

3DSecure

Bem vindos a documentação do 3DSecure da Global Chargeback!

✔ Toda requisição para Globalcbk necessita de autenticação, no caso do Antifraude, solicitamos o envio no header a sua ClientId e ClientKey.

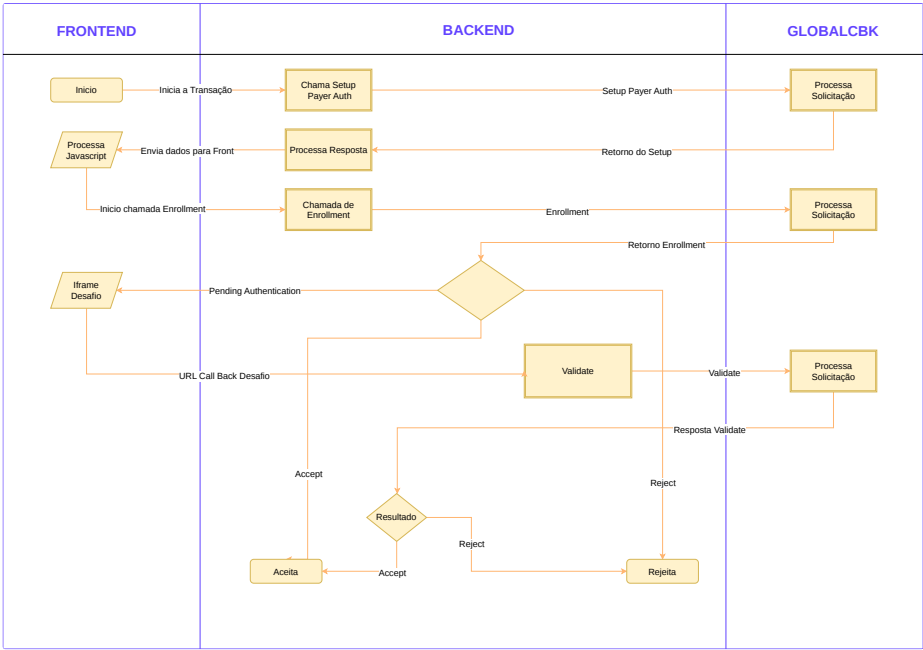
A autenticação no ambiente sandbox será com a mesma ClientId e ClientKey, porém em rotas diferentes:

sandbox: {baseUrl}/sandbox/antifraud/...

produção: {baseUrl}/antifraud/...

⚠ SDK Mobile Para integrar sua aplicação mobile com 3DS, solicite a disponibilização do SDK (Android e IOS) e da documentação, ao seu representante técnico na Global Chargeback.

Fluxo Sugerido:



1. Setup Payer Auth

No início do fluxo de autenticação de uma transação, deve ser realizada a chamada ao endpoint de setup payer auth, para iniciar o processo:

POST: {baseUrl}/sandbox/antifraud/3ds/setup

⚠ Todos os campos abaixo são obrigatórios

✓ REQUEST PAYLOAD

```
1 {
2   "clientReferenceInformation": {
3     "code": "123456"
4     //Referência ou número de rastreamento do pedido gerado pelo comerciante.
5     //Recomenda-se que você envie um valor único para cada transação,
6     //para que possa realizar buscas significativas pela transação.
7   },
8   "merchant": {
9     // Informações da loja que está vendendo os produtos.
10    // Padronize esses dados para manter o controle de suas lojas em nosso sistema.
11    "name": "Loja do Lojista",
12    "cnpj": "0561203165498",
13    "mcc": "2999"
14    // mcc = Identificador do tipo de negócio.
15  },
16  "paymentInformation": {
17    "card": {
18      "type": "001",
19      "number": "402400XXXXX2382",
20      "expirationMonth": "12",
```

```
21         "expirationYear": "2020"
22     }
23 }
24 }
```

Cartões para teste (qualquer data expiração a partir do dia atual):

Número	CVV
4622 9431 2701 3705	838
4622 9431 2701 3713	043
4622 9431 2701 3721	258

Teremos três possíveis retornos para requisições encaminhadas corretamente, são eles:

Parâmetro	Status na API
Mensagem processada com sucesso.	COMPLETED
Falha na requisição, verifique detalhes.	FAILED
Solicitação contém dados inválidos	INVALID_REQUEST

Exemplo de resposta:

