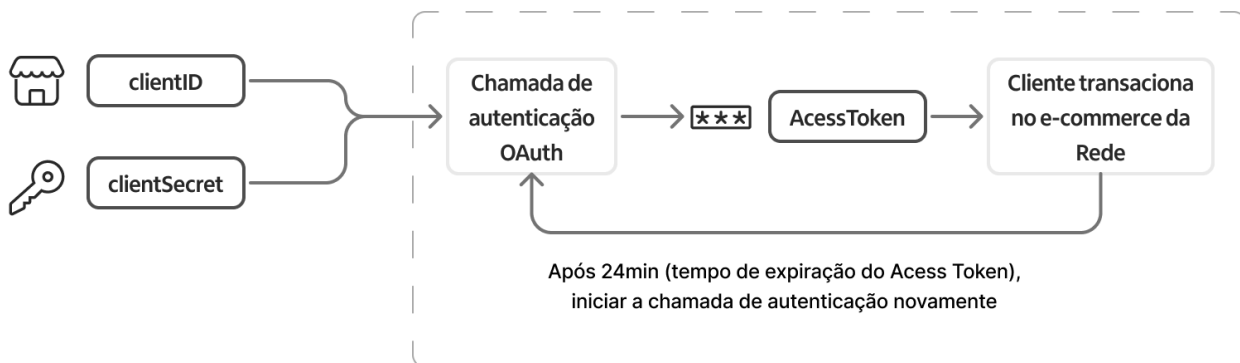
5- O **access_token** tem validade de 24 minutos. Após esse período, é necessário fazer uma nova chamada ao endpoint para gerar um novo token

OAuth Authorization

OAuth Authorization

PV + Chave de integração eRede

Camada de autenticação OAuth

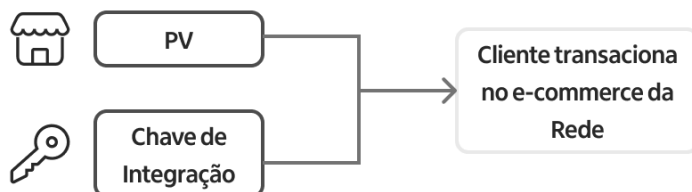


Atenção

Caso você seja um cliente que já transacionava com a Rede e ainda utiliza o protocolo BASIC, entenda as mudanças. Antes, a autenticação era feita seguindo o protocolo BASIC e usando apenas PV e chave de de integração gerada no [Portal Use Rede](#).

BASIC Authorization

PV + Chave de integração eRede



Agora, adotamos o modelo **OAuth 2.0**, que proporciona mais segurança para suas transações. Por isso, precisamos adicionar mais uma etapa no processo de autenticação. Assim que as credenciais forem atualizadas, deve ser feito um novo chamado de endpoint para gerar o **access_token**, necessário para transacionar com o e.Redde.

 **Informações sobre a Chave de Integração(clientSecret).**

Se você já possui uma Chave de integração, pode continuar usando a mesma.

Em caso de **perda ou esquecimento** da chave de integração, uma nova deverá ser gerada no [Portal Use Rede](#).

Para gerar a Chave, seu usuário precisa ter **perfil de administrador**. Acesse o menu: *e-commerce* > *chave de integração* e clique em **“Gerar chave de integração”**.

Se uma nova chave de integração for gerada, é necessário **atualizar imediatamente** no campo **clientSecret** da API para que o fluxo transacional se mantenha.

Como realizar autenticação no padrão OAuth 2.0

Endpoint de Autenticação

Ambiente	URL para gerar Token
Sandbox	https://rl7-sandbox-api.useredecloud.com.br/oauth2/token
Produção	https://api.userede.com.br/redelabs/oauth2/token

Autenticação

Gerar access_token

Com o **clientId** e o **clientSecret**, é possível gerar o token de acesso dinâmico utilizando a chamada:

```
curl --request POST \  
--url '{base_url}' \  
--header 'Authorization: Basic Base64(clientId:clientSecret)' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data grant_type=client_credentials
```

Headers:

Parâmetro	Obrigatório	Descrição
Authorization	<input checked="" type="checkbox"/>	Junte o client_id e o client_secret com dois-pontos (:) e converta o resultado para base64
Content-Type	<input checked="" type="checkbox"/>	application/x-www-form-urlencoded

Form:

Parâmetro	Obrigatório	Descrição
grant_type	<input checked="" type="checkbox"/>	Tipo de geração do token, com o valor fixo “client_credentials”

Response:

Parâmetro	Obrigatório	Descrição
access_token	✓	Token usado para chamar as APIs da Rede, com duração padrão de 24 minutos
token_type	✓	Tipo do token gerado, padrão é "Bearer"
expires_in	✓	Tempo de expiração em segundos do access_token
scope	✓	Lista de escopos separados por espaço, representando os acessos concedidos à aplicação

Autorização

Utilizar o Token de acesso

Para transacionar utilizando o e.Red, você deve:

1. Ter um access_token gerado, para ser usado nas APIs de negócio
2. Atualizar o access_token gerado anteriormente

Qual a diferença entre autenticação e autorização?

A **autenticação** é feita quando o um token de acesso (access_token) é gerado e a sua identidade confirmada.

A **autorização** acontece quando o **access_token** é utilizado em uma requisição e o **OAuth** permite acesso aos recursos.

Depois de realizar as etapas anteriores, você já pode chamar as APIs da Rede. Para isso, é necessário enviar o **access_token** gerado do no cabeçalho de todas as requisições.

Header

Authorization: Bearer {access_token}.

Atenção

O **access_token** deve ser armazenado com segurança

Como sua duração é de 24 minutos, uma nova chamada deverá ser feita antes desse período para atualizar a credencial.

O token de acesso possui validade de 24 minutos e pode ser reutilizado dentro desse intervalo. Para evitar expiração durante o uso, recomenda-se renová-lo entre 15 e 23 minutos após sua emissão.

A escolha de como realizar o chamado e atualizar os **access_token** gerados ficam sob sua responsabilidade

Codificação OAuth

UTF8

Configure sua aplicação para usar codificação UTF-8.

Codificação de URL

A codificação URL é usada para codificar informações em URIs e usada também para dados do tipo application/x-www-formurlencoded, como em formulários HTML.

JSON

JSON é o padrão usado para troca de dados entre sistemas. Para chamadas POST e PUT, é necessário especificar o cabeçalho:

Content-Type: application/json

Boas práticas de segurança

- Armazene o **access_token** em cache seguro e criptografado.
- Evite expor o token em logs ou interfaces públicas
- Implemente controle de acesso para uso do token
- Utilize HTTPS em todas as chamadas às APIs da Rede

Glossário

Termo	Descrição
PV	Código do estabelecimento utilizado nas transações com a Rede.
clientId	Identificador do cliente, equivalente ao PV.
clientSecret	Chave de integração gerada no portal da Rede.
access_token	Token de acesso gerado OAuth 2.0 , utilizado para autenticação nas APIs.
OAuth 2.0	Protocolo padrão da indústria para autenticação e autorização de aplicações.
Endpoint de autenticação	URL utilizada para gerar o access_token.
Scope	Lista de permissões concedidas ao token de acesso.

- Para mais informações de como realizar a migração para o modelo de autenticação **OAuth 2.0**, consulte nosso [tutorial](#).
- Caso tenha mais dúvidas sobre o processo de migração e possíveis impactos, consulte nossa [FAQ](#).

Endpoint de Autorização

Os endpoints são as URLs que serão utilizadas para a chamada de determinado serviço. Elas podem variar dependendo do ambiente e método HTTP.

A composição é realizada da seguinte forma:

- URL base
- Versão da API
- Serviço

Ambiente	URL
Sandbox	https://sandbox-erede.useredecloud.com.br/v2/transactions
Produção	https://api.userede.com.br/erede/v2/transactions

A cada tipo de serviço, um complemento será adicionado à URL base para que em seguida a requisição seja realizada. No decorrer desta documentação listaremos todas elas.

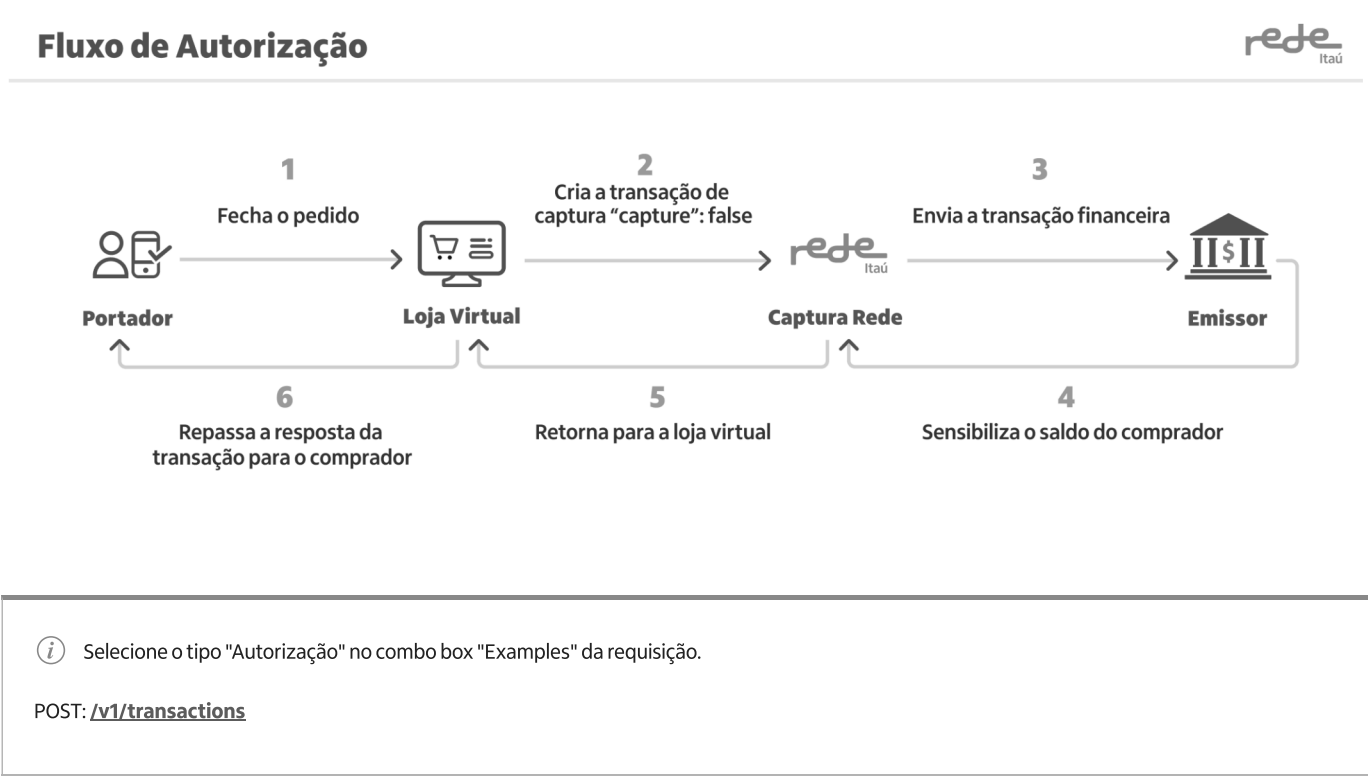
Fluxo de Autorização

A autorização é o primeiro passo para realizar uma transação. O valor da transação sensibiliza o limite do cartão do portador, porém não gera cobrança na fatura enquanto não houver a confirmação (captura).

Caso a autorização não seja capturada no prazo máximo de acordo com o ramo do estabelecimento, ela é automaticamente cancelada.

Para transações parceladas, informar o número mínimo de “2” e máximo de “12” parcelas.

O diagrama abaixo mostra o fluxo da transação de permissão sem a captura automática:



Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture		Booleano	Não	Defina se a transação terá captura automática ou posterior. O não envio desse campo será considerado a captura automática (true). Para transações de débito e Zero dollar, em caso de envio, o valor do parâmetro deve ser definido como true, indicando captura automática.
kind		Alfanumérico	Não	Tipo de transação a ser realizada. <ul style="list-style-type: none">• Para transações de crédito, utilizar credit• Para transações de débito, utilizar debit O não envio desse campo será considerado crédito.
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.

Nome	Tamanho	Tipo	Obrigatório	Descrição
amount	Até 10	Numérico	Sim	<p>Valor total da transação sem separador de milhar e decimal. Exemplos:</p> <ul style="list-style-type: none"> • R\$10,00 = 1000 • R\$0,50 = 50
installments	Até 2	Numérico	Não	<p>Número de parcelas em que uma transação será autorizada. De 2 a 12. O não envio desse campo será considerado à vista.</p>
cardholderName	Até 30	Alfanumérico	Não	<p>Nome do portador impresso no cartão. Não enviar caracteres especiais.</p>
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do cartão. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	<p>Ano de vencimento do cartão. Ex.: 2028 ou 28.</p>
securityCode	Até 4	Alfanumérico	Não	<p>Código de segurança do cartão geralmente localizado no verso do cartão. O envio desse parâmetro garante maior possibilidade de aprovação da transação.</p>
softDescriptor	Até 18 *	Alfanumérico	Não	Frase personalizada que será impressa na fatura do portador.
subscription		Booleano	Não	<p>Informa ao emissor se uma transação é proveniente de uma recorrência. Se transação por uma recorrência, enviar true. Caso contrário, envie false. O não envio desse campo será considerado o valor false. A Rede não gerencia os agendamentos de recorrência, apenas permite aos lojistas indicarem se uma transação originada é de um plano recorrente.</p>
origin	Até 2	Numérico	Não	<p>Identifica uma origem da transação.</p> <ul style="list-style-type: none"> • e.Redre - 1 <p>O não envio desse campo será considerado uma transação e.Redre (1).</p>
distributorAffiliation	Até 9	Numérico	Não	Número de filiação do distribuidor (PV).
brandTid	Até 21	Alfanumérico	Não	<p>Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file</p>

Nome	Tamanho	Tipo	Obrigatório	Descrição
transactionLinkId	Até 22	Alfanumérico	Não	Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file
securityAuthentication	-	-	-	Grupo securityAuthentication
sai	Até 02	Alfanumérico	Obrigatório para as bandeiras Visa e ELO. Opcional em transações card-on-file	Identificador de transação eletrônica (ECI). Para transações da bandeira Mastercard, esse campo não é enviado. Nas transações que não forem tokenizadas (apenas card-on-file) o envio deste campo não é necessário. Para mais detalhes desse campo verifique o tópico “uso do sai”.
transactionCredentials	-	-	-	Grupo transactionCredentials
transactionCredentials/ credentialId	Até 02	Alfanumérico	Sim, se storagecard=1 ou =2 e cartão mastercard	Indica a categoria da transação com credencial armazenada. Consulte a seção “Categorização de transações card-on-file” para mais detalhes

Uso do “sai”: O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e Cloud Token Visa), **quando autenticado como 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso.**

Atenção: Ao fazer o envio do grupo threeDSecure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Data e hora	Dados da transação no formato YYYY-MM-DDhh: mm: ss.sTZD .
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.

Nome	Tamanho	Tipo	Descrição
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file
brand/transactionLinkId	Até 22	Alfanumérico	Código identificador da transação na bandeira Mastercard. Para mais detalhes consulte a seção Recorrência e Card-on-file

Documentação

Pré-requisitos técnicos

O mecanismo de integração é simples, de modo que conhecimentos em linguagem de programação para web, requisições HTTPS e manipulação de arquivos JSON sejam necessários para implantar a solução com sucesso.

Credenciamento

Para solicitar o credenciamento do e.Red e realizar a integração à sua aplicação, entre em contato com a Central de atendimento da Rede:

4001 4433 (*capitais e regiões metropolitanas*) **0800 728 4433** (*demais localidades*)

Quando o credenciamento for realizado, o responsável pelo estabelecimento será notificado via e-mail com o número de filiação (PV), orientações para acessar ao portal da Rede e suas credenciais para integração.

Certificado Digital Rede

O que é um certificado digital? Certificado digital é um arquivo eletrônico que serve como identidade virtual para uma empresa e por ele pode se fazer transações online com garantia de autenticidade. Como uma prática de mercado para garantir toda a proteção das informações trocadas entre sua empresa e a Rede, é realizada a atualização do Certificado Digital Rede anualmente.

Por que ele deve ser atualizado? Para garantir maior segurança em suas vendas realizadas online.

Como fazer a atualização do Certificado Digital Rede? Para que seja feita a atualização do certificado dentro da sua empresa, pedimos que você direcione esta atividade ao seu time de tecnologia ou a quem tenha acesso ao seu servidor e seja responsável pela sua aplicação e-commerce. Caso o seu contato com a Rede seja feito por meio de sua plataforma, gateway ou módulo pedimos que entre em contato com eles para a atualização.

Ela deve ser realizada a partir do servidor que é responsável pela comunicação entre a sua empresa e a Rede e no qual o certificado já esteja instalado. Baixe o certificado digital de acordo com o seu sistema operacional determinado nas caixas sinalizadas abaixo nesta página.

Para efetuar a instalação ou atualização do Certificado Digital Rede utilize o link abaixo e siga as instruções.

<https://www.userede.com.br/n/documentos/certificado-digital-rede>

Caso seu e-commerce não faça uso de certificado digital, essa etapa não é necessária.

Homologação e certificado SSL

Para transacionar com a API do e.Red é necessário que o estabelecimento possua instalado na página de pagamento um certificado de segurança SSL com criptografia 2048 bits ou superior, para garantir o sigilo das informações transferidas e certificar ao portador do cartão que está realmente acessando o site desejado, evitando problemas com fraude.

Para garantir que os estabelecimentos tenham o certificado SSL instalado, a Rede faz o processo de homologação automaticamente da loja ou serviço virtual do estabelecimento após a realização da primeira transação.

IMPORTANTE: Periodicamente, o processo de homologação é realizado e a Rede se reserva o direito de suspender o uso da plataforma até que a loja ou serviço virtual estejam adequados às normas de segurança solicitadas.

Para identificar se a página possui o certificado SSL, ao acessar o site, a URL deve ser exibida com o protocolo “https” possibilitando a visualização do cadeado de segurança nos navegadores.

Exemplos:

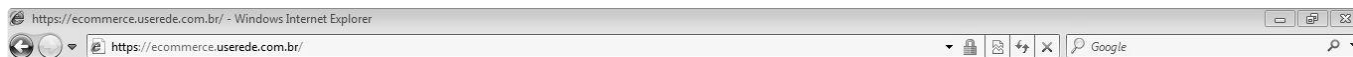
Firefox:



Google Chrome:



Internet Explorer:



Caso o estabelecimento tenha sido suspenso por não estar certificado, acesse o portal da Rede no menu *para vender > e-commerce > homologação* e clique em “Solicitar homologação” após a regularização do certificado SSL.

Filiação e Chave de Integração

Para que o estabelecimento comece a transacionar com o e.Red, é necessário configurar a API com suas credenciais: número de filiação (PV) e chave de integração.

A **chave de integração** é uma chave de uso confidencial, gerada no [Portal da Rede](#). Para gerá-la, certifique-se que seu usuário possua perfil de administrador (usuário master). Acesse o menu: *_e.Red > para vender > e-commerce > chave de integração* e clique em “Gerar chave de integração”.

Em caso de perda ou esquecimento da chave de integração, uma nova deverá ser gerada e a configuração da API deverá ser alterada, para que as transações continuem sendo enviadas à Rede.

Métodos HTTP

Os métodos HTTP para serviços RESTful serão frequentemente utilizados para requisição das transações.

VERBO HTTP	DESCRIÇÃO
POST	Utilizado na criação dos recursos ou no envio de informações que serão processadas. Por exemplo, criação de uma transação.
GET	Utilizado para consultas de recursos já existentes. Por exemplo, consulta de transações.
PUT	Utilizado para atualização de um recurso já existente. Por exemplo, captura de uma transação previamente autorizada.

As variações serão utilizadas conforme o serviço requisitado: autorização, captura, autorização com captura automática, consulta, cancelamento e consulta de cancelamento.

Códigos de retorno

Os códigos de retorno HTTP são utilizados para indicar o sucesso ou fracasso de uma solicitação da API. Os códigos iniciados com 2xx indicam sucesso, os códigos iniciados com 4xx indicam um erro devido a alguma informação incorreta fornecida na requisição e os códigos iniciados com 5xx indicam erro nos servidores.

Códigos de sucesso

RETORNO	DESCRIÇÃO	MÉTODO
200	Indica que o processamento foi realizado corretamente e o retorno será conforme a expectativa.	GET
201	Indica que o recurso foi criado com sucesso, deverá existir o header location indicando a url do novo recurso.	POST
202	Indica que o processamento será assíncrono, portanto, além do header location, deverá retornar o conteúdo com um atributo status.	POST E PUT
204	Indica que o recurso foi alterado ou excluído com sucesso.	PUT

Códigos de erro

RETORNO	DESCRIÇÃO
400	Requisição mal formatada.
401	Requisição requer autenticação.
403	Requisição negada.
404	Recurso não encontrado.
405	Método não permitido.
408	Tempo esgotado para requisição.
413	Requisição excede o tamanho máximo permitido.
415	Tipo de mídia inválida (verificar o header content-type da requisição)
422	Exceção de negócio. Verificar return code e return message.
429	Requisição excede a quantidade máxima de chamadas permitidas à API.

OBS: Caso você receba o erro "HTTP 401: Requisição requer autenticação" ao realizar uma requisição utilizando o protocolo de autenticação OAuth 2.0, significa que o access_token utilizado está expirado e um novo deve ser gerado.

Exceção lançada por erro de servidor(es)

RETORNO	DESCRIÇÃO
500	Erro de servidor.

Observação

Caso ocorra o erro 500 durante uma transação 3DS ou DATA ONLY, recomenda-se a verificação do status da transação. Essa verificação deve ser realizada na API de Consulta de transação pelo código do pedido campo (Reference):

GET: /v2/transactions?reference={codigo_reference}

Formatação

Encoding

Para utilizar as APIs da Rede será necessário configurar em sua aplicação o uso do encoding UTF-8.

JSON

JSON (JavaScript Object Notation) é um padrão para descrição de dados para intercâmbio entre sistemas. Ele é mais simples e mais leve que o XML. Por padrão, toda API trafega JSON, tanto para receber informações (métodos POST e PUT) quanto no retorno (método GET).

Devido esta padronização, para as chamadas POST e PUT é necessário informar no HTTP Header content-type: application/json. Do contrário, você receberá um erro HTTP 415: Unsupported Media Type.

Campos do tipo Datetime

Todos os atributos do tipo Datetime, tanto atributos que são retornados em objetos quanto os que são passados como parâmetros nas operações, seguem o padrão ISO-8601, representado abaixo:

Date: YYYY-MM-DDThh:mm:ss.sTZD Exemplo: 2015-11-28T08:54:00.000-03:00

Transações

As transações são divididas de forma com que o lojista possa optar em realizar a captura de forma posterior ou automática.

Na **autorização com captura posterior**, o valor da transação sensibiliza o limite do cartão do portador, porém não gera cobrança na fatura enquanto não houver a confirmação (captura).

Já na **autorização com captura automática**, o valor da transação é confirmado de maneira instantânea, sem a necessidade de realizar a transação de captura.

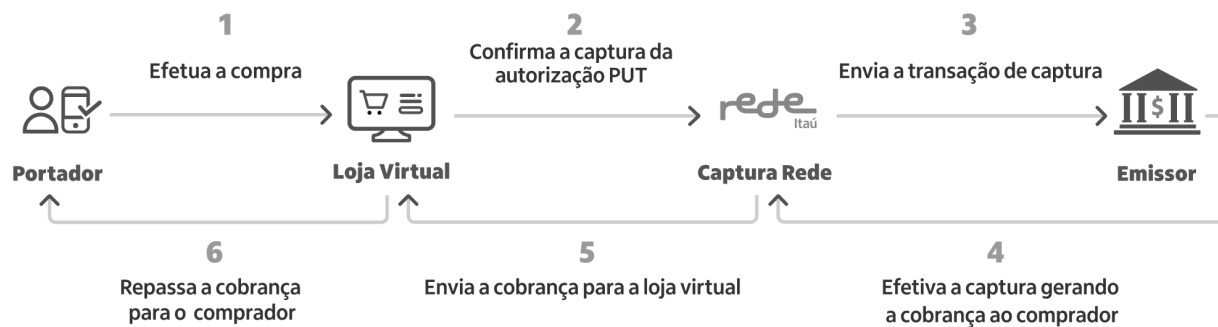
Captura

Ao realizar uma autorização, é necessária a confirmação desta transação (captura). Nesse momento é gerada a cobrança na fatura do portador do cartão.

A autorização deverá ser capturada no período máximo de acordo com o ramo do estabelecimento.

IMPORTANTE: Sempre aguardar a resposta da transação antes de realizar nova tentativa de captura da mesma.

O diagrama abaixo mostra o fluxo da transação de captura:



PUT: [/v2/transactions/{tid}](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
amount	Até 10	Númerico	Não	Valor da captura sem separador de milhar e decimal.
				Exemplos:
				- R\$10,00 = 1000
				- R\$0,50 = 50

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.STZD.
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.


Nome	Tamanho	Tipo	Descrição
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Companhias aéreas

Companhias aéreas possuem um tipo de transação diferenciada, que permite o envio do valor da taxa de embarque separado do valor da passagem aérea. A transação pode ser “à vista” ou “parcelada”.

As transações de companhias aéreas devem ser do tipo crédito, com captura automática (capture = true) e devem ser enviadas juntamente com o **BODY** da transação.

IMPORTANTE: Cancelamentos de transações do tipo IATA só podem ser realizados à partir de D+1.

 Selecione o tipo "Companhias aéreas" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
iata		iata		
iata/code	Até 9	Numérico	Sim	Código iata da companhia aérea.
iata/departureTax	Até 10	Numérico	Sim	Valor da taxa de embarque sem separador de milhar e decimal.
				Exemplos:
				- R\$10,00 = 1000
				- R\$0,50 = 50

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.

Nome	Tamanho	Tipo	Descrição
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Númérico	Valor total da transação sem separador de milhar e decimal.
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

3D Secure 2.0

Transações autenticadas 3D Secure ou 3DS são transações que necessitam de uma autenticação adicional para garantir maior segurança para o portador do cartão nas compras online. A autenticação 3DS é efetuada através da validação de dados que apenas o portador do cartão e o banco possuem, como por exemplo, senha do cartão, data de nascimento, código de segurança, token do banco. **Em caso de sucesso da autenticação, o emissor assume o risco da transação.**

O 3D Secure 2.0 é um novo padrão de autenticação para fornecer segurança adicional às transações e é a primeira solução capaz de autenticar uma transação sem intervenção do cliente (autenticação sem desafio), pois o emissor terá acesso a mais informações da transação e não apenas os dados de valor e cartão. Nos casos que necessitam de autenticação (com desafio) o processo é intuitivo e pode ocorrer via biometria, reconhecimento de voz/facial ou envio de SMS, ajudando a evitar o abandono do carrinho. Quem decide se a transação deverá ser com desafio ou não, é o emissor.

Em termos de mercado, atualmente a Rede proporciona a utilização da versão 2.2 do protocolo 3DS. Estamos trabalhando para disponibilizar a versão 2.3 em breve. Resumidamente, o protocolo 3D Secure 2.0 acelera a autenticação, aumenta a segurança e aumenta as taxas de conversão proporcionando aos compradores uma rápida finalização da compra extremamente fluída, especialmente no celular, e trazendo proteção extra para o lojista. Veja a tabela de funcionalidades abaixo:

Funcionalidades do 3DS 2.0	Benefícios agregados
Substitui senhas estáticas por 2 fatores fortes: RBA, OTP, Biometria ou Canal Alternativo (Out of Band).	<ul style="list-style-type: none"> • Maior segurança • Maior conveniência • Menor fricção
Suporte a diferentes canais de pagamento (in-app, IoT, navegador, etc).	<ul style="list-style-type: none"> • Melhor UX • Maior abrangência • Controle melhorado para os estabelecimentos
Suporte a compra e casos de uso adicionais (provisionamento de Card on File, Carteiras Digitais, Pagamentos Recorrentes, Tokenização, etc).	<ul style="list-style-type: none"> • Maior aplicabilidade • Maior segurança

A autenticação 3DS é obrigatória para todas as transações efetuadas com cartões de débito. Para os cartões de crédito, sua utilização é opcional.

O MPI (merchant plug-in) é o serviço que provê a integração do estabelecimento com diferentes emissores, alinhado às certificações das bandeiras para processamento da autenticação 3D Secure (3DS).

O e.Redre disponibiliza duas formas de utilização do serviço 3DS, através do MPI Rede ou MPI Cliente. A utilização do MPI estará a critério do estabelecimento.

- MPI Rede: serviço já embarcado na plataforma e.Redre, sem necessidade de contratação adicional. Nesse cenário, a Rede realiza o fluxo de autenticação e autorização da transação.
- MPI Cliente: serviço contratado **adicionalmente** pelo cliente para integração com o e.Redre, sem influência da Rede na autenticação da transação. Portanto, nesse cenário, a Rede realiza apenas o fluxo de autorização.

Para que as transações 3DS possam ser realizadas, os emissores também precisam estar preparados para receber as informações de autenticação do comprador. Os principais emissores do Brasil já disponibilizam esse serviço a seus clientes.

3DS 2.0 - MPI Rede

O e.Redre já possui o MPI embarcado em sua plataforma. Portanto, utilize o parâmetro *embedded* para sinalizar que o MPI contratado é o da Rede, vide tabela de “Parâmetros da requisição”.

As transações que utilizam o serviço 3DS com o MPI Rede podem ser do tipo crédito ou débito e devem ser enviadas juntamente com o **BODY** da transação de autorização.

O MPI Rede permite a autenticação do 3DS2.0 em transações das bandeiras Visa, Mastercard e Elo.

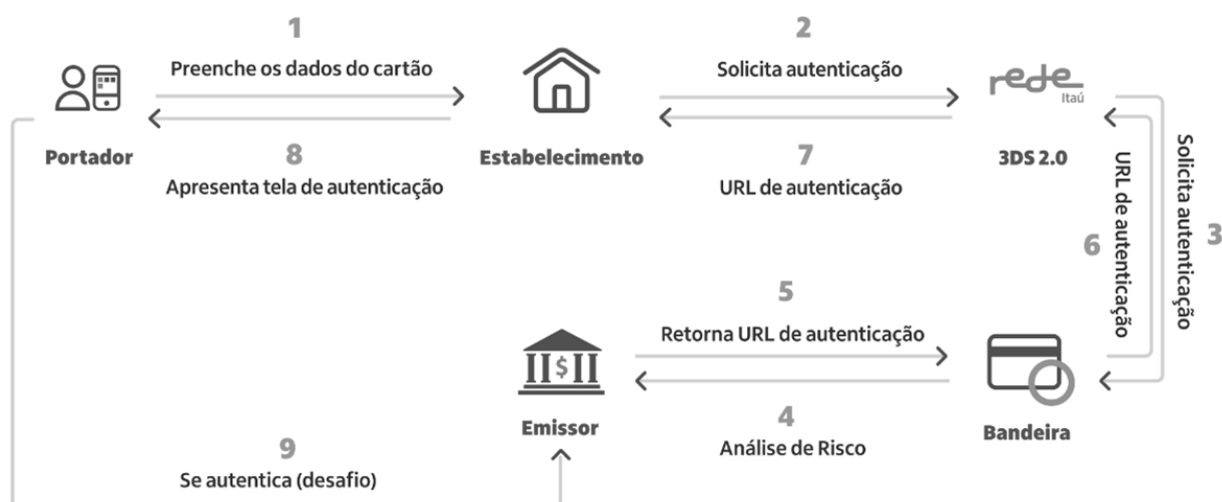
Para as transações de crédito, caso a transação não tenha sido autenticada com sucesso, existe a possibilidade de prosseguir com a transação sem a devida autenticação 3DS, e o risco da transação passa a ser do lojista, voltando ao ciclo transacional “comum”.

Para transações de débito o valor deste parâmetro é automaticamente definido devido à obrigatoriedade da autenticação.

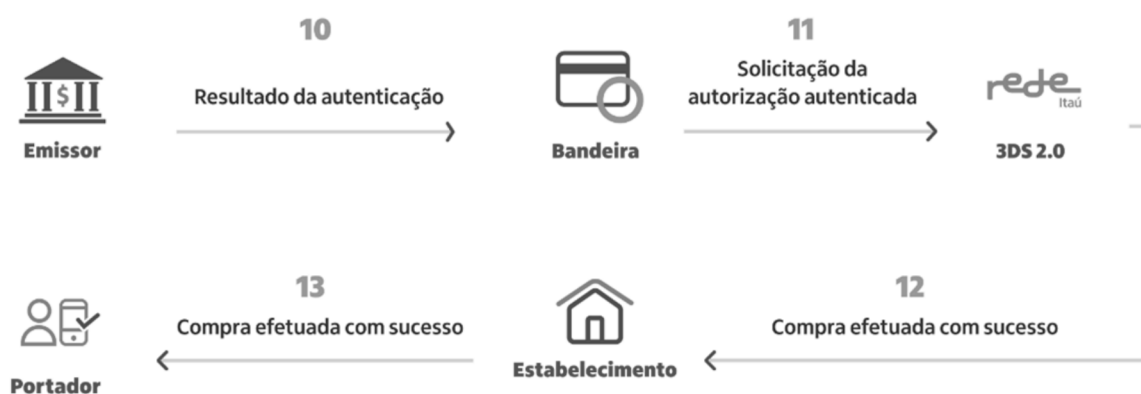
Para habilitar o serviço, acesse o portal “userede.com.br”, *menu vender online > e-commerce > 3DS/Data Only > Contratar*.

Em algumas horas, a Rede retornará informando o status da solicitação de habilitação do serviço.

Os diagramas abaixo mostram o fluxo da transação autenticada (1) e autorizada (2) utilizando o MPI Rede, quando há a solicitação do desafio por parte do emissor:

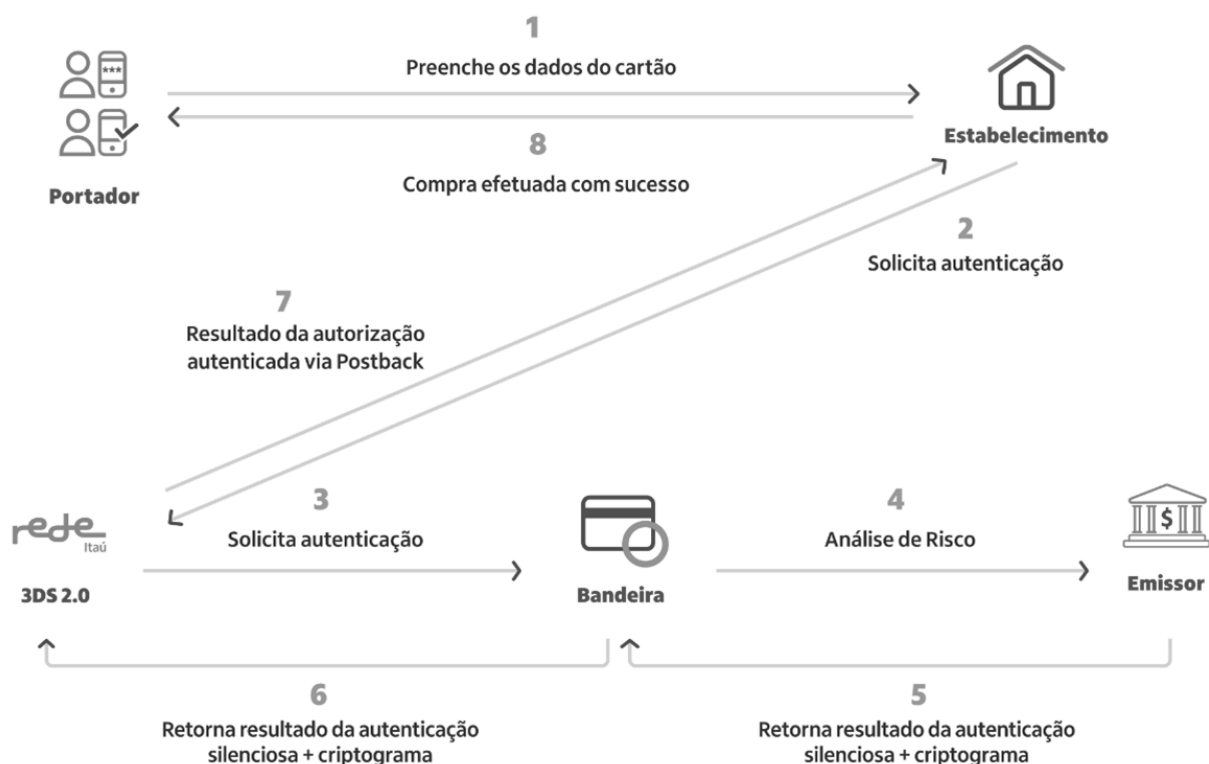


Fluxograma 1 de autenticação (com desafio)



Fluxograma 2 de autorização (com desafio)

Já o diagrama abaixo, ilustra o fluxo da transação autenticada e autorizada quando o emissor **não** solicita o desafio ao comprador:



Fluxograma 3 de autenticação + autorização (sem desafio)

IMPORTANTE: Para verificar o status da transação, utilize o endpoint de consulta. [Clique aqui](#) para obter mais informações.

