



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do SUS
Coordenação de Interoperabilidade em Saúde

MANUAL DE CONFIGURAÇÃO DE AMBIENTES POSTMAN

Versão 1.0

1. Objetivo	3
2. Certificado Digital	3
3. Segurança	4
4. Download POSTMAN	5
5. Configurar ambientes POSTMAN	6
5.1. Configurando o ambiente de homologação	6
5.2. Configurando o ambiente de produção	8
6. Configuração da Collection	10
7. Realizar consultas em ambiente de homologação	14
7.1. Gerar token em ambiente de homologação	14
7.2. Consulta por número CNS	15
7.3. Consulta por número CPF	16
8. Realizar consultas em ambiente de produção	17
8.1. Gerar token em ambiente de produção	17
8.2. Consulta por número CNS	18
8.3. Consulta por número CPF	19
9. Erros possíveis	20
9.1. Erro 401 Unauthorized	20
9.2. Erro 404 Not Found	21
9.3. Erro INCORRECT_PASSWORD	22
10. Suporte	23

1. Objetivo

Este documento tem por objetivo detalhar tecnicamente como será realizada a autenticação nos serviços da API do Cartão Nacional de Saúde (CNS), do Ministério da Saúde (MS), utilizando o serviço **GET@/api/osb/token** no componente EHR Auth, por meio da ferramenta de testes de API POSTMAN.

2. Certificado Digital

O certificado digital é premissa obrigatória para acesso à API do CNS, e ele é um dos controles principais de segurança utilizado na rede. O certificado digital permite a identificação incontestável do autor de uma mensagem ou transação feita em meios eletrônicos (não-repúdio).

Para obter credencial de acesso e realizar transações na API, é necessária a utilização do certificado digital do estabelecimento de saúde principal. Vale contextualizar que os estabelecimentos que emitem nota fiscal ou acessam algum portal do governo já possuem um certificado A1 do tipo e-CNPJ.

No contexto de uso do CPF da pessoa responsável pelo estabelecimento e custódia da credencial de acesso à API (solicitante do acesso no Portal de Serviços), vinculada ao estabelecimento de saúde, este pode ser realizado com a utilização do certificado A1 do tipo e-CPF. Os certificados devem ser da cadeia Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Para a solicitação da credencial no Portal de Serviços do DataSUS (disponível em: <https://servicos-datasus.saude.gov.br/>), quando o usuário carrega (*upload*) o seu certificado digital (chave pública “.cer” ou privada “.pfx”), ocorre a captura das informações de CNPJ ou CPF e o respectivo período de vigência do certificado.

Em nenhum momento é capturada a informação da sua chave privada, ela precisa ser instalada na máquina porque é necessária ao esquema de autenticação “*two way ssl*”, onde é imprescindível ter um certificado digital em cada um dos serviços (pontas) para poder trocar um token (assinado entre ambos), promovendo assim uma comunicação segura.

Nota 1: O certificado digital usado na integração com a API **deverá ser o mesmo informado na solicitação da credencial de acesso**, realizada no Portal de Serviços do DataSUS, e ficará associado ao estabelecimento de saúde informado na solicitação de acesso.

Nota 2: A ferramenta de testes de API Postman não aceita certificado digital do tipo .CER. Com isso, sugerimos que para melhor fluxo de testes e integração com as API`s, seja utilizado o certificado digital do tipo A1 de extensão .PFX.

3. Segurança

Somente com uma solicitação de acesso aprovada será possível realizar o consumo dos serviços (Web Services) do EHR Services.

Após a aprovação, o primeiro passo para realizar o consumo dos serviços é realizar a autenticação utilizando o serviço **GET@/api/osb/token** no componente EHR Auth. Durante o processo de autenticação, é verificado se o certificado digital está dentro do respectivo período de vigência e, se ele, ou um de seus superiores na cadeia, foi revogado.

Caso não ocorra nenhum destes problemas, a operação de autenticação será realizada com sucesso e será retornado um *token* (access_token) com tempo de vida de 30 (trinta) minutos. Este token deverá ser utilizado como token de autenticação nas chamadas dos serviços (web services). A estrutura do *token* retornado é a seguinte:

```
{
  "access_token":
  "eyJraWQiOiJybRzIGhvbSIsImFsZyI6IiJTMjU2In0.eyJzdWliOiIxMDE2NDMzMzYwNiIsInBlc3
  NvYSI6eyJmaXNpY2EiOnRydWUsImkZW50aWZpY2Fkb3liOiIxMDE2NDMzMzYwNiJ9LCJpc3
  MiOiJSTkRTLUhNRylsImV4cCI6MTY3MjkyOTUzOSwiaWF0IjoxNjcyOTI3NzYwMjYwZp
  Y2Fkbyl6eyJzdWJqZWN0IjoiQ049TUFSQ1VTIFZJTkdSVVtIERFIE9MSVZFSVJBIFNB
  TIRPUzoxMDE2NDMzMzYwNixPVT12aWRlbnV4bmZlcmV4Y2lhLE9VPTE1NTkwOTIxMDAw
  MTI5LE9VPShtFTSBCUkFOQ08pLE9VPVJGQibILUNQRiBBMSxPVT1TZWNyZXRhcmIhIGR
  hIFJl...",
  "scope": "read write",
  "token_type": "jwt",
  "expires_in": 1800000
}
```

A autenticação com certificado digital da API utiliza a técnica chamada “Two-way SSL”, comunicação SSL de duas vias (cliente e servidor). No “Two-way SSL”, além do certificado do servidor, o cliente também deve utilizar um certificado válido. A validade do certificado digital será verificada no momento da autenticação. Por outro lado, na autenticação SSL (ou “One-way SSL”) somente o certificado digital do servidor deve ser válido e verificado.

Nota 3: Ressalta-se que o certificado digital deve ser usado somente para realizar a autenticação e gerar o token.

A partir desse momento, o token é seu ‘ticket’ de passe e todas as chamadas devem ser realizadas utilizando somente este, o que não gera degradação de performance relacionada ao uso do certificado digital. Por isso, recomenda-se reutilizar o ‘ticket ao máximo durante seu tempo de vida’ e, só então, gerar um novo token repetindo a operação de autenticação com ‘Two-way SSL’.

4. Download POSTMAN

a. Faça o download do Postman, disponível no link: <https://www.postman.com/>

produtos ▾ Preços Empreendimento ▾ Recursos e Suporte ▾ Explorar

Procurar cartão

Entrar Inscreva-se gratuitamente

Deb... APIs juntas

Mais de 20 milhões de desenvolvedores usam o Postman. Comece inscrevendo-se ou baixando o aplicativo para desktop.

jsmith@example.com Inscreva-se gratuitamente

Baixe o aplicativo de área de trabalho

O que é Carteiro?

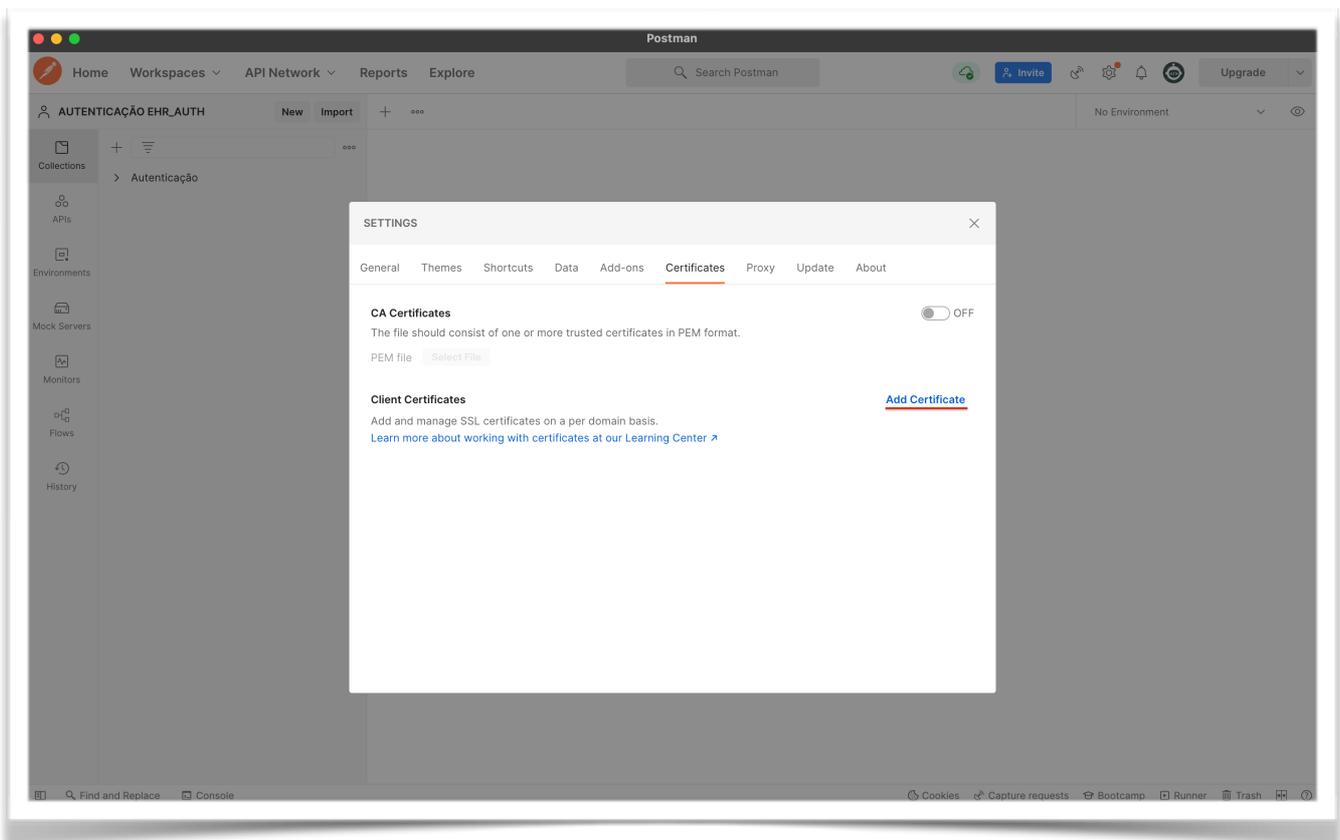
O Postman é uma plataforma de API para criar e usar APIs. O Postman simplifica cada etapa do ciclo de vida da API e agiliza a colaboração para que você possa criar APIs melhores com mais rapidez.