▼ RESPONSE

```

1 {
2   "clientReferenceInformation": {
3     "code": "123456"
4   },
5   "consumerAuthenticationInformation": {
6     "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiIxY2Q0Mzc1Ni05NjBiLTQzZTtYtYlMS1hODQ0Wlx0ZWlnMiLCJpYXQiOjE2MTgwMDMyOTMsImZyI6IjVkbGkiLCJ1aWQiOiJkaW50IiwiaWF0Ijoi2021-04-09T21:21:33Z",
7     "deviceDataCollectionUrl": "https://centinelapistag.cardinalcommerce.com/V1/Cruise/Collect",
8     "referenceId": "a80f428d-e8b2-4a06-8b3a-ac8ad263918b",
9     "token": "AxizbwSTTWuviabJHiPmABEBURxA/B9GAES4ZNJMvriuZhTAGAAAYQGS"
10  },
11  "id": "618003293336226604006",
12  "status": "COMPLETED",
13  "submitTimeUtc": "2021-04-09T21:21:33Z"
14 }

```

2. Processar a URL de coleta de dados no Front-end

A URL e o Access Token recebidos na resposta do Setup, serão utilizados para inicializar o iframe de Device Data Collection.

2.1. Iniciar um form POST em um “hidden” iframe.

O form Action e o parametro JWT devem ser alterados com o valor recebido na URL e AccessToken.

▼ IFRAME

```

1  iframe name="ddc-iframe" height="1" width="1" style="display: none; ">
2  </iframe>
3  <form id="ddc-form" target="ddc-iframe" method="POST"
4  action="https://centinelapistag.cardinalcommerce.com/V1/Cruise/
5  Collect">
6  <input type="hidden" name="JWT" value="
7  eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiI1YWZlNGRkY2ZmNjI2YjIzNzAzOWZhM2Q1cJl3pYX
8  Q10jE0TE0tM2YtNgZlIiwiaXNzImV4cCI6MTU5MTY5MTUyOTQ3MiwiianRlPjoiNWU0MDg5MGEtN2UyNi00Z
9  tMzI3ThiTYtMTUyOTQ2ZDZmJmZiMzBiIiwiaWF0IjE5OTY5bG9hZCI6eyJB3Rpb25Db2RlIjo1U1VDOQVU
10 UyIsImlkL3Npb25ZJCiE1Yj0Y2TY2NjQ4LTFlY2YtNDZjMS1hNGYzLTBkY2E2MzQwZmFmMTA
11 iJlCjFnJvc3B1bWl1ciE1bG9hZC1lY2Y2ZmJmZiMzBiIiwiaWF0IjE5OTY5bG9hZCI6eyJB3Rpb25Db2RlIjo1U1VDOQVU
12 Edf85HyQcxZfXxmHgHFTlptSQTJfBgFTLLjA" />
13 </form>

```

2.2. Adicionar Java Script para enviar o formulario acima.


✓ SCRIPT ENVIAR FORMULARIO

```
1 <script>
2 window.onload = function() {
3   var ddForm = document.querySelector('#ddc-form');
4   if(ddForm) // ddc form exists
5     ddcForm.submit();
6 }
```

```
6 }
7 </script>
```

2.3. Criar um Listener para o retorno do Device Data Collection.

Ao receber uma resposta da URL de Device Data Collection, significa que o processo foi finalizado. A resposta é um evento de callback que possui uma mensagem com o status do processo de Device Data Collection.

 **IMPORTANTE:** A URL varia de acordo com o ambiente:

Teste: <https://centinelapistag.cardinalcommerce.com>

Produção: <https://centinelapi.cardinalcommerce.com>

SCRIPT LISTENER


```
1 <script>
2 window.addEventListener("message", (event) => {
3   if (event.origin === "https://centinelapistag.cardinalcommerce.com") {
4     let data = JSON.parse(event.data);
5     console.log('Merchant received a message:', data);
6     if (data !== undefined && data.Status) {
7       console.log('Songbird ran DF successfully');
8     }
9   } else{
10    console.log('Message from different origin.');
```


Payload do Callback:

```
1 {
2   "MessageType": "profile.completed",
3   "Session Id": "f54ea591-51ac-48de-b908-eecf4ff6beff",
4   "Status": true
5 }
```

3. Efetuar a chamada ao Enrollment do 3DS

Este passo descreve a chamada via backend que será realizada para solicitar a autenticação da transação. Deve ser executada sempre após a execução de todos os itens dos passos anteriores. Os campos descritos abaixo são os mínimos/obrigatórios, para que a transação siga no fluxo de verificação.