 Selecione o tipo "3D Secure 2.0: MPI Rede" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure		threeDSecure	Sim	
threeDSecure /embedded		Booleano	Não	<p>Informa se o serviço MPI utilizado será da Rede ou terceiro.</p> <ul style="list-style-type: none">true: utiliza o serviço MPI da Redefalse: utiliza serviço MPI terceiro <p>O não envio desse campo será considerado o uso do MPI da Rede.</p>

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure /onFailure		Alfanumérico	Não	<p>Define como prosseguir com a transação caso a autenticação 3DS não obtenha sucesso.</p> <ul style="list-style-type: none"> • continue: prossegue com a transação financeira mesmo se a autenticação falhar • decline: não prossegue com a transação financeira caso a autenticação falhar <p>Para transações de débito o valor deste parâmetro é automaticamente definido para decline devido à obrigatoriedade da autenticação.</p>
threeDSecure /userAgent	Até 255	Alfanumérico	Sim	Identificador do browser utilizado pelo comprador no momento da compra.
threeDSecure /ipAddress	11	Alfanumérico	Sim	Suporta informações somente em IPv4. Exemplo: 10.0.0.1
threeDSecure /device				
threeDSecure /device/colorDepth	2	Numérico	Sim	Campo que representa a estimativa da paleta de cores usada para a exibição de imagens, em bits por pixel. Obtido no navegador do cliente através da propriedade.
threeDSecure /device/deviceType3ds	20	Alfanumérico	Sim	Campo que indica tipo de dispositivo no qual a autenticação ocorre.
threeDSecure /device/javaEnabled		Booleano	Sim	Campo booleano que representa a capacidade do navegador para executar Java. O valor é aquele retornado pela propriedade navigator.javaEnabled, true ou false.
threeDSecure /device/language	10	Alfanumérico	Sim	Idioma do navegador no formato IETF BCP47, contendo entre 1 e 8 caracteres.
threeDSecure /device/screenHeight	6	Numérico	Sim- para browser e Mobile	A altura total da tela do cliente em pixels. O valor é aquele retornado pela propriedade screen.height.
threeDSecure /device/screenWidth	6	Numérico	Sim- para browser e Mobile	A largura total da tela do cliente em pixels. O valor é aquele retornado pela propriedade screen.width.
threeDSecure /device/timeZoneOffset	10	Alfanumérico	Sim	Diferença de horário, em horas, entre o UTC e a hora local do navegador do titular do cartão.
cardholderName	Até 30	Alfanumérico	Sim	Nome do portador impresso no cartão. Não enviar caracteres especiais.
threeDSecure /billing		billing	Sim	Dados referentes ao portador do cartão
threeDSecure /billing /address	Até 128	Alfanumérico	Sim	Endereço
threeDSecure /billing /city	Até 64	Alfanumérico	Sim	Cidade

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeD Secure /billing /postalcode	9	Numérico	Sim	CEP
threeD Secure /billing /state	Até 64	Alfanumérico	Sim	Estado
threeD Secure /billing /country	Até 64	Alfanumérico	Sim	País
threeD Secure /billing /emailAddress	Até 128	Alfanumérico	Sim	E-mail
threeD Secure /billing /phoneNumber	Até 32	Numérico	Sim	Telefone
urls		urls		
urls/kind		Alfanumérico	Sim	<p>Campo que identifica qual o tipo da url.</p> <ul style="list-style-type: none"> • threeD SecureSuccess • threeD SecureFailure • threeD SecureCallback
urls/url	Até 87	Alfanumérico	Sim	<p>Campo para informar a url que o comprador deverá ser redirecionado após a autenticação e ser notificado via postback (application/x-www-form-urlencoded) ou callback com os dados da transação.</p> <p>Caso o urls/kind seja preenchido com o threeD SecureSuccess ou threeD SecureFailure, será recebido um postback conforme documentação Clique aqui.</p> <p>Caso seja enviado o threeD SecureCallback, será recebido um callback conforme documentação Clique aqui.</p> <p>Os processos podem ser usados de maneira conjunta como estratégia de redundância no recebimento das informações.</p>

Ponto de atenção: É possível utilizar o 3DS MPI Interno somente com as seguintes mensagens:

- [MCC dinâmico](#): Mensageria específica para os clientes que atuam com mais de um MCC
- [Carteira digital escalonada \(SDWO\)](#)
- [Tokenização de bandeira Rede](#)
- [Tokenização de bandeira externa \(captura\)](#)
- [Recorrência e Card-on-File](#) **Importante:** Ao combinar as duas mensagens, a autenticação é realizada e válida apenas para a **primeira** transação da recorrência. As transações subsequentes não terão autenticação 3DS, nem o benefício do liability shift.

As mensagens podem ser utilizadas em conjunto ou individualmente.

Observação:

1. Não é possível utilizar o 3DS em transações Zero Dollar.
2. Não é possível fazer simulações de Iframe com 3DS em sandbox.

Erro 500 em transações 3DS

Caso ocorra o erro 500 durante uma transação 3DS, recomenda-se a verificação do status da transação. Essa verificação deve ser realizada na API de Consulta de transação pelo código do pedido campo (Reference):

GET: /v2/transactions?reference={codigo_reference}

Para ver um exemplo de todas as mensagens juntas na requisição:

Selecione o tipo "3D Secure 2.0: MPI Rede + Token + MCC Dinâmico + SDWO" no combo box "Examples" da requisição.

 POST: </v2/transactions>

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
dateTime		Datetime	Data de transação no formato YYYY-MM-DDThh:mm:ss.sTZD
threeDSecure		threeDSecure	
threeDSecure /embedded		Booleano	Informa se o serviço MPI utilizado será da Rede ou terceiro.
threeDSecure /url	Até 500	Alfanumérico	Url de autenticação retornada pelo sistema MPI.
returnCode	3	Alfanumérico	Código de retorno da transação com 3ds (vide tabela retornos 3DS).
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação com 3ds (vide tabela retornos 3DS).
installments	Até 2	Numérico	Número de parcelas em que uma transação será autorizada. De 2 a 12. (vide tabela de Autorização).

Postback

Notificação via application/x-www-form-urlencoded com os seguintes dados da transação:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
date		Date	Data da transação no formato yyyyMMdd .

Nome	Tamanho	Tipo	Descrição
time		Time	Hora da transação no formato HH:mm:ss .
returncode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
threeDSecure.returnCode	Até 4	Alfanumérico	Código de retorno do 3DS (vide tabela retornos 3DS).
brand			Grupo de informações recebidas da bandeira sobre a transação.
brand/name		Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.

O postback será enviado apenas em cenários de autenticação bem-sucedidas. Em casos de falha na autenticação ou de não interação do cliente em um possível fluxo com desafio, nenhum postback será enviado.

IMPORTANTE

No caso de um não recebimento de postback, ou de falha nesse fluxo, recomenda-se a verificação do status da transação. Essa verificação deve ser realizada na API de Consulta de transação pelo código do pedido campo (Reference):

GET: /v2/transactions?reference={codigo_reference}

Lembrando que se a transação financeira (pós autenticação) não for realizada, a consulta apresentará o seguinte retorno: "returnCode": "78", "returnMessage": "Transaction does not exist."

Callback

O Callback é um retorno assíncrono da API, que será enviado no endpoint indicado para receber o método post.

Essa "indicação" é feita na própria requisição da transação, dentro do bloco "urls", enviando o item preenchido com o: "**kind**": "**threeDSecureCallback**" e a "url" com o valor correspondente ao seu endpoint que irá receber o callback através de uma requisição HTTP com o método POST.

No callback será indicado o resultado da autenticação da transação.

Nome	Tamanho	Tipo	Descrição
reference	Até 16	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
expiresAt		Data e hora	Dados de expiração da pré-autorização no formato YYYY-MM-DDThh:mm:ssTZD.
date		Data	Data da transação no formato YYYY-MM-DD.
time		Hora	Hora da transação no formato HH:mm:ss.

Nome	Tamanho	Tipo	Descrição
returncode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
threeDSecure.returnCode	Até 4	Alfanumérico	Código de retorno do 3DS (vide tabela retornos 3DS).
threeDSecure.returnMessage	Até 256	Alfanumérico	Mensagem de retorno do 3DS.
brand			Grupo de informações recebidas da bandeira sobre a transação.
brand/name		Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.

IMPORTANTE: O callback é utilizado para informar os status de autenticação da transação, para consultar e validar os status de autorização, é necessário confirmar o status da transação na API de [Autorização](#).

3DS 2.0 - MPI Cliente

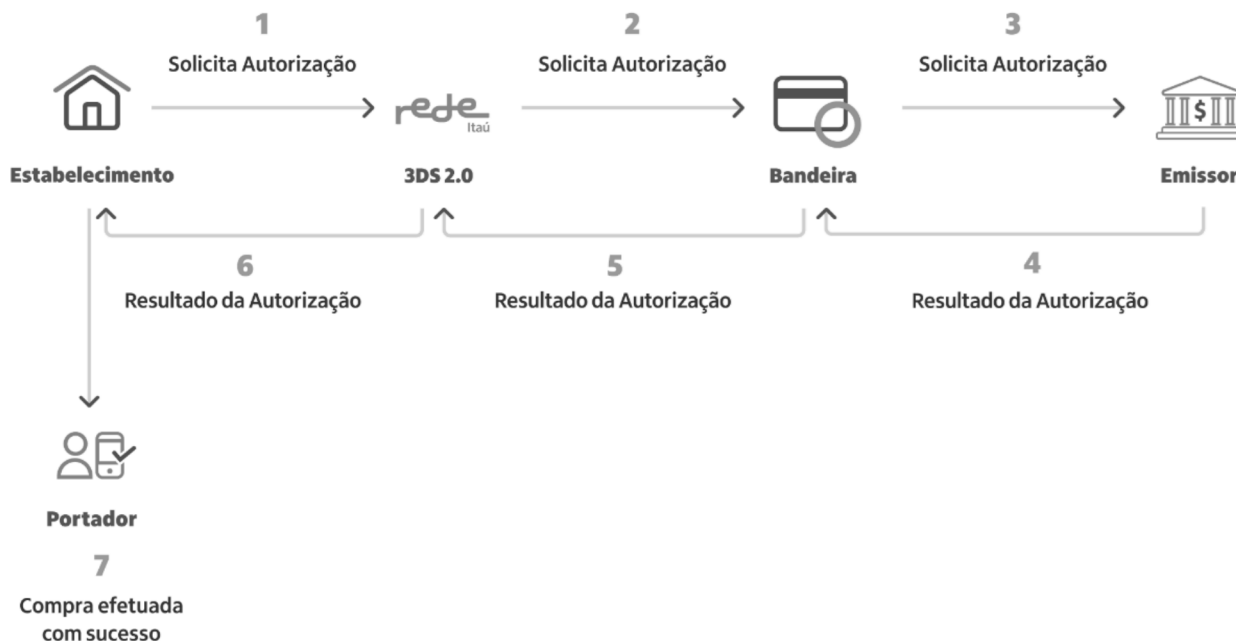
O MPI Cliente é utilizado quando o estabelecimento já possui um MPI contratado. Portanto, utilize o parâmetro *embedded* para sinalizar que o MPI já foi contratado de forma externa à Rede, vide tabela de “Parâmetros da requisição”.

Para que as transações com 3DS sejam autenticadas pelo emissor e posteriormente autorizadas via e.Red, através do MPI Cliente, é necessário que o serviço de MPI seja certificado junto às bandeiras e à Rede. Atualmente, os serviços de MPI certificados são: Lyra, Cardinal e Datacash.


Nesse cenário de autenticação externa, a Rede pode receber transações de todas as bandeiras, entre as que já estão preparadas para o produto, e assim seguir com o fluxo de autorização.

As transações que utilizam o serviço 3DS com o MPI Cliente, podem ser do tipo crédito ou débito e devem ser enviadas juntamente com o **BODY** da transação de autorização.

O diagrama abaixo mostra o fluxo de autorização da transação autenticada utilizando o MPI Cliente:



Fluxograma 4 de autorização (com ou sem desafio)

 Selecione o tipo "3D Secure 2.0: MPI Cliente" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure		threeDSecure	Sim	
threeDSecure /embedded		Booleano	Não	<p>Informa se o serviço MPI utilizado será da Rede ou terceiro.</p> <ul style="list-style-type: none">• true: utiliza o serviço MPI da Rede• false: utiliza serviço MPI terceiro <p>O não envio desse campo será considerado o uso do MPI da Rede.</p>
threeDSecure /eci	2	Alfanumérico	Sim	<p>Código retornado ao MPI pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor. Transações de débito devem ser obrigatoriamente autenticadas.</p>
threeDSecure /cavv	Até 32	Alfanumérico	Sim	<p>Código do criptograma utilizado na autenticação da transação e enviado pelo MPI do estabelecimento (pode conter caracteres especiais).</p>
threeDSecure /threeDIndicator	1	Alfanumérico	Sim	<p>Versão do 3DS usado no processo de autenticação pelo MPI.</p>

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure/xid	28	Alfanumérico	Não	ID da transação de autenticação enviado pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS na versão 1.0. Campo utilizado somente para bandeira Visa.
threeDSecure /directoryServerTransactionId	36	Alfanumérico	Sim	ID da transação de autenticação incluída pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS 2.0. Esse campo também pode ser chamado como dsTransId na Visa.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Númérico	Valor total da transação sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.

Nome	Tamanho	Tipo	Descrição
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Ponto de atenção: Utilizando o 3DS2.0 MPI Cliente, sua autenticação será realizada fora do ambiente da Rede. Neste cenário, alguns clientes estão tendo autenticações negadas devido a falta ou invalidez do parâmetro **"MCC dinâmico"**{target="_blank"}.

Portanto, garanta que este campo está sendo enviado ao provider que realizará a autenticação da transação, aumentando assim as taxas de sucesso e evitando erros inesperados neste fluxo.

Data Only

Dataonly é uma modalidade similar ao 3DS. O objetivo do protocolo é diminuir o índice de fraude e aumentar taxas de aprovação em relação a uma transação comum, pois mais dados serão analisados para embasar a tomada de decisão do emissor.

O Dataonly intermediado pela Rede está disponível no momento, para as bandeiras Mastercard e Visa.

Todas as transações DataOnly são autenticadas silenciosamente, da mesma forma que um 3DS 2.0 frictionless. Isso garante uma experiência de compra fluída para o usuário, mas em contraponto, não aplica o benefício do liability shift, ou seja, em caso de chargebacks, a responsabilidade de pagamento continua com o comércio, diferentemente da autenticação 3DS, que quando bem-sucedida, transfere essa responsabilidade ao emissor.

Para utilização do Produto, é necessário realizar a contratação no portal “[userede.com.br](#)”, para que seja realizada a ativação do Comércio no MPI. Portanto, habilite o serviço através do menu *vender online > e-commerce > 3DS/Data Only > Contratar*.

O MPI (merchant plug-in) é o serviço que provê a integração do estabelecimento com diferentes emissores, alinhado às certificações das bandeiras para processamento da autenticação.

O e.Redre disponibiliza duas formas de utilização do serviço, através do MPI Rede ou MPI Cliente. A utilização do MPI estará a critério do estabelecimento.

- MPI Rede: serviço já embarcado na plataforma e.Redre, sem necessidade de contratação adicional. Nesse cenário, a Rede realiza o fluxo de autenticação e autorização da transação.
- MPI Cliente: serviço contratado adicionalmente pelo cliente para integração com o e.Redre, sem influência da Rede na autenticação da transação. Portanto, nesse cenário, a Rede realiza apenas o fluxo de autorização.

Para que as transações 3DS possam ser realizadas, os emissores também precisam estar preparados para receber as informações de autenticação do comprador. Os principais emissores do Brasil já disponibilizam esse serviço a seus clientes.

Tabela Comparativa:

	Experiência sempre sem desafio	Influência na decisão de aprovação do emissor	Sem latência na transação	Liability Shift
DataOnly	✓	✓	✓	
3DS	Pode ser solicitado ou não	✓		✓

Para mais informações, consulte o infográfico da MasterCard [aqui](#){target="_blank"}.

Data Only - MPI Rede

Para utilizar a modalidade Data Only com o MPI embarcado do e.Redre basta adicionar o parâmetro *challengePreference* na requisição MPI Rede indicando o uso do Data Only, vide tabela de “Parâmetros da requisição”.

 Selecione o tipo "Data Only - MPI Rede" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeD Secure		threeD Secure	Sim	
threeD Secure /embedded		Booleano	Não	<p>Informa se o serviço MPI utilizado será da Rede ou terceiro.</p> <ul style="list-style-type: none">• true: utiliza o serviço MPI da Rede• false: utiliza serviço MPI terceiro <p>O não envio desse campo será considerado o uso do MPI da Rede.</p>
threeD Secure /onFailure		Alfanumérico	Não	<p>Define como prosseguir com a transação caso a autenticação 3DS não obtenha sucesso.</p> <ul style="list-style-type: none">• continue: prossegue com a transação financeira mesmo se a autenticação falhar• decline: não prossegue com a transação financeira caso a autenticação falhar <p>Para transações de débito o valor deste parâmetro é automaticamente definido para decline devido à obrigatoriedade da autenticação.</p>
threeD Secure /userAgent	Até 255	Alfanumérico	Não	Identificador do browser utilizado pelo comprador no momento da compra.
threeD Secure /ipAddress	11	Alfanumérico	Sim	Suporta informações somente em IPv4. Exemplo: 10.0.0.1
threeD Secure /device				
threeD Secure /device/colorDepth	2	Númérico	Sim	Campo que representa a estimativa da paleta de cores usada para a exibição de imagens, em bits por pixel. Obtido no navegador do cliente através da propriedade.
threeD Secure /device/deviceType3ds	20	Alfanumérico	Sim	Campo que indica tipo de dispositivo no qual a autenticação ocorre.
threeD Secure /device/javaEnabled		Booleano	Sim	Campo booleano que representa a capacidade do navegador para executar Java. O valor é aquele retornado pela propriedade navigator.javaEnabled, true ou false.
threeD Secure /device/language	10	Alfanumérico	Sim	Idioma do navegador no formato IETF BCP47 , contendo entre 1 e 8 caracteres.
threeD Secure /device/screenHeight	6	Númérico	Sim- para Browser e Mobile	A altura total da tela do cliente em pixels. O valor é aquele retornado pela propriedade screen.height.

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure /device/screenWidth	6	Numérico	Sim- para Browser e Mobile	A largura total da tela do cliente em pixels. O valor é aquele retornado pela propriedade screen.width.
threeDSecure /device/timeZoneOffset	10	Alfanumérico	Sim	Diferença de horário, em horas, entre o UTC e a hora local do navegador do titular do cartão.
threeDSecure /billing		billing	Sim	Dados referentes ao portador do cartão
threeDSecure /billing /address	Até 128	Alfanumérico	Sim	Endereço
threeDSecure /billing /city	Até 64	Alfanumérico	Sim	Cidade
threeDSecure /billing /postalcode	9	Numérico	Sim	CEP
threeDSecure /billing /state	Até 64	Alfanumérico	Sim	Estado
threeDSecure /billing /country	Até 64	Alfanumérico	Sim	País
threeDSecure /billing /emailAddress	Até 128	Alfanumérico	Sim	E-mail
threeDSecure /billing /phoneNumber	Até 32	Numérico	Sim	Telefone
urls		urls		
urls/kind		Alfanumérico	Sim	<p>Campo que identifica qual o tipo da url.</p> <ul style="list-style-type: none"> threeDSecureSuccess threeDSecureFailure
urls/url	Até 87	Alfanumérico	Sim	<p>Campo para informar a url que o comprador deverá ser redirecionado após a autenticação e ser notificado via postback (application/x-www-form-urlencoded) com os dados da transação. Clique aqui para mais informações.</p>
threeDSecure /challengePreference		Alfanumérico	Não	<p>Campo que indica a preferência de uso do Data Only.</p> <ul style="list-style-type: none"> DATA_ONLY

Ponto de atenção: É possível utilizar o Data Only - MPI Rede somente com as seguintes mensagens:

- MCC dinâmico: Mensageria específica para os clientes que atuam com mais de um MCC
- Carteira digital escalonada (SDWQ)
- Tokenização de bandeira Rede
- Tokenização de bandeira externa (captura)
- Recorrência e Card-on-File **Importante:** Ao combinar as duas mensagens, a autenticação é realizada e válida apenas para a **primeira** transação da recorrência. As transações subsequentes não terão autenticação Data Only.

As mensagens podem ser utilizadas em conjunto ou individualmente.

Observação: Não é possível utilizar o Data Only em transações Zero Dollar.

Para ver um exemplo de todas as mensagens juntas na requisição:

 Selecione o tipo "Data Only: MPI Rede + Token + MCC Dinâmico + SDWO" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Erro 500 em transações Data_ONLY

Caso ocorra o erro 500 durante uma transação DATA ONLY, recomenda-se a verificação do status da transação. Essa verificação deve ser realizada na API de Consulta de transação pelo código do pedido campo (Reference):


> GET: [/v2/transactions?reference={codigo_reference}](#)

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.STZD .
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
installments	Até 2	Numérico	Número de parcelas em que uma transação será autorizada. De 2 a 12. (vide tabela de Autorização).
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.

Data Only - MPI Cliente

Para utilizar a modalidade Data Only com um MPI externo, a requisição será a mesma do 3DS 2.0, com alterações de valores em alguns campos. Vide tabela de "Parâmetros da requisição".

 Selecione o tipo "Data Only – MPI Cliente" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
threeDSecure		threeDSecure	Sim	
threeDSecure /embedded		Booleano	Não	Informa se o serviço MPI utilizado será da Rede ou terceiro. <ul style="list-style-type: none">true: utiliza o serviço MPI da Redefalse: utiliza serviço MPI terceiro O não envio desse campo será considerado o uso do MPI da Rede.
threeDSecure /eci	2	Alfanumérico	Sim	Código retornado ao MPI pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor. Transações de débito devem ser obrigatoriamente autenticadas.
threeDSecure /cavv	Até 32	Alfanumérico	Sim	Código do criptograma utilizado na autenticação da transação e enviado pelo MPI do estabelecimento (pode conter caracteres especiais).
threeDSecure /threeDIndicator	1	Alfanumérico	Sim	Versão do 3DS usado no processo de autenticação pelo MPI.
threeDSecure /xid	28	Alfanumérico	Não	ID da transação de autenticação enviado pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS na versão 1.0. Campo utilizado somente para bandeira Visa.
threeDSecure /directoryServerTransactionId	36	Alfanumérico	Sim	ID da transação de autenticação incluída pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS 2.0. Esse campo também pode ser chamado como dsTransId na Visa.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.

Nome	Tamanho	Tipo	Descrição
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.STZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.

Tabela de ECIs

O parâmetro ECI (Eletronic Commerce Indicator) se baseia no valor retornado ao MPI pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor.

Este, portanto, indica a situação do fluxo de autenticação em uma transação, e se o Risco de chargeback é transferido para o emissor ou permanece com o lojista. Confira abaixo os valores utilizados pelas bandeiras:

Bandeira	ECI	Significado da Transação	Risco Chargeback
ELO	0	Desconhecido/ Não Especificado/ Loja não participa do programa	Risco de chargeback permanece com o estabelecimento
ELO	4	Transação com autenticação In App	Usada em transações Wallets. Risco de chargeback passa a ser do emissor
ELO	5	Portador Autenticado pelo Emissor	Risco de chargeback passa a ser do emissor
ELO	6	Tentativa de Autenticação do Portador pelo Domínio do Credenciador (autenticada pela bandeira)	Risco de chargeback passa a ser do emissor
ELO	7	Transação de eCommerce Não Autenticada	Risco de chargeback permanece com o estabelecimento
MASTERCARD	0	Tentativa de autenticação incompleta ou falhou	Risco de chargeback permanece com o estabelecimento
MASTERCARD	1	Autenticação pelo Stand-In da Mastercard	Risco de chargeback passa a ser do emissor

Bandeira	ECI	Significado da Transação	Risco Chargeback
MASTERCARD	2	Autenticação bem-sucedida	Risco de chargeback passa a ser do emissor
MASTERCARD	4	Autenticação Data Only bem-sucedida	Risco de chargeback permanece com o estabelecimento
MASTERCARD	7	Recorrência	Risco de chargeback permanece com o estabelecimento
VISA	5	Autenticação do Cartão bem-sucedida	Risco de chargeback passa a ser do emissor
VISA	6	A autenticação foi tentada, mas não foi ou não pôde ser concluída; possíveis razões, sendo que o cartão ou seu Banco Emissor ainda não participa. (autenticada pela bandeira)	Risco de chargeback passa a ser do emissor
VISA	7	A autenticação não foi bem-sucedida ou não foi tentada.	Risco de chargeback permanece com o estabelecimento
VISA	7	Autenticação Data Only bem-sucedida	Risco de chargeback permanece com o estabelecimento

Zero Dollar

A transação Zero Dollar, permite uma validação prévia para saber se o cartão do portador e dados enviados antes do processamento da transação são válidos. Esse tipo de transação não gera nenhum tipo de cobrança para o comprador, evitando débitos indevidos em seu saldo.

O serviço está disponível para as bandeiras Visa, MasterCard, Elo e AMEX no crédito. No débito está disponível para as bandeiras Visa, Mastercard e Elo. O Zero Dollar é obrigatório quando pretende-se armazenar o cartão, já para outras operações é altamente recomendado a fim de validar o cartão antes de iniciar o fluxo transacional padrão.

O parâmetro securityCode será obrigatório para validações Zero Dollar em todas as bandeiras.

As transações Zero Dollar deverão ser enviadas como autorização com captura automática (**capture = true**), informando o valor 0 no parâmetro amount.

IMPORTANTE:

- Esse tipo de transação não pode ser cancelada.
- Esse tipo de transação não deve ser enviada como recorrente (subscription = true). Realize primeiro a validação Zero Dollar seguindo os parâmetros especificados a seguir e depois será possível utilizar o cartão para transações recorrentes ou não.

Contratação do Produto Zero Dollar.

A contratação do produto Zero Dollar deve ser realizada através da Central E-commerce. Para isso, entre em contato com a nossa Central de Atendimento, peça para falar com a central E-commerce e informe que deseja habilitar o "Zero Dollar" em seu ponto de venda e-commerce.

Central de Atendimento:


4001-4433 (capitais e regiões metropolitanas)

0800-728-4433 (demais localidades)

Horário de Atendimento: Segunda à sexta, das 08h às 20h.

Custo Zero Dollar

A habilitação do serviço Zero Dollar não possui nenhum custo adicional na Rede. Mas, a utilização das verificações Zero Dollar tem um custo para validação de cartões Mastercard e Visa. Para mais detalhes sobre a precificação, acesse [Tarifas de Bandeiras](#): Não uso de Zero Dollar e Uso de Zero Dollar.



Selecione o tipo "Zero Dollar" no combo box "Examples" da requisição.

POST: </v2/transactions>

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture		Booleano	Não	<p>Define se a transação terá captura automática ou posterior. O não envio desse campo será considerado a captura automática (true).</p> <p>Para transações de débito e Zero Dollar, em caso de envio, o valor do parâmetro deve ser definido como true, indicando captura automática.</p>
kind		credit / debit	Não	<p>Tipo de transação a ser realizada.</p> <ul style="list-style-type: none">Para transações de crédito, utilizar creditPara transações de débito, utilizar debit <p>O não envio desse campo será considerado crédito.</p>
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Para transação Zero Dollar enviar o valor 0.
cardHolderName	Até 30	Alfanumérico	Não	<p>Nome do portador do cartão.</p> <p>Não enviar caracteres especiais.</p>
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do cartão. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	<p>Ano de vencimento do cartão.</p> <p>Exemplo: 2028 ou 28.</p>
securityCode*	Até 4	Alfanumérico	Sim	Código de segurança do cartão geralmente localizado no verso do cartão. O envio desse parâmetro garante maior possibilidade de aprovação da transação.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.

Nome	Tamanho	Tipo	Descrição
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Numérico	Para transação Zero Dollar o retorno será 0
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Cancelamento

O cancelamento pode ser solicitado para todas as transações, conforme instruções abaixo:

- Autorização

A operação de cancelamento da autorização (sem captura automática) é permitida apenas para o cancelamento total da transação e deverá ser solicitada dentro do período estipulado para cada ramo após esse prazo, a autorização é cancelada automaticamente.

- Captura e autorização com captura automática

A operação de cancelamento da captura e da autorização com captura automática pode ser efetuada de forma parcial ou total, através dos canais disponíveis.

No cancelamento total, a transação terá o status “Canceled”, enquanto no cancelamento parcial, o status será mantido como “Approved”, até que a transação seja cancelada integralmente.

As solicitações de cancelamento podem ser realizadas em até 7 dias para transações de débito e para transações de crédito o padrão é de até 90 dias, mas pode variar conforme o ramo de atuação de cada estabelecimento.

Para cancelamentos solicitados no mesmo dia da transação de autorização ou autorização com captura automática, o processamento será realizado imediatamente, caso contrário, o processamento será realizado em D+1.

Cancelamento parcial disponível somente em D+1 e para transações com captura.

Uma requisição de solicitação de cancelamento D+1 que retornou o código 360, não indica que o cancelamento será efetivado com sucesso. O estabelecimento precisa consultar posteriormente para verificar se o cancelamento foi efetivado ou negado.

Caso um cancelamento parcial D+1 esteja no status "Processando", não deve ser enviado um outro pedido de cancelamento parcial, pois isso pode gerar dois cancelamentos distintos.

Observação: Todas as solicitações de cancelamento feitas após as 21h30 serão processadas no próximo dia.

Lembramos que para as transações Maestro (débito), é possível realizar **apenas um** cancelamento parcial. Trata-se de uma regra da bandeira Mastercard, que pode enviar a confirmação/ processamento deste cancelamento em até 5 dias úteis.

Para apoiar nossos clientes na melhor identificação de retornos de cancelamento negados por regras de bandeira, desde 29 de janeiro de 2023 é possível receber dois novos cenários de cancelamento através da API e.Red. Inicialmente, eles serão englobados em retornos já existentes (351 e 354) e você deverá se preparar para receber os retornos definitivos a partir de 01/05/2023.

Para a bandeira Mastercard, em que não é permitido realizar mais de um **cancelamento parcial no débito**, até o dia 01/05/2023 você receberá esse retorno através do código 355, já existente.

Para transações Mastercard débito em **disputa de chargeback**, você receberá o código 351 até 01/05, também já existente.

Após esse período, os novos retornos ficam conforme a tabela abaixo:

Até 01/05/23 Retornos que englobarão os novos cenários provisoriamente		A partir de 01/05/23 Retornos definitivos	
355	Transaction already canceled	373	No further Refund allowed
351	Forbidden	374	Refund not allowed. Chargeback requested

Confira mais detalhes em [Retornos de Cancelamento](#).

Para testar os cenários consulte Tutorial Sandbox > [Simular erros](#).

POST: [/v2/transactions/{tid}/refunds](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
amount	Até 10	Númerico	Sim	Valor do cancelamento sem separador de milhar e casa decimal. Exemplos: <ul style="list-style-type: none">• R\$ 10,00 = 1000• R\$ 0,50 = 50
referenceRefund	Até 50	Alfanumérico	Não	Código do cancelamento gerado pelo estabelecimento.

Nome	Tamanho	Tipo	Obrigatório	Descrição
urls		urls	Não	
Urls/kind		Alfanumérico	Não	Campo que identifica qual o tipo da url: callback.
urls/url	Até 500	Alfanumérico	Não	Url que receberá o callback com o status do cancelamento após processado pela Rede. Também é possível cadastrar as url no portal userede. Clique aqui para mais informações

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação (vide tabela retornos de cancelamento).
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação (vide tabela retornos de cancelamento).
refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede. Caso a transação seja cancelada por outro canal que não seja a API, este campo retornará vazio.
referenceRefund	Até 50	Alfanumérico	Código do cancelamento gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
refundDateTime		Datetime	Data do cancelamento no formato YYYY-MM-DDThh:mm:ss.STZD .
cancelId	Até 15	Alfanumérico	Código identificador da transação de solicitação cancelamento, retornado somente em solicitações D+1.

URL de notificações

A URL de notificações (callback) permite que os dados de uma transação sejam retornados via POST após o processamento dos cancelamentos realizados em D+1. A URL pode ser informada na própria API ou acessando o portal da Rede em menu para *vender > e-commerce > notificação automática*. Ressaltamos que caso a URL seja informada nos 2 canais, a prioridade do envio das notificações será sempre na que foi informada na API.

IMPORTANTE: Alinhado as práticas de mercado para garantir maior segurança, atualize seu certificado público compatível com TLS 1.2. A partir de **29 de junho de 2018**, as versões anteriores, como 1.1 e 1.0, deixarão de funcionar.

Após informar a URL que receberá a notificação, as informações serão retornadas no seguinte formato:

Nome	Tamanho	Tipo	Descrição
type		Alfanumérico	Tipo de evento utilizado para transação: refund .
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
date		Datetime	Data do cancelamento no formato YYYY-MM-DDThh:mm:ss.STZD .

Nome	Tamanho	Tipo	Descrição
amount	Até 10	Alfanumérico	Valor do cancelamento.
status	Até 10	Alfanumérico	<ul style="list-style-type: none">• Done (Cancelamento efetivado)• Denied (Cancelamento negado)• Processing (Cancelamento em processamento)
cancellationNotice	Até 15	Alfanumérico	Código identificador da transação de solicitação cancelamento (cancelld).
refundld	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede. Caso a transação seja cancelada por outro canal que não seja a API, este campo retornará vazio.

Consulta de transação

A consulta da transação pode ser realizada de duas maneiras. A primeira é informando o tid gerado na transação de autorização. Já a segunda, é informando o número do pedido criado pelo estabelecimento (reference).

Obs: O prazo para consulta de pré autorizações pendentes e transações de zero dollar é de 60 dias. Após esse prazo o status da consulta retornará como: not found.

Consulta por tid

GET: /v2/transactions/{tid}
--

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
tid	20	Alfanumérico	Sim	Número identificador único da transação.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
requestDateTime		Datetime	Data da requisição no formato YYYY-MM-DDThh:mm:ss.STZD .
authorization		authorization	
authorization/dateTime		Datetime	Data da transação de autorização no formato YYYY-MM-DDThh:mm:ss.STZD .
authorization/returnCode	Até 3	Alfanumérico	Código de retorno da transação.
authorization/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
authorization/affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV).

Nome	Tamanho	Tipo	Descrição
authorization/status		Alfanumérico	Status da transação: <ul style="list-style-type: none"> • Approved • Denied • Canceled • Pending
authorization/reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
authorization/orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
authorization/tid	20	Alfanumérico	Número identificador único da transação.
authorization/nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorization/authorizationCode	6	Alfanumérico	Número de Autorização da transação retornada pelo emissor do cartão.
authorization/kind	Até 10	Alfanumérico	Método de pagamento utilizado na transação original (Credit ou Debit).
authorization/amount	Até 10	Numérico	Valor total da compra sem separador de milhar. Exemplos: <ul style="list-style-type: none"> • 1000 = R\$10,00 • R\$ 0,50 = 50
authorization/installments	Até 2	Numérico	Número de parcelas.
authorization/cardHolderName	Até 30	Alfanumérico	Nome do portador impresso no cartão.
authorization/cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
authorization/last4	4	Alfanumérico	4 últimos dígitos do cartão.
authorization/softDescriptor	Até 18*	Alfanumérico	Mensagem que será exibida ao lado no nome do estabelecimento na fatura do portador.
authorization/origin	Até 2	Numérico	Identifica a origem da transação. <ul style="list-style-type: none"> • e.Redre - 1
authorization/subscription		Booleano	<p>Informa ao emissor se a transação é proveniente de uma recorrência. Se transação for uma recorrência, enviar true. Caso contrário, enviar false.</p> <p>O não envio desse campo será considerado o valor false.</p> <p>A Rede não gerencia os agendamentos de recorrência, apenas permite aos lojistas indicarem se a transação se originou de uma recorrência.</p>
authorization/distributorAffiliation	Até 9	Numérico	Número de filiação do distribuidor (PV).
capture		capture	

Nome	Tamanho	Tipo	Descrição
capture/dateTime		Datetime	Data da transação de captura no formato YYYY-MM-DDThh:mm:ss.sTZD .
capture/nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede na transação de captura.
capture/amount	Até 10	Numérico	Valor da captura.
threeDSecure		threeDSecure	
threeDSecure/embedded		Booleano	Informa se o serviço MPI utilizado será da Rede ou terceiro.
threeDSecure/ <u>eci</u>	2	Alfanumérico	Código retornado ao MPI pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor. Deve ser enviado apenas para a utilização do serviço de autenticação 3DS. Transações de débito devem ser obrigatoriamente autenticadas.
threeDSecure/cavv	Até 32	Alfanumérico	Código do criptograma utilizado na autenticação da transação e enviado pelo MPI do estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS.
threeDSecure/xid	28	Alfanumérico	ID da transação de autenticação enviado pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS. Campo utilizado somente para bandeira Visa.
threeDSecure/returnCode	3	Alfanumérico	Código de retorno da transação com 3ds.
threeDSecure/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação com 3ds.
refunds		refunds	
refunds/dateTime		Datetime	Data da transação de cancelamento no formato YYYY-MM-DDThh:mm:ss.sTZD .
refunds/refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede.
refunds/referenceRefund	Até 50	Alfanumérico	Código do cancelamento gerado pelo estabelecimento.
refunds/status	Até 10	Alfanumérico	Status da solicitação de cancelamento. <ul style="list-style-type: none"> • Done (Cancelamento efetivado) • Denied (Cancelamento negado) • Processing (Cancelamento em processamento)
refunds/amount	Até 10	Numérico	Valor do cancelamento.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

IMPORTANTE: As consultas transacionais realizadas utilizando o parâmetro *tid* possuem um prazo máximo de visualização dos dados de até **400 dias**. Após esse período, os dados não estarão mais acessíveis para consulta.

Consulta por código do pedido (reference)

GET: /v2/transactions?reference={codigo_reference}

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
requestDateTime		Datetime	Data da requisição no formato YYYY-MM-DDThh:mm:ss.sTZD .
authorization		authorization	
authorization/dateTime		Datetime	Data da transação de autorização no formato YYYY-MM-DDThh:mm:ss.sTZD .
authorization/returnCode	Até 3	Alfanumérico	Código de retorno da transação.
authorization/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
authorization/affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV).
authorization/status		Alfanumérico	Status da transação: <ul style="list-style-type: none">• Approved• Denied• Canceled• Pending
authorization/reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
authorization/orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
authorization/tid	20	Alfanumérico	Número identificador único da transação.
authorization/nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorization/authorizationCode	6	Alfanumérico	Número de Autorização da transação retornada pelo emissor do cartão.
authorization/kind	Até 10	Alfanumérico	Método de pagamento utilizado na transação original (Credit ou Debit).

Nome	Tamanho	Tipo	Descrição
authorization/amount	Até 10	Numérico	<p>Valor total da compra sem separador de milhar.</p> <p>Exemplos:</p> <ul style="list-style-type: none"> 1000 = R\$10,00 R\$ 0,50 = 50
authorization/installments	Até 2	Numérico	Número de parcelas.
authorization/cardHolderName	Até 30	Alfanumérico	Nome do portador impresso no cartão.
authorization/cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
authorization/last4	4	Alfanumérico	4 últimos dígitos do cartão.
authorization/softDescriptor	Até 18*	Alfanumérico	Mensagem que será exibida ao lado no nome do estabelecimento na fatura do portador.
authorization/origin	Até 2	Numérico	<p>Identifica a origem da transação.</p> <ul style="list-style-type: none"> e.Redre - 1
authorization/subscription		Booleano	<p>Informa ao emissor se a transação é proveniente de uma recorrência. Se transação for uma recorrência, enviar true. Caso contrário, enviar false.</p> <p>O não envio desse campo será considerado o valor false.</p> <p>A Rede não gerencia os agendamentos de recorrência, apenas permite aos lojistas indicarem se a transação se originou de uma recorrência.</p>
authorization/distributorAffiliation	Até 9	Numérico	Número de filiação do distribuidor (PV).
capture		capture	
capture/dateTime		Datetime	Data da transação de captura no formato YYYY-MM-DDThh:mm:ss.sTZD .
capture/nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede na transação de captura.
capture/amount	Até 10	Numérico	Valor da captura.
threeDSecure		threeDSecure	
threeDSecure/embedded		Booleano	Informa se o serviço MPI utilizado será da Rede ou terceiro.
threeDSecure/eci	2	Alfanumérico	Código retornado ao MPI pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor. Deve ser enviado apenas para a utilização do serviço de autenticação 3DS.Transações de débito devem ser obrigatoriamente autenticadas.
threeDSecure/cavv	Até 32	Alfanumérico	Código do criptograma utilizado na autenticação da transação e enviado pelo MPI do estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS.

Nome	Tamanho	Tipo	Descrição
threeDSecure/xid	28	Alfanumérico	ID da transação de autenticação enviado pelo MPI ao estabelecimento (pode conter caracteres especiais). Deve ser enviado apenas para a utilização do serviço de autenticação 3DS. Campo utilizado somente para bandeira Visa.
threeDSecure/returnCode	3	Alfanumérico	Código de retorno da transação com 3ds.
threeDSecure/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação com 3ds.
refunds		refunds	
refunds/dateTime		Datetime	Data da transação de cancelamento no formato YYYY-MM-DDThh:mm:ss.TZD .
refunds/refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede.
refunds/referenceRefund	Até 50	Alfanumérico	Código do cancelamento gerado pelo estabelecimento.
refunds/status	Até 10	Alfanumérico	Status da solicitação de cancelamento. <ul style="list-style-type: none">• Done (Cancelamento efetivado)• Denied (Cancelamento negado)• Processing (Cancelamento em processamento)
refunds/amount	Até 10	Numérico	Valor do cancelamento.