- Ferramentas da API
- Repositório de APIs
- espaços de trabalho
- Governança

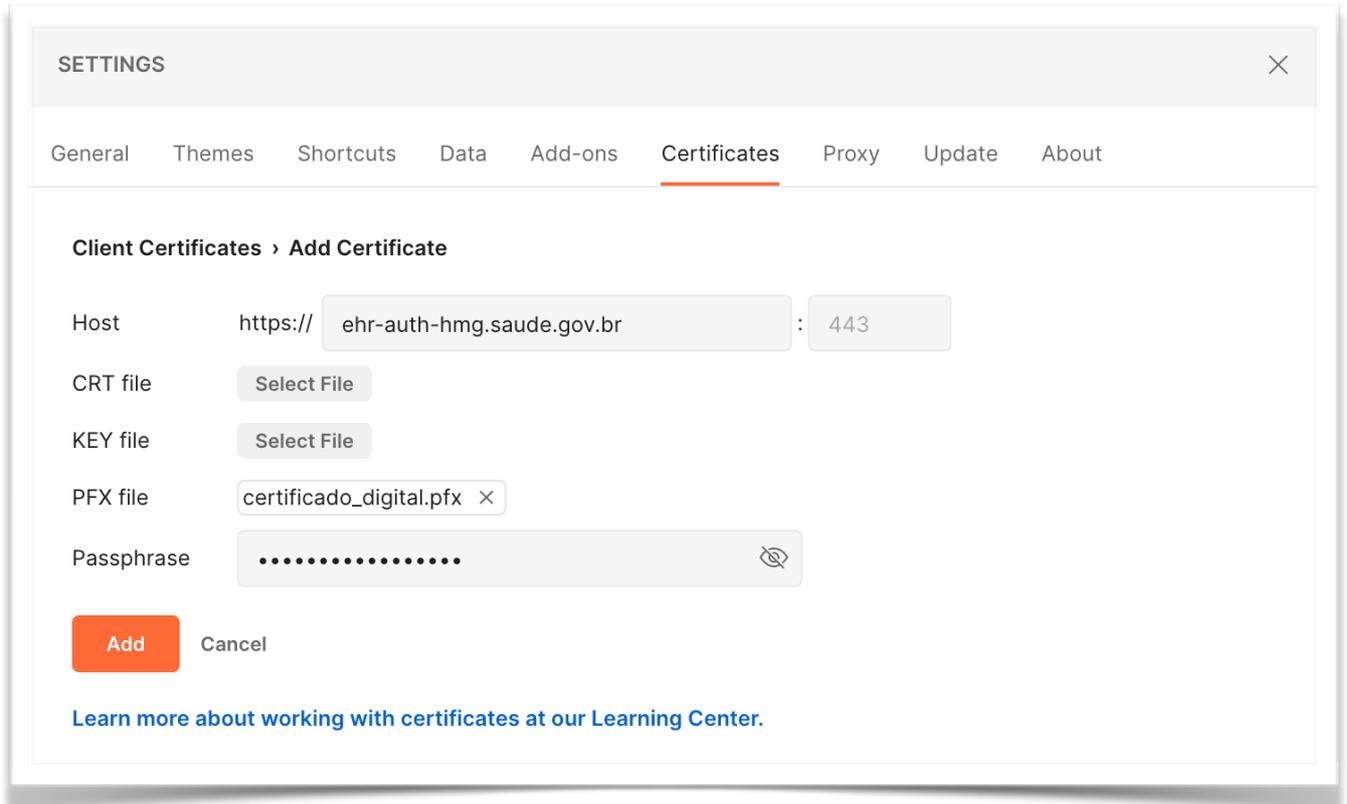
5. Configurar ambientes POSTMAN

5.1. Configurando o ambiente de homologação

- a. Abra o Postman, clique em Configurações (settings), na aba de opções, clique em Certificados (Certificates) e depois em Adicionar Certificado (Add Certificate).

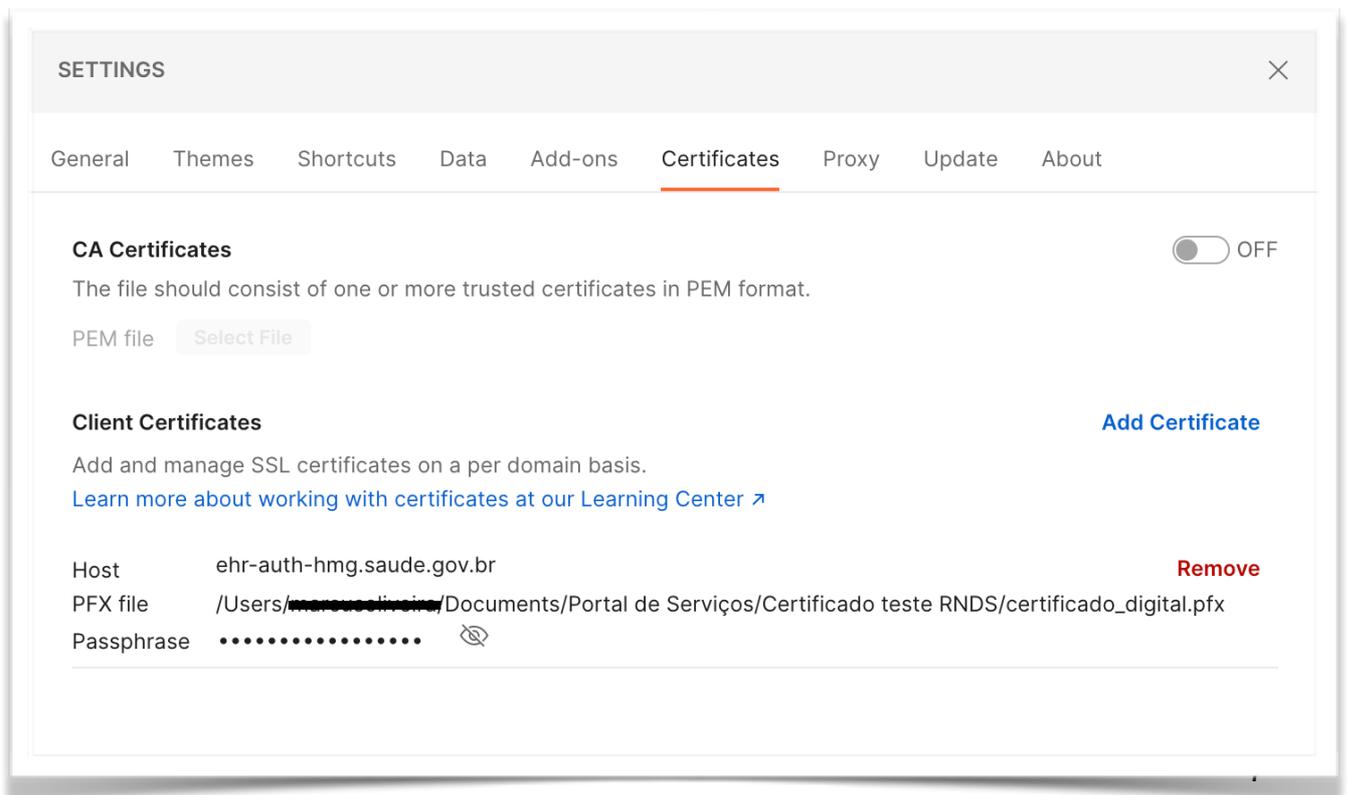


- b. Após abrir a tela de adicionar certificado, digite a URL do host de homologação ehr-auth-hmg.saude.gov.br. Em PFX arquivo (pfx file), adicione o arquivo do certificado digital. Em Senha (Passphrase), digite a senha do certificado digital.



The screenshot shows the 'SETTINGS' window with the 'Certificates' tab selected. The 'Client Certificates > Add Certificate' dialog is open. The 'Host' field contains 'https:// ehr-auth-hmg.saude.gov.br : 443'. The 'CRT file' and 'KEY file' fields have 'Select File' buttons. The 'PFX file' field contains 'certificado_digital.pfx' with a close button. The 'Passphrase' field is masked with dots and has an eye icon. At the bottom, there are 'Add' and 'Cancel' buttons. A link 'Learn more about working with certificates at our Learning Center.' is also present.