 POST: {baseUrl}/sandbox/antifraud/3ds/authentications

 Todos os campos abaixo são obrigatórios

REQUEST PAYLOAD

```
1 {
2   "clientReferenceInformation": {
3     "code": "cybs_test"
4   },
5   "orderInformation": {
6     "amountDetails": {
7       "currency": "BRL",
8       "totalAmount": "10.99"
9     },
10    "lineItems": [
11      {
12        "unitPrice": "144.14",
13        "quantity": "2",
14        "productSKU": "123456",
15        "productName": "teste",
16        "productCode": "1234"
17      }
18    ],
19    "billTo": {
20      "address1": "1 Market St",
21      "administrativeArea": "CA",
22      "country": "US",
23      "locality": "san francisco",
24      "firstName": "John",
25      "lastName": "Doe",
26      "phoneNumber": "4158880000",
27      "email": "test@cybs.com",
28      "postalCode": "94105"
```

```

29     }
30 },
31 "paymentInformation": {
32     "card": {
33         "type": "001",
34         "expirationMonth": "12",
35         "expirationYear": "2025",
36         "number": "XXXXXXXXXXXXXX"
37     }
38 },
39 "buyerInformation": {
40     "merchantCustomerId": "",
41     "mobilePhone": "1245789632"
42 },
43 "deviceInformation": {
44     "ipAddress": "",
45     "httpAcceptBrowserValue": "",
46     "httpAcceptContent": "",
47     "httpBrowserLanguage": "",
48     "httpBrowserJavaEnabled": "",
49     "httpBrowserJavaScriptEnabled": "",
50     "httpBrowserColorDepth": "",
51     "httpBrowserScreenHeight": "",
52     "httpBrowserScreenWidth": "",
53     "httpBrowserTimeDifference": "",
54     "userAgentBrowserValue": ""
55 },
56 "merchantInformation": {
57     "merchantDescriptor": {
58         "url": ""
59     },
60     "merchantName": ""
61 },
62 "acquirerInformation": {
63     "acquirerBin": "",
64     "merchantId": ""
65 },
66 "consumerAuthenticationInformation": {
67     "deviceChannel": "",
68     "mcc": "",
69     "messageCategory": "",
70     "overridePaymentMethod": "",
71     "productCode": "",
72     "returnUrl": "",
73     "requestorId": "",
74     "requestorName": "",
75     "referenceId": "",
76     "transactionMode": "MOTO"
77 }
78 }
79

```

Caso todos os campos especificados no item anterior sejam enviados com valor e formato correto, a mensagem de requisição será processada e vai gerar uma resposta com os campos abaixo.

Obs.: Para casos em que ocorra uma exceção (dados faltantes/inválidos), verifique documentação completa da Globalcbk para os tratamentos. Foram detalhados os campos mais relevantes da resposta.

▼ RESPONSE

```

1  {
2      "clientReferenceInformation": {
3          "code": "398b4815-19ed-425e-a7b2-1781c24289f4"
4      },
5      "consumerAuthenticationInformation": {
6          "eciRaw": "05",
7          "authenticationTransactionId": "Uym2i02tq8zmRD3o13h0",
8          "strongAuthentication": {
9              "OutageExemptionIndicator": "0"
10         },
11         "eci": "05",
12         "token": "AxjzbwSTcFEDvSNUaagZ/+MBURy20E7z7QfIYEQyaSZeJFyPaiAKAAAAxQLR",
13         "cavv": "Y2FyZGluYXxb21tZXJjZWFlRGg=",
14         "paresStatus": "Y",
15         "acsReferenceNumber": "Cardinal ACS",
16         "xid": "Y2FyZGluYXxb21tZXJjZWFlRGg=",
17         "directoryServerTransactionId": "aa1d6c24-a0bf-4e67-9695-19714997a34a",
18         "veresEnrolled": "Y",
19         "threeDSServerTransactionId": "6aa9174a-bb21-4175-bf68-e50445ac7d72",
20         "acsOperatorID": "MerchantACS",
21         "ecommerceIndicator": "v bv",
22         "specificationVersion": "2.1.0",
23         "acsTransactionId": "ba4a1f0b6f7f-4e00-9510-7c01052c8789"

```

```
24 },
25 "id": "679423953662655004953",
26 "paymentInformation": {
27   "card": {
28     "bin": "400000",
29     "type": "VISA"
30   }
31 },
32 "status": "AUTHENTICATION_SUCCESSFUL",
33 "submitTimeUtc": "2023-03-21T18: 39: 14Z"
34 }
```

4. Processamento de um Desafio

Quando o retorno da solicitação de autenticação indicar a necessidade de processar um desafio, deverá ser efetuada a operação no cliente, através da função abaixo.