IMPORTANTE: As consultas realizadas através do parâmetro *reference* possuem um prazo máximo de visualização de até **60 dias** para transações quatro partes (Débito e crédito) e de até **90 dias** para transações Pix.

OBS: Caso você realize uma consulta fora dos prazos informados, tanto para o *tid* quanto para a *reference*, nossa API retornará o código de erro **78 (Transaction does not exist)**.

Consulta de cancelamento

É utilizada para consultar informações de cancelamento a partir de uma solicitação enviada, sendo possível consultar informando o TID, para uma consulta mais detalhada e o refundId para uma consulta de um cancelamento específico.

A consulta do status final do cancelamento poderá ser realizada através da API de consulta de transação, do portal da Rede ou do extrato eletrônico um dia após a requisição de cancelamento ter sido realizada.

Consulta de cancelamento por tid

GET: /v2/transactions/{tid}/refunds

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
tid	20	Alfanumérico	Sim	Número identificador único da transação.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
refundId	36	Alfanumérico	Código de retorno do cancelamento gerado pela Rede. Caso a transação seja cancelada por outro canal que não seja a API, este campo retornará vazio.
refundDateTime		Datetime	Data do cancelamento no formato YYYY-MM-DDThh:mm:ss.STZD .
cancelId	Até 15	Alfanumérico	Código identificador da transação de solicitação cancelamento, retornado somente em solicitações D+1.
status	Até 10	Alfanumérico	Status das solicitações de cancelamentos <ul style="list-style-type: none">• Done (Cancelamento efetivado)• Denied (Cancelamento negado)• Processing (Cancelamento em processamento)
amount	Até 10	Numérico	Valor do cancelamento sem separador de milhar e casa decimal.

Consulta de cancelamento por refundId A consulta de cancelamento por refundId lista uma solicitação de cancelamento específica.

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
refundId	36	Alfanumérico	Sim	Código de retorno do cancelamento gerado pela Rede. Caso a transação seja cancelada por outro canal que não seja a API, este campo retornará vazio, não sendo possível consultar por refundId.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
refundId	36	Alfanumérico	Código de retorno do cancelamento gerado pela Rede. Caso a transação seja cancelada por outro canal que não seja a API, este campo retornará vazio, não sendo possível consultar por refundId.
tid	20	Alfanumérico	Número identificador único da transação
refundDateTime		Datetime	Data do cancelamento no formato YYYY-MM-DDThh:mm:ss.STZD
cancelId	Até 15	Alfanumérico	Código identificador da transação de solicitação cancelamento, retornado somente em solicitações D+1.
amount	Até 10	Numérico	Valor do cancelamento sem separador de milhar e casa decimal.
statusHistory		statusHistory	

Nome	Tamanho	Tipo	Descrição
statusHistory/status	Até 10	Alfanumérico	Histórico do status das solicitações de cancelamentos <ul style="list-style-type: none"> • Done (Cancelamento efetivado) • Denied (Cancelamento negado) • Processing (Cancelamento em processamento)
statusHistory/dateTime		Datetime	Data da solicitação do cancelamento no formato YYYY-MM-DDThh:mm:ss.sTZD
returnCode	Até 3	Alfanumérico	Código de retorno da transação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação

SoftDescriptor

A identificação na fatura (SoftDescriptor ou DBA) é um parâmetro que auxilia o portador a identificar a transação gerada na fatura do cartão.

O parâmetro é composto por 22 caracteres. O SoftDescriptor é dividido em duas partes, no qual a primeira parte é cadastrada no portal da Rede e chamamos de hard descriptor, por ser único por transação daquele PV. A segunda parte é dinâmica, e é enviada a cada requisição de transação via API, essa parte é a que chamamos de SoftDescriptor.

Esses valores são imputados na mensageria de captura para a bandeira, e separados com um * (asterisco).

O hard descriptor pode ter no máximo 12 caracteres e ele será variável dependendo da quantidade de caracteres de SoftDescriptor que vier na requisição. Ou seja, o **cadastro do hard descriptor** é feito uma **única vez**, e a forma como aparece na fatura **varia de acordo com o tamanho do SoftDescriptor**, abaixo exemplificamos as **regras de API** e Rede para combinação de ambos os campos:

- Caso seja enviado na requisição entre 1 e 9 posições no SoftDescriptor, a composição na fatura será 12 caracteres do hard + 1 a 9 caracteres do Soft, com o asterisco, totaliza os 22 caracteres abertos para essa informação.

Exemplo: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODUTO01", na fatura do cliente final aparecerá **REDECOMMERCE*PRODUTO01**

Exemplo com espaços no SoftDescriptor: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODU", na fatura do cliente final aparecerá **REDECOMMERCE*PRODU**

- Caso seja enviado na requisição entre 10 e 14 posições no SoftDescriptor, a composição na fatura será 7 caracteres do hard + 10 a 14 caracteres do Soft, com o asterisco, totaliza os 22 caracteres abertos para essa informação.

Exemplo: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODUTODIGIT01", na fatura do cliente final aparecerá **REDECOM*PRODUTODIGIT01**

Exemplo com espaços no SoftDescriptor: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODU", na fatura do cliente final aparecerá **REDECOM*PRODU**

- Caso seja enviado na requisição entre 15 e 18 posições no SoftDescriptor, a composição na fatura será 3 caracteres do hard + 15 a 18 do Soft, com o asterisco, totaliza os 22 caracteres abertos para essa informação.

Exemplo: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODUTODIGITAL0001", na fatura do cliente final aparecerá **RED*PRODUTODIGITAL0001**

Exemplo com espaços no SoftDescriptor: Supondo que seja cadastrado no portal como hard descriptor "REDECOMMERCE" e SoftDescriptor "PRODU", na fatura do cliente final aparecerá **RED*PRODU**

Importante: Caso utilize a MPI Rede, não utilize espaço ou caracteres especiais no SoftDescriptor, pois isso resultará em erros na autenticação da transação.

Para utilizar essa funcionalidade, acesse o portal da Rede no menu *para vender > e-commerce > Identificação na fatura* ou entre em contato com a Central de atendimento da Rede. Caso o nome não seja cadastrado, o serviço não será habilitado.

Após a habilitação do serviço via portal, a funcionalidade será disponibilizada dentro de um prazo de até 24 horas.


O parâmetro deve ser enviado juntamente à requisição de transações de crédito (autorização ou autorização com captura automática) ou débito.

MCC dinâmico

O código da categoria do estabelecimento, conhecido como MCC, enviado pelo marketplace ou facilitador, pode ser dinâmico conforme as informações do estabelecimento que esteja efetuando a transação.

Para esse cenário, é obrigatório enviar o softdescriptor. [Clique aqui](#) para obter mais informações.

Para informação referente ao MCC dinâmico, o nome cadastrado no portal, menu *para vender > e-commerce > Identificação na fatura*, equivale ao nome do facilitador (subcredenciador).



Selecione o tipo "MCC dinâmico" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
softDescriptor	Até 18*	Alfanumérico	Sim*	Frase personalizada que será impressa na fatura do portador.
paymentFacilitatorID	Até 11	Numérico	Sim*	Código do facilitador de pagamento na respectiva bandeira.
independentSalesOrganizationID	Até 11	Numérico	Não	Código da organização de vendas independente.
subMerchant		SubMerchant		
subMerchant / mcc*	4	Numérico	Sim*	MCC do subestabelecimento comercial.
subMerchant / subMerchantID	Até 15	Alfanumérico*	Sim*	Código do subestabelecimento comercial.
subMerchant / address	Até 48	Alfanumérico ¹	Não*	Endereço do subestabelecimento comercial.
subMerchant / city	Até 13	Alfanumérico ¹	Não*	Cidade do subestabelecimento comercial.
subMerchant / state	2	Alfabético	Sim*	Estado do subestabelecimento comercial.
subMerchant / country	Até 3	Alfanumérico	Sim*	País do subestabelecimento comercial.
subMerchant / cep	Até 9	Alfanumérico	Sim*	Código postal do subestabelecimento comercial.
subMerchant / cnpj	Até 18	Numérico	Não*	CNPJ do subestabelecimento comercial.
subMerchant / taxIdNumber	Até 14	Alfanumérico	Sim*	CPF ou CNPJ do subestabelecimento comercial.
subMerchant / merchantTaxIdName	Até 27	Alfanumérico	Sim	Razão social do subestabelecimento comercial.

Nome	Tamanho	Tipo	Obrigatório	Descrição
subMerchant / patEnabled	•	Booleano	Sim, para transações VOUCHER	True ou False. Indica a adesão das regras PAT por parte do Subseller
subMerchant / internationalSellerIndicator	•	Booleano	Não*	True ou False. Indica se a transação é enviada por um estabelecimento/marketplace internacional.

Importante: o não envio do parâmetro internationalSellerIndicator quando a transação for de um marketplace internacional pode resultar em custos adicionais.

Os campos de cidade, estado e razão devem ser enviados sem caracteres especiais ou acentos.

- Para a bandeira ELO, o campo subMerchantID deve ser enviado como numérico. Caso seja enviado como alfanumérico a transação será negada.
- Devido à LGPD (Lei Geral de proteção de dados), os seguintes campos da chave “subMerchant”: subMerchantID, address, city, state, country, cep e cnpj, mesmo quando enviados na requisição, não são devolvidos nas consultas de transações.
- Este campo (subMerchant/patEnabled) será utilizado para certificar que o estabelecimento está em conformidade com as regras de arranjo do PAT
- **Para garantir o devido processamento da transação, não se deve incluir caracteres especiais.**

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.

Nome	Tamanho	Tipo	Descrição
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Subadquirentes e Marketplaces

Público

Subadquirentes: empresa integrada a um adquirente que habilita outras empresas ou pessoas físicas para a aceitação de pagamentos com cartões mediante intermediação do fluxo financeiro das transações;

Marketplace: e-commerce que vende produtos terceiros, operando como um shopping center virtual. Está sob as mesmas regras de um Subadquirente por fazer intermediação do fluxo financeiro para o Seller;

Mensageria do transacional

A Circular 3978 determina que os Subadquirentes e Marketplace identifique os beneficiários finais no momento da transação. Para cumprimento desta norma, é obrigatório o envio dos campos identificadores na mensageria da transação, conforme orientações abaixo:

- **Softdescriptor:** É um parâmetro que auxilia o portador a identificar a transação gerada na fatura do cartão.

Esse parâmetro é composto por duas partes, a primeira é o **Hard Descriptor**, que é **único do subadquirente**, e a segunda é dinâmica, a que chamamos de **Softdescriptor**, ela identifica o subestabelecimento da transação.

Este campo é obrigatório e deve ter um tamanho de até **22 caracteres**. O *Hard Descriptor* pode ter no máximo 12 caracteres e ele será variável dependendo da quantidade de caracteres de *SoftDescriptor* que vier na requisição.

*O hard descriptor pode ter no máximo 12 caracteres e ele será variável dependendo da quantidade de caracteres de SoftDescriptor que vier na requisição. Ou seja, **o cadastro do hard descriptor** é feito **uma única vez**, e a forma como aparece na fatura **varia de acordo com o tamanho do SoftDescriptor**. Poderá ser enviado na requisição até 18 posições no SoftDescriptor e neste caso, a composição na fatura será 3 caracteres do hard + 18 do Soft, com o asterisco, totaliza os 22 caracteres abertos para essa informação.

Para maiores detalhes sobre o envio deste campo, clique aqui ou acesse a sessão [Softdescriptor](#):

- **PFID (paymentFacilitatorID):** Código do Facilitador de Pagamento em cada bandeira
- **SubmerchantID:** Código do Subestabelecimento (Seller). Este código é gerado pelo facilitador de Pagamento
- **subMerchant / address:** Endereço do Subestabelecimento (Seller)
- **subMerchant / city:** Cidade do Subestabelecimento (Seller)
- **subMerchant / state:** Estado do Subestabelecimento (Seller)
- **subMerchant / country:** País do Subestabelecimento (Seller)
- **subMerchant / cep:** Cep do Subestabelecimento (Seller)
- **subMerchant / mcc:** Código do ramo/MCC do subestabelecimento (Seller) = MCC Dinâmico

Para classificação correta do MCC do Seller, deve-se seguir a regra determinada pela ABECs descrita abaixo:

Regra de definição de MCC

1. CNAE (Código Nacional de Atividade Econômica) primário, atribuído pela Receita Federal para classificar a área de atuação do estabelecimento. A ABECS utiliza uma base de CNPJs enviada pela Serasa, com as informações de DE-PARA de CNAE para CNPJ. Para classificar o cliente em qualquer outro CNAE, ainda que seja o CNAE secundário, é necessário antes demonstrar para as bandeiras a atividade exercida pelo cliente.
2. Avaliação no comitê de BANDEIRAS que sobrepõe a regra 1. É feito a aprovação dos casos de exceção, onde a regra do CNAE/MCC não reflete a atividade do cliente. A avaliação é feita por CNPJ e aplicada após uma defesa à ABECS.

Nota: Para maiores detalhes e acesso a base, consulte o site oficial da ABECS: <https://www.abecs.org.br/consulta-mcc-individual>

- **subMerchant / CPF_cnpj:** CNPJ/CPF do Subestabelecimento (Seller)

Parâmetros de requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
softDescriptor	Até 18	Alfanumérico	Sim	Frase personalizada que será impressa na fatura do portador.
paymentFacilitatorID	Até 11	Numérico	Sim	Código do facilitador de pagamento na respectiva bandeira.
subMerchant		SubMerchant	Sim	
subMerchant / mcc	4	Numérico	Sim	MCC do subestabelecimento comercial.
subMerchant / subMerchantID	Até 15	Alfanumérico	Sim	Código do subestabelecimento comercial.
subMerchant / address	Até 48	Alfanumérico	Sim	Endereço do subestabelecimento comercial.
subMerchant / city	Até 13	Alfanumérico	Sim	Cidade do subestabelecimento comercial.
subMerchant / state	2	Alfabético	Sim	Estado do subestabelecimento comercial.
subMerchant / country	Até 3	Alfanumérico	Sim	País do subestabelecimento comercial.
subMerchant / cep	Até 9	Alfanumérico	Sim	Código postal do subestabelecimento comercial.
subMerchant / cnpj	Até 18	Numérico	Sim	CNPJ do subestabelecimento comercial.
subMerchant / taxIdNumber	Até 14	Alfanumérico	Sim	CPF ou CNPJ do subestabelecimento comercial.
subMerchant / merchantTaxIdName	Até 27	Alfanumérico	Sim	Razão social do subestabelecimento comercial.
subMerchant / patEnabled	•	Booleano	Sim, para transações VOUCHER	True ou False. Indica a adesão das regras PAT por parte do Subseller.
subMerchant / internationalSellerIndicator		Booleano	Não	True ou False. Indica se a transação é enviada por um estabelecimento/marketplace internacional.

Importante: o não envio do parâmetro *internationalSellerIndicator* quando a transação for de um marketplace internacional pode resultar em custos adicionais.

Os campos de cidade, estado e razão social devem ser enviados sem caracteres especiais ou acentos..

Selecione o tipo "MCC dinâmico" no combo box "Examples" da requisição.

POST:
[/v2/transactions](#)

Note que os parâmetros de requisição dentro do grupo “submerchant” devem sempre começar em letra minúscula.

OBS: Devido à LGPD (Lei Geral de proteção de dados), os seguintes campos da chave “subMerchant”: subMerchantID, address, city, state, country, cep e cnpj, mesmo quando enviados na requisição, não são devolvidos nas consultas de transações.

Atenção: Para garantir o devido processamento da transação, não se deve incluir caracteres especiais.

Parâmetros de resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime		Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.

Nome	Tamanho	Tipo	Descrição
brandTid	Até 21	Alfanumérico	Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file

Recorrência e Card-on-File

O que é Recorrência? A recorrência é uma opção de pagamentos que funciona como uma cobrança periódica, o pagamento é feito por prazo e frequência pré-determinados pelo lojista e acordados com o pagador. A principal vantagem é o não comprometimento do limite do cartão do cliente, efetuando cobranças automaticamente. É uma opção que apoia o lojista a não se preocupar em cobrar os clientes frequentemente, uma vez que esse ajuste já foi feito no momento da compra.

Lembramos que o e.Red e não possui um motor de recorrência ou gerencia agendamentos recorrentes, caso seu e-commerce possua esse motor, deve enviar as transações recorrentes para a Rede usando os campos corretamente.

O que é card-on-file? Também conhecido como credential-on-file ou credencial armazenada. As transações com cartão armazenado são aquelas em que o portador autorizou o armazenamento dos dados do seu cartão para iniciar compras futuras ou que possam ser utilizadas pelo lojista para recorrências ou cobranças futuras.

Quando temos um cartão armazenado, não é necessário enviar o securityCode nas transações.

Confira abaixo quais campos usar em cada operação:

Recorrentes	Card-on-file
<ul style="list-style-type: none"> storageCard 	<ul style="list-style-type: none"> storageCard
<ul style="list-style-type: none"> credentialId (para Mastercard) 	<ul style="list-style-type: none"> credentialId (para Mastercard)
<ul style="list-style-type: none"> subscription 	
<ul style="list-style-type: none"> brandTid 	
<ul style="list-style-type: none"> transacionLinkId 	

O que cada um deles significa?

- storageCard: Indica operações que possam ou não estar utilizando COF (Card On File – credencial armazenada)

0 - Utilizado para cartão não armazenado (deve ser acompanhado do securityCode)

1 - Utilizado para cartão que está sendo armazenado pela primeira vez (deve ser acompanhado do securityCode, caso esta seja a primeira transação em que se pretende armazenar o cartão. Esse passo pode ser substituído por uma transação de Zero Dollar, que também deve ser acompanhado do código de segurança)

2 - Utilizado para indicar cartão já armazenado (securityCode não deve ser enviado)

Para a bandeira Elo é obrigatório que antes de indicar cartão armazenado (storageCard=2) tenha sido feito um Zero Dollar ou transação com storageCard = 1.

***Importante:** A Rede só irá sinalizar uma transação com credencial armazenada quando o storageCard for igual a “2”, transações sinalizadas como 1, indicam que o estabelecimento está executando uma transação que irá iniciar o armazenamento da credencial, exigindo então validações de transações comuns. EX: uso de código de segurança do cartão (securityCode).*

- **credentialId:** Campo utilizado atualmente somente pela bandeira Mastercard, para indicar o motivo de armazenamento do cartão e facilitar a análise para aprovação. Para mais detalhes consulte a seção a seguir [Categorização de transações card-on-file](#).
- **subscription:** Parâmetro utilizado para a sinalização de transações recorrentes. Deve ser enviado como true caso a transação seja recorrente, false para transações comuns;
- **brandTid:** Este é um campo único e dinâmico, recebido a cada resposta de transação, e é utilizado para correlacionar planos de recorrência (nos casos das bandeiras Visa e Mastercard) e correlacionar transações iniciadas pelo estabelecimento como incrementais, recorrentes e com cartão armazenado (no caso da bandeira Elo).
- **transactionLinkId:** Este campo é único e dinâmico, recebido a cada resposta de transação, e é utilizado para correlacionar transações iniciadas pelo estabelecimento como incrementais, recorrentes e com cartão armazenado na bandeira Mastercard. Deve ser enviado para a bandeira a partir da segunda transação, e faz uma correlação das transações subsequentes com a primeira. **Este campo passará a ser retornado em outubro de 2025 e deverá ser armazenado pelos estabelecimentos. Em 2026 esse campo substituirá o brandTid em transações recorrentes ou de card-on-file da bandeira Mastercard, a data será divulgada futuramente.**

Deve ser enviado para a bandeira a partir da segunda transação, e faz uma correlação das transações subsequentes com a primeira.

O estabelecimento é responsável por armazenar o brandTid e o transactionLinkId retornado e enviá-lo em todas as transações subsequentes.

Para a bandeira Visa: Quando a transação é identificada como recorrente (subscription=true), a cada transação seguinte que o estabelecimento enviar para aquele plano de recorrência deve enviar também o brandTid fornecido pela bandeira da transação **original**.

Por exemplo: Em um plano recorrente mensal, na terceira transação o estabelecimento deve encaminhar o brandTid recebido na transação que deu início ao plano de recorrência.

No caso de transações **tokenizadas Visa**, o envio desse parâmetro é obrigatório. Nos demais tipos de transação, caso seja feito, deve-se garantir o envio do valor correto para evitar negativas por parte da bandeira.

Para a bandeira Mastercard: Quando a transação é identificada como recorrente (subscription=true), a cada transação seguinte que o estabelecimento enviar para aquele plano de recorrência deve enviar também o brandTid e o transactionLinkId fornecido pela bandeira da transação **original ou anterior**.

Para a bandeira Elo: Sempre que o estabelecimento iniciar uma transação, seja por recorrência, cartão armazenado ou quaisquer outros tipos de transações incrementais, deverá enviar o brandTid fornecido pela bandeira na **transação original**.

Para a Elo, caso tenha sido feita uma validação Zero Dollar antes de utilizar o cartão, deve-se enviar o brandTid recebido no Zero Dollar nas transações financeiras subsequentes.

Lembre-se: O estabelecimento continuará recebendo um brandTid diferente da bandeira em cada nova transação, mas na solicitação de autorização de uma transação recorrente ou iniciada pelo estabelecimento, deverá seguir as regras descritas acima. Fique atento aos formatos e garanta sempre o envio correto do parâmetro para evitar negativas por parte do emissor/bandeira.

Caso não possua o valor correspondente, orientamos que seja iniciado um novo processo de armazenamento do cartão (card-on-file) junto ao portador para obter o parâmetro a ser enviado nas transações subsequentes.

Atente-se aos pontos abaixo de ambas as operações:

- O não envio do campo storageCard será considerado 0 (credencial não armazenada).
- Caso o cliente queira trocar o cartão, será necessário reiniciar o processo desde o envio da primeira transação, ou seja, storageCard=1 para o novo cartão, então nas demais poderá ser enviado o brandTid e storageCard=2, além da indicação de recorrência (subscription=true).
- Ressaltamos que transações recorrentes **não podem ser processadas como pré-autorização**, para isso o campo **capture** deve ser igual a “true”, indicando uma captura automática. **Caso sejam enviadas como capture “false”, a marcação de recorrência não será considerada.**
- Além disso, qualquer alteração na recorrência (Ex: mudança no valor cobrado mensalmente), será considerada uma nova transação e a antiga deverá ser desconsiderada.

- Ao realizar transações por meio de credencial armazenada (card-on-file), se o estabelecimento já desejar iniciar as cobranças ou apenas salvar o cartão para cobranças futuras, as bandeiras **exigem** que antes seja feito uma validação Zero Dólar.
- A validação **Zero Dollar** pode ser utilizada por estabelecimentos para verificar os dados do cartão para checar se a credencial é válida e pode ser armazenada, além possibilitar as cobranças futuras sem o envio do securityCode em cobranças de recorrentes com credencial armazenada ou apenas de credencial armazenada, além de aumentar a possibilidade de conversão.
- **Uso do “sai” em transações card-on-file (credencial armazenada):** O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e Cloud Token Visa), **quando autenticado como 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso.**
- Ao fazer o envio do grupo threeDSecure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.

Categorização de transações card-on-file

Desde outubro de 2022, devido a mudanças regulatórias de bandeiras, as transações card-on-file da bandeira Mastercard passarão a ser categorizadas em 12 tipos de categorias **CIT (Iniciadas pelo portador do cartão – Card Holder)** e **MIT (Iniciadas pelo estabelecimento – Merchant)**. Desde 1 de junho de 2023, a bandeira passou a monitorar o envio do campo, fique atento pois podem ocorrer ações de compliance.

O crescimento contínuo do comércio eletrônico, juntamente com o aumento dos tipos de transação, exige a necessidade de entender a intenção do consumidor. A introdução do indicador CIT ou MIT fornece transparência permitindo o uso para:

- Lógica de autorização do emissor
- Detecção de fraude
- Gestão de disputas

Por isso, é necessário realizar ajustes em sua integração com o e.Red para envio do campo chamado "credentialId", que fará parte do grupo "transactionCredentials". Desse modo, quando storageCard for igual a 1 ou 2, indicando que o cartão está sendo ou já foi armazenado, será **obrigatório** indicar em qual categoria a transação card-on-file (credencial armazenada) está enquadrada.

O envio também deve ser feito em transações Zero Dollar que pretendem armazenar o cartão, ou em transações tokenizadas.

O envio deste campo passou a ser **obrigatório** para a operação Mastercard **desde 01 de junho de 2023**, e a partir de 01 de junho de 2024, a bandeira Mastercard poderá aplicar penalidades em caso de não conformidade dos estabelecimentos, referente ao período fora da norma. Entre os benefícios do envio do campo, está a capacidade de apoiar a bandeira e o emissor na análise de suas transações, o que pode ajudar na conversão. Os outros campos já utilizados atualmente para finalidades semelhantes como storageCard, subscription e installments, precisam continuar a ser populados.

A seguir, a tabela de categorias a ser considerada:

Categorias principais	Indicador a ser enviado (credentialId)	Sub-Categoria correspondente	Definição	Exemplo
1. Iniciada pelo Portador (CIT) Qualquer transação em que o titular do cartão esteja participando ativamente da transação. As transações podem ser realizadas com base nas credenciais fornecidas pelo titular do cartão na hora da transação ou uma credencial armazenada em arquivo de uma interação anterior. As transações podem ocorrer como uma transação de PDV na loja, uma transação de comércio eletrônico, uma transação por correspondência/pedido por telefone ou em um caixa eletrônico.	01	Card on File (Credencial armazenada)	O consumidor concorda que seu cartão seja armazenado com o comerciante para futuras transações que possam ocorrer de tempos em tempos.	Transações de aplicativos de carro.
	02	Ordem Permanente	O consumidor concorda que seu cartão seja armazenado com o comerciante e inicia uma primeira transação em uma série destinada a um valor variável e uma frequência fixa.	Pagamento mensal de serviços.
	03	Assinatura	O consumidor concorda que seu cartão seja armazenado e inicia uma primeira transação em uma série destinada a um valor fixo e uma frequência fixa.	Assinatura mensal de jornal.
	04	Parcelado	O consumidor concorda que seu cartão seja armazenado para estabelecer um plano de parcelamento e inicia uma primeira transação em uma série.	A transações parceladas.

Categorias principais	Indicador a ser enviado (credentialId)	Sub-Categoria correspondente	Definição	Exemplo
2. Iniciadas pelo estabelecimento (MIT), pagamentos recorrentes ou parcelamentos Uma operação decorrente de um acordo entre o titular do em que o titular do cartão concorda que o comerciante armazene os dados do titular do cartão credencial e usar essa credencial armazenada em arquivo para uma aquisição posterior de bens ou serviços.	05	Card on File (Credencial armazenada) – não programada	Transações realizadas por um acordo entre um titular de cartão e um comerciante, pelo qual o consumidor autoriza o comerciante a armazenar e usar os dados da conta do titular do cartão para iniciar uma ou mais transações futuras.	Pedágio Auto recarga
	06	Ordem Permanente	Usar os dados da conta do titular do cartão para uma transação que deve ocorrer em intervalos regulares por um valor variável.	Pagamentos mensais de serviços
	07	Assinatura	Usar os dados da conta do titular do cartão para uma transação que deve ocorrer em intervalos regulares por um valor fixo.	Assinatura mensal ou pagamento de serviço mensal fixo.
	08	Parcelado	Armazenar os dados da conta do titular do cartão para uso do comerciante para iniciar uma ou mais transações futuras por um valor conhecido com uma determinada duração com base em uma única compra.	Comprar uma TV por R\$ 1.000, pagando em quatro parcelas iguais de R\$ 250 (a primeira transação é CIT, as três transações restantes são MIT).

Categorias principais	Indicador a ser enviado (credentialId)	Sub-Categoria correspondente	Definição	Exemplo
3. Iniciadas pelo estabelecimento (MIT) práticas da indústria. Uma transação iniciada pelo comerciante para cumprir uma prática comercial que ocorre com mais frequência após uma interação inicial com o titular do cartão. As transações de prática do setor podem ser realizadas com credenciais armazenadas em arquivo ou credenciais que não são armazenadas em arquivo, mas são temporariamente retidas pelo comerciante conforme acordado pelo consumidor.	09	Remessa Parcial	Ocorre quando uma quantidade acordada de mercadorias encomendadas por e-commerce não está disponível para envio no momento da compra. Cada remessa é uma transação separada.	O consumidor encomendou mercadorias que são enviadas em horários diferentes.
	10	Cobrança atrasada	Uma cobrança adicional da conta após a prestação dos serviços iniciais e o processamento do pagamento.	Cobrança do frigobar do hotel após o titular do cartão fazer check out do hotel.
	11	No show (Multa)	Uma multa cobrada de acordo com a política de cancelamento do comerciante.	O cancelamento de uma reserva pelo titular do cartão sem aviso prévio adequado ao comerciante.
	12	Reenvio	A tentativa de obter autorização para uma transação que foi recusada, mas a resposta do emissor não proíbe que o comerciante tente mais tarde.	Fundos insuficientes/ resposta acima do limite de crédito/ retentativa de transações de trânsito.

Carteiras Digitais

As Carteiras digitais ou Wallets funcionam como dispositivos que armazenam cartões e dados de pagamento para compradores do e-commerce. Permitem que o consumidor cadastre suas credenciais de pagamento e seja capaz de realizar pagamentos de forma rápida e prática pelo celular ou outros dispositivos conectados, por exemplo.

As Wallets que o e.Redde pode receber transações são:

- [Apple Pay](#).
- [Google Pay](#).
- [Samsung Pay](#).

Clicando em cada um dos links acima, é possível acessar o site oficial de cada uma das Wallets com informações para integração do check-out e do fluxo transacional.

Neste momento o e.Redde realiza apenas o processamento dessas transações, isto é, o estabelecimento precisa ser ou possuir um intermediário (como por exemplo, um gateway) que seja PSP (Payment Service Provider). Os PSPs possuem a integração com as Wallets para decifrar os dados das transações e encaminhar ao adquirente (Rede) para processar.

Em breve, a Plataforma de Pagamentos Rede oferecerá também a solução de PSP visando facilitar a integração dos nossos clientes.

Neste momento, a Plataforma de pagamentos Rede processa transações provenientes de Wallets (Apple pay, Google Pay, Samsung Pay) nas bandeiras **Visa, Mastercard e Elo.**

Além dessas opções, as bandeiras Mastercard, Visa, Elo e Amex possuem um programa de Operadoras de carteiras Digitais Escalonadas (SDWO), consulte aqui [Carteiras digitais escalonada \(SDWO\)](#)

Parâmetros da requisição para Apple, Google e Samsung Pay:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	-	Booleano	Não	Define se uma transação terá captura automática ou posterior. O não envio desse campo será considerado uma captura automática (true).
kind	-	Alfanumérico	Não	Tipo de transação a ser realizada. <ul style="list-style-type: none">• Para transações de crédito, utilizar credit• Para transações de débito, utilizar debit O não envio desse campo será considerado crédito.
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Valor total da transação sem separador de milhar e casa decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
installments	Até 2	Numérico	Não	Número de parcelas em que uma transação será autorizada. De 2 a 12 O não envio desse campo será considerado à vista.
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão. Não enviar caracteres especiais.
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do cartão. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	Ano de vencimento do cartão. Exemplo: 2028 ou 28

Nome	Tamanho	Tipo	Obrigatório	Descrição
origin	Até 2	Númerico	Não	<p>Identifica a origem da transação.</p> <ul style="list-style-type: none"> e.Redde: 1 <p>O não envio desse campo será considerado uma transação e.Redde (1).</p>
securityCode	Até 4	Alfanumérico	Não	<p>Código de segurança do cartão geralmente localizado no verso do cartão.</p> <p>O envio desse parâmetro garante maior possibilidade de aprovação da transação.</p>
tokenCryptogram	-	Alfanumérico	Obrigatório (Consulte mais detalhes ao final da tabela)	Token informado pela Bandeira. Identificar transações tokenizadas.
storageCard	Até 1	Alfanumérico	Não	<p>Indica operações que possam ou não estar utilizando COF (Card on File):</p> <p>0 - Transação com credencial não armazenada.</p> <p>1 - Transação com credencial armazenada pela primeira vez.</p> <p>2 - Transação com credencial já armazenada.</p> <p>Atenção: O não envio desse campo será considerado 0 (credencial não armazenada).</p>
wallet*	-	-	-	Grupo wallet para os parâmetros walletId e walletCode
wallet/processingType*	2	Alfanumérico	Sim	<p>Identificação de tipo de operação para Apple, Google e SamsungPay:</p> <ul style="list-style-type: none"> 03 para bandeira ELO 04 para Bandeiras Visa e Mastercard <p>Para checar as informações de SDWO consulte a seção Operadoras de carteira digital escalonada</p>
wallet/walletId	Até 11	Númerico	Obrigatório caso processingType=03 (Elo)	<p>Identifica a Wallet originária da transação, são Ids fixos e obrigatórios para uso Elo:</p> <p>52810030273 – Apple Pay</p> <p>52894351835 – Google Pay</p> <p>52815860843 – Samsung Pay</p>

Nome	Tamanho	Tipo	Obrigatório	Descrição
wallet/walletCode	Até 03	Alfanumérico	Sim	Identifica a Wallet, uso exclusivo para processingType=03 ou 04 AEP = Apple Pay GEP = Google Pay SGP = Samsung Pay CTP = Click to Pay
				Uso exclusivo para processing type 3 ou 4
securityAuthentication	-	-	-	Grupo securityAuthentication
sai	Até 02	Alfanumérico	Obrigatório para as bandeiras Visa e ELO. Opcional em transações card-on-file	Identificador de transação eletrônica (ECI). Nas transações que não forem tokenizadas (apenas card-on-file) o envio deste campo não é necessário. Para transações Wallets com cartão Elo, sempre envie o valor “04” – indicando uma transação in-app e para Wallets com cartão Visa e Mastercard, siga o que foi enviado pela Wallet. Para transações da bandeira Mastercard, esse campo não é enviado. Para mais detalhes desse campo verifique o tópico “uso do sai”.
transactionCredentials				Grupo transactionCredentials
transactionCredentials/ credentialId	Até 02	Alfanumérico	Sim, se storageCard=1 ou =2 e cartão mastercard	Indica a categoria da transação com credencial armazenada. Consulte a seção “Categorização de transações card-on-file” para mais detalhes

Atenção: Cartões Visa que forem tokenizados via Wallets após 30 de julho de 2025 não poderão realizar transações parceladas ou recorrentes. Para estes casos os cartões devem ser tokenizados via [card-on-file](#), com tokens de uso para o estabelecimento.

Ressaltamos que as Wallets utilizam a tokenização de bandeira em suas transações. Desse modo, quando o comprador salva o cartão, um token de bandeira é criado, alterando assim as informações do cartão físico (número, código de segurança e validade).

Por isso, é **obrigatório** enviar nas transações os campos card number + token cryptogram devolvido por cada wallet. Além disso, em transações MIT (Iniciadas pelo estabelecimento) para a bandeira **Visa**, é permitido enviar o número do cartão tokenizado (campo cardnumber), sem o campo tokenCryptogram, mantendo o valor do campo “sai” indicado pela Wallet. Para as demais bandeiras o tokenCryptogram **obrigatoriamente** deve ser enviado.

Uso do “sai”: O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e autenticação de tokens de bandeira), quando autenticado através de desafio 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso. **Para transações Wallets com cartão Elo, sempre envie o valor “04” – indicando uma transação in-app e para Wallets com cartão Visa, siga o que foi enviado pela Wallet.**

Pontos de atenção:

- Ao fazer o envio do grupo threeD Secure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.
- Em caso de envio incorreto dos parâmetros a bandeira poderá fazer o downgrade da transação, isto é, poderá classificá-la como não autenticada, perdendo o liability emissor. Fique atento aos parâmetros solicitados na documentação.
- Transações Wallets também podem ser contestadas caso possuam ECI (enviado no campo “sai”) de transação não segura. Observe os parâmetros enviados pelas Wallets e encaminhe-os em suas requisições do e.Red para garantir que as bandeiras e emissores recebam as informações em sua totalidade.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime	-	Alfanumérico	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Númérico	<p>Valor total da transação sem separador de milhar e casa decimal.</p> <p>Exemplos:</p> <ul style="list-style-type: none"> • R\$10,00 = 1000 • R\$0,50 = 50
cardbin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brandTid	Até 21	Alfanumérico	Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file

Apple Pay

Apple Pay é a carteira digital da Apple disponível nos aparelhos Apple tais como:

- iPhone (Modelos com Touch ID, Face ID, exceto 5s);
- Apple Watch (Apple Watch Series 1 e posterior);
- Mac (Modelos com Touch ID);
- iPad (iPad Pro, iPad Air, iPad e iPad mini com Touch ID ou Face ID).

O pagamento por meio da Apple Pay substitui os dados do cartão por um token de bandeira, tornando a transação mais segura.

Para oferecer Apple Pay para seus clientes, é preciso fazer a afiliação à Apple e ao Apple Pay ou possuir um parceiro integrado como PSP capaz de decriptar o payload da Wallet e depois enviar seguindo as instruções de integração com o e.Red. Você encontra as informações detalhadas buscando por "Apple Pay" nas documentações de tecnologia do [Portal do Desenvolvedor Apple](#){target="_blank"}. Além disso, é imprescindível que seus compradores estejam acessando o site pelo browser Safari ou através do App em um dispositivo iOS compatível com o Apple Pay.

 Selecione o tipo "Carteiras digitais: Apple, Google, Samsung pay e Click to Pay" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Google Pay

O Google Pay é a carteira virtual do Google, disponível em diversos dispositivos Android. Permite que os consumidores realizem pagamentos, de forma prática e segura, com seus cartões de crédito e débito armazenados.

O pagamento por meio da Google Pay substitui os dados do cartão por um token de bandeira, tornando a transação mais segura.

Para realizar a integração é necessário que seu estabelecimento possua o cadastro e integração com a Google Pay ou possua um parceiro integrado como PSP capaz de decriptar o payload da Wallet e depois enviar seguindo as instruções de integração com o e.Red.

Para o Google Pay, existem dois tipos de credenciais:

- Tokenizadas: Cartões salvos através do app do Emissor para a Carteira do Google, promovem liability shift e são armazenados na carteira.
- Convencionais: Cartões oriundos do processo de onboarding através do Google Autofill ou Google Settings/Account (pay.google.com). Esses cartões são Card on File e o Google Pay reconhece o dispositivo e o apresenta em toda e qualquer compra - não promovem liability shift. Nesse caso, é recomendado utilização de autenticação 3DS ou outros mecanismos de segurança da transação como anti-fraude.

Para ambos, existem parâmetros na API Google que permitem identificar se a transação é proveniente de uma credencial tokenizada ou não - essa string é chamada na documentação da Google Pay como AssuranceDetails.

Para maiores detalhes da integração com a Google Pay acima consulte o [Portal do Desenvolvedor Google](#){target="_blank"}.

 Selecione o tipo "Carteiras digitais: Apple, Google e Samsung pay" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Samsung Pay

O Samsung Pay é carteira digital da Samsung, disponível em aparelhos mais recentes, permite que você carregue seus cartões de crédito, débito, presente e de associação em seus dispositivos. Com ele é possível fazer pagamentos e autenticar a compra com sua impressão digital, PIN ou leitura de íris.

O pagamento por meio da Samsung Pay substitui os dados do cartão por um token de bandeira, que é um conjunto aleatório exclusivo de números a serem usados em cada nova transação, para que o número real do cartão nunca seja usado, tornando a transação mais segura.