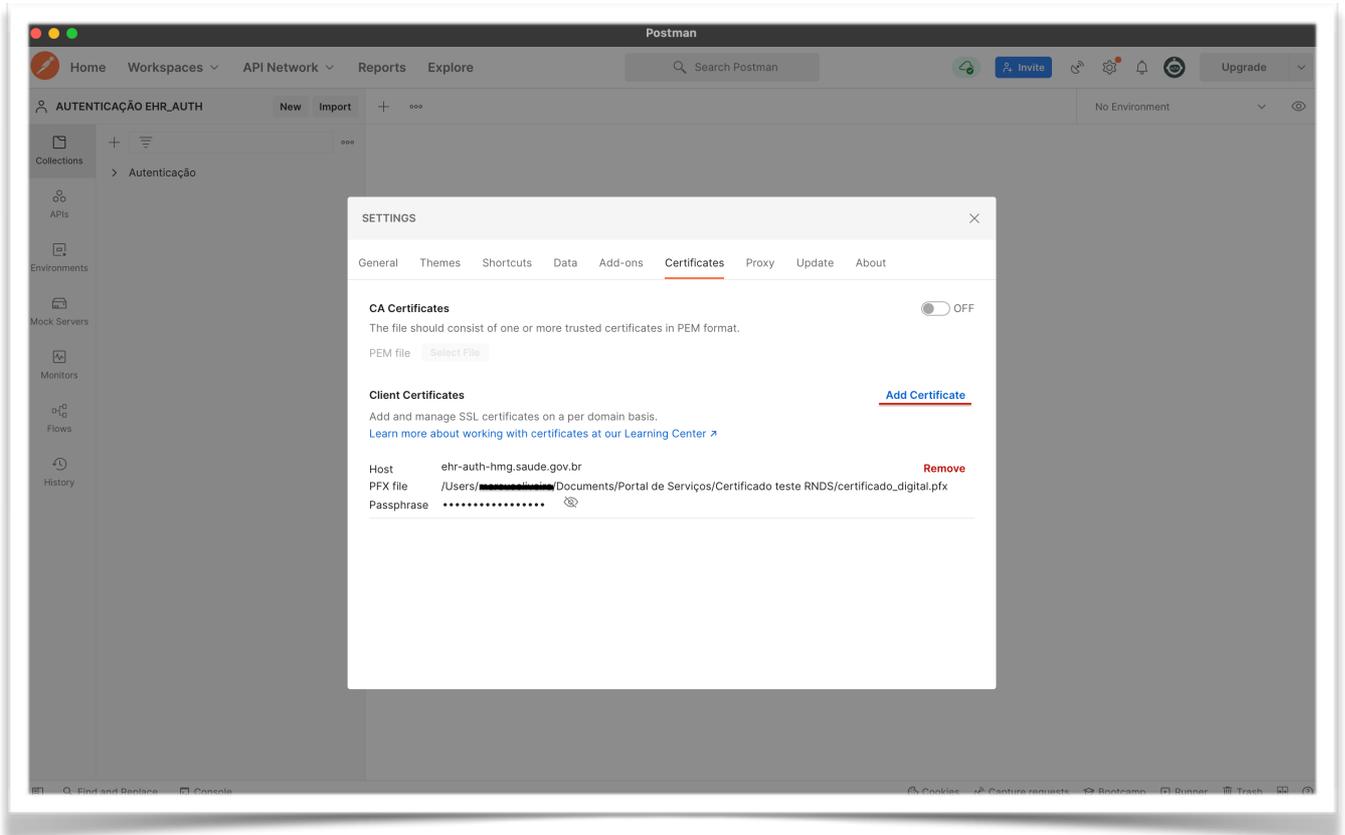
- c. Depois que as configurações estiverem inseridas, clique em Adicionar (add). Na sequência, o certificado digital foi configurado para o ambiente de homologação.



The screenshot shows the 'SETTINGS' window with the 'Certificates' tab selected. The 'CA Certificates' section has a toggle switch set to 'OFF'. The 'Client Certificates' section has an 'Add Certificate' button. Below, a list of certificates is shown with the following details: Host: ehr-auth-hmg.saude.gov.br, PFX file: /Users/mauricio/Documents/Portal de Serviços/Certificado teste RNDS/certificado_digital.pfx, and Passphrase: masked with dots and an eye icon. A 'Remove' button is visible next to the certificate entry.

5.2. Configurando o ambiente de produção

- a. Abra o Postman, clique em Configurações (settings), na aba de opções, clique em Certificados (Certificates) e depois em Adicionar Certificado (Add Certificate).



- b. Após abrir a tela de adicionar certificado, digite a URL do host de produção ehr-auth.saude.gov.br. Em PFX arquivo (pfx file), adicione o arquivo do certificado digital. Em Senha (Passphrase), digite a senha do certificado digital.

The screenshot shows the 'SETTINGS' window with the 'Certificates' tab selected. The 'Add Certificate' form is displayed with the following fields:

- Host: `https://` `:`
- CRT file:
- KEY file:
- PFX file:
- Passphrase:

At the bottom of the form, there are two buttons: (orange) and (grey). Below the buttons is a link: [Learn more about working with certificates at our Learning Center.](#)

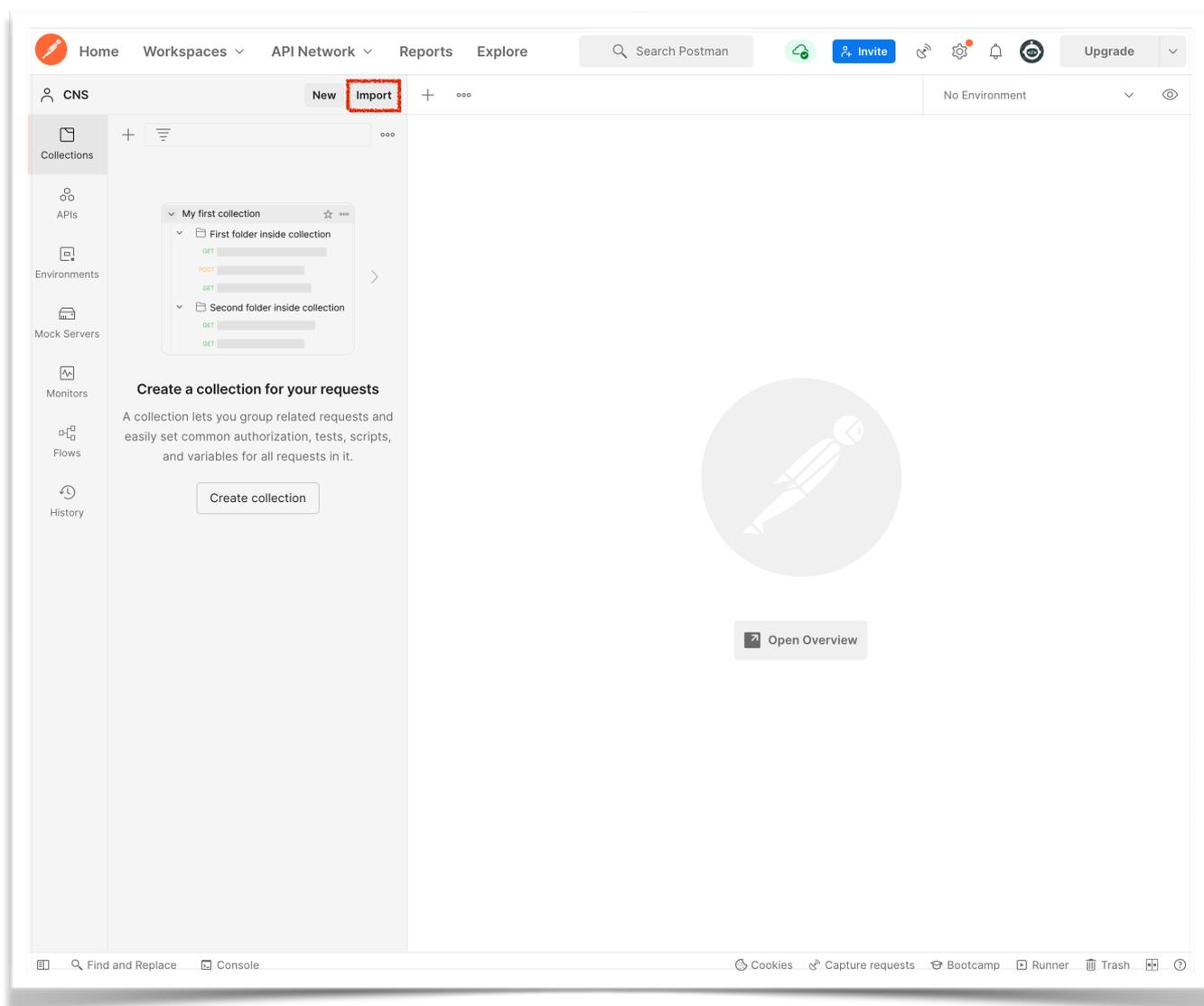
- c. Depois que as configurações estiverem inseridas, clique em Adicionar (add). Pronto, o certificado digital foi configurado para o ambiente de produção.