4.1 - Realizar o decode do dado base64URL retornado no campo consumerAuthentication.paReq. No dado decodificado buscar o valor de challengeWindowSize. O dado retornado indica o tamanho iframe de desafio, conforme tabela abaixo.

Challenge Window Size	Step-up iframe Dimensions (Width x Height)
01	250 x 400
02	390 x 400
03	500 x 600
04	600 x 400
05	Full Screen

4.2 - Iniciar um form POST em um "hidden" iframe. OBS: o form Action e o parametro JWT devem ser alterados com o valor recebido na stepUpUrl e AccessToken. O Height e Width deve levar em consideração a tabela do item (a).

```
1 <iframe name=" step-up-iframe" height="250" width="400"></iframe>
2 <form id="step-up-form" target=" step-up-iframe" method="POST"
3 Action="https://centinelapistag.cardinalcommerce.com/V2/Cruise/StepUp">
4 <input type="hidden" name="JWT" value="
5 eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiI1YWZlNGRKY2ZmNjI2YjIzNzA2OWZhM2Q0iLCJpYX
6 Qi0jE1OTEwMTgyNzIsImV4cCI6MTU5MTEyNTQ3MiwiianRpIjoibWU4MDg5MGEtN2UyNi00Z
7 mI3LThiYTUtNjQ2ZDU0NjJiMzBkIiwiaWF0IjE6eYJBY3Rpb25Db2RlIjoiaUIVDQ0VT
8 UyIsIlNlc3Npb25JZCI6IjY0ZTY2NjQ4LTFkYzYtNDZjMS1hNGYzLTBkYzE2MzQwZmFmMTA
9 iLCJFcnJvc51bWJlciI6MCwiRXJyb3JlZCJmcmVudGlvbiI6I1NlY2Nlc3MiOiF0. j8EPWE
10 EDf85hYQcxFzXxmHqHFTlptSQITJgfBGtLLjA" />
11 </form>
```

4.3 - Adicionar Javascript para invocar o formulário do desafio.

```
1 <script>
2 window.onload = function() { var stepUpForm = document.querySelector('# step-up-form'); if(stepUpForm) // Step-Up form
3 exists stepUpForm.submit(); }
4 </script>
```

4.4 - O retorno do desafio, será enviado para a URL de callback definida e enviada na chamada, com os seguintes dados..

TransactionId=BwNsDeDPsQV4q8uy1Kq1&

MD=null

⚠ IMPORTANTE: O transactionID é o valor recebido no retorno do desafio, será utilizado no próximo passo (Validate) para recuperar o resultado do desafio.

5. Validar o Resultado da Autenticação.

Para receber o resultado do desafio, será necessário realizar a chamada de authentication-results utilizando os dados recebidos na URL de callback do desafio.

i POST: {baseUrl}/sandbox/antifraud/3ds/authentications-results

⚠ Todos os campos abaixo são obrigatórios

```
1 {
2   "clientReferenceInformation": {
3     "code": "123456"
4   },
5   "consumerAuthenticationInformation": {
6     "authenticationTransactionId": "yX2oPizvbGxoeB00A011"
```

```
7 } // TransactionId recebido no callback do desafio.  
8 }
```

6. Apêndice. [↗](#)

Campos relevantes para a avaliação do fluxo de autenticação

a. Retorno da Elegibilidade à Autenticação. [↗](#)

Campo `vres_enrolled`: [↗](#)

- Y – Yes, Bank is participating in 3-D Secure protocol and will return the ACSUrl
- N – No, Bank is not participating in 3-D Secure protocol
- U – Unavailable, The DS or ACS is not available for authentication at the time of the request
- B – Bypass, Merchant authentication rule is triggered to bypass authentication in this use case

b. Identificação do Status de Retorno da Autenticação. [↗](#)

Campo `consumerAuthenticationInformation.paresStatus`: [↗](#)

- Y – Successful Authentication
- N – Failed Authentication / Account Not Verified / Transaction Denied
- U – Unable to Complete Authentication
- A – Successful Attempts Transaction
- C – Challenge Required for Authentication
- R – Authentication Rejected (Merchant must not submit for authorization)
- D – Challenge Required; Decoupled Authentication confirmed.
- I – Informational Only; 3DS Requestor challenge preference acknowledged.