Para realizar a integração é necessário que seu estabelecimento possua o cadastro e integração com a Samsung Pay ou possua um parceiro integrado como PSP capaz de decryptar o payload da Wallet e depois enviar seguindo as instruções de integração com o e.Red. Para maiores detalhes da integração consulte o site da [Samsung Pay](#).{target="_blank"}

 Selecione o tipo "Carteiras digitais: Apple, Google e Samsung pay" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Os retornos das transações Wallets obedecem os de transações comuns no e.Red, disponíveis em nosso portal do desenvolvedor. É importante estar atento a todos os possíveis [Retornos de integração](#).

Esteja atento também aos [Retornos fornecidos pelas bandeiras](#), também disponíveis em nosso portal do desenvolvedor e que podem indicar negativas por parte delas.

Operadoras de carteira digital escalonada (SDWO - Staged Digital Wallet Operators)

Carteira digital é uma solução eletrônica que permite o armazenamento de dados financeiros e de identidade de forma que os mesmos sejam usados com segurança e privacidade durante as operações financeiras.

Existem dois tipos de carteiras digitais escalonadas (Staged Digital Wallets Operators)

- Cash-in
 - A carteira é abastecida com fundos através de uma transação financeira utilizando o cartão cadastrado previamente em sua plataforma, para posterior utilização;
 - Carteiras de pedágio realizam apenas operações de cash-in, e devem utilizar corretamente os parâmetros indicados na tabela de relação de campos de Cash-in por bandeira.

 Selecione o tipo "Cash-in + Carteiras digitais" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

- Purchase
 - A carteira realiza uma transação financeira a um lojista parceiro ou transfere valores entre carteiras, utilizando o cartão cadastrado previamente em sua plataforma.

 Selecione o tipo "Purchase + Carteiras digitais" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Para o correto funcionamento da integração do serviço de Carteiras digitais, além da integração inicial do fluxo transacional (Autorização) é necessário que algumas outras integrações às nossas API's já tenham sido realizadas:

- [MCC Dinâmico \(Merchant Category Code\)](#)
- [SoftDescriptor](#)

O serviço de SDWO, pode ser utilizado em conjunto com os demais serviços disponíveis na Rede:

O Serviço de Pagamento de Contas do Consumidor (CBPS)* (*) Transações CBPS + Carteiras digitais são possíveis nas bandeiras Mastercard e Amex.

 Selecione o tipo "CBPS + Carteiras digitais" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

O serviço de Carteiras digitais, pode ser utilizado nas bandeiras Elo, Mastercard, Visa e Amex.

Para a correta identificação de uma transação do tipo Carteiras digitais, há alguns campos que necessitam ser preenchidos no fluxo transacional de acordo com a modalidade, conforme as regras especificadas por bandeiras.

Confira abaixo a lista de campos existentes e seus respectivos formatos nas operações de Carteira Digital Escalonada. Na sequência será apresentado as regras esperadas para cada bandeira:

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	-	Booleano	Não	Define se uma transação terá captura automática ou posterior. O não envio desse campo será considerado uma captura automática (true).
kind	•	•	•	Tipo de transação a ser realizada. <ul style="list-style-type: none">Para transações de crédito, utilizar creditPara transações de débito, utilizar debit O não envio desse campo será considerado crédito.
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Valor total da transação sem separador de milhar e casa decimal. Exemplos: <ul style="list-style-type: none">R\$10,00 = 1000R\$0,50 = 50
installments	Até 2	Numérico	Não	Número de parcelas em que uma transação será autorizada. De 2 a 12 O não envio desse campo será considerado à vista.

Nome	Tamanho	Tipo	Obrigatório	Descrição
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão. Não enviar caracteres especiais.
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do cartão. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	Ano de vencimento do cartão. Exemplo: 2028 ou 28
securityCode	Até 4	Alfanumérico	Não	Código de segurança do cartão geralmente localizado no verso do cartão. O envio desse parâmetro garante maior possibilidade
softDescriptor	Até 18*	Alfanumérico	Sim	Frase personalizada que será impressa na fatura do portador. Confira o padrão a ser seguido em cada operação com mais detalhes nas especificações na sequência.
subMerchant		subMerchant		
subMerchant/mcc	4	Numérico	Sim	MCC do sublojista.
wallet				
wallet/walletId	Até 11	Alfanumérico	Consulte regras por bandeira	Código-identificador de carteira, conhecido como WID (Wallet Identifier Number), que é o número de identificação das carteiras junto a cada uma das bandeiras.
wallet/processingType	2	Alfanumérico	Sim	Identificação de tipo de operação (01 para Purchase e 02 para Cash-in).

Nome	Tamanho	Tipo	Obrigatório	Descrição
wallet/paymentDestination	2	Alfanumérico	Consulte regras por bandeira	<p>Identifica o destino/finalidade do cash-in:</p> <ul style="list-style-type: none"> 04: M2M (Mesma titularidade, mesma carteira/arranjo) 05: P2P (Para outra titularidade, mesma carteira/arranjo) 06: Transferência para outro arranjo (mesma titularidade) 07: Transferência para outro arranjo (outra titularidade) 08: Transferência para carteira de armazenamento de valor
receiverData				
receiverData/firstName	Até 40	Alfanumérico	Consulte regras por bandeira	Primeiro nome do recebedor do cash-in. Não utilize caracteres especiais.
receiverData/lastName	Até 40	Alfanumérico	Consulte regras por bandeira	Último nome do recebedor do cash-in. Não utilize caracteres especiais.
receiverData/taxIdNumber	Até 14	Alfanumérico	Consulte regras por bandeira	CPF ou CNPJ do recebedor do cash-in.
senderData				
senderData/taxIdNumber	Até 14	Alfanumérico	Consulte regras por bandeira	CPF ou CNPJ do pagador do cash-in.
senderData/firstName	Até 20	Alfanumérico	Consulte regras por bandeira	Primeiro nome do usuário pagador.
senderData/lastName	Até 20	Alfanumérico	Consulte regras por bandeira	Último nome do usuário pagador.
senderData/address	Até 35	Alfanumérico	Consulte regras por bandeira	Endereço do usuário pagador.
senderData/city	Até 25	Alfanumérico	Consulte regras por bandeira	Cidade do usuário pagador.

Nome	Tamanho	Tipo	Obrigatório	Descrição
senderData/country	Até 3	Alfanumérico	Consulte regras por bandeira	País do usuário pagador
receiverData/walletAccountIdentification	Até 50	Numérico	Consulte regras por bandeira	Identificador do usuário na carteira.
consumerBillPaymentService				
consumerBillPaymentService/businessApplicationIdentifier	2	Numérico	Sim, se operação de pagamento de contas	Identificador de transações CBPS. Para esse tipo de transação este campo deve ser preenchido com "01". Quando não tivermos este tipo de transação, o campo não deve ser enviado.
consumerBillPaymentService/merchantTaxId	Até 14	Alfanumérico	Não	Identificador do beneficiário final/ cedente do boleto. Deve ser informado CPF/CNPJ. Para a Mastercard, caso não seja indicado será considerado como boleto não identificado.

Parâmetros de resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número de autorização da transação retornada pelo emissor do cartão.
dateTime	-	Data e hora	Dados da transação no formato YYYY-MM-DDhh:mm:ss.sTZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e casa decimal.
cardbin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.

Nome	Tamanho	Tipo	Descrição
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usados para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número de autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Cash-in:

Observe abaixo a relação de campos obrigatórios para a operação de acordo com cada bandeira:

	Elo	Mastercard	Visa	Amex
softDescriptor	Nome da Carteira* TRANSFERENCIA	Nome da Carteira*Nome do titular da conta recebedora na Carteira	Nome da Carteira*Nome do titular da conta recebedora na Carteira	Nome da Carteira*Nome do titular da conta recebedora na Carteira
submerchant				Grupo submerchant
submerchant/mcc	<ul style="list-style-type: none">6051 ou 6540: Cash-in de carteiras escalonadas (SDWO)4784: Cash-in de carteira de armazenamento de valor (SVDW)	<ul style="list-style-type: none">6540: Cash-in de carteiras escalonadas (SDWO)4784*: Cash-in de carteira de armazenamento de valor (SVDW)	<ul style="list-style-type: none">6051: Cash-in de carteiras escalonadas (SDWO)4784*: Cash-in de carteira de armazenamento de valor (SVDW)4900: Cash-in para pagamento de boleto	<ul style="list-style-type: none">6051: Cash-in de carteiras escalonadas (SDWO)
submerchant/address	Endereço da carteira			
submerchant/country	País da carteira			
submerchant/cep	CEP da carteira			
wallet				Grupo wallet
wallet/processingType	02	02	02	02

	Elo	Mastercard	Visa	Amex
wallet/walletId	11 caracteres (Observar ao final das tabelas como obter)	3 caracteres (Observar ao final das tabelas como obter)	10 caracteres, caso o parâmetro tenha menos de 10 caracteres deve-se preencher a quantidade de zeros faltantes à direita. Ex: 3900370000 (Observar ao final das tabelas como obter)	Enviar os 8 primeiros dígitos do CNPJ da carteira
wallet/paymentDestination	•	Destino/finalidade do cash-in <ul style="list-style-type: none">• 04: M2M (Mesma titularidade, mesma carteira/arranjo)• 05: P2P (Para outra titularidade, mesma carteira/arranjo)• 06: Transferência para outro arranjo (mesma titularidade)• 07: Transferência para outro arranjo (outra titularidade)• 08: Transferência para carteira de armazenamento de valor*	• 08: Transferência para carteira de armazenamento de valor*-	•
receiverData				Grupo receiverData
receiverData/firstName	-	Primeiro nome do recebedor	-	-
receiverData/lastName	-	Último nome do recebedor	-	-
receiverData/taxIdNumber	Documento identificador do recebedor (CPF/CNPJ)	Documento identificador do recebedor (CPF/CNPJ)	Documento identificador do recebedor (CPF/CNPJ)	-

	Elo	Mastercard	Visa	Amex
receiverData/walletAccountIdentification	-	Identificador do usuário na carteira	-	-
senderData				
senderData/taxIdNumber	Documento identificador do pagador (CPF/CNPJ)	-	-	-
senderData/firstName	-	-	Primeiro nome do usuário pagador	-
senderData/lastName	-	-	Último nome do usuário pagador	-
senderData/address	-	-	Endereço do usuário pagador	-
senderData/city	-	-	Cidade do usuário pagador	-
senderData/country	-	-	País do usuário pagador	-

Atenção: O MCC 4784 e paymentDestination = 08 são de uso exclusivo para carteiras de pedágio, outras operações de carteiras digitais devem se restringir a usar o MCC 6051 ou 6540, conforme indicado acima.

Purchase:

Observe abaixo a relação de campos obrigatórios para a operação de acordo com cada bandeira:

	Elo	Mastercard	Visa	Amex
softDescriptor	Nome Carteira*Nome do estabelecimento recebedor	Nome Carteira*Nome do estabelecimento recebedor	Nome Carteira*Nome do estabelecimento recebedor	Nome Carteira*Nome do estabelecimento recebedor
paymentFacilitatorID	Mesmo valor do campo wallet/walletId		Mesmo valor do campo wallet/walletId	
submerchant				Grupo submerchant
submerchant/mcc	MCC do estabelecimento	MCC do estabelecimento	MCC do estabelecimento	MCC do estabelecimento
submerchant/subMerchantID	Código do estabelecimento na carteira.		Código do estabelecimento na carteira.	
submerchant/address	Endereço do estabelecimento		Endereço do estabelecimento	
submerchant/country	País do estabelecimento		País do estabelecimento	
submerchant/cep	CEP do estabelecimento		CEP do estabelecimento	

	Elo	Mastercard	Visa	Amex
submerchant/taxIdNumber	CNPJ do estabelecimento		CNPJ do estabelecimento	
wallet				Grupo wallet
wallet/processingType	01	01	01	01
wallet/walletId	11 caracteres (Observar ao final das tabelas como obter)	3 caracteres (Observar ao final das tabelas como obter)	11 caracteres (Observar ao final das tabelas como obter)	Enviar os 8 primeiros números do CNPJ da carteira

CBPS/Pagamentos de Contas:

Observe abaixo a relação de campos obrigatórios para a operação de acordo com cada bandeira:

	Mastercard	Amex
softDescriptor	Nome Carteira*Nome do estabelecimento recebedor	Nome Carteira*Nome do estabelecimento recebedor
submerchant		Grupo submerchant
submerchant/mcc	6540	Confira a lista de MCCs permitidos aqui
consumerBillPaymentService		Grupo consumerBillPaymentService
consumerBillPaymentService/businessApplicationIdentifier	01	01
consumerBillPaymentService/merchantTaxId	CNPJ cedente do boleto/beneficiário final. Se não enviado é considerado como Boleto não identificado	CNPJ do cedente do boleto/beneficiário final
wallet		Grupo wallet
wallet/processingType	01	01
wallet/walletId	3 caracteres Ex: 3900370000 (Deve ser enviado apenas caso a operação seja CBPS + Carteira) (Observar ao final das tabelas como obter)	Enviar os 8 primeiros números do CNPJ da carteira (Observar ao final das tabelas como obter)

Atenção:

- Para as bandeiras **Master e Visa**: a solicitação para geração do Wallet ID é feito pelo time de facilitadores Rede facilitadores@userede.com.br.
- Para a bandeira **Elo**: o cadastro deve ser feito diretamente pelo cliente através do e-mail aceitacaofacilitadores@elo.com.br.
- Para a bandeira **Amex**: não é feito cadastro de walletId no momento, por isso deve ser enviado os 8 primeiros números do CNPJ no campo walletId para identificação do estabelecimento. No futuro, caso a bandeira crie walletIds específicos, os clientes serão comunicados.

Uso do “sai” em transações Cash-in: O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e Cloud Token Visa), **quando autenticado como 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso.**

Atenção: Ao fazer o envio do grupo threeDSecure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.

Pix

É uma opção de pagamento, recebimento e transferência dentro dos aplicativos de carteiras digitais e de bancos - entre pessoas físicas ou jurídicas.

Atenção: método de pagamento disponível apenas para correntistas Itaú.

Cadastro de chave Pix

Para habilitar sua chave Itaú para transacionar na Rede:

1. Acesse o portal userede.com.br;
2. Efetue seu login;
3. Acesse a rota: Para vender > PIX > Clique em “quero utilizar o Pix” > Aceite de termos de uso > Selecione agência e conta.

Não esqueça de cadastrar sua URL para notificações!

Esteja atento para não excluir sua chave antes de finalizar operações nas suas transações, como pedir devoluções de QR Code pagos.

Para dúvidas sobre precificação, consulte a central de atendimento ou o valor negociado em sua conta no Itaú.

Cadastro de URL

O estabelecimento deverá informar uma URL válida e segura para receber as notificações dos eventos. O cadastro dessa URL será por CNPJ, independente de quantos ou quais PV's foram habilitados para aquele estabelecimento.

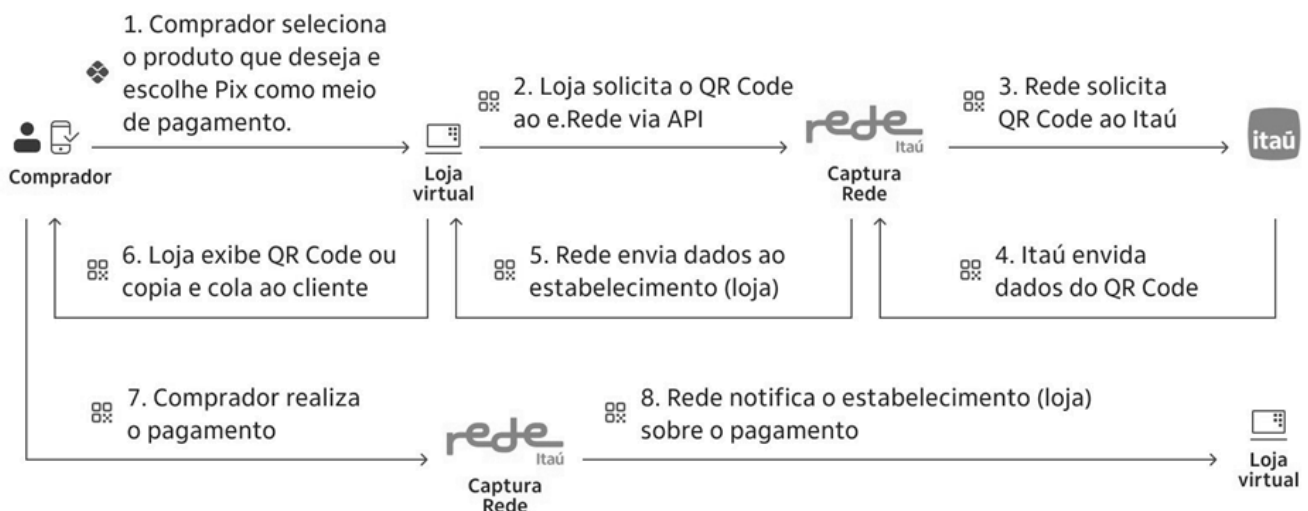
Para esse cadastro, o estabelecimento deve ligar na central de atendimento nos telefones: Central de atendimento: Capitais e regiões metropolitanas 4001 4433 ou Central de atendimento: Demais localidades 0800 728 4433 e informar o número de CNPJ, PV, email para contato e a URL que deseja utilizar para receber as notificações do Pix. O prazo para ativação é de **2 dias uteis após a abertura do chamado**.


Solicitação de QR Code Pix

Fluxo transacional

Para detalhar o fluxo transacional, observe abaixo o fluxo de solicitação, pagamento e recepção de notificações de pagamentos de QR Code Pix:

Pix no e.Redé - Jornada Transacional



 Selecione o tipo "Pix" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
kind		Alfanumérico	Sim	Tipo de transação a ser realizada. Para transações de Pix, utilizar Pix .
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Númerico	Sim	Valor total da transação sem separador de milhar e decimal. Exemplos: R\$10,00 = 1000
qrCode				Grupo QR Code
qrCode/dateTimeExpiration		Data e hora	Sim	Dados da expiração do QR Code no formato YYYY-MM-DDThh:mm:ss. O prazo máximo deve ser de até 15 dias e não deve ser de datas anteriores à atual.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	Até 20	Alfanumérico	Número identificador único da transação.
dateTime		Data e hora	Data da solicitação do QR Code no formato YYYY-MM-DDThh:mm:ss.sTZD.
amount	Até 10	Númerico	Valor total da transação sem separador de milhar e decimal.
qrCodeResponse			Grupo QR Code
qrCodeResponse/dateTimeExpiration		Data e hora	Data de expiração do QR Code da transação no formato YYYY-MM-DDhh:mm:ss.sTZD.
qrCodeResponse/qrCodeImage	Até 999	Alfanumérico	Campo com string do QRCode em base64. Para renderizar a imagem do QR Code, basta utilizar de bibliotecas ou scripts compatíveis com a sua linguagem de programação.
qrCodeResponse/qrCodeData	Até 999	Alfanumérico	Campo com string do QRCode em formato emv (copia e cola).
returnCode	Até 04	Alfanumérico	Código de retorno da Solicitação de QR Code.

Nome	Tamanho	Tipo	Descrição
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da Solicitação de QR Code.

Notificação de atualização de status via webhook

Após a solicitação de um QR Code Pix, a cada atualização referente ao status do pagamento ou devolução (via canais Itaú), será retornada uma notificação na URL informada pelo estabelecimento. O Estabelecimento deverá informar uma URL válida e segura, que deverá ser chamado pelo processo de pagamento de Pix para receber a notificação dos eventos (através de um método POST). O cadastro dessa URL será por CNPJ, independente de quantos ou quais PV's foram habilitados para aquele estabelecimento. Para solicitar o cadastro de sua URL entre em contato conosco através de nossos canais de atendimento e informe:

- CNPJ;
- PV;
- E-mail para contato;
- URL que deseja receber as notificações da Rede

O Cliente só poderá associar uma URL para cada CNPJ, sendo possível, excluir ou alterar o mesmo.

Os eventos possíveis são:

Evento de notificação	Status correspondente
PV.UPDATE_TRANSACTION_PIX	Pago
PV.REFUND_PIX	Devolvido (parcial ou totalmente via canais Itaú)

Para devolução solicitada via API, não haverá notificações, pois, a resposta de sucesso ou falha é dada de forma síncrona.

Para devoluções totais ou parciais feitas via outros canais Itaú como o bankline, você receberá uma notificação e poderá visualizar a relação de devoluções parciais nas APIs de consulta de transações e de consulta de cancelamentos do e.Redre.

Com o recebimento da notificação é opcional retornar à API de consulta do e.Redre com o TID para mais detalhes da transação. Recomendamos que aguarde no mínimo 10 min para realizar consultas após receber uma notificação.

IMPORTANTE: Caso o “endpoint/ URL” de notificações não seja informada, nenhum evento será notificado durante o processo de pagamento ou devolução das suas transações Pix.

Para validar como simular em ambiente de teste, consulte a seção [Simulação de notificação de status via webhook](#).

Parâmetros da notificação:

Nome	Local de envio	Tamanho	Tipo	Descrição
authorization	header	Até 3	Alfanumérico	Header para autorização da requisição na url fornecida pelo estabelecimento – em momento de piloto solicitamos que seja enviado via e-mail caso deseje utilizar autenticação para envio das notificações (opcional)
request-ID	header	Até 36	Alfanumérico	Identificador único da requisição
content-Type	header	--	Alfanumérico	Valor fixo definido como 'application/json'
id	body	6	Alfanumérico	Identificador único da transação (TID)
companyNumber	body	9	Alfanumérico	Número de filiação do estabelecimento (PV)

Nome	Local de envio	Tamanho	Tipo	Descrição
events	body	--	Lista alfanumérica	Nome dos eventos que serão informados ao cliente. Exemplo: ["PV.UPDATE_TRANSACTION_PIX"], ["PV.REFUND_PIX"]

Formato do evento:

```
{
  "companyNumber": "90104480",
  "events": [ "PV.UPDATE_TRANSACTION_PIX" ],
  "data": {
    "id": "41412312010933570004"
  }
}
```

Consulta de transação Pix

Para transações Pix, a consulta segue o padrão do e.Redre, sendo possível de ser realizada através do TID e Reference (número do pedido).

Atenção: Os campos qrCodeData e qrCodeImage só serão retornados na consulta caso o status do QR Code seja **pendente**. Para QR Codes pagos ou devolvidos, estes campos **não serão retornados**.

Para o caso de QR Codes expirados, será devolvido o código 3036 - QrCode Expired.

Parâmetros da resposta com QR Code Pix Pendente:

Nome	Tamanho	Tipo	Descrição
requestDateTime	--	Datetime	Data da requisição no formato YYYY-MM-DDThh:mm:ss.sTZD.
qrCodeResponse	--	--	Grupo QR Code
qrCodeResponse/dateTime	--	Datetime	Data da criação do QrCode da transação no formato YYYY-MM-DDhh: mm:ss.sTZD.
qrCodeResponse/returnCode	Até 04	Alfanumérico	Código de retorno da Solicitação de QR Code.
qrCodeResponse/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da Solicitação de QR Code.
qrCodeResponse/affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV).
qrCodeResponse/kind	Até 10	Alfanumérico	Método de pagamento utilizado na transação (Pix).
qrCodeResponse/reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
qrCodeResponse/amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
qrCodeResponse/tid	Até 20	Alfanumérico	Número identificador único da transação.

Nome	Tamanho	Tipo	Descrição
qrCodeResponse/status	--	Alfanumérico	Status da transação: <ul style="list-style-type: none">• Approved• Canceled• Pending
qrCodeResponse/expirationQrCode	--	Datetime	Data do pagamento do QR Code no formato YYYY-MM-DDThh:mm:ss.sTZD.
qrCodeResponse/qrCodeImage	Até 999	Alfanumérico	Campo com string do QR Code em base64. Para renderizar a imagem do QR Code, basta utilizar de bibliotecas ou scripts compatíveis com a sua linguagem de programação.
qrCodeResponse/qrCodeData	Até 999	Alfanumérico	Campo com string do QR Code em formato emv (copia e cola)

Parâmetros da resposta com QR Code Pix Pago

Nome	Tamanho	Tipo	Descrição
requestDateTime	--	Datetime	Data da requisição no formato YYYY-MM-DDThh:mm:ss.sTZD.
authorization/dateTime	--	Datetime	Data da criação do QrCode da transação no formato YYYY-MM-DDhh: mm: ss.sTZD.
authorization/returnCode	Até 04	Alfanumérico	Código de retorno da Solicitação de QR Code.
authorization/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da Solicitação de QR Code.
authorization/affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV).
authorization/status	--	Alfanumérico	Status da transação: <ul style="list-style-type: none">• Approved• Canceled• Pending
authorization/reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
authorization/orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
authorization/tid	Até 20	Alfanumérico	Número identificador único da transação.
authorization/kind	Até 10	Alfanumérico	Método de pagamento utilizado na transação (Pix).
authorization/amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
authorization/origin	Até 2	Numérico	Identifica a origem da transação. e.Redes: 1
authorization/txid	Até 35	Alfanumérico	Identificador único do Pix gerado pelo Itaú Exibido apenas em transações com status Pago ou devolvido

Nome	Tamanho	Tipo	Descrição
capture/dateTime	--	Datetime	Data do pagamento do QR Code no formato YYYY-MM-DDThh:mm:ss.sTZD.
capture/amount	Até 10	Numérico	Valor do pagamento do QR Code.
refunds/refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede.
refunds/refundDateTime	--	Datetime	Data da devolução no formato YYYY-MM-DDThh:mm:ss.sTZD.
refunds/status	Até 10	Alfanumérico	<ul style="list-style-type: none">• Done (Devolução efetivada)• Denied (Devolução negada)
refunds/amount	Até 10	Alfanumérico	Valor da devolução.

Status possíveis

Ao consultar uma transação Pix, são possíveis os seguintes status:

Status	Descrição
Pending	Seu QR Code ainda não recebeu atualizações de pagamento. Confirme se o pagador já realizou o pagamento no banco de sua preferência.
Approved	Seu QR Code foi pago.
Canceled	Seu QR Code foi devolvido.

Nota: Para transações parcialmente devolvidas, o status permanecerá como “Approved” até que o saldo total seja devolvido.

Para transações expiradas, será exibido o código 3036 – “QRCode: QR Code Expired”.

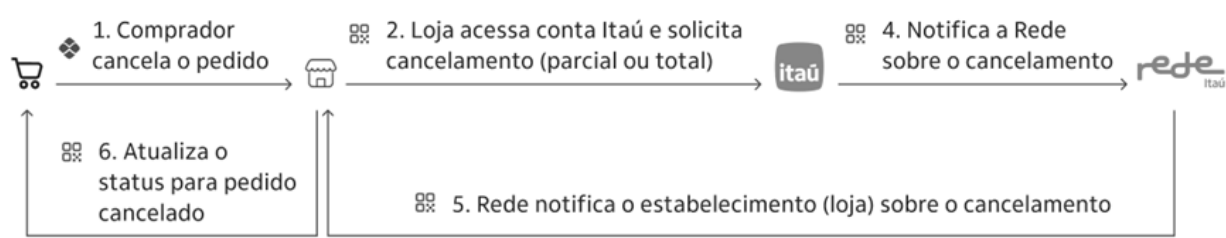
Devolução de transação Pix

Para transações Pix, a devolução segue a normativa definida pelo Banco Central do Brasil, sendo permitida em até 90 dias da data da venda.

Através do e.Redé será possível solicitar a devolução do **valor total e parcial**. A solicitação de devolução via API é síncrona, por isso fique atento aos códigos de retorno que confirmarão se seu pedido ocorreu com sucesso, eles estão disponíveis na seção [Códigos de Retorno](#).

O pedido de devolução via API pode ser realizado através do TID.

Nota: Para solicitações de devolução feitas via canais Itaú, como o bankline você receberá notificações no evento “PV.REFUND_PIX” (caso possua uma URL habilitada) e verá na consulta a lista de devoluções atreladas à sua transação Pix. Para melhor compreensão do fluxo feito via bankline, observe a ilustração abaixo:



Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
amount	Até 10	Numérico	Sim	Valor do cancelamento sem separador de milhar e casa decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50

Parâmetros de resposta:

Nome	Tamanho	Tipo	Descrição
refundDateTime	--	Datetime	Data do cancelamento no formato YYYY-MM-DDThh:mm:ss.sTZD.
returnCode	Até 4	Alfanumérico	Código de retorno da transação (vide tabela códigos de retorno para devolução).
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação (vide tabela códigos de retorno para devolução).

Consulta de devolução de transações Pix

Para transações Pix, a consulta de devolução/ cancelamento é possível através do TID ou refundId.

Consulta de devolução por TID

Parâmetros de resposta:

Nome	Tamanho	Tipo	Descrição
refunds/refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede.
refunds/refundDateTime	--	Datetime	Data da devolução no formato YYYY-MM-DDThh:mm:ss.sTZD.
refunds/status	Até 10	Alfanumérico	<ul style="list-style-type: none">• Done (Devolução efetivada)• Denied (Devolução negada)
refunds/amount	Até 10	Alfanumérico	Valor da devolução.

Consulta de devolução por refundID

Parâmetros de resposta:

Nome	Tamanho	Tipo	Descrição
refundId	36	Alfanumérico	Código de retorno da solicitação de cancelamento gerado pela Rede.
Tid	20	Alfanumérico	Número identificador único da transação.
refundDateTime	--	Datetime	Data da devolução no formato YYYY-MM-DDThh:mm:ss.sTZD.

Nome	Tamanho	Tipo	Descrição
status	Até 10	Alfanumérico	<ul style="list-style-type: none">• Done (Devolução efetivada)• Denied (Devolução negada)
amount	Até 10	Alfanumérico	Valor da devolução.

Códigos de retorno

Os [códigos e mensagens de retorno](#) podem ocorrer nos cenários de **solicitação, consulta ou devolução de um QR Code Pix**.

Esteja atento às orientações de cada um dos processos para adequar sua integração.

Solicitação de QR Code Pix: Momento da requisição de QR Code.

Voucher

O Voucher é um novo produto que está habilitado para integrar em um só cartão benefícios de refeição, alimentação, cultura, transporte e as demais opções flexíveis como auxílio home office, educação, saúde e bem-estar.

O pagamento com o cartão Voucher será capturado em um trilho exclusivo, dando mais facilidade à operação. Este produto é aderente aos novos termos das regras do Programa de Alimentação ao Trabalhador (PAT).

Benefícios do Voucher:

Empresas de arranjo fechado poderão emitir cartões bandeirados, fazendo com que estabelecimentos possam processar o modelo fechado através do ecossistema de bandeira, reduzindo a necessidade de integrações com arranjo fechados, e centralizando os recebíveis.

Transacionar com Voucher

Para garantir que sua transação com o produto Voucher seja processada corretamente, é necessário que seu estabelecimento esteja classificado nos MCCs (Merchant Category Codes) elegíveis.

Importante: Caso seu MCC não esteja listado, não será possível processar a transação com o Voucher na atividade principal.

Credenciamento elegível ao MCC: Para solicitar o credenciamento do e.Red e realizar a integração à sua aplicação, entre em contato com a Central de Atendimento da Rede:

- 4001 4433 (capitais e regiões metropolitanas)
- 0800 728 4433 (demais localidades)

Quando o credenciamento for realizado, o responsável pelo estabelecimento será notificado via e-mail com o número de filiação (PV), orientações para acessar o portal da Rede e suas credenciais para integração.

Ponto de atenção: Se o ramo do seu estabelecimento não for elegível, é necessário que o estabelecimento inclua no seu CNAE (Classificação Nacional das Atividades Econômicas) a atividade compatível com o programa para comercializar.

RAMO	MCC
Alimentação	5300, 5411, 5422, 5441, 5451, 5462, 5499, 5811
Refeição	5812, 5813, 5814
Cultura	4722, 5311, 5733, 5735, 5815, 5932, 5942, 5943, 5994, 7832, 7841, 9399, 8699, 7998, 7996, 7991, 7929, 7922, 7911

Lembrando que o MCC é um código numérico de quatro dígitos utilizado para classificar o tipo de bens ou serviços que o seu estabelecimento oferece.

Em caso de dúvida, consultar o nosso portal : <https://developer.userede.com.br/e-rede#documentacao-mcc-dinamico>

Para voucher existem dois tipos de arranjos de pagamentos, são eles:

Arranjo aberto:

Consiste em um conjunto de normas e procedimentos que permitem a utilização de um meio de pagamento em qualquer estabelecimento comercial incluindo e-commerce. No caso dos cartões, a emissão é realizada por um emissor associado a uma bandeira específica, como a Elo, Visa ou Mastercard.

Arranjo fechado:

Consiste em um cartão que é emitido por uma empresa (por exemplo, supermercados ou outras grandes lojas de varejo) e o cliente pagador só poderá usá-lo no estabelecimento que emitiu ou em empresas parceiras.

Empresas como Pluxee, Ticket, Alelo, Sodexo, entre outras, fazem parte do arranjo fechado. Conhecido como modelo VAN.

Para maiores informações sobre arranjo fechado, procure o atendimento Rede.

Para maiores informações sobre o fluxo transacional verifique na Lista de APIs, conforme indicado a seguir:

 Selecione o tipo "Voucher" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Solicitação de transação voucher

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	--	Booleano	Sim	Defina se a transação terá captura automática ou posterior. O não envio desse campo será considerado a captura automática (true). Para transações voucher dever ser enviado como TRUE.
kind	--	Alfanumérico	Sim	voucher Tipo de transação a ser realizada.
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Valor total da transação sem separador de milhar e decimal.
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão. Não enviar caracteres especiais.
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão
expirationMonth	Até 02	Numérico	Sim	Mês de vencimento do cartão. De 1 a 12.

Nome	Tamanho	Tipo	Obrigatório	Descrição
expirationYear	02 ou 04	Numérico	Sim	expirationYear 2 ou 4 Numerico Sim Ano de vencimento do cartão. Ex .: 2028 ou 28.
securityCode	Até 04	Alfanumérico	Não	Código de segurança do cartão geralmente localizado no verso do cartão. O envio desse parâmetro garante maior possibilidade de aprovação da transação.
softDescriptor	Até 18*	Alfanumérico	Não	Frase personalizada que será impressa na fatura do portador.
storageCard	Até 01	Alfanumérico	Não	indica operações que possam ou não estar utilizando COF (Card on File): 0 - Transação com credencial não armazenada 1 - Transação com credencial armazenada pela primeira vez. 2 - Transação com credencial já armazenada. Atenção: O não envio desse campo será considerado 0 (credencial não armazenada).

Parâmetros de resposta:

Parâmetro de Resposta Arranjo Aberto

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	Até 20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
dateTime	--	Data e hora	Dados da solicitação do QR Code no formato YYYY-MM-DDhh:mm:ss.sTZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
brand	--	--	Grupo de informações recebidas da bandeira sobre a transação
brand/name	--	--	Nome da bandeira. Ex.: Elo
brand/returnCode	Até 04	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.

Nome	Tamanho	Tipo	Descrição
brand/authorizationCode	06	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file
brand/voucher	--	--	Grupo de informações recebidas da bandeira sobre a transação voucher .
brand/voucher/voucherRemainingBalance	Até 10	Numérico	Saldo disponível no voucher, no momento da transação.

Parâmetro de Resposta Arranjo Fechado

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	Até 20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
dateTime	--	Data e hora	Dados da solicitação do QR Code no formato YYYY-MM-DDhh:mm:ss.sTZD.
amount	Até 10	Numérico	Valor total da transação sem separador de milhar e decimal.
cardBin	06	Alfanumérico	6 primeiros dígitos do cartão.
last4	04	Alfanumérico	4 últimos dígitos do cartão.
brand	--	--	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	--	--	Nome da bandeira. Ex.: Elo
brand/returnCode	Até 04	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/authorizationCode	06	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file
brand/voucher	--	--	Grupo de informações recebidas da bandeira sobre a transação voucher .
brand/voucher/voucherIssuer	--	--	Nome do emissor. Ex.: Ticket
brand/voucher/voucherIssuerTaxId	Até 14	Alfanumérico	Código CNPJ
brand/voucher/voucherRemainingBalance	Até 10	Numérico	Saldo disponível no voucher, no momento da transação.

Códigos de retorno

Os [códigos e mensagens de retorno](#) podem ocorrer nos cenários de **solicitação, consulta ou devolução de uma Transação Pix**.

Esteja atento às orientações de cada um dos processos para adequar sua integração.

Solicitação de Transação Pix: Momento da requisição de Voucher.

Retornos

Para melhor experiência na visualização da negativa, a Rede possui campos que exibem a justificativa completa do motivo de negativa da bandeira:

- Grupo Brand (padrão ABECS);

Importante: A utilização do grupo Brand é obrigatória, pois fornece informações reais sobre o motivo de negativa.

Outro caso possível é a utilização do antigo encapsulado Rede, vide [retornos de emissor](#):

- Return code – fora do grupo Brand (encapsulado Rede);
- Return message – fora do grupo Brand (encapsulado Rede);

Importante: A utilização do antigo encapsulado Rede não é recomendada pois não fornece informações concretas sobre o motivo de negativa, em breve deixará de ser utilizado.

Retornos da bandeira

A partir do dia 15 de julho de 2020 passamos a oferecer aos nossos clientes a opção do recebimento dos códigos da bandeira abertos, enviados pelos bancos, dependendo do motivo de negada da transação.

Junto com essa opção, passamos a atender a normativa 21 da Abecs que padroniza as mensagens em relação as essas transações negadas no processo de autorização.

O objetivo é proporcionar maior transparência e padronização, buscando aumentar a taxa de aprovação.

Além do retorno padronizado para as principais bandeiras (ELO, Visa, Master/Hiper e Amex) será possível, através da tabela abaixo, verificar se aquela recusa é reversível ou irreversível. Muito importante para o processo de retentativas. Por isso, fique atento aos códigos retornados.

Para as demais bandeiras, as mensagens de transação negada permanecem as mesmas atuais, no entanto, com os códigos abertos.

Vale acrescentar que para passar a ter acesso aos códigos de retorno abertos com a padronização da mensagem, é preciso um pequeno ajuste na sua API, segue abaixo procedimento de ativação.

Caso você não realize esse ajuste, os retornos atuais continuam no padrão Rede, sem qualquer mudança ou impacto.

Ativação:

Para habilitar mais essa funcionalidade e passar a receber as mensagens padronizadas pela normativa da Abecs e demais retornos da bandeira com os códigos abertos, basta realizar o ajuste no campo custom header, **"Transaction-Response"**, com o valor **"brand-return-opened"** preenchido, isso vale tanto para a transação quanto na consulta.

Header	Valor
Transaction-Response	brand-return-opened

Dessa forma, o response em caso de transação aprovada, passa a retornar o objeto **"Brand"** com os campos da bandeira, **"authorizationCode"** e **"brandTid"**, e adicionalmente **"Name"**, **"returnCode"** e **"returnMessage"**. Em caso de transação negada, no objeto **"Brand"** teremos apenas os campos **"Name"**, **"returnCode"** e **"returnMessage"**.

Caso o header **"Transaction-Response"** com o valor **"brand-return-opened"** não seja enviado na transação, pode ser enviado normalmente na consulta e a informação da bandeira (Brand) será retornada.

Os campos returnCode e returnMessage de fora do "Brand", que são os que conhecemos hoje, passam a ter somente os códigos de retorno de transações negadas na Rede, novamente.