The screenshot shows the 'SETTINGS' window with the 'Certificates' tab selected. The 'CA Certificates' section is turned OFF. The 'Client Certificates' section is active, showing a list of configured certificates:

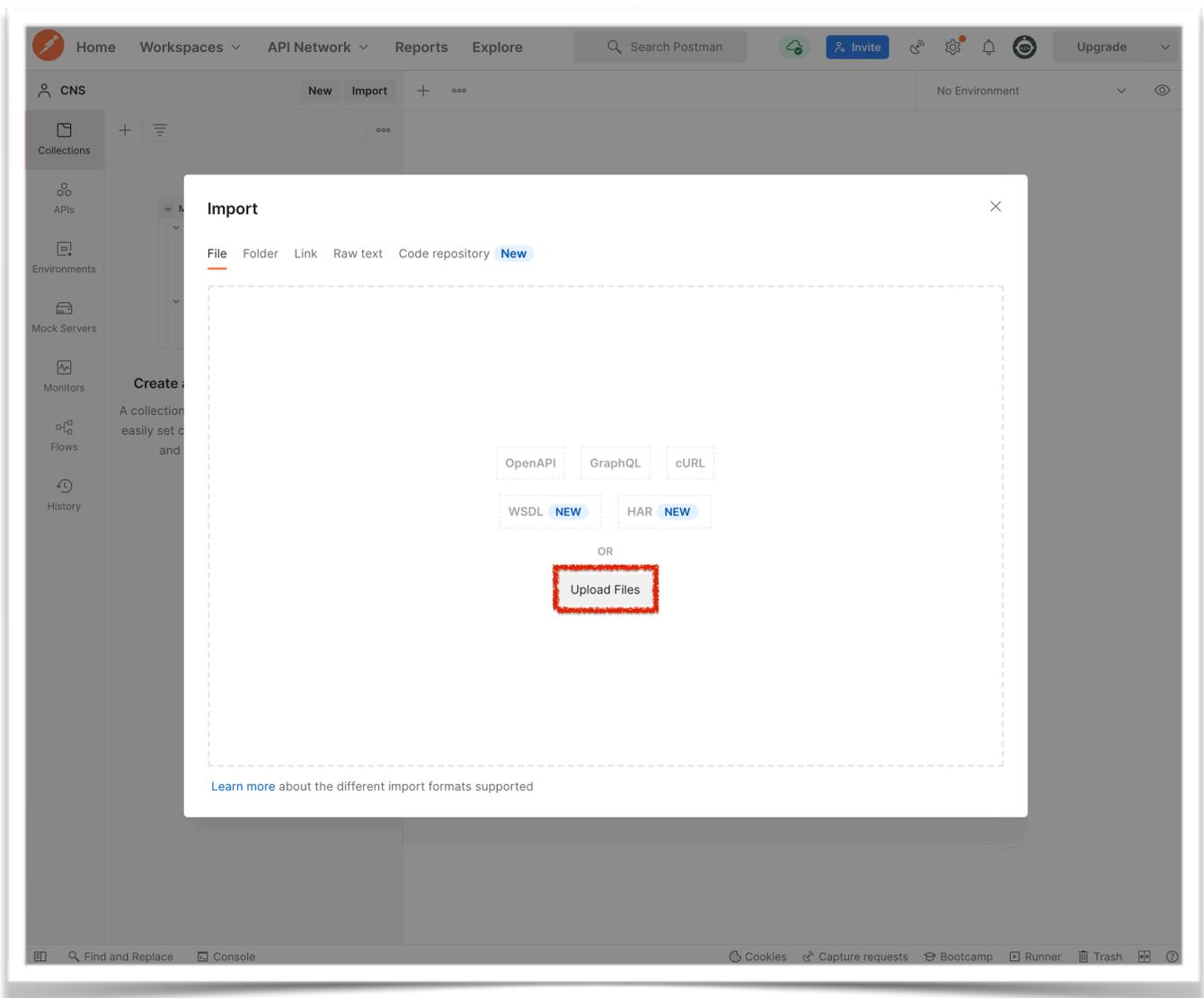
- CA Certificates** OFF
The file should consist of one or more trusted certificates in PEM format.
PEM file
- Client Certificates**
Add and manage SSL certificates on a per domain basis.
[Learn more about working with certificates at our Learning Center](#)
- Host: `ehr-auth-hmg.saude.gov.br`
PFX file: `/Users/mauricio.lima/Documents/Portal de Serviços/Certificado teste RNDS/certificado_digital.pfx`
Passphrase:
- Host: `ehr-auth.saude.gov.br`
PFX file: `/Users/mauricio.lima/Documents/Portal de Serviços/Certificado teste RNDS/certificado_digital.pfx`
Passphrase:

6. Configuração da Collection

- Acesse o banner do CNS no Portal de Serviços do DataSUS (<https://servicos-datasus.saude.gov.br/detalhe/tgKoKpju8s>) e faça o download do arquivo CNS-PDQ.postman_collection.json.
- Após o download da collection, clique em Import.

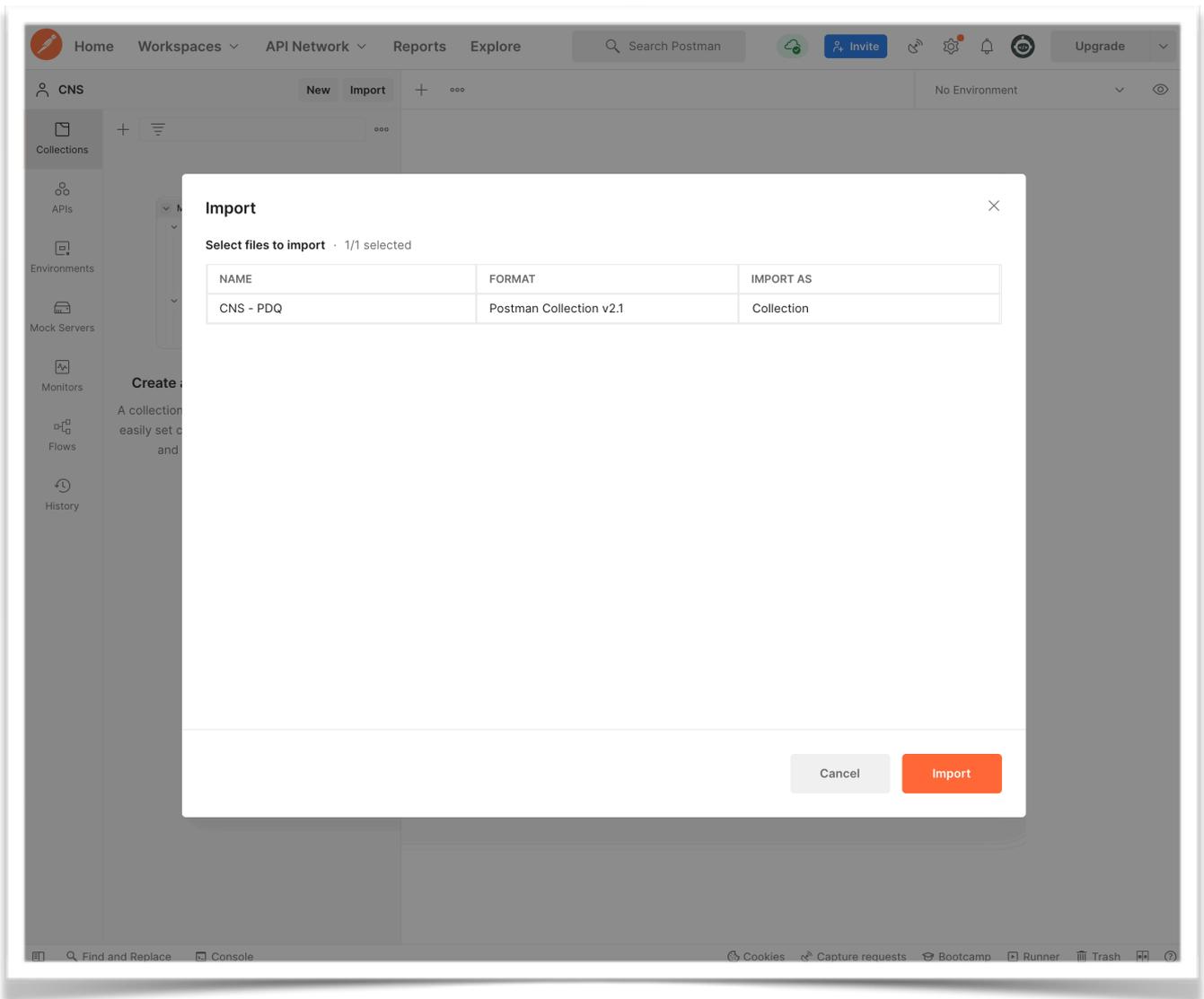


- c. Após clicar em Import, apresenta-se uma tela para que seja localizado o arquivo da Collection baixada. Clique em Upload Files.