c. Indicador de Autenticação. [↗](#)

Campo `consumerAuthenticationInformation.eciRaw`: [↗](#)

- 02 or 05 – Fully Authenticated Transaction
- 01 or 06 – Attempted Authentication Transaction
- 00 or 07 – Non 3-D Secure Transaction
- 04 – Data Only

d. Razão dos Status da Transação [↗](#)

Campo `Status`: [↗](#)

- AUTHENTICATION_SUCCESSFUL
- PENDING_AUTHENTICATION
- INVALID_REQUEST
- AUTHENTICATION_FAILED
- INFORMATIONAL ONLY

Campo `errorInformation.reason`: [↗](#)

- INVALID_MERCHANT_CONFIGURATION
- CONSUMER_AUTHENTICATION_REQUIRED
- CONSUMER_AUTHENTICATION_FAILED
- AUTHENTICATION_FAILED

e. Informações Complementares para melhor experiência de Autenticação [↗](#)

Campo `consumerAuthenticationInformation.cardholderMessage` [↗](#)

Mensagem de texto fornecida pelo ACS/Emissor para o portador durante um processo de autenticação Frictionless. Envio da informação opcional para o emissor.

7. Cenários dos Fluxos de Autenticação 2.0

Quando **vres_enrolled = N** – Emissor não participante do Protocolo 2.x
Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação não Segura (não autenticada).

Quando **vres_enrolled = U** – Indisponível, Campos do 3DS inválidos
Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação Não Segura (não autenticada) e **directoryServerErrorCode** e **directoryServerErrorDescription** com maior detalhamento do motivo.
Obs.: Importante verificar os campos mandatórios e seus respectivos conteúdos.

Desafio Requerido (Challenge)

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = PENDING_AUTHENTICATION**

Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação não Segura (não autenticada).

Autenticação Declínada

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = AUTHENTICATION_FAIL**

E, Campo **consumerAuthenticationInformation.paresStatus = R** – Autenticação Rejeitada Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação não Segura (não autenticada)

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = AUTHENTICATION_FAIL**

E, Campo **consumerAuthenticationInformation.paresStatus = N** – Falha na Autenticação

Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação não Segura (não autenticada).

Autenticação Processada

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = AUTHENTICATION_SUCCESSFUL**

E, Campo **consumerAuthenticationInformation.paresStatus = A** – Attempt

Então, Campo **consumerAuthenticationInformation.eciRaw = 06/01**

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = AUTHENTICATION_SUCCESSFUL**

E, Campo **consumerAuthenticationInformation.paresStatus = Y** – Autenticação com Sucesso Então, Campo **consumerAuthenticationInformation.eciRaw = 05/02** – Transação Segura (autenticada)

Quando **vres_enrolled = Y** – Emissor participante do Protocolo 3DS 2.x

E, Campo **Status = AUTHENTICATION_SUCCESSFUL**

E, Campo **consumerAuthenticationInformation.paresStatus = U** – Autenticação não completa Então, Campo **consumerAuthenticationInformation.eciRaw = 07/00** – Transação não Segura (não autenticada)

Ou Campo **consumerAuthenticationInformation.eciRaw = 04** – Mastercard DataOnly (não autenticada)

8. Informações Adicionais

Dados de Adquirente e Registro nas Bandeiras:

Os dados de adquirente (AcquirerBIN, AcquirerMID, MCC) devem ser solicitados ao adquirente que fará o processo de autorização com as bandeiras.

Algumas bandeiras como Mastercard e ELO, solicitam um cadastramento prévio do estabelecimento para participação no programa 3DS 2. Este cadastramento é sempre realizado pelo adquirente.

Para formatação dos dados de requestorID e requestorName, converse com seu representante técnico na GlobalCbK.

Card Types:

Numero	Bandeira
001	Visa
002	Mastercard, Eurocard
003	American Express
004	Discover

005	Diners Club
006	Carte Blanche
007	JCB
014	EnRoute
021	JAL
024	Maestro (UK Domestic)
033	Visa Electron (SIX)
034	Dankort
036	Cartes Bancaires
037	Carta Si
039	Encoded account number
040	UATP
042	Maestro (International)
050	Hipercard
051	Aura
054	Elo
058	Carnet
062	China UnionPay