Tabela de códigos de retorno da bandeira e padronização da mensagem:

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Genérica	5 – reversível	5 - reversível	5 - reversível	100 - reversível	Contate a central do seu cartão Please contact issuer	Please contact issuer
Saldo Limite insuficiente	51 – reversível	51 - reversível	51 - reversível	116 - reversível	Não autorizada	Refused
Senha inválida	55 - reversível	55 - reversível 86 - reversível	55 - reversível 86 - reversível	117 - reversível	Senha inválida	Invalid pin
Transação não permitida para o cartão	57 - irreversível	57 - irreversível	57 - reversível	200 - irreversível	Visa e Elo: Transação não permitida para o cartão - não tente novamente Mastercard: Não permitida para o cartão	Visa e Elo: Transaction not permitted to cardholder. Do not retry. Amex: Unauthorized transaction. Do not try again Mastercard: Transaction not permitted to cardholder
Nº cartão não pertence ao emissor Nº cartão inválido	-14 - irreversível 56 - irreversível	14 - irreversível	14 - irreversível 1 - irreversível	122 - irreversível	Verifique os dados do cartão	Format error. Verify card data Visa: Invalid card. Do not retry
Violação de segurança Inválido ou não presente	63 - irreversível	N7 - irreversível	63 - reversível	122 - irreversível	Verifique os dados do cartão	Format error. Verify card data Visa: invalid card. Do not retry
Suspeita de fraude Aviso de viagem	59 - reversível	59 - reversível	63 - reversível	100 - reversível	Contate a central do seu cartão	Please contact issuer
Comerciante inválido	58 - irreversível	3 - irreversível	3 - irreversível	109 - irreversível	Transação não permitida - não tente novamente	Unauthorized transaction. Do not try again
Refazer a transação (emissor solicita retentativa)	4 - reversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Refazer a transação	Please, retry this transaction.

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Consultar credenciador	6 - reversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Lojista, contate o adquirente	Contact card issuer
Problema no adquirente	19 - irreversível	19 - irreversível	30 - irreversível	Sem código correspondente	Erro no cartão – não tente novamente	Invalid card. Do not retry
Erro no cartão	12 - irreversível	6 - irreversível	Sem código correspondente	115 - irreversível	Verifique os dados do cartão	Format error. Verify card data Visa: invalid card. Do not retry Amex: function not supported. Do not retry
Erro de formato (mensageria)	30 - irreversível	12 - irreversível	30 - irreversível	181 - irreversível	Erro no cartão – não tente novamente	Invalid card. Do not retry
Valor da transação inválida	13 - irreversível	13 - irreversível	13 - irreversível	110 - irreversível	Valor da transação não permitido - não tente novamente	Transaction amount no permitted. Do not retry
Valor da parcela inválida	23 - irreversível	Sem código correspondente	12 - irreversível	115 - irreversível	Parcelamento inválido - não tente novamente	Function not supported. Do not retry
Excedidas tentativas de senha Compras	38 - reversível	75 - reversível	75 - reversível	106 - reversível	Excedidas tentativas de senha. contate a central do seu cartão	Invalid pin. Contact card issuer
Cartão perdido	41 - irreversível	41 - irreversível	41 - irreversível	200 - irreversível	Transação não permitida - não tente novamente	Unauthorized transaction. Do not try again
Cartão roubado	43 - irreversível	43 - irreversível	43 - irreversível	200 - irreversível	Transação não permitida - não tente novamente	Unauthorized transaction. Do not try again
Cartão vencido Dt expiração inválida	54 - irreversível	54 - irreversível	54 - irreversível	101 - irreversível	Verifique os dados do cartão	Format error. Verify card data Visa: invalid card. Do not retry
Transação não permitida Capacidade do terminal	57 - irreversível	58 - irreversível	58 - irreversível	116 - irreversível	Transação não permitida para o cartão - não tente novamente	Transaction not permitted to cardholder. Do not retry Amex: refused
Valor excesso Saque	61 - reversível	61 - reversível n4 - reversível	61 - reversível	Sem código correspondente	Valor excedido. Contate a central do seu cartão	Transaction amount no permitted. Contact card issuer

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Bloqueio Temporário (ex: Inadimplência)	62 - reversível	62 - reversível	57 - reversível	Sem código correspondente	Contate a central do seu cartão	Contact card issuer
Valor mínimo da transação inválido	64 - irreversível	Sem código correspondente	13 - irreversível	Sem código correspondente	Valor da transação não permitido - não tente novamente	Transaction amount not permitted. Do not retry
Quant. de saques excedido	65 - reversível	65 - reversível	65 - reversível	Sem código correspondente	Quantidade de saques excedida.contate a central do seu cartão	Exceeds withdrawal limit. Contact card issuer
Senha vencida Erro de criptografia de senha	83 - irreversível	74 - irreversível 81 - irreversível	88 - irreversível	180 - irreversível	Senha inválida - não tente novamente	Invalid pin. Contact card issuer
Excedidas tentativas de senha Saque	75 - reversível	75 - reversível	75 - reversível	106 - reversível	Excedidas tentativas de senha.contate a central do seu cartão	Invalid pin. Contact card issuer
Conta destino inválida ou inexistente	76 - irreversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Conta destino inválida - não tente novamente	Format error. Do not try again (invalid account)
Conta origem inválida ou inexistente	77 - irreversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Conta origem inválida - não tente novamente	Format error. Do not try again (invalid account)
Cartão novo sem desbloqueio Inclui cartão bloqueado pelo cliente no aplicativo (ecom, nfc)	78 - reversível	78 - reversível	57 - reversível	Sem código correspondente	Desbloqueie o cartão	Card not initialized
Cartão inválido (criptograma)	82 - irreversível	82 - irreversível	88 - irreversível	180 - irreversível	Erro no cartão – não tente novamente	Invalid card. Do not retryMaster/Hiper: invalid pin. Contact card issuerAmex: invalid pin. Contact card issuer
Emissor fora do ar	91 - reversível	91 - reversível	91 - reversível	912 - reversível	Falha de comunicação - tente mais tarde	Error. Retry transaction

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Falha do sistema	96 - reversível	96 - reversível	96 - reversível	911 - reversível	Falha de comunicação - tente mais tarde	Error. Retry transaction
Diferença - pré autorização	Sem código correspondente	N8 - irreversível	Sem código correspondente	Sem código correspondente	Valor diferente da pré autorização - não tente novamente	Format error. Do not retry (authorization amount differs)
Função incorreta (débito)	Ab - Reversível	52 - Reversível 53 - Reversível	Sem código correspondent	Sem código correspondent	Utilize função crédito	Not supported. Submit transaction as credit
Função incorreta (crédito)	Ac - Reversível	39 - Reversível	Sem código correspondente	Sem código correspondente	Utilize função débito	Not supported. Submit transaction as debit
Função incorreta (voucher)	AV - reversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Utilize função voucher	Not supported. Submit transaction as voucher.
Troca de senha Desbloqueio	P5 - irreversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Senha inválida - não tente novamente	Invalid pin. Contact card issuer
Nova senha não aceita	P6 - reversível	Sem código correspondente	55 - Reversível	Sem código correspondente	Senha inválida utilize a nova senha	Invalid pin. Contact card issuer
Recolher cartão	Sem código correspondente	4 - irreversível	4 - irreversível	Sem código correspondente	Contate a central do seu cartão - não tente novamente	Contact card issuer. Do not retry
Erro por mudança de chave dinâmica	Sem código correspondente	N7 - irreversível	Sem código correspondente	Sem código correspondente	Erro no cartão – não tente novamente	Invalid card. Do not retry
Fraude confirmada	57 - irreversível	7 - irreversível	4 - irreversível	200 - irreversível	Transação não permitida para o cartão - não tente novamente	Transaction not permitted to cardholder. Do not retryAmex:unauthorized transaction. Do not try again
Emissor não localizado - bin incorreto (negativa do adquirente)	Sem código correspondente	15 - irreversível	15 - irreversível	Sem código correspondente	Dados do cartão inválido - não tente novamente	Invalid card number. Do not retry

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Não cumprimento pelas leis de ante lavagem de dinheiro	Sem código correspondente	64 - irreversível	Sem código correspondente	Sem código correspondente	Contate a central do seu cartão - não tente novamente	Contact card issuer. Do not retry
Reversão inválida	Sem código correspondente	76 - irreversível	Sem código correspondente	Sem código correspondente	Contate a central do seu cartão - não tente novamente	Contact card issuer. Do not retry
Não localizado pelo roteador	Sem código correspondente	92 - irreversível	92 - irreversível	Sem código correspondente	Contate a central do seu cartão - não tente novamente	Contact card issuer. Do not retry
Transação negada por infração de lei	57 - irreversível	93 - irreversível	62 - irreversível	Sem código correspondente	Transação não permitida para o cartão - não tente novamente	Transaction not permitted to cardholder. Do not retry
Valor do tracing data duplicado	Sem código correspondente	94 - irreversível	94 - irreversível	Sem código correspondente	Contate a central do seu cartão - não tente novamente	Contact card issuer. Do not retry
Surcharge não suportado	Sem código correspondente	B1 - reversível	Sem código correspondente	Sem código correspondente	Contate a central do seu cartão	Please contact issuer
Surcharge não suportado pela rede de débito	Sem código correspondente	B2 - reversível	Sem código correspondente	Sem código correspondente	Contate a central do seu cartão	Please contact issuer
Forçar stip	Sem código correspondente	N0 - reversível	Sem código correspondente	Sem código correspondente	Contate a central do seu cartão	Please contact issuer
Saque não disponível	Sem código correspondente	N3 - irreversível	Sem código correspondente	Sem código correspondente	Saque não disponível - não tente novamente	Withdrawal not permitted. Do not retry
Suspensão de pagamento recorrente para um serviço	Sem código correspondente	R0 - irreversível	Sem código correspondente	Sem código correspondente	Suspensão de pagamento recorrente para serviço - não tente novamente	Recurring payment not permitted. Do not retry
Suspensão de pagamento recorrente para todos serviço	Sem código correspondente	R1 - irreversível	Sem código correspondente	Sem código correspondente	Suspensão de pagamento recorrente para serviço - não tente novamente	Recurring payment not permitted. Do not retry

Motivo	ELO	Visa	Master/Hiper	Amex	Mensagem	Mensagem E-commerce
Transação não qualificada para visa pin	Sem código correspondente	R2 - irreversível	Sem código correspondente	Sem código correspondente	Transação não permitida para o cartão - não tente novamente	Transaction not permitted to cardholder. Do not retry
Suspensão de todas as ordens de autorização	Sem código correspondente	R3 - irreversível	Sem código correspondente	Sem código correspondente	Suspensão de pagamento recorrente para serviço - não tente novamente	Recurring payment not permitted. Do not retry
Conta encerrada	46- Irreversível	46- Irreversível	62-irreversível	Sem código correspondente	Transação não permitida para o cartão - não tente novamente	Transaction not permitted to cardholder. Do not retry
Falha validação de id	Sem código correspondente	6P- Irreversível	Sem código correspondente	Sem código correspondente	Falha na verificação do id	Id validation failure
Utilizar o chip	FM- irreversível	Sem código correspondente	Sem código correspondente	Sem código correspondente	Utilize o chip	Use the chip
Segurança Fraude	79 - Irreversível (consultar MAC)	Sem código correspondente	Sem código correspondente	Sem código correspondente	Transação não autorizada	Unauthorized transaction

Outros Retornos

Os retornos abaixo são de uso exclusivo das bandeiras e não estão na dentro da Normativa 21 ABECS, mas podem ocorrer em casos que o emissor/bandeira aplicar.

Bandeira	Código	Mensagem	Mensagem e-commerce
Mastercard	1	Consultar o emissor do cartão	Please contact issuer
Mastercard	70	Entrar em contato com o emissor	Please contact issuer
Mastercard	76	“Para Conta” especificado Inválido/inexistente	Invalid account. Do not try again
Mastercard	77	“Da Conta” especificado Inválido/inexistente	Invalid account. Do not try again
Mastercard	78	Conta especificada inválida/ inexistente (geral)	Invalid account. Do not try again
Mastercard	84	Ciclo de Vida da Autorização Inválida	Invalid Authorization Lifecycle
Mastercard	89	Senha Inaceitável — Transação Recusada — Tente Novamente	Invalid PIN. Try again
Visa	1	Consulte emissor do cartão	Please contact issuer
Visa	2	Consulte emissor do cartão - condição especial	Please contact issuer
Visa	60	Falha na verificação [a identificação do titular do cartão não corresponde aos registros do emissor]"	Please contact issuer

Bandeira	Código	Mensagem	Mensagem e-commerce
Visa	62	Função não suportada. Não tente novamente.	Function not supported. Do not retry (domestic transaction only)
Visa	70	Senha requerida	PIN data required
Visa	80	Sem impacto financeiro	No financial impact
Visa	85	Não há motivo para recusar uma solicitação de verificação de endereço, verificação de CVV2 ou comprovante de crédito ou devolução de mercadoria	Please contact issuer
Visa	1A	Autenticação adicional do cliente necessária	Unauthorized transaction, try again
Visa	P5	Desbloqueio de PIN negado - alteração de PIN ou solicitação de desbloqueio recusada pelo emissor	Invalid PIN. Do not retry
Visa	P6	Alteração de PIN negada - PIN solicitado inseguro	Invalid PIN. Do not retry
Visa	5C	Transação não suportada/bloqueada pelo emissor	Unauthorized transaction, try again
Visa	9G	Bloqueado pelo portador/entre em contato com o portador	Unauthorized transaction, try again
Amex	107	Entre em contato com o emissor	Please contact issuer
Amex	111	Conta Inválida	Invalid Account
Amex	121	Limite excedido	Limit exceed
Amex	122	Código de segurança do cartão impresso com chave inválido (PCSC)	Format error. Verify card data
Amex	130	Autenticação forte necessária	Unauthorized transaction, try again
Amex	190	Incompatibilidade de Identificação Nacional	Unauthorized transaction. Do not try again
Amex	191	Referência de Voz	Please contact issuer
Amex	900	Conselho aceito	Please contact issuer

Em caso de infração nas diretrizes do programa de retentativas de bandeiras, a Rede apresentará um código de retorno de integração conforme a classificação da retentativa

1. Códigos de negativa – dentro do grupo brand (ABECS)

Código	Mensagem	Descrição	Como atuar
N01	Declined by Rede: Issuer will never approve	Recusado pela Rede: Emissor nunca aprovará	Analise os códigos de retorno das negativas, barre retentativas excessivas seja do portador ou de processos de cobrança automática e revise sua base de cartões armazenados
N02	Declined by Rede: Excessive Reattempts	Recusado pela Rede: Retentativas excessivas	
N03	Declined by Rede: Attention – verify your Data	Recusado pela Rede: Atenção – verifique seus dados	

Código	Mensagem	Descrição	Como atuar
N04	Declined by Rede: Subseller is not allowed to operate	Recusado pela Rede: Subseller não é autorizado para operar	Consulte a central de atendimento para avaliar a situação cadastral do subestabelecimento
N05	Declined by Rede: Policy. Merchant not allowed to operate.	Recusado pela Rede: Política Subseller não é autorizado para operar	
N06	Declined by Rede: High risk MCC not allowed to operate.	Recusado pela Rede: MCC de alto risco não é autorizado para operar.	Contate a Rede para obter mais informações sobre o programa de monitoramento de MCCs de alto risco.
N99	Declined by Rede: Contact us	Recusado pela Rede: Contate-nos	Contate a Rede pois algo na operação precisa ser revisado e avalie nossas Dicas de segurança

2. Retornos de emissor – fora do grupo brand (não ABECS)

Código	Mensagem	Descrição
124	Unauthorized. Contact Rede	Não autorizado, consulte a Rede.

Importante: Para perfeita visualização dos motivos de negativas da ferramenta Rede a utilização do código ABECS é necessária. Clique aqui para instruções de uso [Retornos da Bandeira](#).

Caso não seja feito o ajuste no campo custom header para habilitar os retornos no padrão ABECS, as transações serão respondidas apenas com o código de Retorno do emissor (124).

Para saber mais sobre o programa de retentativas e suas regras clique aqui [Tarifas de Bandeira](#).

Retornos da central do cartão

Os retornos da central do cartão são exibidos quando é obtida uma resposta de uma requisição de transação de crédito ou débito.

returnCode	returnMessage	Descrição
00	Success	Sucesso
101	Unauthorized. Problems on the card, contact the issuer.	Problemas no cartão, contate a central do cartão
102	Unauthorized. Check the situation of the store with the issuer.	Confirme a situação da loja com a central do cartão
103	Unauthorized. Please try again.	Não autorizado. Por favor, tente novamente.
104	Unauthorized. Please try again.	Não autorizado. Por favor, tente novamente.
105	Unauthorized. Restricted card.	Cartão restrito
106	Error in issuer processing. Please try again.	Erro no processamento. Tente novamente
107	Unauthorized. Please try again.	Por favor, tente novamente.
108	Unauthorized. Value not allowed for this type of card.	Valor não permitido para este tipo de cartão.
109	Unauthorized. Nonexistent card.	Cartão inexistente

returnCode	returnMessage	Descrição
110	Unauthorized. Transaction type not allowed for this card.	Tipo de transação não permitida para este cartão
111	Unauthorized. Insufficient funds.	Saldo insuficiente
112	Unauthorized. Expiry date expired.	Cartão expirado.
113	Unauthorized. Identified moderate risk by the issuer.	Emissor identificou risco moderado
114	Unauthorized. The card does not belong to the payment network.	O cartão não pertence a rede de pagamento
115	Unauthorized. Exceeded the limit of transactions allowed in the period.	Limite de transações permitidas no período foi excedido.
116	Unauthorized. Please contact the Card Issuer.	Por favor, contate a central do cartão.
117	Transaction not found.	Transação não encontrada.
118	Unauthorized. Card locked.	Cartão bloqueado.
119	Unauthorized. Invalid security code	Código de segurança inválido.
121	Error processing. Please try again.	Erro no processamento. Por favor, tente novamente.
122	Transaction previously sent	Transação enviada previamente.
123	Unauthorized. Bearer requested the end of the recurrences in the issuer.	Portador solicitou encerramento da recorrência na central do cartão.
124	Unauthorized. Contact Rede	Não autorizado. Contate a Rede.
170	Zero dollar transaction not allowed for this card.	Transação Zero Dollar não permitida para este cartão.
172	CVC2 required for Zero Dollar Transaction.	CVC2 exigido para transação Zero Dollar.
174	Zero dollar transaction success.	Transação Zero Dollar aprovada.
175	Zero dollar transaction denied.	Transação Zero Dollar negada.

Retornos de integração

Os retornos de integração são exibidos sempre que houver algo de errado na sua requisição, permitindo assim a correção imediata.

returnCode	returnMessage	Descrição
1	expirationYear: Invalid parameter size	Parâmetro enviado com tamanho inválido
2	expirationYear: Invalid parameter format	Formato do parâmetro inválido
3	expirationYear: Required parameter missing	Parâmetro obrigatório não está presente
4	cavv: Invalid parameter size	Parâmetro enviado com tamanho inválido
5	cavv: Invalid parameter format	Formato do parâmetro inválido

returnCode	returnMessage	Descrição
6	postalCode: Invalid parameter size	Parâmetro enviado com tamanho inválido
7	postalCode: Invalid parameter format	Formato do parâmetro inválido
8	postalCode: Required parameter missing	Parâmetro obrigatório não está presente
9	complement: Invalid parameter size	Parâmetro enviado com tamanho inválido
10	complement: Invalid parameter format	Formato do parâmetro inválido
11	departureTax: Invalid parameter format	Formato do parâmetro inválido
12	documentNumber: Invalid parameter size	Parâmetro enviado com tamanho inválido
13	documentNumber: Invalid parameter format	Formato do parâmetro inválido
14	documentNumber: Required parameter missing	Parâmetro obrigatório não está presente
15	securityCode: Invalid parameter size	Parâmetro enviado com tamanho inválido
16	securityCode: Invalid parameter format	Formato do parâmetro inválido
17	distributorAffiliation: Invalid parameter size	Parâmetro enviado com tamanho inválido
18	distributorAffiliation: Invalid parameter format	Formato do parâmetro inválido
19	xid: Invalid parameter size	Parâmetro enviado com tamanho inválido
20	eci: Invalid parameter format	Formato do parâmetro inválido
21	xid: Required parameter for Visa card is missing	Parâmetro obrigatório para Visa não está presente
22	street: Required parameter missing	Parâmetro obrigatório não está presente
23	street: Invalid parameter format	Formato do parâmetro inválido
24	affiliation: Invalid parameter size	Parâmetro enviado com tamanho inválido
25	affiliation: Invalid parameter format	Formato do parâmetro inválido
26	affiliation: Required parameter missing	Parâmetro obrigatório não está presente
27	Parameter cavv or eci missing	Parâmetro cavv ou eci não está presente
28	code: Invalid parameter size	Parâmetro enviado com tamanho inválido
29	code: Invalid parameter format	Formato do parâmetro inválido
30	code: Required parameter missing	Parâmetro obrigatório não está presente
31	softdescriptor: Invalid parameter size	Parâmetro enviado com tamanho inválido
32	softdescriptor: Invalid parameter format	Formato do parâmetro inválido
33	expirationMonth: Invalid parameter format	Formato do parâmetro inválido

returnCode	returnMessage	Descrição
34	code: Invalid parameter format	Formato do parâmetro inválido
35	expirationMonth: Required parameter missing	Parâmetro obrigatório não está presente
36	cardNumber: Invalid parameter size	Parâmetro enviado com tamanho inválido
37	cardNumber: Invalid parameter format	Formato do parâmetro inválido
38	cardNumber: Required parameter missing	Parâmetro obrigatório não está presente
39	reference: Invalid parameter size	Parâmetro enviado com tamanho inválido
40	reference: Invalid parameter format	Formato do parâmetro inválido
41	reference: Required parameter missing	Parâmetro obrigatório não está presente
42	reference: Order number already exists	Número de pedido já existente
43	number: Invalid parameter size	Parâmetro enviado com tamanho inválido
44	number: Invalid parameter format	Formato do parâmetro inválido
45	number: Required parameter missing	Parâmetro obrigatório não está presente
46	installments: Not correspond to authorization transaction	Quantidade de parcelas não corresponde com a transação autorizada
47	origin: Invalid parameter format	Formato do parâmetro inválido
48	brandTid: Invalid parameter size	Parâmetro enviado com tamanho inválido
49	The value of the transaction exceeds the authorized	O valor da transação excede o valor autorizado
50	installments: Invalid parameter format	Formato do parâmetro inválido
51	Product or service disabled for this merchant. Contact Rede	Produto ou serviço desabilitado para esse lojista. Contate a Rede
53	Transaction not allowed for the issuer. Contact Rede.	Transação não permitida para este emissor. Contate a Rede
54	installments: Parameter not allowed for this transaction	Parâmetro não permitido para esta transação
55	cardHolderName: Invalid parameter size	Parâmetro enviado com tamanho inválido
56	Error in reported data. Try again.	Erro nos dados reportados. Tente novamente
57	affiliation: Invalid merchant	Lojista inválido enviado no parâmetro
58	Unauthorized. Contact issuer.	Não autorizado. Contate a central do cartão
59	cardHolderName: Invalid parameter format	Formato do parâmetro inválido
60	street: Invalid parameter size	Parâmetro enviado com tamanho inválido
61	subscription: Invalid parameter format	Formato do parâmetro inválido

returnCode	returnMessage	Descrição
63	softdescriptor: Not enabled for this merchant	Produto não habilitado
64	Transaction not processed. Try again	Transação não processada. Tente novamente
65	token: Invalid token	Chave de integração não está presente
66	departureTax: Invalid parameter size	Parâmetro enviado com tamanho inválido
67	departureTax: Invalid parameter format	Formato do parâmetro inválido
68	departureTax: Required parameter missing	Parâmetro obrigatório não está presente
69	Transaction not allowed for this product or service.	Transação não permitida para este produto ou serviço
70	amount: Invalid parameter size	Parâmetro enviado com tamanho inválido
71	amount: Invalid parameter format	Formato do parâmetro inválido
72	Contact issuer.	Contate a central do cartão
73	amount: Required parameter missing	Parâmetro obrigatório não está presente
74	Communication failure. Try again	Falha na comunicação, tente novamente
75	departureTax: Parameter should not be sent for this type of transaction	Parâmetro não deve ser enviado para este tipo de transação
76	kind: Invalid parameter format	Formato do parâmetro inválido
78	Transaction does not exist	Transação não existe
79	Expired card. Transaction cannot be resubmitted. Contact issuer.	Cartão vencido. Não tente novamente e contate a central do cartão
80	Unauthorized. Contact issuer. (Insufficient funds)	Saldo insuficiente. Contate a central do cartão
82	Unauthorized transaction for debit card.	Transação não autorizada para cartão de débito
83	Unauthorized. Contact issuer.	Não autorizado. Contate a central do cartão
84	Unauthorized. Transaction cannot be resubmitted. Contact issuer.	Não autorizado. Não tente novamente e contate a central do cartão
85	complement: Invalid parameter size	Parâmetro enviado com tamanho inválido
86	Expired card	Cartão vencido
87	At least one of the following fields must be filled: tid or reference	Campo tid ou reference não está preenchido.
88	Merchant not approved. Regulate your website and contact the Rede to return to transact.	Lojista não aprovado. Regularize seu site e contate a Rede para voltar a transacionar.
89	token: Invalid token	Chave de integração inválida
97	tid: Invalid parameter size	Parâmetro enviado com tamanho inválido

returnCode	returnMessage	Descrição
98	tid: Invalid parameter format	Formato do parâmetro inválido
99	BusinessApplicationIdentifier: Invalid parameter format.	Formato do parâmetro inválido.
100	WalletId: Invalid parameter format.	Formato do parâmetro inválido.
132	DirectoryServerTransactionId: Invalid parameter size.	Parâmetro enviado com tamanho inválido
133	ThreedIndicator: Invalid parameter value.	Valor do parâmetro inválido
150	Timeout. Try again	Tempo esgotado. Tente novamente
151	installments: Greater than allowed	Valor do parâmetro maior do que o permitido
153	documentNumber: Invalid number	Valor do parâmetro inválido
154	embedded: Invalid parameter format	Formato do parâmetro inválido
155	eci: Required parameter missing	Parâmetro obrigatório não está presente
156	eci: Invalid parameter size	Parâmetro enviado com tamanho inválido
157	cavv: Required parameter missing	Parâmetro obrigatório não está presente
158	capture: Type not allowed for this transaction	Valor não permitido para esta transação
159	userAgent: Invalid parameter size	Parâmetro enviado com tamanho inválido
160	urls: Required parameter missing (kind)	Parâmetro obrigatório não está presente
161	urls: Invalid parameter format	Formato do parâmetro inválido
167	Invalid request JSON	Pedido JSON inválido
169	Invalid Content-Type	Content-Type inválido
171	Operation not allowed for this transaction	Operação não permitida para essa transação
173	Authorization expired	Autorização expirou
176	urls: Required parameter missing (url)	Parâmetro obrigatório não está presente
370	Request failed. Contact Rede	Pedido falhou. Contate a Rede
898	PV with invalid ip origin	PV com ip de origem inválido
899	Unsuccessful. Please contact Rede.	Sem sucesso. Por favor, contate a Rede
1002	Wallet Id: Invalid Parameter Size.	Parâmetro enviado com tamanho inválido
1003	Wallet Id: Required parameter missing.	Parâmetro obrigatório não está presente.
1018	MCC Invalid Size.	Parâmetro enviado com tamanho inválido
1019	MCC Parameter Required.	Parâmetro obrigatório não está presente

returnCode	returnMessage	Descrição
1020	MCC Invalid Format.	Formato do parâmetro inválido
1021	PaymentFacilitatorID Invalid Size.	Parâmetro enviado com tamanho inválido
1023	PaymentFacilitatorID Invalid Format.	Formato do parâmetro inválido
1027	SubMerchant: SubMerchantID Invalid Size.	Parâmetro enviado com tamanho inválido
1030	CitySubMerchant Invalid Size.	Parâmetro enviado com tamanho inválido
1032	SubMerchant: Estate Invalid Size.	Parâmetro enviado com tamanho inválido
1034	CountrySubMerchant Invalid Size.	Parâmetro enviado com tamanho inválido
1036	CepSubMerchant Invalid Size	Parâmetro enviado com tamanho inválido
1038	CnpjSubMerchant Invalid Size	Parâmetro enviado com tamanho inválido
3020	Cryptogram: Invalid parameter size.	Parâmetro enviado com tamanho inválido
3025	Deny Category 01: This card should not be used	Negativa de categoria 01: Este cartão não deve ser usado novamente
3026	Deny Category 02: This card should not be used in this PV	Negativa de categoria 02: Esse cartão não deve ser usado novamente nesse PV
3027	Deny Category 03: No cards must be used in this PV	Negativa de categoria 03: Esse cartão não deve ser usado novamente nesse PV
3028	Wallet Processing Type: Invalid Parameter Missing	Parâmetro obrigatório não está presente
3029	Wallet Processing Type: Invalid Parameter Size	Parâmetro enviado com tamanho inválido
3030	Wallet Processing Type: Invalid Parameter Format	Formato do parâmetro inválido
3031	Wallet Sender Tax Identification: Invalid Parameter Missing	Parâmetro obrigatório não está presente
3032	Wallet Sender Tax Identification: Invalid Parameter Size	Parâmetro enviado com tamanho inválido
3033	Wallet Sender Tax Identification: Invalid Parameter Format	Parâmetro enviado com tamanho inválido
3034	SubMerchant: Tax Identification Number Invalid Size.	Parâmetro enviado com tamanho inválido
3035	DSubMerchant: Tax Identification Number Invalid Format.	Formato do parâmetro inválido
3036	QrCode Expired.	QrCode expirado.
3052	Wallet Code: Required parameter missing.	Parâmetro obrigatório não está presente
3053	Wallet Code: Invalid Parameter format.	Formato do parâmetro inválido
3054	Wallet Code: Invalid Parameter size.	Parâmetro enviado com tamanho inválido
3055	Wallet Code: Parameter not allowed.	Parâmetro não permitido para esta transação
3056	Wallet Id: Parameter not allowed.	Parâmetro não permitido para esta transação

returnCode	returnMessage	Descrição
3064	Sai: Invalid parameter size.	Parâmetro enviado com tamanho inválido
3065	Sai: Invalid parameter format.	Formato do parâmetro inválido.
3066	Sai: Required parameter missing.	Parâmetro obrigatório não está presente.
3067	Cryptogram: Required parameter missing.	Parâmetro obrigatório não está presente.
3068	Credential Id: Required parameter missing.	Parâmetro obrigatório não está presente.
3069	Credential Id: Invalid parameter format.	Formato do parâmetro inválido
3070	Credential Id: Invalid parameter size.	Parâmetro enviado com tamanho inválido
3076	QrCode: Expiration Date parameter missing.	QrCode: Campo Expiration Date não foi informado.
3077	QrCode: Expiration Date Invalid parameter value.	QrCode: Campo Expiration Date enviado com valor inválido.
3078	QrCode: Expiration Date invalid format.	QrCode: Campo Expiration Date enviado em formato inválido.
3079	QrCode not processed. Try again.	QrCode não processado. Tente novamente.
3081	QrCode: Expiration Date invalid size.	QrCode: Campo Expiration Date enviado em tamanho inválido.
3084	Error generating QrCode Image. Please use the GET Transaction for this operation.	Erro na geração do campo qrCodeImage. Use a API de Consulta para obter essa informação, caso seja necessário.
3085	Error generating QrCode Image. Please try again	Erro na geração do campo qrCodeImage. Tente novamente.
3086	OrderId: Invalid parameter size.	Tamanho do parâmetro inválido.
3089	QRCode not generated, please contact Rede	Qr Code não gerado, contate a Rede.
3090	Invalid Pix Key	Chave Pix Inválida na geração de qrCode.
3091	Error, not generated. Try again	Erro na devolução, tente novamente.
3092	Fail QrCode generate, please try again;	Falha na geração de qrCode, tente novamente.
3094	Unsucessful. Please contact Rede.	Sem sucesso. Contate a Rede.
3095	Unknown Pix Key.	Chave Pix não cadastrada.
3096	Unsucessful. Try again later.	Sem sucesso. Tente novamente mais tarde.
3097	Unavailable. Please try again later.	Não disponível. Tente novamente mais tarde.
3098	Service not authorized	Serviço não autorizado.
3099	Communication failure. Try again later.	Falha na comunicação. Tente novamente mais tarde.

returnCode	returnMessage	Descrição
3100	Receiver Data Last Name: Invalid parameter format.	Formato do parâmetro inválido.
3101	Receiver Data Tax Id Number: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3102	Receiver Data Tax Id Number: Invalid parameter format.	Formato do parâmetro inválido.
3103	Receiver Data Wallet Account Identification: Invalid parameter size.	Parâmetro enviado com tamanho inválido
3104	Receiver Data Wallet Account Identification: Invalid parameter format.	Formato do parâmetro inválido.
3105	Payment Destination: Invalid parameter format.	Formato do parâmetro inválido.
3106	Payment Destination: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3107	Receiver Data: Required parameter missing.	Parâmetro obrigatório não está presente.
3108	Receiver Data First Name: Required parameter missing.	Parâmetro obrigatório não está presente.
3109	Receiver Data Last Name: Required parameter missing.	Parâmetro obrigatório não está presente.
3110	Receiver Data Tax Id Number: Required parameter missing.	Parâmetro obrigatório não está presente.
3111	Receiver Data Account Identification: Required parameter missing.	Parâmetro obrigatório não está presente.
3112	Payment Destination: Parameter not allowed.	Parâmetro não permitido para esta transação.
3113	Merchant Tax Id Invalid Size: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3114	Merchant Tax Id Invalid Format: Invalid parameter format.	Formato do parâmetro inválido.
3115	Receiver Data First Name: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3116	Receiver Data First Name: Invalid parameter format.	O Formato do parâmetro inválido.
3117	Receiver Data Last Name: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3118	Capture Expiration Hours: Invalid parameter format.	Formato do parâmetro inválido.
3119	Capture: Invalid parameter format.	Formato do parâmetro inválido
3120	Capture Expiration Hours: Invalid parameter size.	Parâmetro enviado com tamanho inválido.
3121	Invalid Amount.	
3122	Invalid Amount.	
3123	Devolution not confirmed.	O processo de devolução não foi concluído com sucesso. Por favor, repita a solicitação.
3125	Incorrect devolution data	Devolução negada por dados incorretos Revise os dados da transação e tente novamente.
3128	Devolution blocked	Devolução negada por bloqueio em conta junto a emissor, tente novamente.
3130	Sender Data: Invalid parameter format.	Formato do parâmetro inválido.

returnCode	returnMessage	Descrição
3131	Sender Data: Invalid parameter size.	Tamanho do parâmetro inválido.
3132	SubMerchant : Merchant Tax Id Name Invalid Size.	Tamanho do parâmetro inválido.
3133	SubMerchant: Merchant Tax Id Name Invalid Format.	Formato do parâmetro inválido.
3134	Sender firstName: invalid parameter format	Formato do parâmetro inválido.
3135	Sender firstName: invalid parameter size	Tamanho do parâmetro inválido.
3136	Sender lastName: invalid parameter format	Formato do parâmetro inválido.
3137	Sender lastName: invalid parameter size	Tamanho do parâmetro inválido.
3138	Sender address: invalid parameter format	Formato do parâmetro inválido.
3139	Sender address: invalid parameter size	Tamanho do parâmetro inválido.
3140	Sender city: invalid parameter format	Formato do parâmetro inválido.
3141	Sender city: invalid parameter size	Tamanho do parâmetro inválido.
3142	Sender country: invalid parameter format	Formato do parâmetro inválido.
3143	Sender country: invalid parameter size	Tamanho do parâmetro inválido.

Caso receba o retorno 370 em uma requisição de venda (captura automática ou pré), realize uma consulta por Reference para verificar a situação da sua transação. Caso ocorra o retorno 78 "Transaction does not exist", a transação deverá ser reenviada.

Retornos 3DS

As transações autenticadas possuem retornos e mensagens específicas.

returnCode	returnMessage	Descrição
200	Cardholder successfully authenticated	Autenticação realizada com sucesso
201	Authentication not required	Autenticação não exigida.
203	Authentication service not registered for the merchant. Please contact Rede	Serviço não habilitado. Por favor, contate a Rede
202	Unauthenticated cardholder	Portador não autenticado.
204	Cardholder not registered in the issuer's authentication program	Portador não registrado no programa de autenticação da central do cartão
220	Transaction request with authentication received. Redirect URL sent	Pedido de transação com autenticação recebida. URL de redirecionamento enviada.
250	onFailure: Required parameter missing	Parâmetro obrigatório não está presente.
251	onFailure: Invalid parameter format	Formato do parâmetro inválido

returnCode	returnMessage	Descrição
252	urls: Required parameter missing (url/threeDSecureFailure)	Parâmetro obrigatório não está presente.
253	urls: Invalid parameter size (url/threeDSecureFailure)	Parâmetro enviado com tamanho inválido
254	urls: Invalid parameter format (url/threeDSecureFailure)	Formato do parâmetro inválido
255	urls: Required parameter missing (url/threeDSecureSuccess)	Parâmetro obrigatório não está presente.
256	urls: Invalid parameter size (url/threeDSecureSuccess)	Parâmetro enviado com tamanho inválido
257	urls: Invalid parameter format (url/threeDSecureSuccess)	Formato do parâmetro inválido
258	userAgent: Required parameter missing	Parâmetro obrigatório não está presente.
259	urls: Required parameter missing	Parâmetro obrigatório não está presente.
260	urls: Required parameter missing (kind/threeDSecureFailure)	Parâmetro obrigatório não está presente.
261	urls: Required parameter missing (kind/threeDSecureSuccess)	Parâmetro obrigatório não está presente.
269	ChallengePreference: Invalid parameter format	ChallengePreference: Formato do parâmetro inválido
3000	ColorDepth: Required parameter missing	ColorDepth: Parâmetro obrigatório não está presente
3001	DeviceType3ds: Required parameter missing	DeviceType3ds: Parâmetro obrigatório não está presente
3002	JavaEnabled: Required parameter missing	JavaEnabled: Parâmetro obrigatório não está presente
3003	Language: Required parameter missing	Language: Parâmetro obrigatório não está presente
3004	TimeZoneOffset: Required parameter missing	TimeZoneOffset: Parâmetro obrigatório não está presente
3005	ScreenHeight: Required parameter missing	ScreenHeight: Parâmetro obrigatório não está presente
3006	ScreenWidth: Required parameter missing	ScreenWidth: Parâmetro obrigatório não está presente
3007	ColorDepth: Invalid parameter size	ColorDepth: Tamanho do parâmetro inválido
3008	DeviceType3ds: Invalid parameter size	DeviceType3ds: Tamanho do parâmetro inválido
3009	Language: Invalid parameter size	Language: Tamanho do parâmetro inválido
3010	TimeZoneOffset: Invalid parameter size	TimeZoneOffset: Tamanho do parâmetro inválido
3011	ScreenHeight: Invalid parameter size	ScreenHeight: Tamanho do parâmetro inválido
3012	ScreenWidth: Invalid parameter size	ScreenWidth: Formato do parâmetro inválido
3013	ColorDepth: Invalid parameter format	ColorDepth: Formato do parâmetro inválido
3014	DeviceType3ds: Invalid parameter format	DeviceType3ds: Formato do parâmetro inválido
3015	JavaEnabled: Invalid parameter format	JavaEnabled: Formato do parâmetro inválido
3016	Language: Invalid parameter format	Language: Formato do parâmetro inválido

returnCode	returnMessage	Descrição
3017	TimeZoneOffset: Invalid parameter format	TimeZoneOffset: Formato do parâmetro inválido
3018	ScreenHeight: Invalid parameter format	ScreenHeight: Formato do parâmetro inválido
3019	ScreenWidth: Invalid parameter format	ScreenWidth: Formato do parâmetro inválido

Retornos de cancelamento

As transações canceladas possuem retornos e mensagens específicas.

returnCode	returnMessage	Mensagem
351	Forbidden	Cancelamento não permitido
353	Transaction not found	Transação não encontrada
354	Transaction with period expired for refund	Período de estorno expirado
355	Transaction already canceled.	Transação já cancelada
357	Sum of amount refunds greater than the transaction amount	Soma dos valores de estorno supera o valor da transação
358	Sum of amount refunds greater than the value processed available for refund	Soma dos valores de estorno supera o valor processado disponível para estorno
359	Refund successful	Estorno realizado com sucesso.
360	Refund request has been successful	Pedido de estorno realizado com sucesso.
362	RefundId not found	RefundID não encontrado
363	Callback Url characters exceeded 500	Limite de caracteres da URL de Callback foi excedido
365	Partial refund not available.	Estorno parcial não disponível
368	Unsuccessful. Please try again	Sem sucesso. Por favor, tente novamente.
369	Refund not found	Estorno não encontrado
370	Request failed. Contact Rede	Pedido falhou. Contate a Rede
371	Transaction not available for refund. Try again in a few hours	Transação não disponível para estorno. Tente novamente em algumas horas
373	No further Refund allowed	Sem mais estornos permitidos
374	Refund not allowed. Chargeback requested	Estorno não permitido. Chargeback foi solicitado.