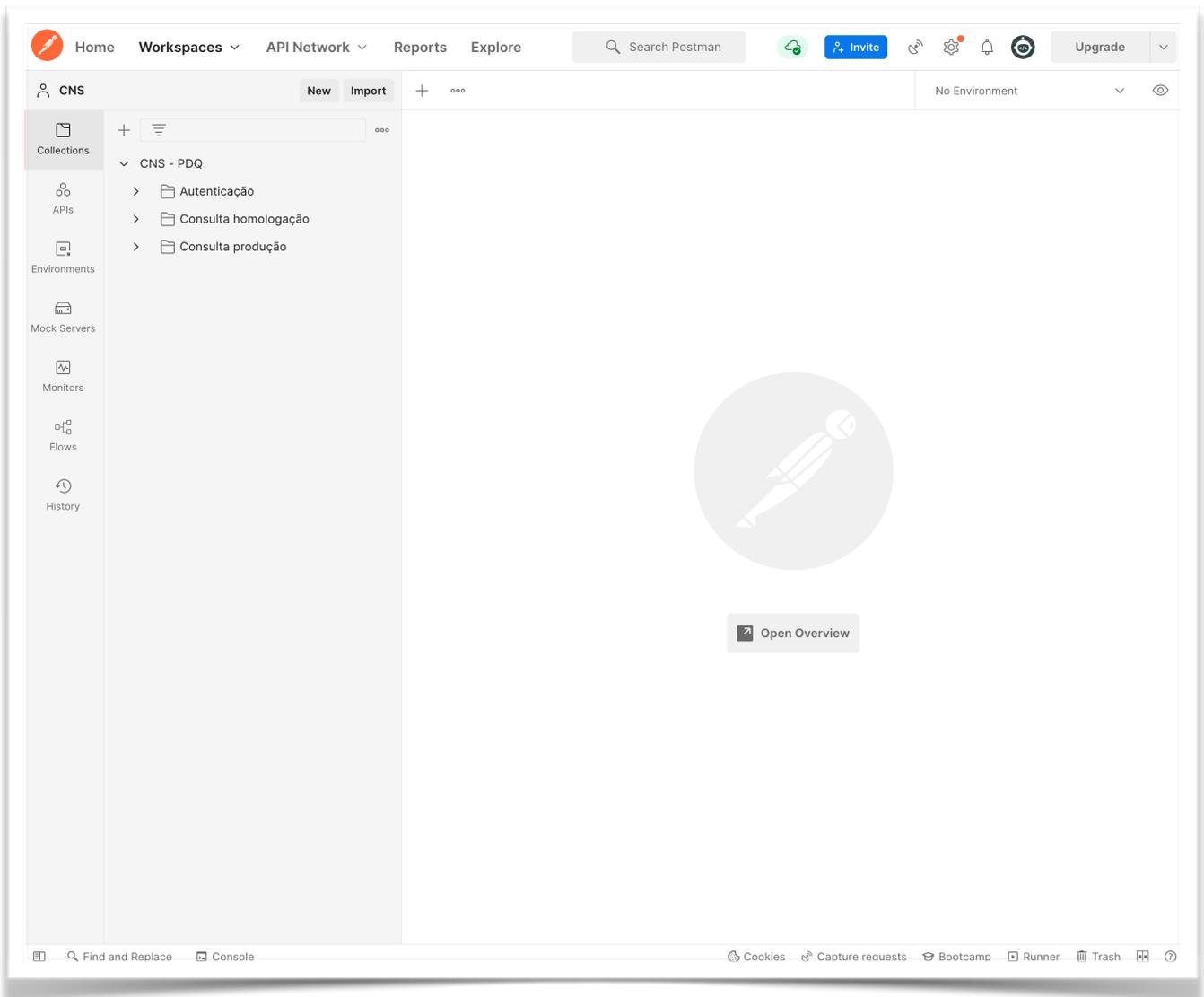


- d. Após clicar Upload Files, apresenta-se uma tela para que seja localizado o arquivo da Collection baixada. Localize o arquivo e clique em Open (abrir).

e. Após clicar em Abrir, apresenta-se uma tela com os detalhes da Collection. Clique em Importar (Import).



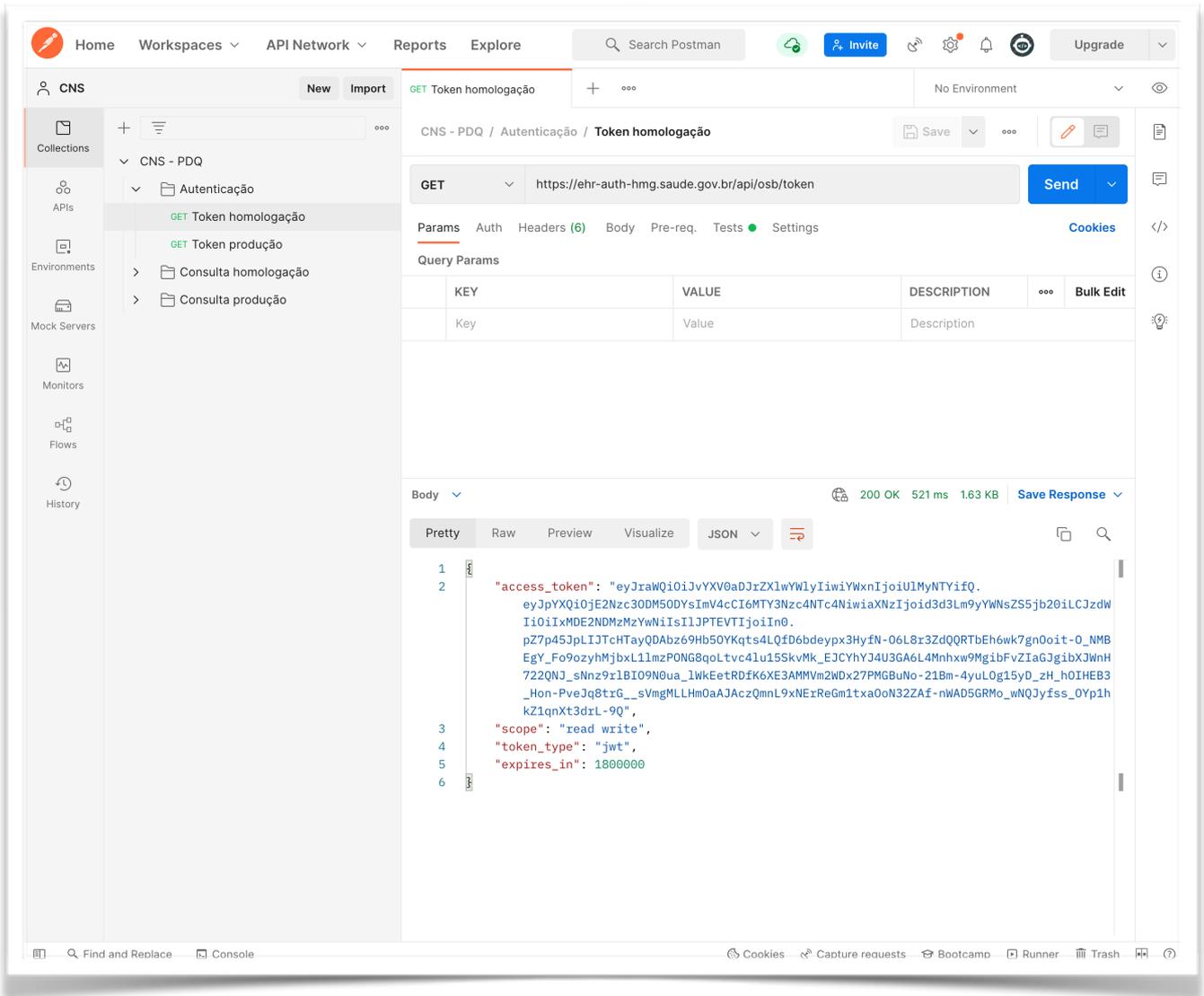
f. Após clicar em Importar, a Collection estará pronta para ser usada.



7. Realizar consultas em ambiente de homologação

7.1. Gerar token em ambiente de homologação

- Em seu espaço de trabalho (Workspace), dentro de sua coleção (Collection), clique na pasta Autenticação e após clique em Token homologação. Basta clicar em Send que será gerado o token para o ambiente de homologação.



The screenshot displays the Postman interface for a workspace named 'CNS'. The left sidebar shows a collection structure: 'CNS - PDQ' containing 'Autenticação' and 'Token homologação'. The main area shows a GET request to 'https://ehr-auth-hmg.saude.gov.br/api/osb/token'. The response is displayed in JSON format, showing a long 'access_token', 'scope', 'token_type', and 'expires_in'.