Atenção: Para o Código 360, lembre-se que a Rede recebeu seu cancelamento, mas é preciso consultá-lo novamente posteriormente para confirmar se ocorreu com sucesso.

Soluções de Tokenização

As soluções de tokenização de cartões permitem o armazenamento e tráfego seguro de dados sensíveis de cartão de crédito e débito, relacionando essas informações com um token.

Tipos de Tokenização

O e.Redé oferece os seguintes tipos de tokenização para o seu E-commerce:

Tipo de tokenização	Como funciona	Características	Bandeiras
Cofre de Cartões	Rede cria um token para o cartão (tokenizationId) através da integração do Estabelecimento Comercial na API de Cofre de Cartões da Rede. Esse campo pode ser usado para transacionar ao invés do uso do cartão.	É ideal para estabelecimentos que desejam uma integração mais simplificada. Os dados do cartão são criptografados no ambiente da Rede e não trafegam pelo servidor da loja no fluxo transacional, pois toda a comunicação é feita pelo tokenizationId gerado.	Todas as bandeiras de crédito e débito aceitas pelo e.Redé
Tokenização de Bandeira Rede	A loja integra com a tokenização convencional da Rede, que adicionalmente irá criar o token diretamente na bandeira.	A loja poderá armazenar tanto o token gerado pela Rede, quanto o token gerado pelas bandeiras. Nesse cenário, a geração de criptogramas será responsabilidade do estabelecimento.	Visa e Mastercard
Tokenização de Bandeira externa (captura)	A loja realiza a tokenização de cartões usando uma solução do mercado externa à Rede.	A loja é responsável por gerenciar o token do cartão, e a Rede será capaz de aceitar o token do cartão durante as transações.	Visa, Mastercard e Elo.

Cofre de Cartões

O Cofre de Cartões oferece mais segurança ao comprador e permite que o estabelecimento comercial armazene o cartão para compras futuras.

Com essa solução, os dados de pagamento, como número do cartão e validade, são enviados de forma segura diretamente para o sistema da Rede, sem trafegar pelo ambiente do e-commerce. Esses dados são armazenados de forma criptografada como um token. Assim, o Estabelecimento pode usar o token em compras futuras, sem precisar que o comprador insira novamente as informações de pagamento, proporcionando a experiência de "Card on File".

Benefícios

- O uso da solução Cofre de Cartões traz mais agilidade e segurança no processo de compra, possibilitando a compra com um clique;
- Possibilita que o Estabelecimento Comercial tenha a experiência Card on File;
- **Funcionalidade 2 em 1:** benefícios de token PCI e token de bandeira na mesma solução;
- Possibilita a geração de tokens de bandeira, com as vantagens abaixo:
 - Credenciais sempre atualizadas;
 - Aumento de conversão;
 - Aumento de segurança;
 - Flexibilidade na autorização.

Pontos importantes

- A solução Cofre de Cartões tem por padrão executar uma transação Zero Dollar, para validar se o cartão é válido, antes de armazená-lo. Essa é uma recomendação de todas as bandeiras e impacta positivamente na taxa de autorização do estabelecimento. Para entender o processo de ativação do produto Zero Dollar no seu Ponto de Venda e seus custos relacionados, acesse a seção [Zero Dollar](#).

Observação: Caso o Estabelecimento tente utilizar o Cofre de Cartões como canal para o Zero Dollar sem ter essa funcionalidade habilitada, o Zero Dollar não será efetuado. Isso poderá afetar negativamente a taxa de sucesso de tokenização; por isso, é imprescindível que a habilitação do Zero Dollar seja solicitada ao utilizar o Cofre de Cartões e a Tokenização de Bandeira da Rede.

- Caso seja de interesse do estabelecimento à não execução do Zero Dollar, basta enviar o parâmetro `embeddedZeroDollar = false`. Essa prática não é recomendada e pode afetar negativamente a taxa de aprovação das transações.
- Não armazene cartões sem o consentimento do portador.
- Não mantenha o armazenamento de cartões que estejam vinculados a qualquer tipo de fraude confirmada: ao receber uma notificação de suspeita de fraude, exclua o cartão relacionado à fraude da base de cartões.

Como contratar?

Antes de iniciar a integração com o produto, é necessário fazer a habilitação no portal logado da Rede “userede.com.br”. Basta acessar o menu vender online > e-Commerce > tokenização de bandeira e selecionar o PV de interesse. A contratação será efetivada em alguns instantes.

A contratação e utilização do produto Cofre de Cartões não gera custos adicionais para os clientes do e.Red.

Primeiros passos

O processo de solicitação de Tokenização do cartão realizado na Rede é feito em algumas etapas:

1. Primeiro, o usuário manda os dados do cartão para o Estabelecimento;
2. O Estabelecimento Comercial manda os dados do cartão que serão criptografados e salvos na base da Rede;
3. Após realizar a criptografia, o Estabelecimento Comercial recebe da Rede um identificador único daquele cartão (`tokenizationID`);
4. O Estabelecimento Comercial armazena o `tokenizationID` recebido da Rede, após isso, todos os pedidos transacionais serão feitos em cima desse `tokenizationID`.

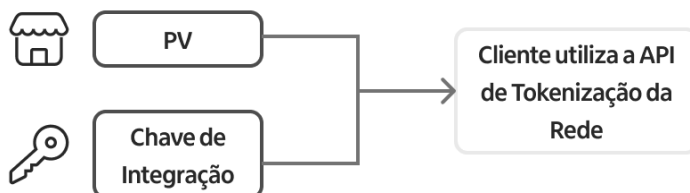
Autenticação da Rede via APIs

Atenção

Caso você seja um cliente que utiliza a API de Tokenização com a Rede e ainda utiliza o protocolo BASIC, entenda as mudanças. Antes, a autenticação era feita seguindo o protocolo BASIC e usando apenas PV e chave de integração gerada no [Portal Use Rede](#).

BASIC Authorization

PV + Chave de integração eRede



Agora, adotamos o modelo **OAuth 2.0**, que proporciona mais segurança para suas chamadas com a Rede. Por isso, precisamos adicionar mais uma etapa no processo de autenticação. Assim que as credenciais forem atualizadas, deve ser feito um novo chamado de endpoint para gerar o **access_token**, necessário para transacionar com o e.Red.

As APIs da Rede utilizam o protocolo de autenticação **OAuth 2.0**, um padrão da indústria para autorização e autenticação de aplicações. Esse protocolo foi projetado para simplificar o desenvolvimento de fluxos de autorização para aplicações web, desktop, smartphones e outros.

Passo a passo para integração OAuth 2.0

1. Obtenha as credenciais de acesso PV e Chave de Integração no [Portal Use Rede](#).

Com a utilização do protocolo **OAuth 2.0**, essas credenciais foram renomeadas para o novo padrão, conforme a tabela. Confira todas credenciais usadas em ambiente de desenvolvimento:

Portal Use Rede	Credencial para OAuth 2.0
PV	clientId
Chave de Integração	clientSecret
Token de acesso dinâmico	access_token

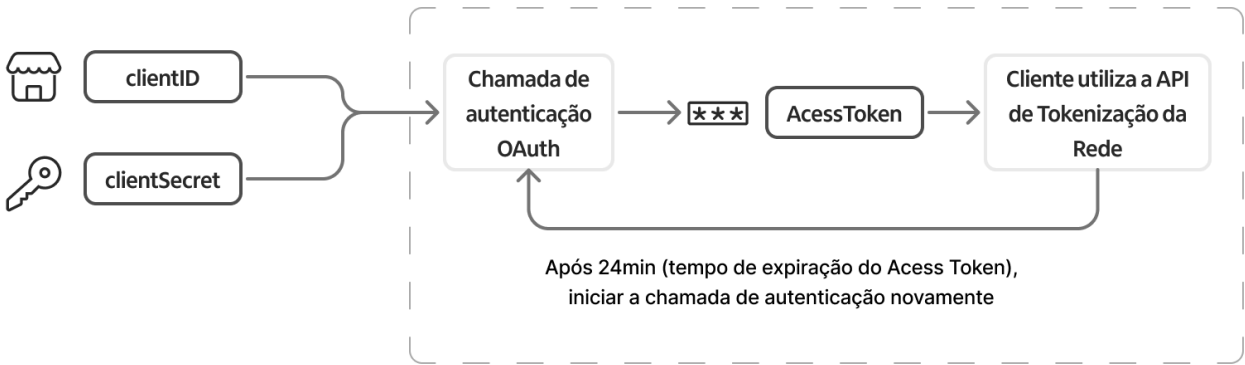
- 2. Com essas credenciais, faça uma chamada ao endpoint de autenticação: <https://api.userede.com.br/redelabs/oauth2/token>
- 3. Essa chamada gera uma **access_token**, que será usado para tokenizar com a Rede
- 4. O **access_token** deve ser armazenado de forma segura, evitando exposição ou uso indevido
- 5. O **access_token** tem validade de 24 minutos. Após esse período, é necessário fazer uma nova chamada ao endpoint para gerar um novo token

OAuth Authorization

OAuth Authorization

PV + Chave de integração eRede

Camada de autenticação OAuth



 **Informações sobre a Chave de Integração(clientSecret).**

Se você já possui uma Chave de integração, pode continuar usando a mesma.

Em caso de **perda ou esquecimento** da chave de integração, uma nova deverá ser gerada no [Portal Use Rede](#).

Para gerar a Chave, seu usuário precisa ter **perfil de administrador**. Acesse o menu: *e-commerce* > *chave de integração* e clique em **“Gerar chave de integração”**.

Se uma nova chave de integração for gerada, é necessário **atualizar imediatamente** no campo **clientSecret** da API para que o fluxo de tokenização se mantenha.

Como realizar autenticação no padrão OAuth 2.0

Endpoint de Autenticação

Ambiente	URL para gerar Token
Sandbox	https://rl7-sandbox-api.useredecloud.com.br/oauth2/token
Produção	https://api.userede.com.br/redelabs/oauth2/token

Autenticação

Gerar access_token

Com o **clientId** e o **clientSecret**, é possível gerar o token de acesso dinâmico utilizando a chamada:

```
curl --request POST \  
--url '{urlToken}' \  
--header 'Authorization: Basic Base64(clientId:clientSecret)' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data grant_type=client_credentials
```

Headers:

Parâmetro	Obrigatório	Descrição
Authorization	<input checked="" type="checkbox"/>	Junte o client_id e o client_secret com dois-pontos (:) e converta o resultado para base64
Content-Type	<input checked="" type="checkbox"/>	application/x-www-form-urlencoded

Form:

Parâmetro	Obrigatório	Descrição
grant_type	<input checked="" type="checkbox"/>	Tipo de geração do token, com o valor fixo “client_credentials”

Response:

Parâmetro	Obrigatório	Descrição
access_token	<input checked="" type="checkbox"/>	Token usado para chamar as APIs da Rede, com duração padrão de 24 minutos
token_type	<input checked="" type="checkbox"/>	Tipo do token gerado, padrão é "Bearer"
expires_in	<input checked="" type="checkbox"/>	Tempo de expiração em segundos do access_token
scope	<input checked="" type="checkbox"/>	Lista de escopos separados por espaço, representando os acessos concedidos à aplicação

Tokenização

Utilizar o Token de acesso

Para utilizar a API de Tokenização da Rede, você deve:

1. Ter uma access_token gerado, para ser usado nas APIs de negócio
2. Atualizar o access_token gerado anteriormente

 **Header**

Authorization: Bearer {access_token}.

Atenção

O **access_token** deve ser armazenado com segurança.

Como sua duração é de 24 minutos, uma nova chamada deverá ser feita antes desse período para atualizar a credencial.

O token de acesso tem validade de 24 minutos e pode ser reutilizado durante esse período. Para evitar expiração, recomenda-se renová-lo entre 15 e 23 minutos após a emissão.

A escolha de como realizar o chamado e atualizar os **access_token** gerados ficam sob sua responsabilidade.

Codificação OAuth

UTF8

Configure sua aplicação para usar codificação UTF-8.

Codificação de URL

A codificação URL é usada para codificar informações em URIs e usada também para dados do tipo application/x-www-form-urlencoded, como em formulários HTML.

JSON

JSON é o padrão usado para troca de dados entre sistemas. Para chamadas POST e PUT, é necessário especificar o cabeçalho:

Content-Type: application/json

Boas práticas de segurança

- Armazene o **access_token** em cache seguro e criptografado
- Evite expor o token em logs ou interfaces públicas
- Implemente controle de acesso para uso do token
- Utilize HTTPS em todas as chamadas às APIs da Rede

Solicitação de tokenização

Envio de solicitação de tokenização do cartão para a bandeira:

POST: </token-service/oauth/v2/tokenization>

Parâmetros da requisição:

O corpo da requisição (body) deve estar em formato JSON contendo os campos descritos na tabela abaixo:

Nome	Tamanho	Tipo	Obrigatório	Descrição
email	Até 200	Alfanumérico	Sim	E-mail do portador do cartão, cliente ou estabelecimento comercial
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão
expirationMonth	2	Alfanumérico	Sim	Mês de vencimento do cartão (entre "01" e "12")
expirationYear	4	Alfanumérico	Sim	Ano de vencimento do cartão
cardholderName	Até 200	Alfanumérico	Não	Nome do portador impresso no cartão
securityCode	Até 4	Alfanumérico	Não	Código de segurança localizado no verso do cartão
storageCard	Até 2	Numérico	Sim	Indica operações que possam ou não estar utilizando COF (Card on File): 0 - Transação com credencial não armazenada. 2 - Transação com credencial já armazenada. Para transações tokenizadas este parâmetro deve ter o valor "2".
kind	-	Alfanumérico	Não	Tipo de transação a ser realizada: <ul style="list-style-type: none">• Para transações de crédito, utilizar credit• Para transações de débito, utilizar debit O não envio desse campo será considerado crédito.
embeddedZeroDollar	-	Booleano	Não	Ao armazenar um cartão é obrigatório se fizer o zero dollar, portanto é recomendado que seja enviado true. Caso o cartão já tenha sido armazenado previamente e o estabelecimento não tiver o cvv, pode ser enviado false, para que o zero dollar não seja feito. Caso o campo não seja enviado, o zero dollar será feito.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Identificador único da solicitação de tokenização do cartão pela Rede

Cadastro da URL para receber as atualizações do token via webhook

Após a contratação do produto de Cofre de Cartões no portal "userede.com.br", será possível cadastrar a URL para receber as atualizações do token via webhook. Basta acessar o menu vender online > e-Commerce > tokenização de bandeira > cadastro de url e fazer o cadastro.

IMPORTANTE: Caso a url de notificações não seja informada, nenhum evento será entregue durante o processo de tokenização. Além disso, a Rede não se responsabiliza pelo cadastro de URLs inválidas por parte do estabelecimento.

URLs Autenticadas e Não Autenticadas

A REDE deve ser informada durante o cadastro se a URL possui autenticação ou não.

- URL Sem Autenticação:

Neste caso a Rede não fará nenhum tipo de verificação de segurança antes de entregar o evento na url informada.

- URL Com Autenticação:

A Rede possibilita a utilização de autenticação basic ou bearer e em ambos os casos o token de acesso deve ser cadastrado no portal, no momento do cadastro da url.

Ponto de Atenção:

A URL cadastrada será utilizada para todos os PVs cadastrados no mesmo CNPJ.

Callback realizado pelo webhook

Após a realização da solicitação de tokenização, assim que a criação do token de bandeira for finalizada, o cliente receberá um evento em uma URL previamente cadastrada no [Portal da Rede](#).

Além disso, eventos também serão enviados quando houver alguma atualização no token, como por exemplo, se ele for excluído devido ao cancelamento do cartão. Ou então, caso o cartão original seja atualizado, todas essas atualizações serão informadas ao Estabelecimento Comercial através desse webhook.

As tentativas de notificações de evento são de 12 vezes a cada 30 segundos, após isso é tentado de 1 em 1 hora por 14 dias.

Após o recebimento do evento é essencial que o estabelecimento faça uma consulta daquele token, para identificar qual foi a atualização sofrida. Não será informado no evento a atualização.

Nota: No ambiente sandbox, esse callback será realizado 2 minutos após o envio da solicitação de tokenização.

Os parâmetros recebidos no evento serão:

Nome	Local de envio	Tamanho	Tipo	Descrição
Authorization	header	Até 3	Alfanumérico	Header para autorização da requisição na url fornecida pelo estabelecimento através do portal logado.
Request-ID	header	Até 36	Alfanumérico	Identificador único da requisição
Content-Type	header	-	Alfanumérico	Valor fixo definido como 'application/json'
id	body	6	Alfanumérico	Identificador único do callback
merchantId	body	9	Alfanumérico	Número de filiação do estabelecimento (PV)
events	body	-	Lista Alfanumérica	Nome dos eventos que serão informados ao cliente. Exemplo: ["PV.TOKENIZACAO-BANDEIRA"]
data/tokenizationId	body	Até 36	Alfanumérico	Token do cartão

Exemplo do evento:

```
{
  "id": "123456",
  "merchant_id": "123415678",
  "events": [ "PV.TOKENIZACAO-BANDEIRA" ],
  "data": {
    "tokenizationId": "0c299dab-2b7a-41a1-8514-e54f9dd18297"
  }
}
```

Consulta do token

A consulta à solicitação de tokenização pode ser feita logo após a obtenção do tokenizationId da Rede (o token de bandeira é gerado de maneira assíncrona, dessa forma, a consulta deve ser feita somente após o recebimento do evento), que será sempre realizada quando o Estabelecimento Comercial receber um evento pelo webhook, permitindo verificar o status da solicitação e demais informações listadas abaixo.

Requisição para a consulta dos dados da solicitação de tokenização:

```
GET: /token-service/oauth/v2/tokenization/{tokenizationId}
```

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV)
tokenizationId	36	Alfanumérico	Token do cartão

Nome	Tamanho	Tipo	Descrição
tokenizationStatus	-	Alfanumérico	Status da solicitação de tokenização da Rede: <ul style="list-style-type: none"> • Pending • Active • Inactive • Suspended • Failed • Delete
brand/name	-	Alfanumérico	Nome da bandeira do BIN do cartão enviado na solicitação de tokenização
brand/message	Até 256	Alfanumérico	Mensagem de retorno da bandeira em caso de falha na solicitação do token para um determinado cartão. O tokenizationStatus nesse cenário será Failed e as informações de token não estarão disponíveis
brand/tokenStatus	Até 30	Alfanumérico	Status da solicitação de tokenização da bandeira: <ul style="list-style-type: none"> • Pending • Active • Inactive • Suspended • Failed • Delete
brand/brandTid	Até 21	Alfanumérico	Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file
lastModifiedDate	-	Datetime	Data da última atualização do registro no formato YYYY-MM-DDThh:mm:ssTZD
bin	Até 9	Alfanumérico	2 a 9 primeiros dígitos do cartão
last4	4	Alfanumérico	4 últimos dígitos do cartão
token/code	Até 16	Numérico	Número do token do cartão descriptografado, gerado pela bandeira
token/expirationDate	7	Alfanumérico	Data de expiração (no formato MM/YYYY) do token gerado pela bandeira para o cartão enviado

Gestão do token

Após a criação do token é possível gerenciar o status dele. Isto é, o estabelecimento tem autonomia para deletar, suspender e reativar os tokens sob sua responsabilidade.

PUT: </token-service/oauth/v2/tokenization/{tokenizationId}>

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
tokenizationStatus	100	Alfanumérico	Sim	Se o status atualizado para qual o do token for deletar, será o delete : Se o status atualizado para qual o do token for suspender, será o suspend Se o status atualizado para qual o do token for reativar, será o resume
reason	2	Númérico	Sim	Motivo da atualização: 1 - Solicitação do Cliente 2 - Suspeita de Fraude

Parâmetros da Resposta:

Caso a alteração do token ocorra com sucesso os seguintes campos serão retornados:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Token do cartão, que deve ser armazenado e utilizado em futuras transações
Brand/name*	-	Alfanumérico	Nome da bandeira. Ex: Visa
Brand/message*	-	Alfanumérico	Mensagem de erro da bandeira. Ex: Card not allowed. *Esse campo só é retornado em caso de erro na tokenização de bandeira

Gerando transações com uso de Tokens

Após a criação do token (tokenizationId), é possível criar transações, onde esse parâmetro irá substituir algumas informações transacionais.

URL de ambientes transacionais:

Ambiente	URL
Sandbox	https://sandbox-eredede.useredecloud.com.br/v2/transactions
Produção	https://api.userede.com.br/eredede/v2/transactions

Para acionar o produto de Cofre de Cartões na API transacional do e.Redde, faça a troca dos campos base abaixo:

Nome	Tamanho	Tipo	Obrigatório	Descrição
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão.
expirationMonth	Até 2	Númérico	Sim	Mês de vencimento do cartão. De 1 a 12.

Nome	Tamanho	Tipo	Obrigatório	Descrição
expirationYear	2 ou 4	Numérico	Sim	Ano de vencimento do cartão. Ex.: 2028 ou 28

Pelo novo campo indicativo de uso do nosso produto de Cofre de Cartões:

Nome	Tamanho	Tipo	Obrigatório	Descrição
cardToken	Até 64	Alfanumérico	Sim	Valor de referência para o cartão tokenizado (tokenizationID)

IMPORTANTE: Ao utilizar o parâmetro “cardToken” não é necessário fazer a solicitação do criptograma antes de solicitar a transação. Para informações sobre os parâmetros necessários em cada modelo de transação com token, acesse a seção [Tipos de Tokenização](#)

Exemplo de parâmetros de requisição para uma transação com token:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	-	Booleano	Não	Defina se uma transação terá captura automática ou posterior. O não envio desse campo será considerado uma captura automática (true).
kind	-	Alfanumérico	Não	Tipo de transação a ser realizada. <ul style="list-style-type: none">• Para transações de crédito, utilizar credit• Para transações de débito, utilizar debit O não envio desse campo será considerado credit .
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Valor total da transação sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
installments	Até 2	Numérico	Não	Número de parcelas em que uma transação será autorizada. De 2 a 12 O não envio desse campo será considerado à vista.
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão.
cardToken	Até 64	Alfanumérico	Sim	Valor de referência para o cartão tokenizado (tokenizationID).
softDescriptor	Até 13	Alfanumérico	Não	Frase personalizada que será impressa na fatura do portador.

Nome	Tamanho	Tipo	Obrigatório	Descrição
subscription	-	Booleano	Não	Informa ao emissor se a transação é proveniente de uma recorrência. Se transação for uma recorrência, enviar true. Caso contrário, enviar false. O não envio desse campo será considerado o valor false. A Rede não gerencia os agendamentos de recorrência, apenas permite aos lojistas indicarem se a transação originada é de um plano recorrente.
storageCard	Até 1	Alfanumérico	Não	Indica operações que possam ou não estar utilizando COF (Card on File): 0 - Transação com credencial não armazenada. 1 - Transação com credencial armazenada pela primeira vez. 2 - Transação com credencial já armazenada. Para transações tokenizadas este parâmetro deve ter o valor "2". Atenção: O não envio desse campo será considerado 0 (credencial não armazenada).
transactionCredentials				Grupo transactionCredentials
transactionCredentials/ credentialId	Até 02	Alfanumérico	Sim, se storageCard=1 ou =2 e cartão mastercard	Indica a categoria da transação com credencial armazenada. Consulte a seção "Categorização de transações card-on-file" para mais detalhes

IMPORTANTE: A prioridade da Rede será sempre autorizar com o token de bandeira, ou seja, se a geração do token de bandeira foi feita com sucesso, ele será priorizado na autorização. Os dados do cartão original só serão utilizados, quando o token de bandeira não estiver disponível.

Notas: 1.Para informações sobre autenticação, autorização e configurações na API transacional da Rede acesse a seção [Autenticação e Autorização](#).

2.Para mais combinações transacionais confira a seção [Sobre](#).

Tokenização de Bandeira Rede

O serviço de Tokenização de Bandeira protege as informações do cartão substituindo-as por um token. Cada token é único para o usuário e estabelecimento e não pode ser usado por nenhuma outra loja.

Essa funcionalidade está disponível para crédito e débito, para as bandeiras Visa e Mastercard.

Benefícios

- A tokenização do cartão garante a proteção dos dados reais, visto que substitui o número do cartão por um número aleatório, denominado token de bandeira.
- Em caso de vazamento de dados, os cartões de seus clientes permanecem seguros, visto que os tokens só podem ser utilizados dentro do seu estabelecimento.
- Além disso, é uma funcionalidade que garante a conformidade com as normas de regulamentação previstas em lei como a LGPD e PCI DSS (Data Security Standard).

Como contratar?

Antes de iniciar a integração com o produto é necessário fazer a habilitação no portal logado da Rede “userede.com.br”. Basta acessar o menu vender online > e-Commerce > tokenização de bandeira e selecionar o PV de interesse. A contratação será efetivada em alguns instantes.

A contratação e utilização do produto Tokenização de Bandeira não gera custos adicionais para os clientes do e.Red.

Primeiros passos

O processo de solicitação de Tokenização do cartão realizado na Rede é feito em algumas etapas:

- 1.** Primeiro o usuário manda os dados do cartão para o Estabelecimento;
- 2.** O Estabelecimento Comercial manda os dados enviados para a bandeira e recebe uma resposta com um identificador único daquela solicitação (tokenizationId);
- 3.** Em seguida (num processo assíncrono), a bandeira enviará as informações do token que serão atualizadas no registro, possibilitando a consulta delas pelo portador.

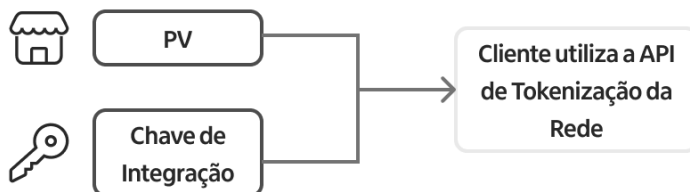
Autenticação da Rede via APIs

Atenção

Caso você seja um cliente que utiliza a API de Tokenização com a Rede e ainda utiliza o protocolo BASIC, entenda as mudanças. Antes, a autenticação era feita seguindo o protocolo BASIC e usando apenas PV e chave de integração gerada no [Portal Use Rede](#).

BASIC Authorization

PV + Chave de integração eRede



Agora, adotamos o modelo **OAuth 2.0**, que proporciona mais segurança para suas chamadas com a Rede. Por isso, precisamos adicionar mais uma etapa no processo de autenticação. Assim que as credenciais forem atualizadas, deve ser feito um novo chamado de endpoint para gerar o **access_token**, necessário para transacionar com o e.Red.

As APIs da Rede utilizam o protocolo de autenticação **OAuth 2.0**, um padrão da indústria para autorização e autenticação de aplicações. Esse protocolo foi projetado para simplificar o desenvolvimento de fluxos de autorização para aplicações web, desktop, smartphones e outros.

Passo a passo para integração OAuth 2.0

1. Obtenha as credenciais de acesso PV e Chave de Integração no [Portal Use Rede](#).

Com a utilização do protocolo **OAuth 2.0**, essas credenciais foram renomeadas para o novo padrão, conforme a tabela. Confira todas credenciais usadas em ambiente de desenvolvimento:

Portal Use Rede	Credencial para OAuth 2.0
PV	clientId
Chave de Integração	clientSecret
Token de acesso dinâmico	access_token

2. Com essas credenciais, faça uma chamada ao endpoint de autenticação: <https://api.userede.com.br/redelabs/oauth2/token>

3. Essa chamada gera uma **access_token**, que será usado para tokenizar com a Rede

4. O **access_token** deve ser armazenado de forma segura, evitando exposição ou uso indevido

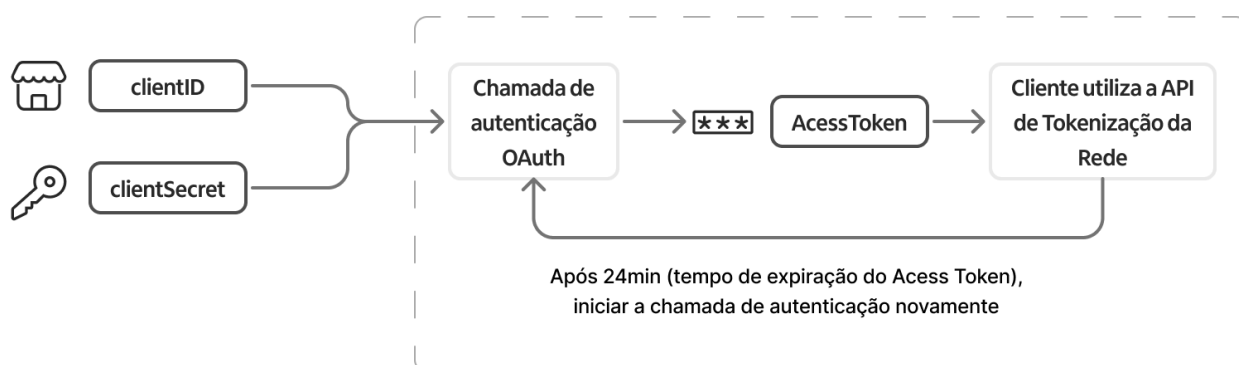
5. O **access_token** tem validade de 24 minutos. Após esse período, é necessário fazer uma nova chamada ao endpoint para gerar um novo token

OAuth Authorization

OAuth Authorization

PV + Chave de integração eRede

Camada de autenticação OAuth



Informações sobre a Chave de Integração(clientSecret).

Se você já possui uma Chave de integração, pode continuar usando a mesma.

Em caso de **perda ou esquecimento** da chave de integração, uma nova deverá ser gerada no [Portal Use Rede](#).

Para gerar a Chave, seu usuário precisa ter **perfil de administrador**. Acesse o menu: *e-commerce* > *chave de integração* e clique em **“Gerar chave de integração”**.

Se uma nova chave de integração for gerada, é necessário **atualizar imediatamente** no campo **clientSecret** da API para que o fluxo de tokenização se mantenha.

Como realizar autenticação no padrão OAuth 2.0

Endpoint de Autenticação

Ambiente	URL para gerar Token
Sandbox	https://rl7-sandbox-api.useredecloud.com.br/oauth2/token
Produção	https://api.userede.com.br/redelabs/oauth2/token

Autenticação

Gerar access_token

Com o **clientId** e o **clientSecret**, é possível gerar o token de acesso dinâmico utilizando a chamada:

```
curl --request POST \
--url '{urlToken}' \
--header 'Authorization: Basic Base64(clientId:clientSecret)' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data grant_type=client_credentials
```

Headers:

Parâmetro	Obrigatório	Descrição
Authorization	<input checked="" type="checkbox"/>	Junte o client_id e o client_secret com dois-pontos (:) e converta o resultado para base64
Content-Type	<input checked="" type="checkbox"/>	application/x-www-form-urlencoded

Form:

Parâmetro	Obrigatório	Descrição
grant_type	<input checked="" type="checkbox"/>	Tipo de geração do token, com o valor fixo "client_credentials"

Response:

Parâmetro	Obrigatório	Descrição
access_token	<input checked="" type="checkbox"/>	Token usado para chamar as APIs da Rede, com duração padrão de 24 minutos
token_type	<input checked="" type="checkbox"/>	Tipo do token gerado, padrão é "Bearer"
expires_in	<input checked="" type="checkbox"/>	Tempo de expiração em segundos do access_token
scope	<input checked="" type="checkbox"/>	Lista de escopos separados por espaço, representando os acessos concedidos à aplicação

Tokenização

Utilizar o Token de acesso

Para utilizar a API de Tokenização da Rede, você deve:

1. Ter uma `access_token` gerado, para ser usado nas APIs de negócio
2. Atualizar o `access_token` gerado anteriormente

Header

Authorization: Bearer {access_token}.

Atenção

O **access_token** deve ser armazenado com segurança.

Como sua duração é de 24 minutos, uma nova chamada deverá ser feita antes desse período para atualizar a credencial.

O token de acesso tem validade de 24 minutos e pode ser reutilizado durante esse período. Para evitar expiração, recomenda-se renová-lo entre 15 e 23 minutos após a emissão.

A escolha de como realizar o chamado e atualizar os **access_token** gerados ficam sob sua responsabilidade.

Codificação OAuth

UTF8

Configure sua aplicação para usar codificação UTF-8.

Codificação de URL

A codificação URL é usada para codificar informações em URIs e usada também para dados do tipo `application/x-www-form-urlencoded`, como em formulários HTML.

JSON

JSON é o padrão usado para troca de dados entre sistemas. Para chamadas POST e PUT, é necessário especificar o cabeçalho:

```
Content-Type: application/json
```

Boas práticas de segurança

- Armazene o **access_token** em cache seguro e criptografado
- Evite expor o token em logs ou interfaces públicas
- Implemente controle de acesso para uso do token
- Utilize HTTPS em todas as chamadas às APIs da Rede

Solicitação de tokenização

Envio de solicitação de tokenização do cartão para a bandeira:

POST: </token-service/oauth/v2/tokenization>

Parâmetros da requisição:

O corpo da requisição (body) deve estar em formato JSON contendo os campos descritos na tabela abaixo:

Nome	Tamanho	Tipo	Obrigatório	Descrição
email	Até 200	Alfanumérico	Sim	E-mail do portador do cartão, cliente ou estabelecimento comercial
cardNumber	Até 19	Alfanumérico	Sim	Número do cartão
expirationMonth	2	Alfanumérico	Sim	Mês de vencimento do cartão (entre "01" e "12")
expirationYear	4	Alfanumérico	Sim	Ano de vencimento do cartão
cardholderName	Até 200	Alfanumérico	Não	Nome do portador impresso no cartão
securityCode	Até 4	Alfanumérico	Não	Código de segurança localizado no verso do cartão
storageCard	Até 2	Numérico	Sim	Indica operações que possam ou não estar utilizando COF (Card on File): 0 - Transação com credencial não armazenada. 2 - Transação com credencial já armazenada. Para transações tokenizadas este parâmetro deve ter o valor "2".
kind	-	Alfanumérico	Não	Tipo de transação a ser realizada: <ul style="list-style-type: none">Para transações de crédito, utilizar creditPara transações de débito, utilizar debit O não envio desse campo será considerado crédito.
embeddedZeroDollar	-	Booleano	Não	Ao armazenar um cartão é obrigatório se fizer o zero dollar, portanto é recomendado que seja enviado true. Caso o cartão já tenha sido armazenado previamente e o estabelecimento não tiver o cvv, pode ser enviado false, para que o zero dollar não seja feito. Caso o campo não seja enviado, o zero dollar será feito.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Identificador único da solicitação de tokenização do cartão pela Rede

Cadastro da URL para receber as atualizações do token via webhook

Após a contratação do serviço de tokenização de bandeira no portal "userede.com.br", será possível cadastrar a URL para receber as atualizações do token via webhook. Basta acessar o menu vender online > e-Commerce > tokenização de bandeira > cadastro de url e fazer o cadastro.

IMPORTANTE: Caso a url de notificações não seja informada, nenhum evento será entregue durante o processo de tokenização. Além disso, a Rede não se responsabiliza pelo cadastro de URLs inválidas por parte do estabelecimento.

URLs Autenticadas e Não Autenticadas

A REDE deve ser informada durante o cadastro se a URL possui autenticação ou não.

- URL Sem Autenticação:

Neste caso a Rede não fará nenhum tipo de verificação de segurança antes de entregar o evento na url informada.

- URL Com Autenticação:

A Rede possibilita a utilização de autenticação basic ou bearer e em ambos os casos o token de acesso deve ser cadastrado no portal, no momento do cadastro da url.

Ponto de Atenção:

A URL cadastrada será utilizada para todos os PVs cadastrados no mesmo CNPJ.

Callback realizado pelo webhook

Após a solicitação de tokenização do cartão, quando a bandeira finalizar a geração do token, será enviado um evento para a url cadastrada no portal da Rede.

Eventos também serão enviados quando houver alguma atualização no token, como por exemplo, se ele for excluído devido ao cancelamento do cartão. Ou então, caso o cartão original seja atualizado.

As tentativas de notificações de evento são de 12 vezes a cada 30 segundos, após isso é tentado de 1 em 1 hora por 14 dias.

Após o recebimento do evento é essencial que o estabelecimento faça uma consulta daquele token, para identificar qual foi a atualização sofrida. Não será informado no evento a atualização.

Nota: No ambiente sandbox, esse callback será realizado 2 minutos após o envio da solicitação de tokenização.

Os parâmetros recebidos no evento serão:

Nome	Local de envio	Tamanho	Tipo	Descrição
authorization	header	Até 3	Alfanumérico	Header para autorização da requisição na url fornecida pelo estabelecimento através do portal logado.
request-ID	header	Até 36	Alfanumérico	Identificador único da requisição
content-Type	header	-	Alfanumérico	Valor fixo definido como 'application/json'
id	body	6	Alfanumérico	Identificador único do callback
merchantId	body	9	Alfanumérico	Número de filiação do estabelecimento (PV)

Nome	Local de envio	Tamanho	Tipo	Descrição
events	body	-	Lista alfanumérica	Nome dos eventos que serão informados ao cliente. Exemplo: ["PV.TOKENIZACAO-BANDEIRA"]
data/tokenizationId	body	Até 36	Alfanumérico	Token do cartão

Exemplo do evento:

```
{
  "id": "123456",
  "merchant_id": "123415678",
  "events": [ "PV.TOKENIZACAO-BANDEIRA" ],
  "data": {
    "tokenizationId": "0c299dab-2b7a-41a1-8514-e54f9dd18297"
  }
}
```

Consulta do token

A consulta à solicitação de tokenização pode ser feita logo após a obtenção do tokenizationId da Rede será sempre realizada quando o Estabelecimento Comercial receber um evento pelo webhook, onde será possível ver o status da solicitação e demais informações listadas abaixo.

Requisição para a consulta dos dados da solicitação de tokenização:

```
GET: /token-service/oauth/v2/tokenization/{tokenizationId}
```

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
affiliation	Até 9	Numérico	Número de filiação do estabelecimento (PV)
tokenizationId	36	Alfanumérico	Token do cartão
tokenizationStatus	-	Alfanumérico	Status da solicitação de tokenização: <ul style="list-style-type: none">PendingActiveInactiveSuspendedFailedDelete
brand/name	-	Alfanumérico	Nome da bandeira do BIN do cartão enviado na solicitação de tokenização

Nome	Tamanho	Tipo	Descrição
brand/message	Até 256	Alfanumérico	Mensagem de retorno da bandeira em caso de falha na solicitação do token para um determinado cartão. O tokenizationStatus nesse cenário será Failed e as informações de token não estarão disponíveis
brand/brandTid	Até 21	Alfanumérico	Correlaciona a primeira e demais transações através do envio deste campo. Para mais detalhes consulte a seção Recorrência e Card-on-file
lastModifiedDate	-	Datetime	Data da última atualização do registro no formato YYYY-MM-DDThh:mm:ssTZD
bin	Até 9	Alfanumérico	2 a 9 primeiros dígitos do cartão
last4	4	Alfanumérico	4 últimos dígitos do cartão
token/code	Até 16	Numérico	Número do token do cartão decriptografado, gerado pela bandeira
token/expirationDate	7	Alfanumérico	Data de expiração (no formato MM/YYYY) do token gerado pela bandeira para o cartão enviado

Gestão do token

Após a criação do token é possível gerenciar o status dele. Isto é, o estabelecimento tem autonomia para deletar, suspender e reativar os tokens sob sua responsabilidade.

PUT: </token-service/oauth/v2/tokenization/{tokenizationId}>

Parâmetros de Requisição

Nome	Tamanho	Tipo	Obrigatório	Descrição
tokenizationStatus	100	Alfanumérico	Sim	Se o status atualizado para qual o do token for deletar, será o delete : Se o status atualizado para qual o do token for suspender, será o suspend Se o status atualizado para qual o do token for reativar, será o resume
reason	2	Numérico	Sim	Motivo da atualização: 1 - Solicitação do Cliente 2 - Suspeita de Fraude

Caso a alteração do token ocorra com sucesso os seguintes campos serão retornados:

Parâmetros de Resposta

Caso a alteração do token ocorra com sucesso os seguintes campos serão retornados:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Token do cartão, que deve ser armazenado e utilizado em futuras transações
Brand/name*	-	Alfanumérico	Nome da bandeira. Ex: Visa
Brand/message*	-	Alfanumérico	Mensagem de erro da bandeira. Ex: Card not allowed. *Esse campo só é retornado em caso de erro na tokenização de bandeira

Criptograma

Toda transação com token de bandeira precisará de um criptograma, que será enviado no parâmetro tokenCryptogram. Este criptograma é de uso único e não pode ser reutilizado, visto que sua intenção é trazer uma camada adicional de segurança para a transação.

Para um token excluído ou suspenso um criptograma não poderá ser solicitado.

A bandeira Visa permite a solicitação de até 6.000 criptogramas, para um mesmo token, dentro de uma janela de 90 dias.

A geração do criptograma é feita de forma síncrona, basta enviar a seguinte requisição:

POST: </token-service/oauth/v2/cryptogram/{tokenizationId}>

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
subscription	-	Booleano	Não	<p>Informa ao emissor se uma transação é proveniente de uma recorrência.</p> <p>Se transação for uma recorrência, enviar true. Caso contrário, envie false.</p> <p>O não envio desse campo será considerado o valor false.</p>

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Identificador único da solicitação de tokenização do cartão pela Rede
cryptogramInfo/tokenCryptogram	28	Alfanumérico	Criptograma do token gerado pela bandeira no processo de solicitação de tokenização do cartão. Valor no formato Base64, com quantidade máxima de 28 caracteres

Nome	Tamanho	Tipo	Descrição
cryptogramInfo/eci	2	Alfanumérico	Código retornado pelas Bandeiras que indica o resultado da autenticação do portador junto ao Emissor.
cryptogramInfo/expirationDate**	24	Datetime	Data de expiração (no formato YYYY-MM-DDThh:mm:ss.sssZ) do criptograma do token gerado pela bandeira para o cartão enviado

cryptogramInfo/expirationDate:** A data de expiração do criptograma do token pode não ser retornada por algumas bandeiras.

Gerando transações com uso de tokens de bandeira

Após a criação do token (tokenizationId), é possível criar transações, onde esse parâmetro irá substituir os dígitos reais do cartão do portador pelo Token criado na bandeira.

URL de ambientes transacionais:

Ambiente	URL
Sandbox	https://sandbox-erede.useredecloud.com.br/v2/transactions
Produção	https://api.userede.com.br/erede/v2/transactions

Exemplo de uma requisição com Token de Bandeira:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	-	Booleano	Não	Defina se uma transação terá captura automática ou posterior. O não envio desse campo será considerado uma captura automática (true).
kind	-	Alfanumérico	Não	Tipo de transação a ser realizada. <ul style="list-style-type: none">Para transações de crédito, utilizar creditPara transações de débito, utilizar debit O não envio desse campo será considerado crédito.
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	Valor total da transação sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">R\$10,00 = 1000R\$0,50 = 50

Nome	Tamanho	Tipo	Obrigatório	Descrição
installments	Até 2	Numérico	Não	Número de parcelas em que uma transação será autorizada. De 2 a 12 O não envio desse campo será considerado à vista.
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão.
cardNumber	Até 19	Alfanumérico	Sim	Número do token.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do token. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	Ano de vencimento do token. Exemplo: 2028 ou 28
securityCode	Até 4	Alfanumérico	Não	Código de segurança do cartão geralmente localizado no verso do cartão. O envio desse parâmetro garante maior possibilidade de aprovação da transação.
tokenCryptogram	-	Alfanumérico	Obrigatório para CIT e opcional para MIT	Criptograma do token gerado pela Bandeira no momento de solicitação do criptograma do token criado. Valor no formato Base64, com quantidade máxima de 28 caracteres. Nas transações iniciadas pelo portador (CIT) este campo é obrigatório, mas em transações iniciadas pelo estabelecimento (MIT) é opcional.
storageCard	Até 1	Alfanumérico	Não	Indica operações que possam ou não estar utilizando COF (Card on File): 0 - Transação com credencial não armazenada. 1 - Transação com credencial armazenada pela primeira vez. 2 - Transação com credencial já armazenada. Para transações tokenizadas este parâmetro deve ter o valor "2". Atenção: O não envio desse campo será considerado 0 (credencial não armazenada).
securityAuthentication	-	-	-	Grupo securityAuthentication

Nome	Tamanho	Tipo	Obrigatório	Descrição
sai	Até 02	Alfanumérico	Obrigatório para as bandeiras Visa e ELO. Opcional em transações card-on-file	Identificador de transação eletrônica (ECI). Para transações da bandeira Mastercard, esse campo não é enviado. Nas transações que não forem tokenizadas (apenas card-on-file) o envio deste campo não é necessário. Para mais detalhes desse campo verifique o tópico “uso do sai”.
transactionCredentials	-	-	-	Grupo transactionCredentials
transactionCredentials/ credentialId	Até 02	Alfanumérico	Sim, se storageCard=1 ou =2 e cartão mastercard	Indica a categoria da transação com credencial armazenada. Consulte a seção “ Categorização de transações card-on-file ” para mais detalhes

Uso do “sai”: O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e Cloud Token Visa), **quando autenticado como 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso.**

Atenção: Ao fazer o envio do grupo threeDSecure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.


Envio do securityCode: Para a bandeira Visa, o envio do código de segurança incorreto fará com que a transação seja negada.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
dateTime	-	Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Numérico	Valor total do pedido sem separador de milhar e decimal. Exemplos: <ul style="list-style-type: none">• R\$10,00 = 1000• R\$0,50 = 50
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.

Nome	Tamanho	Tipo	Descrição
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Para maiores informações sobre o fluxo transacional verifique na Lista de APIs, conforme indicado a seguir:

 Selecione o tipo "Tokenização de Bandeiras" no combo box "Examples" da requisição.

POST: [/v2/transactions](#)

Notas: 1.Para informações sobre autenticação, autorização e configurações na API transacional da Rede acesse a seção [Autenticação e Autorização](#).

2.Para mais combinações transacionais confira a seção [Sobre](#).

Tokenização de Bandeira externa (captura)

O serviço de Tokenização de Bandeira é prestado por um Token Requestor, sua utilização pode melhorar a conversão junto a bandeira, pois no caso de cartões tokenizados as informações do cartão são protegidas com a devida segurança, substituindo-as por um token. Cada token é único para o usuário e estabelecimento e não pode ser usado por nenhuma outra loja.

Ao realizar a transação, um criptograma é enviado juntamente com o token, impedindo clonagens de cartão e operações fraudulentas. O emissor identifica o uso do token e confirma a autenticidade do criptograma, autorizando assim a transação, pois sabe que é do portador genuíno.

Atualmente, a Rede já está preparada para **transacionar** utilizando token das bandeiras Mastercard, Visa e Elo. O serviço que promoverá a Tokenização de bandeira provisionada pela Rede já está disponível na bandeira Visa, confira no menu [Tokenização de Bandeira Rede](#).

Para transacionar os criptogramas gerados por qualquer Token Requestor no e.Red, verifique os campos necessários abaixo e na Lista de APIs, conforme indicado a seguir:

Para transações que não sejam de Wallets, o envio do campo tokenCryptogram é obrigatório em todas as transações iniciadas pelo portador (CIT), mas opcional em transações iniciadas pelo estabelecimento (MIT).

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
capture	-	Booleano	Não	Defina se uma transação terá captura automática ou posterior. O não envio desse campo será considerado uma captura automática (true).

Nome	Tamanho	Tipo	Obrigatório	Descrição
kind	-	Alfanumérico	Não	<p>Tipo de transação a ser realizada.</p> <ul style="list-style-type: none"> Para transações de crédito, utilizar credit Para transações de débito, utilizar debit <p>O não envio desse campo será considerado crédito.</p>
reference	Até 50	Alfanumérico	Sim	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Não	Código do pedido gerado pelo estabelecimento.
amount	Até 10	Numérico	Sim	<p>Valor total da transação sem separador de milhar e decimal.</p> <p>Exemplos:</p> <ul style="list-style-type: none"> R\$10,00 = 1000 R\$0,50 = 50
installments	Até 2	Numérico	Não	<p>Número de parcelas em que uma transação será autorizada.</p> <p>De 2 a 12</p> <p>O não envio desse campo será considerado à vista.</p>
cardholderName	Até 30	Alfanumérico	Não	Nome do portador impresso no cartão.
cardNumber	Até 19	Alfanumérico	Sim	Número do token.
expirationMonth	Até 2	Numérico	Sim	Mês de vencimento do token. De 1 a 12.
expirationYear	2 ou 4	Numérico	Sim	<p>Ano de vencimento do token.</p> <p>Exemplo: 2028 ou 28</p>
securityCode	Até 4	Alfanumérico	Não	<p>Código de segurança do cartão geralmente localizado no verso do cartão.</p> <p>O envio desse parâmetro garante maior possibilidade de aprovação da transação.</p>
tokenCryptogram	-	Alfanumérico	Obrigatório para CIT e opcional para MIT	Token informado pela Bandeira. Identificar transações tokenizadas. Nas transações iniciadas pelo portador (CIT) este campo é obrigatório, mas em transações iniciadas pelo estabelecimento (MIT) é opcional.

Nome	Tamanho	Tipo	Obrigatório	Descrição
storageCard	Até 1	Alfanumérico	Não	<p>Indica operações que possam ou não estar utilizando COF (Card on File):</p> <p>0 - Transação com credencial não armazenada.</p> <p>1 - Transação com credencial armazenada pela primeira vez.</p> <p>2 - Transação com credencial já armazenada.</p> <p>Para transações tokenizadas este parâmetro deve ter o valor “2”.</p> <p>Atenção: O não envio desse campo será considerado 0 (credencial não armazenada).</p>
securityAuthentication	-	-	-	Grupo securityAuthentication
sai	Até 02	Alfanumérico	Obrigatório para as bandeiras Visa e ELO. Opcional em transações card-on-file	Identificador de transação eletrônica (ECI). Para transações da bandeira Mastercard, esse campo não é enviado. Nas transações que não forem tokenizadas (apenas card-on-file) o envio deste campo não é necessário. Para mais detalhes desse campo verifique o tópico “uso do sai”.
transactionCredentials				Grupo transactionCredentials
transactionCredentials/ credentialId	Até 02	Alfanumérico	Sim, se storageCard=1 ou =2 e cartão mastercard	Indica a categoria da transação com credencial armazenada. Consulte a seção “Categorização de transações card-on-file” para mais detalhes

Uso do sai

O parâmetro deverá ser utilizado sempre que a transação possuir um ECI específico, que não esteja atrelado a autenticação 3DS (ex: Wallets e Cloud Token Visa), **quando autenticado como 3DS faz-se necessário que o “eci” seja informado dentro do grupo 3D Secure, não sendo necessária a utilização do “sai” neste caso.**

Atenção: Ao fazer o envio do grupo threeD Secure em qualquer requisição, o campo “sai” será ignorado e a prioridade será do fluxo de 3DS.

Envio do securityCode: Para a bandeira Visa, o envio do código de segurança incorreto fará com que a transação seja negada.

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
reference	Até 50	Alfanumérico	Código da transação gerado pelo estabelecimento.
orderId	Até 50	Alfanumérico	Código do pedido gerado pelo estabelecimento.
tid	20	Alfanumérico	Número identificador único da transação.
nsu	Até 12	Alfanumérico	Número sequencial retornado pela Rede.
authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.

Nome	Tamanho	Tipo	Descrição
dateTime	-	Datetime	Data da transação no formato YYYY-MM-DDThh:mm:ss.sTZD .
amount	Até 10	Númérico	<p>Valor total do pedido sem separador de milhar e decimal.</p> <p>Exemplos:</p> <ul style="list-style-type: none"> • R\$10,00 = 1000 • R\$0,50 = 50
cardBin	6	Alfanumérico	6 primeiros dígitos do cartão.
last4	4	Alfanumérico	4 últimos dígitos do cartão.
returnCode	Até 4	Alfanumérico	Código de retorno da transação.
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand	-	-	Grupo de informações recebidas da bandeira sobre a transação.
brand/name	-	Alfanumérico	Nome da bandeira. Ex: Mastercard.
brand/returnCode	Até 4	Alfanumérico	Código de retorno da transação.
brand/returnMessage	Até 256	Alfanumérico	Mensagem de retorno da transação.
brand/merchantAdviceCode	Até 2	Alfanumérico	Código de Aviso para Estabelecimento Comercial. É um conjunto de códigos usado para fornecer informações adicionais sobre uma resposta de transação de uso exclusivo da bandeira Mastercard.
brand/authorizationCode	6	Alfanumérico	Número da autorização da transação retornada pelo emissor do cartão.
brand/brandTid	Até 21	Alfanumérico	Código identificador da transação na respectiva bandeira. Para mais detalhes consulte a seção Recorrência e Card-on-file

Para maiores informações sobre o fluxo transacional verifique na Lista de APIs, conforme indicado a seguir:

 Selecione o tipo "Tokenização de Bandeiras" no combo box "Examples" da requisição.

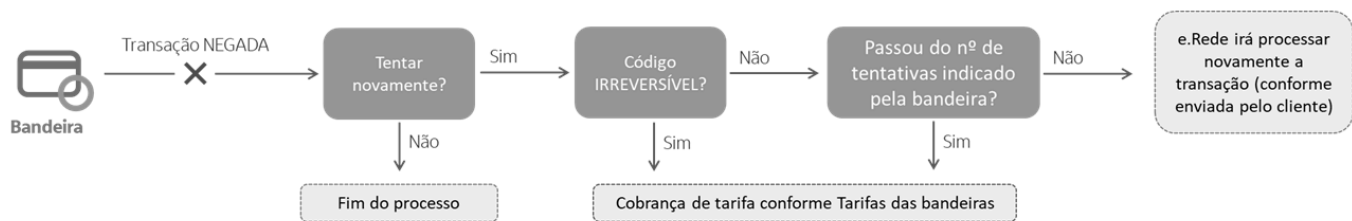
POST: [/v2/transactions](#)

Tarifas de Bandeiras

Retentativas

Sempre que o estabelecimento recebe uma transação negada é possível que envie a mesma transação novamente para buscar uma aprovação. Porém as bandeiras estabeleceram regras para essas retentativas de transação que, a depender do código de negativa inicial ou quantas retentativas foram feitas, podem acarretar tarifas ao estabelecimento. Por isso, para ajustar seus fluxos de retentativa devem ser consideradas as categorizações das bandeiras.

Fluxo de retentativa a partir de uma transação negada



Regras das bandeiras

Bandeira Visa

A bandeira Visa em seu programa de retentativas utiliza os códigos ABECS como base, separados em 4 categorias:

VISA	Título	Descrição	Códigos
Categoria 1	Emissor nunca aprovará.	Informam Estabelecimentos/Credenciadores que o cartão foi cancelado ou nunca existiu ou que a negativa é resultado de uma restrição permanente ou condição de erro que impedirá uma aprovação futura.	4, 7, 12, 14, 15, 41, 43, 46, 57, R0, R1, R3
Categoria 2	Emissor não pode aprovar neste momento.	Indicam que a negativa é resultado de uma condição temporária tal como risco de crédito, controles de velocidade do emissor ou outras restrições do cartão que podem permitir uma retentativa da transação ser aprovada. Em alguns casos, a negativa requer uma ação do portador ou emissor para remover a restrição antes que uma aprovação possa ser obtida.	3, 19, 39, 51, 52, 53, 59, 60, 61, 62, 65, 75, 78, 86, 91, 93, 96, N3, N4, Z5, 5C, 9G
Categoria 3	Qualidade de dados/revisar dados.	Quando um erro de dados é identificado pelo emissor e a transação é declinada como consequência. Estabelecimentos devem revalidar dados de pagamentos antes de retentar. Estabelecimentos e Credenciadores devem monitorar estes códigos de negativas devido a exposição potencial a fraudes.	54, 55, 82, N7, 1A, 70, 6P
Categoria 4	Códigos de respostas genéricos.	Todos os demais Códigos de Respostas, muitos dos quais são de uma natureza técnica ou provêm pouco ou nenhum valor para Estabelecimentos/Credenciadores.	Todos os outros códigos de retorno que não estão inclusos na categoria 1, 2 e 3.

Pontos de atenção

- O código 57 é uma exceção à regra da Categoria 1: Mesmo sendo um código irreversível ele pode ser retentado até 15 vezes dentro do período de 30 dias.
- O código 14 contabiliza tanto para a categoria 1 quanto para a categoria 3.

Bandeira Mastercard

A bandeira Mastercard não considera as classificações dos códigos ABECS, mas sim a classificação dos códigos complementares de recusa chamados de MAC – Merchant Code Advice, que fornecem instruções sobre que ações o estabelecimento pode tomar para aprovar a transação.

Os códigos MAC acompanham o código de negativa quando uma transação é negada e indicam se aquela transação pode ser retentada (reversível) ou não (irreversível).

Os valores de MAC possíveis são:

Valor do MAC	Descrição do MAC	Classificação
01	Informações atualizadas/adicionais necessárias (Updated/additional information needed)	Reversível

Valor do MAC	Descrição do MAC	Classificação
02	Tente novamente mais tarde (Try Again Later)	Reversível
03	Não Tente Novamente (Do Not Try Again)	Irreversível
04	Requisitos de token não atendidos para este tipo de token (Token requirements not fulfilled for this token type)	Reversível
21	Cancelamento de Pagamento (Payment Cancellation)	Irreversível
24	Tente após 1 hora	Reversível
25	Tente após 24 horas	Reversível
26	Tente após 2 dias	Reversível
27	Tente após 4 dias	Reversível
28	Tente após 6 dias	Reversível
29	Tente após 8 dias	Reversível
30	Tente após 10 dias	Reversível
40	Cartão pré-pago não recarregável de consumo	Irreversível
41	Número do cartão virtual de uso único do consumidor	Irreversível
43	Cartão virtual de uso múltiplo	-

Os MACs 40 e 41 avisam o estabelecimento de que aquele cartão só pode ser usado uma vez.

O MAC 43 retornará apenas em transações aprovadas ou de Zero Dollar.

Também, a Mastercard passará a consolidar alguns códigos de resposta da padronização em códigos de uso exclusivo da bandeira:

- 79 (Ciclo de vida)
- 82 (Política)
- 83 (Fraude/ Segurança)

Ou seja, os códigos de uso exclusivo para Mastercard em conjunto com o MAC funcionam da seguinte forma:


Quando	Então	E o código de resposta
O emissor recusar a transação usando o código de resposta 54 (Expired card).	A Mastercard substituirá o código 54 para o código 79 (Recusa por ciclo de vida).	Acompanhado pelo devido Merchant Advice Code (MAC).

Atenção: o MAC pode acompanhar quaisquer códigos de negativa, não apenas os de uso exclusivo da Mastercard

Bandeira Elo

A bandeira Elo utiliza a categorização ABECS como regra para seu fluxo de retentativas, na [Tabela de códigos de retorno da bandeira e padronização da mensagem](#) estão os códigos de negativa e a classificação indicando se aquele código pode ser retentado (reversível) ou não (irreversível).

A partir de fevereiro de 2025, a bandeira ELO irá categorizar seus códigos de negativa em 3 categorias para retentativas:

	Título	Descrição	Códigos
Categoria 1	Códigos irreversíveis	Informam Estabelecimentos/Credenciadores que a negativa é resultado de uma restrição permanente ou condição de erro que impedirá uma aprovação futura.	57, 14, 56, 58, 46, FM, 19, 12, 30, 13, 23, 41, 43, 64, 83, 76, 77
Categoria 2	Códigos reversíveis	Indicam que a negativa é resultado de uma condição temporária que pode permitir uma retentativa da transação ser aprovada. Em alguns casos, a negativa requer uma ação do portador ou emissor para remover a restrição antes que uma aprovação possa ser obtida.	51, 59, 04, 06, 38, 61, 62, 65, 75, 78, 91, 96, AB, AC, P6
Categoria 3	Ataques de força bruta	Ataques de força bruta Estabelecimentos devem monitorar estes códigos de negativas devido a exposição potencial a fraudes.	14, 54, 55, 63, 82

Pontos de atenção

- O código 14 contabiliza tanto para a categoria 1 quanto para a categoria 3.

Para transações negadas pelo código 79 – Segurança/ Suspeita de Fraude, a Elo fornece um código adicional retornado no campo chamado de MAC – Merchant Code Advice, que fornecem instruções sobre que ações o estabelecimento pode tomar para aprovar a transação.

Os códigos MAC acompanham o código de negativa quando uma transação é negada e indicam se aquela transação pode ser retentada (reversível) ou não (irreversível).

Os valores de MAC possíveis são:


Código de resposta (ABECS)	Código MAC (campo merchantAdviceCode)	Descrição da combinação	Orientação no processo de retentativas
79	1	Precisa de uma atualização de conta	Não tente novamente (Irreversível)
79	2	Precisa alterar as informações de conta	Refazer após corrigir os dados (Reversível)

Bandeira Hipercard

A bandeira Hipercard utiliza a categorização ABECS como regra para seu fluxo de retentativas, na [Tabela de códigos de retorno da bandeira e padronização da mensagem](#) estão os códigos de negativa e a classificação indicando se aquele código pode ser retentado (reversível) ou não (irreversível).

Tarifas da bandeira

Bandeira Visa


	Emissor nunca aprovará	Excesso de retentativa	Qualidade de dados
	Códigos da Categoria 1	Códigos da Categoria 2, 3 e 4	Código da Categoria 3
Limite máximo para novas tentativas de transações negadas.	Não há limite, essas transações não devem ser retentadas .	15 tentativas em 30 dias.	10.000 transações em 30 dias no mesmo PV.
Tarifa cobrada ao ultrapassar o limite (transações nacionais).	0,10 USD	0,10 USD	0,10 USD

	Emissor nunca aprovará	Excesso de retentativa	Qualidade de dados
	Códigos da Categoria 1	Códigos da Categoria 2, 3 e 4	Código da Categoria 3
Tarifa cobrada ao ultrapassar o limite (transações internacionais).	0,25 USD	0,25 USD	0,25 USD

A cobrança de tarifas da bandeira **Visa** está vigente **desde abril de 2021**.

A partir de 25/05/2025, o limite de transações para Excesso de retentativa aumentará para 20 tentativas em 30 dias. Também, a contagem de transações tarifáveis será separada entre transações iniciadas pelo portador e transações iniciadas pelo estabelecimento.

Bandeira Mastercard

	Emissor nunca aprovará	Excesso de retentativa
	Quaisquer códigos de negativa acompanhados pelo MAC 03 ou 21	Quaisquer transações, independente do código de negativa ou MAC (inclusive transações sem MAC)
Limite máximo para novas tentativas de transações negadas.	Não há limite, essas transações não devem ser retentadas .	7 tentativas em 24h - 35 tentativas em 30 dias
Tarifa cobrada ao ultrapassar o limite (transações nacionais e internacionais).	R\$ 2,50	R\$ 2,00

A cobrança de tarifas da bandeira **Mastercard** está vigente desde **janeiro de 2022**.

Importante: Retentar excessivamente transações que foram negadas por MAC 03 ou 21 podem resultar em dupla tarificação.


Exemplo de dupla tarificação Mastercard:

Estabelecimento "A" realiza uma transação que é negada e retorna acompanhada por MAC 03. Após a negativa, ao longo dos 30 dias do mês, o estabelecimento retenta a transação 40 vezes – sem superar o limite de 7 tentativas em 24h – resultando nas tarifas:

- R\$ 2,50 x 40 na tarifa de Emissor nunca aprovará – Totalizando em R\$ 100,00
- R\$ 2,00 x 5 (quantidade de retentativas acima de 35 em 30 dias) na tarifa de Excesso de Retentativa – Totalizando em R\$ 10,00


Dessa forma, a mesma transação foi tarifada em ambas as categorias, totalizando uma cobrança de R\$ 110,00.

Bandeira Elo

	Código irreversível	Código Reversível	Ataques de força bruta
	Categoria 1	Categoria 2	Categoria 3
Limite máximo para novas tentativas de transações negadas.	Não há limite, essas transações não devem ser retentadas .	15 tentativas em 30 dias.	10.000 transações em 30 dias no mesmo CNPJ dentro do mês de apuração
Tarifa cobrada a cada tentativa que ultrapassar o limite (transações nacionais e internacionais).	R\$ 0,80	R\$ 0,80	R\$ 0,80

A cobrança de tarifas da bandeira **Elo** está vigente desde **agosto de 2022**.

Bandeira Hipercard

	Emissor nunca aprovará	Excesso de tentativa
	Código Irreversível	Código Reversível
Limite máximo para novas tentativas de transações negadas.	Não há limite, essas transações não devem ser retentadas .	8 tentativas do primeiro ao último dia do mês.
Tarifa cobrada ao ultrapassar o limite (transações nacionais e internacionais).	0,03% do valor da transação por retentativa, com mínimo de R\$ 0,15 e máximo de R\$ 0,80	R\$ 1,85 por retentativa. Após ultrapassar o limite de 8 tentativas mensais, a bandeira cobrará por cada transação feita após a inicial.

A cobrança de tarifas da bandeira **Hipercard** está vigente desde **julho de 2022**.

Importante: Atingido o limite de 8 tentativas possíveis. A bandeira cobrará por cada transação feita.

Exemplo de critério de tarifação Hipercard:

Estabelecimento "A" realiza uma transação que é negada por código reversível. Após a negativa, ao longo dos 30 dias do mês, o estabelecimento retenta a transação 15 vezes, totalizando em 16 transações. Isso resultará em uma tarifa por R\$1,85 x 15, totalizando em uma tarifa de R\$27,75.

Não uso de Zero Dollar

Uma prática existente é realizar transações de baixo valor para verificar o “status” do cartão - checando se existe algum bloqueio ou restrição, se o cartão é válido e até se há limite disponível. Uma vez que a compra é aprovada, o estorno é realizado em seguida. No entanto, esta prática - considerada inapropriada - acarretará tarifas a serem aplicadas pelas bandeiras.

Para garantir o melhor funcionamento dos meios de pagamento e oferecer mais segurança para o uso do cartão, as bandeiras estabeleceram regras para transações de verificação de conta.

Com o uso do produto Zero Dollar a validação será feita conforme as exigências das bandeiras, com uma transação de valor zero, sem gerar custos ao portador do cartão.

Para mais detalhes sobre o produto Zero Dollar, [clique aqui](#).

Importante: antes de armazenar um cartão é **obrigatório** o uso de uma validação **Zero Dollar**.

Regras das bandeiras

Bandeiras Mastercard e Elo


As bandeiras Mastercard e Elo definiram que transações realizadas com valor de até R\$ 5,00 e que forem estornadas subsequentemente serão tarifadas.

Tarifas da bandeira

Bandeira Mastercard

	Transações com valor de até R\$ 5,00 e subsequentemente estornadas.
Tarifa cobrada por transação infratora	R\$ 0,21

Bandeira Elo

	Transações com valor de até R\$ 5,00 e estornadas na mesma data
Tarifa cobrada por transação infratora	R\$ 0,2212

Uso de Zero Dollar

Regras das bandeiras

Bandeira Mastercard

As bandeiras Visa e Mastercard, possuem a aplicação de um custo para transações Zero Dollar. Este é um custo atrelado a utilização do produto Zero Dollar, ou seja, a cada transação com valor zero enviada para aprovação. Confira a seguir os detalhes:

Tarifas da bandeira

Bandeira Mastercard

Bandeira	Tipo	Custo por transação
Mastercard	Transações Nacionais	R\$ 0,054445
Mastercard	Transações Internacionais	R\$ 0,065334

Bandeira Visa

Bandeira	Tipo	Custo por transação
Visa	Transações Nacionais	USD 0,0035
Visa	Transações Internacionais	USD 0,06

Pré-autorizações

A partir de uma pré-autorização, o lojista pode reservar o valor na fatura do cartão do seu cliente, para checar seu estoque, ou enviar os dados da transação para seu processo de prevenção a fraude. Após isso e com a análise concluída, o lojista poderá decidir entre capturar a transação ou apenas liberar o limite reservado e devolvendo o valor pré-capturado da compra feita em seu site.

Para o portador, esse processo é igual ao de qualquer compra em um site, ele irá ver seu limite utilizado, e posteriormente débito em sua fatura em caso de confirmação da captura por parte do lojista. Caso a confirmação não seja efetuada pelo estabelecimento o portador terá acesso à informação de estorno.

Regras das bandeiras

Bandeira Mastercard

Para toda pré-autorização feita para transações da bandeira Mastercard, o estabelecimento será tarifado pela utilização do produto.

Tarifas da bandeira

Bandeira Mastercard

A partir de agosto de 2023, sempre que o lojista utilizar o produto pré autorização na bandeira Mastercard, será cobrado conforme tabela abaixo:

Tipo	Aplicável a valores de transação	Custo por transação
Transações nacionais	Maior ou = R\$ 68,96	0,058% sobre o valor da transação
Transações nacionais	Menor que R\$ 68,96	R\$ 0,04
Transações internacionais	Maior ou = R\$ 100,00	0,093% sobre o valor da transação
Transações internacionais	Menor que R\$ 100,00	R\$0,04

Transações autenticadas e não autenticadas

Tarifa de transações autenticadas

Tarifas de Autenticação 3DS Elo

A bandeira Elo tem o custo fixo de R\$0,20 referente a todas as transações enviadas para autenticação via protocolo 3DS dentro do mês. Essa tarifa será repassada a partir de maio de 2025.

Importante: Houve uma revisão desta tarifa e com a nova revisão, a tarifa será reduzida e seu novo valor tem o início da vigência em julho de 2025. Confira as novas regras:

A bandeira Elo tem o custo fixo de R\$0,22 referente a todas as transações enviadas para autenticação via protocolo 3DS dentro do mês. Essa tarifa será repassada a partir de julho de 2025.

Transações autenticadas Mastercard

A bandeira **Mastercard®** aplica uma tarifa de 0.9bps (0,009%), com teto de R\$17,00 **em transações autenticadas via 3DS**.

Sobre Transações Autenticadas via Data Only e via Carteiras Digitais (Apple, Google e Samsung Pay), nenhuma das tarifas será aplicada.

Importante: Houve uma revisão desta tarifa, com a nova revisão, a tarifa será reduzida e seu novo valor tem o início da vigência em 2025. Confira as novas regras:

- Sobre Transações Autenticadas via 3DS, a bandeira **Mastercard®** aplicará uma tarifa no valor de 0.9bps (0,009%), com teto de R\$ 17,00;
- Sobre Transações Autenticadas via Data Only e via Carteiras Digitais (Apple, Google e Samsung Pay), nenhuma das tarifas será aplicada.

Tarifa de transações não autenticadas

Transações não autenticadas Mastercard

A bandeira **Mastercard®** aplica uma tarifa de 1.9bps (0,019%), com teto de R\$ 17,00 **em transações que não utilizam nenhum método de autenticação**.

- Sobre Transações Autenticadas via Data Only e via Carteiras Digitais (Apple, Google e Samsung Pay), nenhuma das tarifas será aplicada.

OBS: Transações via Carteiras Digitais não terão incidência destas tarifas da bandeira **Mastercard®** desde que sejam trafegadas com todos os parâmetros necessários, indicando um nível de segurança equivalente a uma transação autenticada. É possível verificar os níveis de segurança de uma transação através do campo “ECI”. Confira o detalhe dos valores para este campo [“aqui”](#).

Para que nenhuma destas duas tarifas da bandeira **Mastercard®** incida em sua operação, considere a implementação destes produtos. Confira mais detalhes sobre as integrações e funcionalidades do Data Only [aqui](#), e de Carteiras Digitais [aqui](#).

Transações não tokenizadas

A tokenização permite que as informações do cartão sejam protegidas já que são substituídas por um token no momento de compra, garantindo mais segurança e conversão.

A bandeira Visa, buscando incentivar o uso de tokens, estabeleceu um custo adicional para todas as transações que não utilizarem um método de tokenização.

Para mitigar a incidência dessa tarifa, é recomendado utilizar métodos de tokenização, como:

- [Tokenização de bandeira](#)
- [Transações tokenizadas e autenticadas via Carteiras Digitais \(Wallets\)](#)


Clique em cada um dos itens acima para saber mais.

Regras das bandeiras

Bandeira Visa

Todas as transações que não utilizarem nenhum método de tokenização são passíveis de tarifação.

Tarifas das bandeiras

	Transações não tokenizadas
Tarifa cobrada por transação infratora	0,05% do valor da transação

O repasse iniciará a partir de 2025.

Carteiras digitais escalonadas

As carteiras digitais escalonadas permitem que o usuário armazene fundos nelas antes do pagamento de uma conta ou produto.

Para a bandeira Visa, está previsto, a partir de janeiro de 2024, o início do custo abaixo:

Bandeira	Valor
Visa	USD 0,01

Cancelamento

- Para transações de débito Mastercard canceladas a partir do dia seguinte à autorização (D+1) até 10 dias após a autorização (D+10), é cobrada uma taxa de R\$ 10,881 por transação cancelada.
- Para transações de débito Mastercard canceladas há mais de 10 dias após sua autorização, será cobrada uma taxa de R\$ 36,27 por transação cancelada.

A cobrança das taxas da bandeira Mastercard está em vigor desde outubro de 2023.

APIs e.Rede

1.0.0

AS3

<https://developer.userede.com.br/dev-portal-swaggers/erede/swagger.yaml>

Introdução

Uma solução de pagamento para quem quer vender a débito e crédito pela internet com facilidade e segurança. Os pagamentos são processados pela Rede e direto na página da loja. O e.Rede também oferece uma solução de tokenização de cartões de diversas bandeiras de forma simples e segura.