GET Token homologação

CNS - PDQ / Autenticação / Token homologação

GET https://ehr-auth-hmg.saude.gov.br/api/osb/token

Params Auth Headers (6) Body Pre-req. Tests Settings Cookies

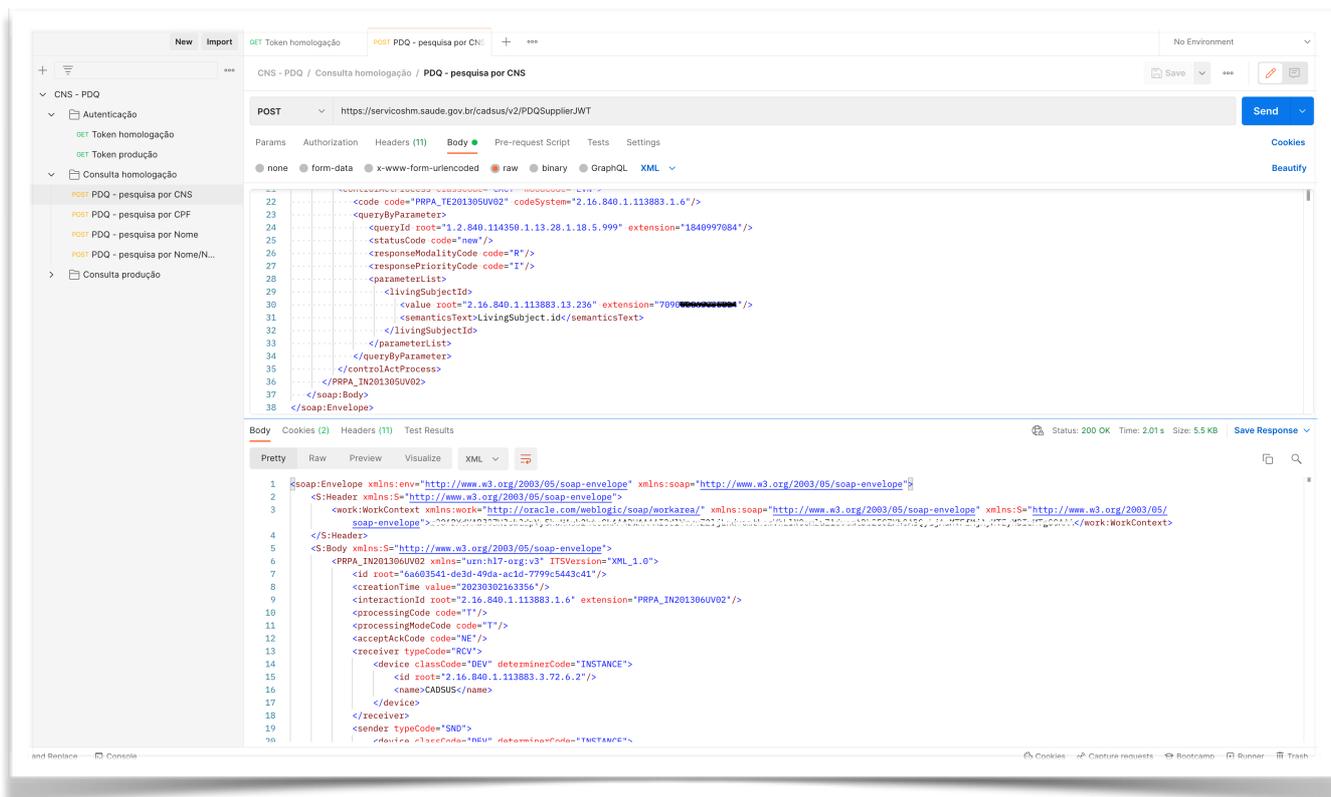
KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

Body

```
1  {
2    "access_token": "eyJraWQiOiJvYXV0aDJrZXl1wYlYiwiYXNjaWoiU1MyNTYifQ.eyJpYXQiOiJlZ2Nzc3ODM5ODYsImV4cCI6MTY3Nzc4NTc4NiwiXNzIjoid3d3Lm9yYWNsZS5jb20iLCJzdWUiOiIXMDE2NDMzMzYwNiIsIlJPEVTIjoiIn0.pZ7p45JpLIJTcHTayQDAbz69Hb50YKqts4LQfD6bdeyxp3HyfN-06L8r3ZdQRTbEh6wk7gn0oit-0_NMBEgY_Fo9ozyhmjbxL1lmzPONG8qoLtvcl4u155skvMk_EJCYhYJ4U3GA6L4Mnhxw9MgibFvZiaGjgibXJwnH722QNj_sNnz9r1lBIO9N0ua_lWkEetRDfK6XE3AMMvm2Wdx27PMGBuNo-21Bm-4yuLog15yD_zH_h0IHEB3_Hon-PveJq8trG_sVmgMLLHm0aAJaczQmnL9xNErReGm1txa0n322Af-nWAD5GRMo_wNQJyJfss_0Yp1hkZ1qnXt3drL-9Q",
3    "scope": "read write",
4    "token_type": "jwt",
5    "expires_in": 1800000
6  }
```

7.2. Consulta por número CNS

- a. Após ter gerado o Token homologação, clique na pasta Consulta homologação e após clique em PDQ - pesquisa por CNS. Após abrir a tela de request, clique na aba Body e insira o número de CNS na tag "`<value root="2.16.840.1.113883.13.236" extension="xxxxxxxxxxxxxxxxx"/>`". Na sequência, deve-se inserir o número do CNS, clicar em **Send**, e serão retornados os dados do cidadão pertencente ao número do CNS passado.



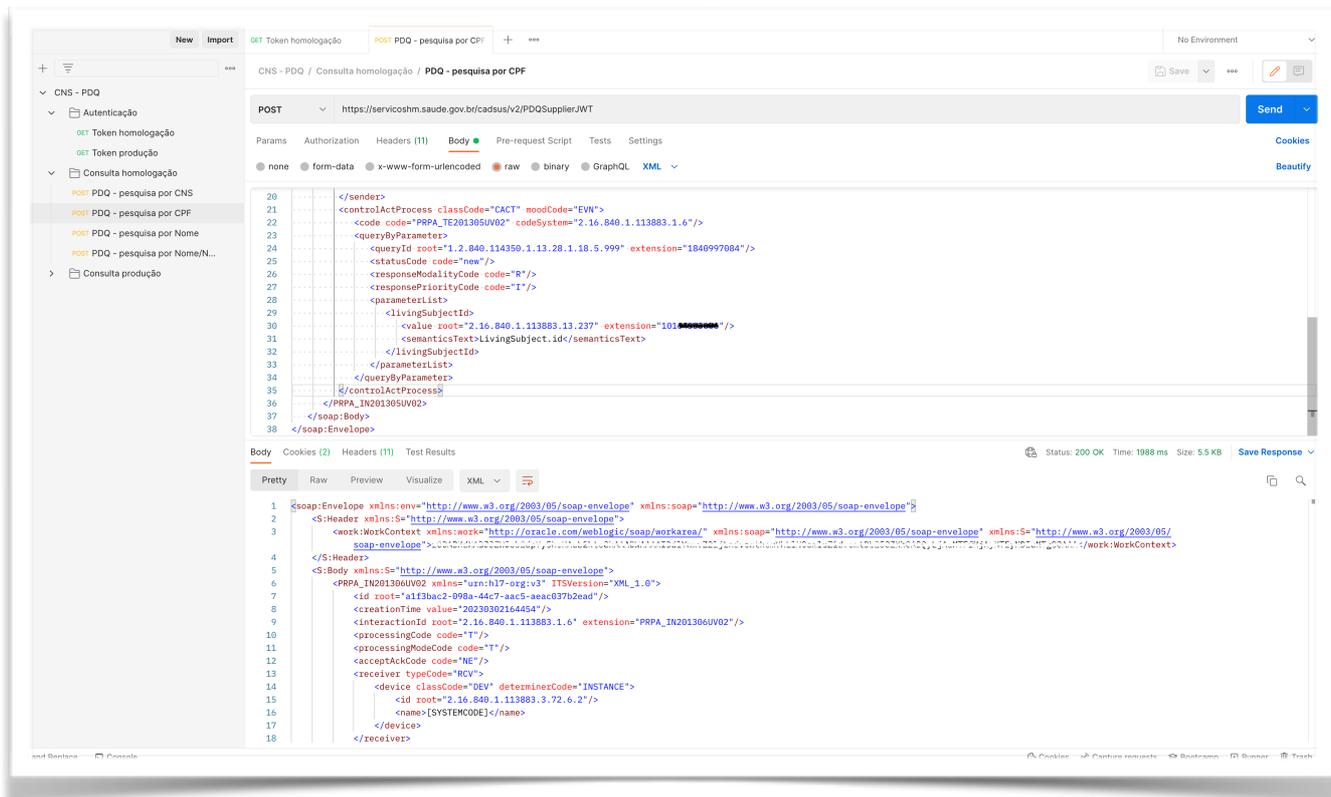
The screenshot displays a REST client interface with a sidebar on the left containing a project tree. The main area shows a POST request to `https://servicososhm.saude.gov.br/cadsus/v2/PDQSupplier/JWT`. The request body is a SOAP XML document. The response body is also a SOAP XML document, showing details such as `<id root="6a603541-de3d-49da-ac1d-7799c5443c41"/>`, `<interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201306U02"/>`, and `<device classCode="DEV" determinerCode="INSTANCE" id root="2.16.840.1.113883.3.72.6.2"/>`.

```
22 <code code="PRPA_TE201305U02" codeSystem="2.16.840.1.113883.1.6"/>
23 <queryByParameter>
24 <queryId root="1.2.840.114350.1.13.28.1.10.5.999" extension="1840997084"/>
25 <statusCode code="new"/>
26 <responseModalityCode code="R"/>
27 <responsePriorityCode code="I"/>
28 <parameterList>
29 <livingSubjectId>
30 <value root="2.16.840.1.113883.13.236" extension="709XXXXXXXXXX"/>
31 <semanticText>LivingSubject.id</semanticText>
32 </livingSubjectId>
33 </parameterList>
34 </queryByParameter>
35 </controlActProcess>
36 </PRPA_IN201305U02>
37 </soap:Body>
38 </soap:Envelope>
```

```
1 <soap:Envelope xmlns:en="http://www.w3.org/2003/05/soap-envelope" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
2 <S:Header xmlns:S="http://www.w3.org/2003/05/soap-envelope">
3 <work:WorkContext xmlns:work="http://oracle.com/weblogic/soap/workarea/" xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:S="http://www.w3.org/2003/05/
4 </S:Header>
5 <S:Body xmlns:S="http://www.w3.org/2003/05/soap-envelope">
6 <PRPA_IN201306U02 xmlns="urn:h17-org:v3" ITSVersion="XML_1.0">
7 <id root="6a603541-de3d-49da-ac1d-7799c5443c41"/>
8 <creationTime value="20230302163356"/>
9 <interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201306U02"/>
10 <processingCode code="I"/>
11 <processingModeCode code="I"/>
12 <acceptAckCode code="NE"/>
13 <receiver typeCode="RCV">
14 <device classCode="DEV" determinerCode="INSTANCE">
15 <id root="2.16.840.1.113883.3.72.6.2"/>
16 <name CADSUS</name>
17 </device>
18 </receiver>
19 <sender typeCode="SND">
20 <device classCode="DEV" determinerCode="INSTANCE">
```

7.3. Consulta por número CPF

- a. Após ter gerado o Token homologação, clique na pasta Consulta homologação e na sequência em PDQ - Pesquisa por CPF. Após abrir a tela de request, clique na aba Body e insira o número de CPF na tag "`<value root="2.16.840.1.113883.13.236" extension="xxxxxxxxxx"/>`". Em seguida, ao inserir o número do CPF, clicar em Send e serão retornados os dados do cidadão pertencente ao número do CPF passado.



The screenshot displays a REST client interface with a sidebar on the left showing a project structure under 'CNS - PDQ'. The main area shows a POST request to the URL `https://servicosm.saude.gov.br/cadusu/v2/PDQSupplierJWT`. The request body is a SOAP envelope with the following XML structure:

```
20 </sender>
21 <controlActProcess classCode="CACT" moodCode="EVN">
22   <code code="PRPA_IN201305U02" codeSystem="2.16.840.1.113883.1.6"/>
23   <queryByParameter>
24     <queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="1840997084"/>
25     <statusCode code="new"/>
26     <responseModalityCode code="R"/>
27     <responsePriorityCode code="I"/>
28     <parameterList>
29       <livingSubjectId>
30         <value root="2.16.840.1.113883.13.236" extension="101xxxxxxxxx"/>
31         <semanticsText>LivingSubject.id</semanticsText>
32       </livingSubjectId>
33     </parameterList>
34   </queryByParameter>
35 </controlActProcess>
36 </PRPA_IN201305U02>
37 </soap:Body>
38 </soap:Envelope>
```

The response body is shown in XML format:

```
1 <soap:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
2   <S:Header xmlns:S="http://www.w3.org/2003/05/soap-envelope">
3     <work:WorkContext xmlns:work="http://oracle.com/weblogic/soap/workarea/" xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:S="http://www.w3.org/2003/05/soap-envelope">
4     </S:Header>
5     <S:Body xmlns:S="http://www.w3.org/2003/05/soap-envelope">
6       <PRPA_IN201305U02 xmlns:urn="urn:h17-org:v3" ITISVersion="XML_1.0">
7         <id root="a1f3bac2-896a-44c7-aa65-aaac037a2ead"/>
8         <creationTime value="20230302164454"/>
9         <interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201306U02"/>
10        <processingCode code="I"/>
11        <processingModeCode code="I"/>
12        <acceptAckCode code="NE"/>
13        <receiver typeCode="RCV">
14          <device classCode="DEV" determinerCode="INSTANCE">
15            <id root="2.16.840.1.113883.3.72.6.2"/>
16            <name>[SYSTEMCODE]</name>
17          </device>
18        </receiver>
```

8. Realizar consultas em ambiente de produção

8.1. Gerar token em ambiente de produção

- Em seu espaço de trabalho (Workspace), dentro de sua coleção (Collection), clique na pasta Autenticação e após clique em Token produção. Clique em Send e será gerado o token para o ambiente de produção.

The screenshot displays the Postman interface for a REST client request. The request is a GET method to the URL `https://ehr-auth.saude.gov.br/api/osb/token`. The response is a JSON object with the following structure:

```
1  {
2    "access_token": "eyJraWQiOiJvYXV0aDRjZlxlYmlyIiwiaWF0IjoiMTYNTYif0.eyJpYXQiOiJlZ2Nzc3D0cwMjYsImV4cCI6MTY3Nzc4ODgyNiwiXmZlIjoiaWw0dDlUFYqXKJtxoumHYQGvDNH8EGK3JEAw2-c0Ph2sFp7YC8u3K2WnsRfs200Da2BddCa6k7vrcT9hVAz-wUfDYTsMKhpsiiICbm1PrJwRo7oHo-jxKH1PM-iPCJA30yUizTpr_o6JAajTkaAbKEVGZ6snM_uzmQZ1D80JML5H_4Zhr1JB-GNY9ZAsgLpb22Io-qqCQrFjyzyu0Gk00UkXfBV2PSviIc9TR61XM6pZV2s3in_P44n0-iHJLR7y2pjmV-o3fKsD7zqb-m5C6w-83KiKf1deVUn2TCF8yrtadmYrCK0HMJLpCGkTh30bAEKGB3s8nC6FPNpywqASmQ",
3    "scope": "read write",
4    "token_type": "jwt",
5    "expires_in": 1800000
6  }
```


8.3.Consulta por número CPF

- a. Após ter gerado o Token produção, clique na pasta **Consulta produção** e após clique em PDQ - pesquisa por CPF. Após abrir a tela de request, clique na aba Body e insira o número de CPF na tag "`<value root="2.16.840.1.113883.13.236" extension="xxxxxxxxxx"/>`". Em seguida, basta clicar em Send que serão retornados os dados do cidadão pertencente ao número do CPF passado.

The screenshot displays a REST client interface with a sidebar on the left containing a tree view of folders: 'CNS - PDQ', 'Autenticação', 'Consulta produção', and 'Consulta homologação'. The main area shows a POST request to 'https://servicos.saude.gov.br/cadus/v2/PDQSupplierJWT'. The 'Body' tab is active, showing an XML payload. The XML includes a header with 'xmlns:soap="http://www.w3.org/2003/05/soap-envelope"', a body with 'xmlns:S="http://www.w3.org/2003/05/soap-envelope"', and a 'device' element with 'id root="2.16.840.1.113883.3.72.6.2"'. The 'value' tag in the 'livingSubjectId' element is highlighted in red in the original image, corresponding to the instruction in the text above.

```
20 .....</senders>
21 .....<controlActProcess classCode="CACT" moodCode="EW">
22 .....<code code="PRPA_I201385UV02" codeSystem="2.16.840.1.113883.1.6"/>
23 .....<queryByParameter>
24 .....<queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="1840997084"/>
25 .....<statusCode code="none"/>
26 .....<responseModalityCode code="R"/>
27 .....<responsePriorityCode code="I"/>
28 .....<parameterList>
29 .....<livingSubjectId>
30 .....<value root="2.16.840.1.113883.13.236" extension="101XXXXXXXXX"/>
31 .....<semanticText>livingSubject.id</semanticText>
32 .....</livingSubjectId>
33 .....</parameterList>
34 .....</queryByParameter>
35 .....</controlActProcess>
36 .....</PRPA_I201385UV02>
37 .....</soap:Body>
38 .....</soap:Envelope>
```