Servers

https://sandbox-erede.useredecloud.com.br - Endereço de Sandbox do e.Red

Transação

GET	/v2/transactions	Consultar transação por reference
POST	/v2/transactions	Realizar transação
GET	/v2/transactions/{tid}	Consultar transação por tid
PUT	/v2/transactions/{tid}	Confirmar autorização da transação (captura)

Cancelamento

GET	/v2/transactions/{tid}/refunds	Consultar cancelamento por tid
POST	/v2/transactions/{tid}/refunds	Cancelar transação
GET	/v2/transactions/{tid}/refunds/{refundId}	Consultar cancelamento por refundId

Tokenização

POST	/oauth/v2/tokenization	Enviar solicitação de tokenização
GET	/oauth/v2/tokenization/{tokenizationId}	Consultar solicitação de tokenização por tokenizationId
PUT	/oauth/v2/tokenization/{tokenizationId}	Fazer a gestão do token
POST	/oauth/v2/cryptogram/{tokenizationId}	Solicitar criptograma do token por tokenizationId

Schemas



Transação - POST Realizar transação - Request Body - Autorização

Transação - POST Realizar transação - Request Body - Companhias Aéreas

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Rede

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Rede + SDWO + MCC Dinâmico + Token

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Rede + SDWO + MCC dinâmico + CBPS + Token

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Rede + Recorrência + Card-on-File

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Cliente + SDWO + MCC dinâmico + CBPS + Token

Transação - POST Realizar transação - Request Body - Data Only: MPI Rede + SDWO + MCC dinâmico + CBPS + Token

Transação - POST Realizar transação - Request Body - Data Only: MPI Cliente + SDWO + MCC dinâmico + CBPS + Token

Transação - POST Realizar transação - Request Body - 3D Secure 2.0: MPI Cliente

Transação - POST Realizar transação - Request Body - Data Only: MPI Rede

Transação - POST Realizar transação - Request Body - MPI Rede: Data Only + SDWO + MCC Dinâmico + Token

Transação - POST Realizar transação - Request Body - MPI Cliente: Data Only

Transação - POST Realizar transação - Request Body - Data Only: MPI Rede + Recorrência + Card-on-File

Transação - POST Realizar transação - Request Body - Zero dollar

Transação - POST Realizar transação - Request Body - MCC dinâmico

Transação - POST Realizar transação - Request Body - MCC dinâmico + Voucher

Transação - POST Realizar transação - Request Body - Carteiras digitais: Apple, Google, Samsung e Click to Pay

Transação - POST Realizar transação - Request Body - Carteiras Digitais: SDWO - CBPS

Transação - POST Realizar transação - Request Body - Carteiras digitais: SDWO - CASH-IN

Transação - POST Realizar transação - Request Body - Carteiras digitais: SDWO - PURCHASE

Transação - POST Realizar transação - Request Body - Tokenização de Bandeiras

Transação - POST Realizar transação - Request Body - Tokenização de Bandeiras Cofre de Cartões

Transação - POST Solicitação de QR Code Pix - Request Body - Pix

Transação - POST Realizar transação - Response - Abstract

Transação - POST Realizar transação - Response - Autorização

Transação - POST Realizar transação - Response - Companhias Aéreas

Transação - POST Realizar transação - Response - 3D Secure 2.0: MPI Rede

Transação - POST Realizar transação - Response - 3D Secure 2.0: MPI Cliente

Transação - POST Realizar transação - Response - Data Only: MPI Rede

Transação - POST Realizar transação - Response - Data Only: MPI Cliente

Transação - POST Realizar transação - Response - Zero dollar

Transação - POST Realizar transação - Response - MCC dinâmico

Transação - POST Realizar transação - Response - MCC dinâmico + Voucher

Transação - POST Realizar transação - Response - Carteiras digitais: Apple, Google, Samsung e Click to Pay

Transação - POST Realizar transação - Response - CBPS + Carteiras digitais

Transação - POST Realizar transação - Response - Carteiras digitais: SDWO - CASH-IN

Transação - POST Realizar transação - Response - Carteiras digitais: SDWO - PURCHASE

Transação - POST Realizar transação - Response - Tokenização de Bandeiras

Transação - POST Realizar transação - Response - Tokenização de Bandeiras Cofre de Cartões

Transação - POST Solicitação QR Code Pix - Response - Pix

Transação - GET Consultar transação - Response - 200

Transação - GET QR Code Pix pago - Response - 200

Transação - GET QR Code Pix pendente - Response - 200

Transação - POST Realizar transação - Response - 400

Transação - PUT Confirmar autorização da transação (captura) - Request Body

Transação - PUT Confirmar autorização da transação (captura) - Response 200

Cancelamento - POST Cancelar transação - Request Body

Cancelamento - POST Cancelar transação Pix - Request Body

ObjectResponse200CancelarTransacao

ObjectResponse200CancelarTransacaoPix

ObjectResponse200CallbackDeCancelamento

Cancelamento - GET Consultar cancelamento por tid - Response 200

Cancelamento - GET Consultar cancelamento Pix - Response 200

Cancelamento - GET Consultar cancelamento Múltiplos Pix - Response 200

Cancelamento - GET Consultar cancelamento por refundId - Response 200

Cancelamento - GET Consultar cancelamento Pix por refundId - Response 200

Tokenização - POST Enviar solicitação de tokenização - Request

Transação - POST Enviar solicitação de transação Voucher - Request

Tokenização - POST Callback realizado pelo Webhook - Request

Tokenização/Criptograma - POST Enviar solicitação de criptograma - Request

Tokenização/Criptograma - PUT Enviar solicitação de criptograma - Request

Objeto events retornado no callBack da Tokenização

Tokenização - POST Enviar solicitação de tokenização - Response - 200

Voucher - POST Response Arranjo aberto - Response - 200

Voucher - POST Response Arranjo fechado - Response - 200

Tokenização - POST Enviar solicitação de tokenização - Response - 400

Tokenização - GET Consultar solicitação de tokenização - Response - 200

Tokenização - GET Consultar solicitação de tokenização - Response - 400

Tokenização - GET Consultar criptograma - Response - 200

Tokenização - GET Consultar criptograma - Response - 400

Tokenização - Response - 500

Gestão token - PUT Deletar e suspender token - Response - 200

Gestão token - PUT Resume token - Response - 200

Gestão token - PUT Erro de reason inválido - Response - 400

Gestão token - PUT Consultar solicitação de tokenização - Response - 400

Gestão token - Response - 500

Object - Authorization

Object - Authorization - Pix

Object - QrCodeResponse - Pix

Object - Capture

Object - Capture - Pix

Object - lata

Object - Link

Object - Refund

Object - Refund Pix

Object - Refunds do consultar transação

Object - SecurityAuthentication

Object - ConsumerBillPaymentService

ObjectConsumerBillPaymentServiceCBPS

Object - Status History

Object - SubMerchant

Object - MCC Dinâmico + Voucher

Object - ReceiverData

Object - ThreeDSecure do consultar transação

Object - ThreeDSecureClient

Object - ThreeDSecureClientDataOnly

Object - ThreeDSecureClient v2.0

Object - ThreeDSecureClientDataOnly v2.0

Object - ThreeDSecureRede

Object - ThreeDSecureRede v2.0

Object - Billing

Object - TransactionCredentials

Object - Url Callback

Object - Url ThreeDSecureRede

Object - ThreeDSecureRede Device

Object - Wallet

ObjectWalletCashIn

ObjectWalletPurchase

ObjectWalletCBPS

Object - Wallet3DS

Object - ReceiverData

Object - SenderData

Object - Wallet

Object - Link

Object - Link Voucher

Object - Brand

Object - Brand Voucher arranjo aberto

Object - Brand Voucher arranjo fechado

Object - Voucher arranjo aberto

Object - Voucher arranjo fechado

Object - Token

Object - CryptogramInfo

Object - Authorization

Object - Authorization Brand

Tutorial Sandbox

O fluxo de Autenticação e Autorização é apenas uma camada no acesso as APIs. Para utilizar o nosso ambiente Sandbox, é necessário acessar o menu [Meus Projetos](#) na área logada desse portal e criar um projeto associado ao pacote de APIs que deseja integrar. Neste momento, serão geradas credenciais de teste que devem ser utilizadas somente em nosso ambiente Sandbox.

Na página [Ponto de Partida](#) mostramos um passo a passo de como utilizar as credenciais Sandbox nas coleções do Postman.

Ponto de Partida

Na página [Ponto de Partida](#) mostramos um passo a passo de como utilizar as credenciais Sandbox nas coleções do Postman e também a **como realizar o processo de autenticação no protocolo OAuth 2.0**.

Cartões

Nosso sandbox funciona somente com dados de cartões selecionados, conforme tabela abaixo:

Bandeira	Tipo	Cartão	Validade	Código de Segurança	Token Informado pela Bandeira (tokenCode)	Criptograma do token Informado pela Bandeira (tokenCryptogram)
Mastercard	Débito	5277696455399733	jan/35	123	Este cartão não possui token	Este cartão não possui token
Mastercard	Crédito	5448280000000007	jan/35	123	Este cartão não possui token	Este cartão não possui token
Mastercard (BIN 2)	Débito	2223000148400010	jan/35	123	Este cartão não possui token	Este cartão não possui token
Mastercard (BIN 2)	Crédito	2223020000000005	jan/35	123	Este cartão não possui token	Este cartão não possui token
Visa	Débito	4761120000000148	jan/35	123	Este cartão não possui token	Este cartão não possui token
Visa	Crédito	4235647728025682	jan/35	123	Este cartão não possui token	Este cartão não possui token
Hipercard	Crédito	6062825624254001	jan/35	123	Este cartão não possui token	Este cartão não possui token
Hiper	Crédito	6370950847866501	jan/35	123	Este cartão não possui token	Este cartão não possui token
Diners	Crédito	36490101441625	jan/35	123	Este cartão não possui token	Este cartão não possui token
JCB	Crédito	3569990012290937	jan/35	123	Este cartão não possui token	Este cartão não possui token
JCB (19 dig)	Crédito	3572000100200142753	jan/35	123	Este cartão não possui token	Este cartão não possui token
Credz	Crédito	6367600001405019	jan/35	123	Este cartão não possui token	Este cartão não possui token

Bandeira	Tipo	Cartão	Validade	Código de Segurança	Token Informado pela Bandeira (tokenCode)	Criptograma do token Informado pela Bandeira (tokenCryptogram)
Elo	Crédito	4389351648020055	jan/35	123	Este cartão não possui token	Este cartão não possui token
Amex	Crédito	371341553758128	jan/35	1234	Este cartão não possui token	Este cartão não possui token
Cabal	Crédito	6042034400069940	jan/35	123	Este cartão não possui token	Este cartão não possui token
Sorocred	Crédito	6364142000000122	jan/35	123	Este cartão não possui token	Este cartão não possui token
Credsystem	Crédito	6280281038975334	jan/35	123	Este cartão não possui token	Este cartão não possui token
Banescard	Crédito	6031828795629272	jan/35	123	Este cartão não possui token	Este cartão não possui token
Visa	Crédito	4895370010000005	jan/35	123	4830442035272279 ou 4830447374649789 ou 4894093711004024	AgAAAAAIR8CQrXSoHbQAAAAA=
Visa	Débito	4824810010000006	jan/35	123	4894092622280160 ou 4894096020766258 ou 4894094167345770	AAABakREQAAAAAAAAAAAAAAAAA=
Mastercard (BIN 2)	Crédito	2223000250000004	jan/35	123	_	ANbuvvxndbK2AAEShHmWGgADFA==
Mastercard (BIN 2)	Débito	5204970000000007	jan/35	123	_	AOPAIMgflr8UAAiShHmWGgADFA==
Elo	Débito	4514166653413658	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Débito	4389356784017450	jan/35	123	Este cartão não possui token	ANfuuvxnDbK2AAESiXmWGgAEFw==
Elo	Crédito	4389358876174389	jan/35	123	Este cartão não possui token	Aleb2oot61nRAAHBnZ8HAAADFA==
Elo	Débito	5067230000009011	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Voucher	5041758436269362	jan/35	123	Este cartão não possui token	Este cartão não possui token
Ticket	Voucher	4514166603616681	jan/35	123	Este cartão não possui token	Este cartão não possui token

Bandeira	Tipo	Cartão	Validade	Código de Segurança	Token Informado pela Bandeira (tokenCode)	Criptograma do token Informado pela Bandeira (tokenCryptogram)
Alelo	Voucher	4389357063526690	jan/35	123	Este cartão não possui token	Este cartão não possui token
Sodexo	Voucher	6363688827373622	jan/35	123	Este cartão não possui token	Este cartão não possui token
Caju	Voucher	5284776885068867	jan/35	123	Este cartão não possui token	Este cartão não possui token
Flex	Voucher	5490630354637860	jan/35	123	Este cartão não possui token	Este cartão não possui token

Para transações tokenizadas com cartões **MASTERCARD®, utilize o **número do cartão** no parâmetro **tokenCode + tokenCryptogram**, ou apenas o **cardToken**. Para cartões **Visa**, use a combinação **tokenCode + tokenCryptogram** ou apenas o **cardToken**. Para as demais bandeiras, utilize apenas o **cardToken**.*

Caso seja enviada transação com cartão diferente dos informados, o sandbox retornará o seguinte erro:

Código de erro	Descrição
58	Unauthorized. Contact issuer.

Nesse momento, só os cartões da Visa estão disponíveis para realizar a solicitação de tokenização de bandeira. Caso seja enviada uma solicitação com um cartão Mastercard, o seguinte erro será retornado:

Código de erro	Descrição
27	Card is from a brand not enabled for tokenization

Simular erros

Para simular códigos de erros, basta enviar transações com os valores correspondentes aos códigos de erro, conforme tabela abaixo:

Para o correto funcionamento da bandeira Elo faz se obrigatório o envio do campo securityCode.

Código de erro	Amount	Descrição
53	53	Transaction not allowed for the issuer. Contact Rede.
56	56	Error in reported data. Try again.
57	57	affiliation: Invalid merchant.
58	58	Unauthorized. Contact issuer.
69	69	Transaction not allowed for this product or service.
72	72	Contact issuer.

Código de erro	Amount	Descrição
74	74	Communication failure. Try again.
79	79	Expired card. Transaction cannot be resubmitted. Contact issuer.
80	80	Unauthorized. Contact issuer. (Insufficient funds).
83	83	Unauthorized. Contact issuer.
84	84	Unauthorized. Transaction cannot be resubmitted. Contact issuer.
85	85	Please contact issuer.
101	101	Unauthorized. Problems on the card, contact the issuer.
102	102	Unauthorized. Check the situation of the store with the issuer.
103	103	Unauthorized. Please try again.
104	104	Unauthorized. Please try again.
105	105	Unauthorized. Restricted card.
106	106	Error in issuer processing. Please try again.
108	108	Unauthorized. Value not allowed for this type of card.
109	109	Unauthorized. Nonexistent card.
110	110	Unauthorized. Transaction type not allowed for this card.
111	111	Unauthorized. Insufficient funds.
112	112	Unauthorized. Expiry date expired.
113	113	Unauthorized. Identified moderate risk by the issuer.
114	114	Unauthorized. The card does not belong to the payment network.
115	115	Unauthorized. Exceeded the limit of transactions allowed in the period.
116	116	Unauthorized. Please contact the Card Issuer.
117	117	Transaction not found.
118	118	Unauthorized. Card locked.
119	119	Unauthorized. Invalid security code.
121	121	Error processing. Please try again.
122	122	Transaction previously sent.
123	123	Unauthorized. Bearer requested the end of the recurrences in the issuer.
124	124	Unauthorized. Contact Rede.

Código de erro	Amount	Descrição
204	204	Cardholder not registered in the issuer's authentication program.
373	373	No further Refund allowed.
374	374	Refund not allowed. Chargeback requested.
899	899	Unsuccessful. Please contact Rede.
3025	3025	Deny Category 01: This card should not be used
3026	3026	Deny Category 02: This card should not be used in this PV
3027	3027	Deny Category 03: No cards must be used in this PV

Simular transação com data retroativa

Para simular transação com data retroativa, nosso sandbox esta associado ao valor da transação.

Transações enviadas entre **R\$30,01 e R\$30,99** retornará com a data da captura retroativa da data atual sendo que os números dos centavos equivalem aos dias retroativos.

Por exemplo, para simular o cancelamento de uma transação em D-3.

Data atual: 23/10

Valor da transação: 30,03* (amount: 3003*)

***03 são referentes aos dias retroativos**

Data da transação gerada: 20/10

Simular transação Zero Dollar

Para simular transação zero dollar, basta enviar na requisição o "amount: 0" que a transação Zero dollar é realizada.

Lembre-se que nas transações produtivas o campo securityCode é obrigatório para Mastercard, Visa e Elo.

Para simular os retornos do emissor possíveis nas validações Zero Dollar, utilize os cenários abaixo:

Código de erro	Amount	returnMessage	Como Simular
170	0	Zero dollar transaction not allowed for this card.	Utilize o amount indicado e algum cartão de débito (exceto Elo) da tabela de Cartões de Teste
172	0	CVC2 required for Zero Dollar Transaction.	Utilize o amount indicado e qualquer cartão Elo da tabela de Cartões de Teste sem enviar o securityCode
174	0	Zero dollar transaction success.	Utilize o amount indicado e qualquer cartão de crédito (todas as bandeiras) ou débito (somente Elo) da tabela de Cartões de Teste
175	0	Zero dollar transaction denied.	Utilize o amount indicado, e qualquer cartão de crédito da tabela de Cartões de Teste e envie o campo subscription=true

Simular transação 3DS 2.0 – MPI Rede

Para simular transação 3DS 2.0 com MPI Rede, envie na requisição as informações referentes ao threeDSecure.

O retorno será "**220 - Transaction request with authentication received. Redirect URL sent**" contendo o parâmetro URL preenchido. Copie e cole a URL no seu browser para simular a tela de autenticação do emissor, pois nosso ambiente sandbox permite que seja emulado o sucesso ou falha da autenticação.

Para simular o sucesso, informe o código que é exibido na tela, caso seja informado um valor diferente, a transação será recusada.

A interface de simulação 3D Secure 2.0 da Rede. No topo, há o logo da Rede (uma empresa Itaú) e o texto "desenvolvedor". Abaixo, o título "Simulação 3D Secure 2.0" é seguido pelo valor "Valor: R\$ 25,00". Um texto instrutivo diz: "Para autenticar com sucesso, digite abaixo o código XXXX". Há um campo de entrada rotulado "código de autenticação" e um botão "confirmar" abaixo dele.

Atenção: A tela é de simulação. Em produção, a tela e as informações solicitadas variam de acordo com cada emissor.

Outra forma de estressar cenários e observar o comportamento de uma transação via 3DS2.0 no Sandbox é através dos valores preenchidos no parâmetro "Amount". Confira as possibilidades abaixo:

207 - 3DS autenticado **SEM** desafio (Jornada frictionless)

208 - 3DS autenticado com desafio **MANUAL** (Necessário interação manual, inserindo o código do desafio para autenticação)

209 - 3DS autenticado com desafio **AUTOMÁTICO** (Desafio preenchido automaticamente e encaminhado para tela de sucesso)

OBS: Indica-se a utilização dos cartões de teste já disponibilizados na documentação (Menu lateral "Tutorial Sandbox", seção "Cartões")

Simular transações com brandTid

Como mencionado na seção [Recorrência e Card-on-file](#), a bandeira Visa realiza a validação do conteúdo do campo brandTid, e pode negar a transação caso seja enviado um valor inválido.

Atualmente, a negativa dada pela Rede para este caso está contida no código *58 - Unauthorized. Contact issuer*.

Para simular esse cenário, envie sua requisição com os campos subscription= "true", storagecard=2 e amount=5,12, com qualquer valor de brandTid dentro do campo.

Simular transações Pix

Para simular a solicitação de QR Code, consultas, devoluções e consultas de devolução, utilize como base as instruções das respectivas seções apresentadas anteriormente.

Abaixo confira como simular códigos de erros específicos e o recebimento do webhook, que para apoiar sua integração possuem algumas especificidades no ambiente de testes.

Simulação de notificação de status via webhook

Para simular como ocorre o recebimento de notificação do webhook via Sandbox, faça o envio dos campos especificados abaixo que permitirão o cadastro dos eventos de Pix no seu Pv Teste. Em ambiente de testes, não é possível editar ou excluir a URL cadastrada, caso queira trocar, faça o envio de uma nova requisição com a nova URL, que substituirá a anterior automaticamente.

Nota: No ambiente sandbox, a notificação de pagamento será realizada de forma automática 2 minutos após o envio da solicitação de geração de um QR Code Pix, simulando um **pagamento** (Evento "PV.UPDATE_TRANSACTION_PIX").

Para simular o recebimento de **webhooks de devoluções** parciais feitas via canais Itaú, envie uma solicitação de QR Code no valor de R\$50,00. Após 2 minutos, você receberá a notificação no evento PV.REFUND_PIX. Em seguida, caso deseje, simule uma consulta para ver o histórico do cancelamento.

POST: </v2/transactions/notification-url>

Parâmetros da requisição:

Nome	Local de envio	Tamanho	Tipo	Descrição
authorization	header	Até 3	Alfanumérico	Header para autorização da requisição na URL fornecida pelo estabelecimento (opcional).
url	body	Até 500	Alfanumérico	URL de callback para envio de informações ao solicitante da tokenização pelo Webhook.
Authorization/type	body	--	Alfanumérico	Tipo de autorização a ser realizada na URL de callback fornecida pelo estabelecimento. Os valores possíveis são: <ul style="list-style-type: none">• Bearer• Basic
Authorization/token	body	--	Alfanumérico	Token a ser utilizado no processo de autorização na URL de callback fornecida pelo estabelecimento. Deve ser enviado no formato 'Bearer XXX' ou 'Basic XXX', de acordo com o tipo fornecido no campo anterior, onde o XXX será o token propriamente dito.

****_****Vale ressaltar que, uma vez passando o objeto authorization, o envio dos campos type e token passam a ser obrigatórios._**

Confira abaixo um exemplo de payload que deve ser enviado no sandbox para testes desse cenário

```
{
  url": "https://exemplo.userede.com.br",
  authorization:{
    "type": "Basic",
    "token": "Basic XXXXX"
  }
}
```

Em caso de envio incorreto ou erro de formato, os códigos a seguir poderão ser retornados.

Código	Mensagem	Descrição
S01	Callback URL: Required parameter missing.	Callback URL: Campo URL não foi informado
S02	Authorization Token: Required parameter missing	Authorization Token: Token não foi informado

Código	Mensagem	Descrição
503	Authorization Type: Required parameter missing	Authorization Type: Tipo de autorização não foi informado
504	Authorization Type: Invalid parameter format	Authorization Type: Campo enviado em formato inválido
505	Authorization Token: Invalid parameter format	Authorization Token: Campo enviado em formato inválido
363	Callback URL characters exceeded 500.	Callback URL: Campo URL excedeu o limite de 500 caracteres
372	Callback URL invalid format (https required).	Callback Url: Campo URL enviado em formato inválido (requer https)

Simular códigos de retorno

Para simular códigos de erros, basta enviar requisições com os valores correspondentes aos códigos de erro, conforme tabela abaixo:

Amount	Código	Mensagem	Fluxo de ocorrência
123	3036	QrCode Expired.	Consulta do QR Code
3079	3079	QrCode not processed. Try again.	Solicitação do QR Code
3081	3081	QrCode: Expiration Date invalid size.	Solicitação do QR Code
3084	3084	Error generating QrCode Image. Please use the GET Transaction for this operation.	Solicitação do QR Code
3085	3085	Error generating QrCode Image. Please try again	Consulta da transação
3089	3089	QRCode not generated, please contact Rede	Solicitação do QR Code
3090	3090	Invalid PIX Key	Solicitação do QR Code
3091	3091	Error, not generated. Try again	Devolução
3092	3092	Fail QrCode generate, please try again;	Solicitação do QR Code
3094	3094	Unsucessful. Please contact Rede.	Solicitação e devolução
3095	3095	Unknown PIX Key.	Solicitação e devolução
3096	3096	Unsucessful. Try again later.	Solicitação e devolução
3097	3097	Unavailable. Please try again later.	Solicitação e devolução
3098	3098	Service not authorized	Solicitação do QR Code
3099	3099	Communication failure. Try again later.	Solicitação e devolução
3123	3123	Devolution not confirmed.	O processo de devolução não foi concluído com sucesso. Por favor, repita a solicitação.
3125	3125	Incorrect devolution data	Devolução negada por dados incorretos Revise os dados da transação e tente novamente.

Amount	Código	Mensagem	Fluxo de ocorrência
3128	3128	Devolution blocked	Devolução negada por bloqueio em conta junto a emissor, tente novamente.
898	898	PV with invalid ip origin	Solicitação e devolução

Simular transações Voucher

Nosso sandbox funciona somente com dados de cartões selecionados, conforme tabela abaixo:

Bandeira	Tipo	Issuer	Cartão	Validade	Código de segurança	Token Informado pela Bandeira (tokenCode)	Criptograma do token Informado pela Bandeira (tokenCryptogram)
Elo	Voucher	GoodCard	4514166603616681	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Voucher	Ticket	5284776885068867	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Voucher	Alelo	4389357063526690	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Voucher	Sodexo	6363688827373622	jan/35	123	Este cartão não possui token	Este cartão não possui token
Elo	Voucher	VR	5490630354637860	jan/35	123	Este cartão não possui token	Este cartão não possui token
Visa	Voucher	-	40258800100027018	jan/35	123	Este cartão não possui token	Este cartão não possui token
Mastercard	Voucher	-	2340636000146346	jan/35	123	Este cartão não possui token	Este cartão não possui token

Para testar o campo remainingBalance, envie uma transação conforme tabela abaixo:

cardNumber	amount	remainingBalance
Qualquer cartão voucher	6000	0
Qualquer cartão voucher	6001	100

Tokenização de Bandeira Rede

Simular status das solicitações

Para simular solicitações de tokenização em diferentes status do ciclo de vida, é possível enviar os valores pré-definidos na tabela abaixo no campo cardNumber no momento da solicitação, e em seguida realizar a consulta a partir do tokenizationId gerado.

cardNumber	tokenizationStatus
0000000000000008	Inactive
0000000000000009	Suspended
0000000000000010	Delete

Simular erros de regra de negócio

Para simular erros relacionados às regras de negócio da API, é necessário realizar o envio de uma solicitação de tokenização com um valor de cardNumber dentre os listados na lista abaixo:

cardNumber	Código de erro	Mensagem de erro
0000000000000001	23	Service not enabled for this establishment

Atenção: Não é possível realizar o teste de compartilhamento de tokens entre Pontos de Venda do mesmo CNPJ no Sandbox, apenas em produção.

Simular erros de consulta de criptograma

Para simular os possíveis erros apresentados pela bandeira na solicitação do criptograma, é necessário realizar as consultas informando um dos tokenizationId disponíveis na tabela abaixo:

tokenizationId	Código de erro	Mensagem de erro
Guid_0001	29	Service temporarily unavailable
Guid_0002	30	Declined: This card is considered ineligible for tokenization at this moment
Guid_0003	31	NotAllowed: This card is considered ineligible for tokenization at this moment
Guid_0004	38	TokenCryptogram unavailable. Check the token status
Guid_0005***	-	-

Para o último caso, não será mostrado um código/mensagem de erro, mas sim a omissão da informação do campo cryptogramInfo/expirationDate.

Simular erros de bandeira

Para simular mensagens de erro da bandeira, basta enviar solicitações de tokenização um valor de cardNumber dentre os listados na lista abaixo e realizar a consulta com o tokenizationId que for gerado:

cardNumber	Bandeira	returnCode	returnMessage	brand/message	HTTP Status Code
0000000000000002	Visa	33	Failed	provisionDataExpired: The PAN information provided is considered stale	400
0000000000000003	Visa	33	Failed	cardVerificationFailed: Invalid field	403

cardNumber	Bandeira	returnCode	returnMessage	brand/message	HTTP Status Code
0000000000000004	Visa	33	Failed	cardNotEligible: This card cannot be used for tokenization at this moment	403
0000000000000005	Visa	33	Failed	cardNotAllowed: The requested action is not allowed for a given PAN	403
0000000000000006	Visa	33	Failed	declined: This card is considered not eligible for tokenization at this time	403
0000000000000007	Visa	33	Failed	notAllowed: Further operations for this card are no longer allowed. Contact your bank to resolve this issue	409

Simular configuração de webhook

Ciclo de Vida

Os cartões terão de “um-a-muitos” relacionamentos com tokens, o que significa que um único cartão estará associado a múltiplos tokens.

Os tokens são associados a um número de cartão de crédito. Um único cartão pode ter diferentes tokens associados a ele, entretanto cada token é único e específico para um determinado Merchant.

Quando um evento do ciclo de vida do cartão acontece, eles são atualizados com as informações do novo cartão. Isso traz fluidez a jornada com o Cliente tornando a gestão do ciclo de vida um dos principais benefícios da tokenização.

O status de cada token de um determinado cartão, também é independente.

Uma das funções principais do Token é controlar o seu ciclo de vida, que possui 4 status diferentes no momento: Ativo, Inativo, Suspenso e Excluído

- **Solicitado:** é o estado inicial de um token que já foi criado, mas ainda não disponibilizado e não funcional.
- **Ativo:** quando o token é disponibilizado e já pode ser utilizado
- **Suspenso:** o token está temporariamente suspenso pelo emissor, consumidor ou pelo titular do cartão.
- **Excluído:** o token está permanentemente inabilitado e não pode mais ser utilizado.

O cadastro de url para recebimento de notificações segue as definições mostradas nas tabelas a seguir.

Nota: Essa requisição, em ambiente produtivo, será feita pelo portal logado. Portanto, esse exemplo é para **direcionar o uso/simulação do recurso no ambiente de Sandbox.**

Cadastro da url de callback para o webhook de notificações:

GET: /token-service/v1/tokenization/seturl
--

Parâmetros da requisição:

Nome	Tamanho	Tipo	Obrigatório	Descrição
url	Até 256	Alfanumérico	Sim	Url de callback para envio de informações ao solicitante da tokenização pelo Webhook
authorization/type	-	Alfanumérico	Não**	Tipo de autorização a ser realizada na url de callback fornecida pelo estabelecimento. Os valores possíveis são: <ul style="list-style-type: none">• Bearer• Basic Token a ser utilizado no processo de autorização na url de callback fornecida pelo estabelecimento. Deve ser enviado no formato 'Bearer XXX' ou 'Basic XXX', de acordo com o tipo fornecido no campo anterior, onde o XXX será o token propriamente dito.
authorization/token	-	Alfanumérico	Não**	

Vale ressaltar que, uma vez passando o objeto authorization, o envio dos campos type e token passam a ser obrigatórios

Parâmetros da resposta:

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação

Simular erros de consulta da gestão do token

Para simular os possíveis erros apresentados pela bandeira ao fazer a gestão do token, é necessário realizar as consultas informando um dos tokenizationId disponíveis na tabela abaixo:

PUT: /token-service/oauth/v2/tokenization/{tokenizationId}
--

Parâmetros da Requisição

Nome	Tamanho	Tipo	Obrigatório	Descrição
tokenizationStatus	100	Alfanumérico	Sim	Se o status atualizado para qual o do token for deletar, será o delete : Se o status atualizado para qual o do token for suspender, será o suspend Se o status atualizado para qual o do token for reativar, será o resume
reason	2	Númérico	Sim	Motivo da atualização: 1 - Solicitação do Cliente 2 - Suspeita de Fraude

Parâmetros de Resposta

Nome	Tamanho	Tipo	Descrição
returnCode	Até 3	Alfanumérico	Código de retorno da solicitação
returnMessage	Até 256	Alfanumérico	Mensagem de retorno da solicitação
tokenizationId	36	Alfanumérico	Identificador único da solicitação de tokenização do cartão pela Rede
Brand/name*	-	Alfanumérico	Nome da bandeira. Ex: Visa
Brand/message*	-	Alfanumérico	Mensagem de erro da bandeira. Ex: Card not allowed

Mensagens de retorno de erros de bandeira

Os retornos de erro nas bandeiras são exibidos sempre que houver algo de errado no processo de tokenização, permitindo assim a correção imediata.

Bandeira	Return message
Visa	provisionDataExpired: The Pan information provided is considered stale.
Visa	cardVerificationFailed: Invalid field.
Visa	cardNotEligible: This card cannot be used for tokenization at this moment.
Visa	cardNotAllowed: The requested action is not allowed for a given PAN.
Visa	declined: This card is considered not eligible for tokenization at this time.
Visa	notAllowed: Further operations for this card are no longer allowed. Contact your bank to resolve this issue.
Visa	cardNotAllowed: The maximum number of tokens has been exceeded for the given PAN.
Visa	cardNotEligible: Further operations are no longer allowed. Please contact your bank to resolve the issue.
Visa	cardNotEligible: This card cannot be used for tokenization at this moment.
Visa	cardNotEligible: This card cannot be used for tokenization at this moment.
Visa	cardNotEligible: This card cannot be used for tokenization at this moment.
Visa	cardNotEligible: Further operations are no longer allowed. Please contact your bank to resolve the issue.
Visa	cardNotEligible: This card cannot be used for tokenization at this moment.
Visa	cardVerificationFailed: Further operations for this card are no longer allowed. Contact the bank to resolve this issue.
Visa	cardVerificationFailed: Your request does not have valid set of parameters required to process the business function.
Visa	cardVerificationFailed: Your request does not have valid set of parameters required to process the business function.
Visa	cardVerificationFailed: This card cannot be used for tokenization at this moment.
Visa	cardVerificationFailed: Your request does not have valid set of parameters required to process the business function.
Visa	cardVerificationFailed: This card cannot be used for tokenization at this moment.

Bandeira	Return message
Visa	declined: Visa declined this transaction because this is a case of a duplicate request while another one is inflight.
Visa	declined: Further operations are no longer allowed. Please contact your bank to resolve the issue.
Visa	declined: This card is considered not eligible for tokenization at this time.
Visa	declined: This card is considered not eligible for tokenization at this time.
Visa	invalidParameter: Unsupported token.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	invalidParameter: Your request does not have valid set of parameters required to process the business function.
Visa	failed: The requested action returned an error.
Visa	serviceError: Unknown failure BndrErrorCode in processing the request.
Visa	trConfigIssue: Input to tokenRequestorId is invalid.
Visa	trConfigIssue: Input to tokenRequestorId is invalid.
Visa	trConfigIssue: Visa declined this transaction. Please check the configurations and try again.
Mastercard	UNKNOWN: An error has occurred.
Mastercard	INVALID_PAN: The PAN information provided is invalid!
Mastercard	TOKENIZATION_INELIGIBLE: This card cannot be used for tokenization at this moment.
Mastercard	PAN_INELIGIBLE: This card's pan is ineligible for tokenization.
Mastercard	ISSUER_DECLINED: The issuer declined the tokenization attempt.
Mastercard	INVALID_STATE: Request cannot be executed due to the incorrect field value.

Retornos

Retornos de sucesso

Por padrão, sempre que uma requisição for realizada com sucesso junto a Rede, serão exibidos o código e a mensagem descrita na tabela abaixo:

Código de retorno	Descrição
00	Success

Retornos de integração - Token Requestor

Os retornos de integração são exibidos sempre que houver algo de errado na sua requisição, permitindo assim a correção imediata.

Código de erro	Descrição	HTTP Status Code
01	TokenizationId: Required parameter missing	400
02	TokenizationId: Invalid guid value	400
03	There is no data with the given guid	404
04	Email: Required parameter missing	400
05	Email: Invalid parameter size	400
06	Email: Invalid parameter format	400
07	CardNumber: Required parameter missing	400
08	CardNumber: Invalid parameter size	400
09	CardNumber: Invalid parameter format	400
10	ExpirationMonth: Required parameter missing	400
11	ExpirationMonth: Invalid parameter value	400
12	ExpirationMonth: Invalid parameter format	400
13	ExpirationYear: Required parameter missing	400
14	ExpirationYear: Invalid parameter size	400
15	ExpirationYear: Invalid parameter format	400
16	CardholderName: Required parameter missing	400
17	CardholderName: Invalid parameter size	400
18	CardholderName: Invalid parameter format	400
19	SecurityCode: Required parameter missing	400
20	SecurityCode: Invalid parameter size	400
21	SecurityCode: Invalid parameter format	400
22	Expired card	400
23	Service not enabled for this establishment	403

Código de erro	Descrição	HTTP Status Code
24	Affiliation: Invalid parameter size	401
25	Affiliation: Invalid parameter format	401
26	Affiliation: Required parameter missing	401
27	Card is from a brand not enabled for tokenization	403
28	Url: Required parameter missing	400
29	Service temporarily unavailable	503
30	Declined: This card is considered ineligible for tokenization at this moment	403
31	NotAllowed: This card is considered ineligible for tokenization at this moment	409
33	Failed	-
34	Authorization Token: Required parameter missing	400
35	Authorization Token: Invalid parameter format	400
36	Authorization Type: Required parameter missing	400
37	Authorization Type: Invalid parameter format	400
38	TokenCryptogram unavailable. Check the token status	400
39	"Service temporarily unavailable"	400
40	Authorization Type: Invalid parameter format	400
41	Declined: This card is considered ineligible for tokenization at this moment	400
42	NotAllowed: This card is considered ineligible for tokenization at this moment	400
43	NotAllowed: This affiliation is not valid (inactive/not found)	400
44	Internal error occurred. Please, contact Rede	400
45	storageCard: Required parameter missing	400
46	storageCard: Invalid parameter format	400
47	subscription: Invalid parameter format	400
48	TokenizationStatus: Required parameter missing	400
49	TokenizationStatus: Invalid value	400
50	Reason: Required parameter missing	400
51	Reason: Invalid value	400
65	Token: Required parameter missing	401

Código de erro	Descrição	HTTP Status Code
89	Token: Invalid token	401

Simular Retornos

Simular MAC

Para transações Mastercard:

- Utilizar um cartão Mastercard disponibilizado em nossa lista de cartões atrelando a ele os meses e anos para cada retorno esperado. Exemplo: ao enviar o cartão, mês: 01; ano: 2028 irão retornar o MAC 01
- Estar recebendo os retornos ABECS. Para isso, basta realizar o ajuste no campo custom header, "Transaction-Response", com o valor "brand-return-opened" preenchido.

Basta simular as transações com os valores correspondentes aos códigos de erro, conforme tabela abaixo:

Mês	Ano	amount	MAC retornado
1	2028	Sem valor específico	01
2	2028	Sem valor específico	02
3	2028	Sem valor específico	03
4	2028	Sem valor específico	04
9	2029	Sem valor específico	21
1	2030	1051	24
2	2030	1051	25
3	2030	1051	26
4	2030	1051	27
5	2030	1051	28
6	2030	1051	29
7	2030	1051	30
5	2031	Sem valor específico	40
6	2031	Sem valor específico	41
8	2031	Sem valor específico	43

Atenção: Para os MACs exclusivos do código 51 (MACs 24, 25, 26, 27, 28, 29 e 30), é necessário o envio do amount "1051".

Para transações Elo:

- Utilizar um cartão Elo disponibilizado em nossa lista de cartões atrelando a ele os meses e anos para cada retorno esperado. Exemplo: ao enviar o cartão, mês: 01; ano: 2028 irão retornar o MAC 01
- Estar recebendo os retornos ABECS. Para isso, basta realizar o ajuste no campo custom header, "Transaction-Response", com o valor "brand-return-opened" preenchido.

Basta simular as transações com os valores correspondentes aos códigos de erro, conforme tabela abaixo:

Mês	Ano	amount	MAC retornado
1	2028	Sem valor específico	01
2	2028	Sem valor específico	02

Simular retornos de retentativas

- Estar recebendo os retornos ABECS. Para isso, basta realizar o ajuste no campo custom header, “Transaction-Response”, com o valor “brand-return-opened” preenchido.

Basta simular as transações utilizando qualquer cartão, com os valores correspondentes aos códigos de erro, conforme tabela abaixo:

Amount	Código retornado
2001	N01
2002	N02
2003	N03
2004	N04
2005	N05
2006	N06
2099	N99

Dicas de Segurança

O que é um ataque de robô?

É quando os fraudadores utilizam páginas de pagamento ou tokens de APIs vazados para testar listas de cartões geradas por programas maliciosos.

Como ele acontece?

O ataque robô pode acontecer de diversas maneiras, as principais são:

Através da Página de Pagamento:

Sites e Plataformas que não possuem mecanismos de segurança para evitar spam de pedidos são alvos dos carders (fraudadores de cartões de crédito). Os fraudadores estudam a aplicação web através dos payloads HTTP POST enviados do navegador para o site. Depois de entenderem exatamente qual é a requisição que envia os dados do cartão, eles a utilizam em um script responsável pela alteração dos cartões no payload, e automatizar o envio das requisições.

Dicas para evitar este ataque:

1. Utilize o reCaptcha do Google ou o Captcha do CloudFlare: O Captcha analisa e interpreta o tráfego para bloquear as requisições feitas por bots (robôs, scripts automatizados etc.). É importante que o Captcha esteja vinculado ao back-end, impossibilitando que o fraudador tente enviar a requisição diretamente para ele. É importante configurar o tempo de validade do token gerado pelo Captcha, tornando-o curto e invalidando-o após o envio da requisição. A ausência dessas configurações pode permitir que os ataques retornem rapidamente.

2. Realize a validação do e-mail ou número de telefone: Antes de enviar a requisição para a API do e.Red, envie um código de uso único para o e-mail ou número cadastrado, para validar a transação. É importante que a validação esteja vinculada ao back-end, impossibilitando que o fraudador tente enviar a requisição diretamente para ele. Esta etapa deve preceder o envio dos dados para a API de Pagamentos.

3. Bloqueie de proxies: Realize o bloqueio de Proxies.

4. Bloqueie serviços de e-mails temporários como temp-mail.org, mohmal.com, tempmail.com, etc.

Através dos tokens comprometidos:

O comprometimento dos Tokens acontece por meio de vulnerabilidades em sites e plataformas. Através das vulnerabilidades os fraudadores conseguem acessar o banco de dados e obter os Tokens da API.

Dicas para evitar o comprometimento da Chave de Integração:

1. A chave/token deve ser criptografada usando métodos mais complexos do que o MD5.

Por exemplo:

Chave de integração armazenada no banco de dados: vzy6313fx0q0s57xullkyw589a109wd

Chave de integração criptografada em SHA256: 9a48909b9f83b827a2c4eec2a340d3534e2ea4a5fb8b0e8abd8eace00872f431

Chave de integração criptografada em SHA256 com adição de salt* (8H1n@5) na geração do hash:

a2c8d68ea678213e0e9471bf10fb888ba8b3f0ad92d869226dbbc7bc68ad8121

*O salt é utilizado para evitar que duas senhas idênticas produzam *hashes* idênticos, tornando a criptografia mais segura.

Dessa forma, mesmo que o fraudador acesse o banco de dados, a informação estará criptografada, tornando impossível tentar adivinhá-la por meio de ataques de força bruta.

2. Após inserir o Token no painel de gerenciamento da plataforma e-commerce (caso utilize), ele deve ser criptografado impossibilitando sua exibição após a inserção.

informações

[termos e condições de uso do portal](#)

[política de privacidade da Rede](#)

central de atendimento

atendimento todos os dias. 24 horas por dia.

capitais e regiões metropolitanas

(11) 4001 4433

demais localidades

0800 728 4433

acompanhe as redes sociais



para melhor navegação utilize
o browser Google Chrome