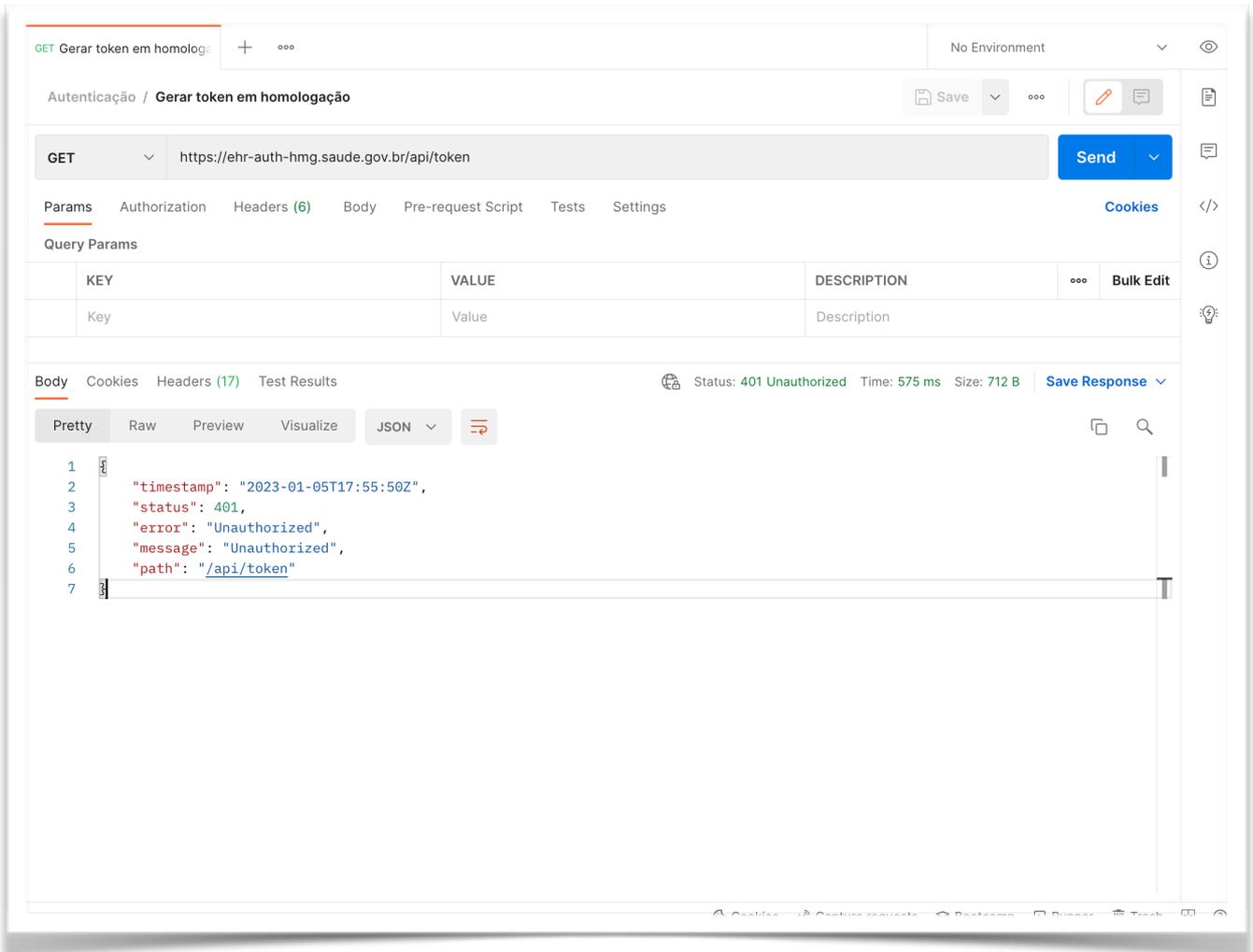
Body Cookies (2) Headers (11) Test Results Status: 200 OK Time: 782 s Size: 5.5 KB Save Response

```
1 .....<?xml version="1.0" encoding="UTF-8" ?>
2 .....<soap:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
3 .....<S:Header xmlns:S="http://www.w3.org/2003/05/soap-envelope">
4 .....<workContext xmlns:work="http://oracle.com/weblogic/soap/workarea/" xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:S="http://www.w3.org/2003/05/
5 .....</S:Header>
6 .....<S:Body xmlns:S="http://www.w3.org/2003/05/soap-envelope">
7 .....<PRPA_I201386UV02 xmlns:urn="urn:h17-org:v3" ITSVersion="XML_1.0">
8 .....<id root="30840aa-b167-4809-9901-8450693e0ed"/>
9 .....<creationTime value="20230302172340"/>
10 .....<interactionId root="2.16.840.1.113883.1.6" extension="PRPA_I201386UV02"/>
11 .....<processingCode code="I"/>
12 .....<processingModeCode code="I"/>
13 .....<acceptAckCode code="NC"/>
14 .....<receiver typeCode="RCV">
15 .....<device classCode="DEV" determinexCode="INSTANCE">
16 .....<id root="2.16.840.1.113883.3.72.6.2"/>
17 .....<name>[SYSTEMCODE]</name>
18 .....</device>
19 .....</PRPA_I201386UV02>
```

9. Erros possíveis

9.1. Erro 401 Unauthorized

Este erro ocorre quando o certificado digital não foi devidamente configurado. Siga os passos do [Item 5. Configurar ambientes Postman](#), deste manual.

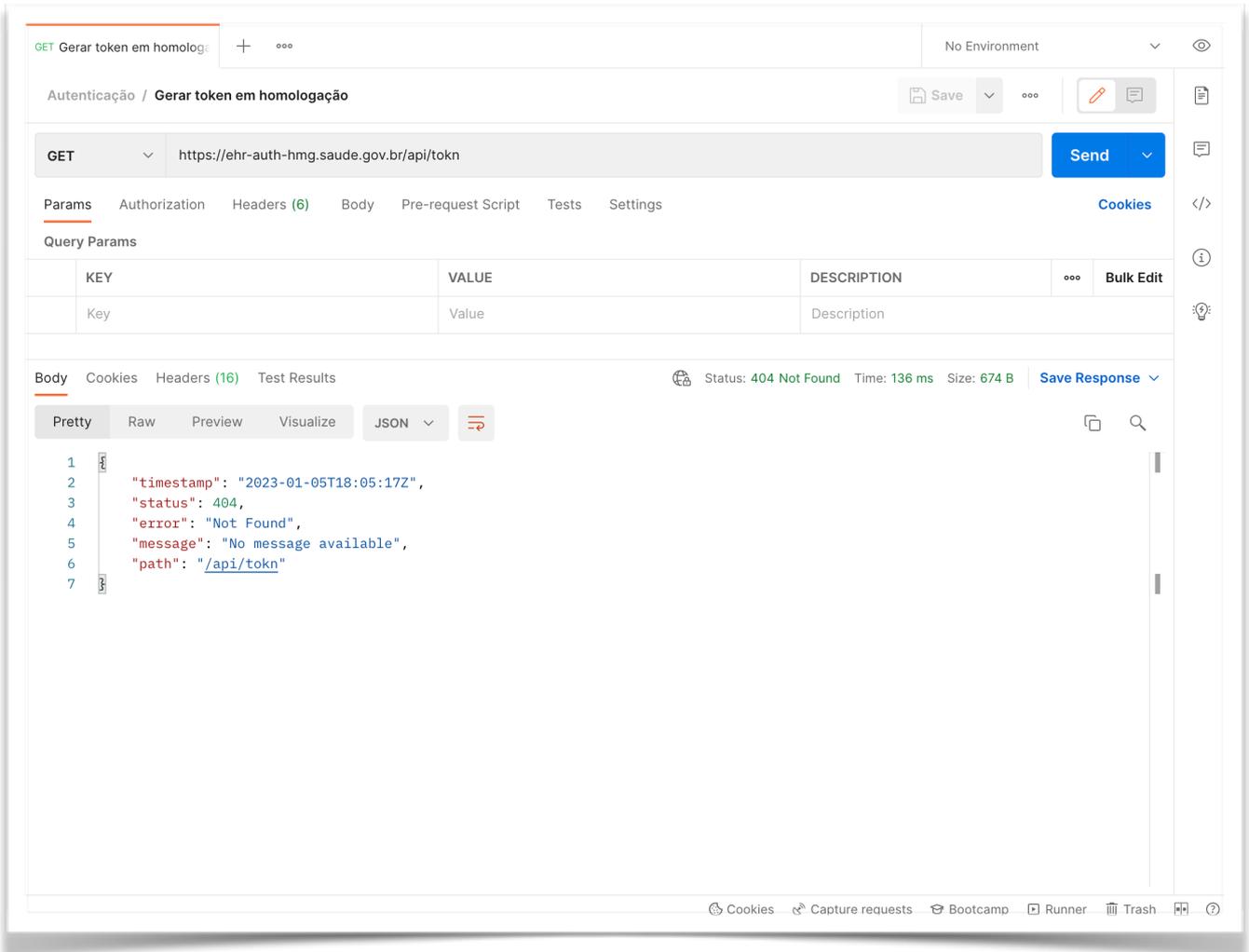


The screenshot displays the Postman interface for a GET request to `https://ehr-auth-hmg.saude.gov.br/api/token`. The response status is `401 Unauthorized` with a time of `575 ms` and a size of `712 B`. The response body is shown in JSON format:

```
1  {"timestamp": "2023-01-05T17:55:50Z",  
2    "status": 401,  
3    "error": "Unauthorized",  
4    "message": "Unauthorized",  
5    "path": "/api/token"}  
6  
7
```

9.2. Erro 404 Not Found

Este erro ocorre quando a URL de Requisição (Request) não foi devidamente digitada. Siga os passos do [Item 7. Realizar consultas em ambiente de homologação.](#)



The screenshot displays a REST client interface with the following details:

- Request:** Method: GET, URL: `https://ehr-auth-hmg.saude.gov.br/api/tokn`
- Response:** Status: 404 Not Found, Time: 136 ms, Size: 674 B
- Response Body (JSON):**

```
1 {
2   "timestamp": "2023-01-05T18:05:17Z",
3   "status": 404,
4   "error": "Not Found",
5   "message": "No message available",
6   "path": "/api/tokn"
7 }
```

9.3. Erro INCORRECT_PASSWORD

Este erro ocorre quando a senha do certificado digital não foi devidamente digitada. Siga os passos do [Item 7. Realizar consultas em ambiente de homologação.](#)

The screenshot shows a REST client interface with the following details:

- Request Method: GET
- URL: `https://ehr-auth-hmg.saude.gov.br/api/token`
- Response Status: 500 (Internal Server Error)
- Response Body:

```
{}
Error: INCORRECT_PASSWORD

```

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

Response

Could not send request

Error: INCORRECT_PASSWORD | [View in Console](#)

[Learn more about troubleshooting API requests](#)

Footer: Cookies | Capture requests | Bootcamp | Runner | Trash | ?

10. Suporte

Para mais informações sobre a utilização da ferramenta Postman, acesse:

<https://learning.postman.com/docs/getting-started/introduction/>

Para mais informações sobre as APIs do Ministério da Saúde acesse o Portal de Serviços do DataSUS:

<https://servicos-datasus.saude.gov.br/>

Caso tenha dúvidas ou problemas relacionados à utilização da API do Cartão Nacional de Saúde - CNS, acesse:

<https://webatendimento.saude.gov.br/faq/cadsus>