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

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":
“eyJraWQiOiJybmRzIGhvbSIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiIxMDE2NDMzMzYwNiIsInBlc3
NvYSI6eyJmaXNpY2EiOnRydWUsImlkZW50aWZpY2Fkb3IiOiIxMDE2NDMzMzYwNiJ9LCJpc3
MiOiJSTkRTLUhNRyIsImV4cCI6MTY3MjkyOTUzOSwiaWF0IjoxNjcyOTI3NzM5LCJjZXJ0aWZp
Y2FkbyI6eyJzdWJqZWN0IjoiQ049TUFSQ1VTIFZJTklDSVVTIERFIE9MSVZFSVJBIFNBTlRPU
zoxMDE2NDMzMzYwNixPVT12aWRlb2NvbmZlcmVuY2lhLE9VPTE1NTkwOTIxMDAwMTI5LE9
VPShFTSBCUkFOQ08pLE9VPVJGQiBlLUNQRiBBMSxPVT1TZWNyZXRhcmlhIGRhIFJl…”,
   "scope": "read write",
   "token_type": "jwt",
   "expires_in": 1800000
}
```

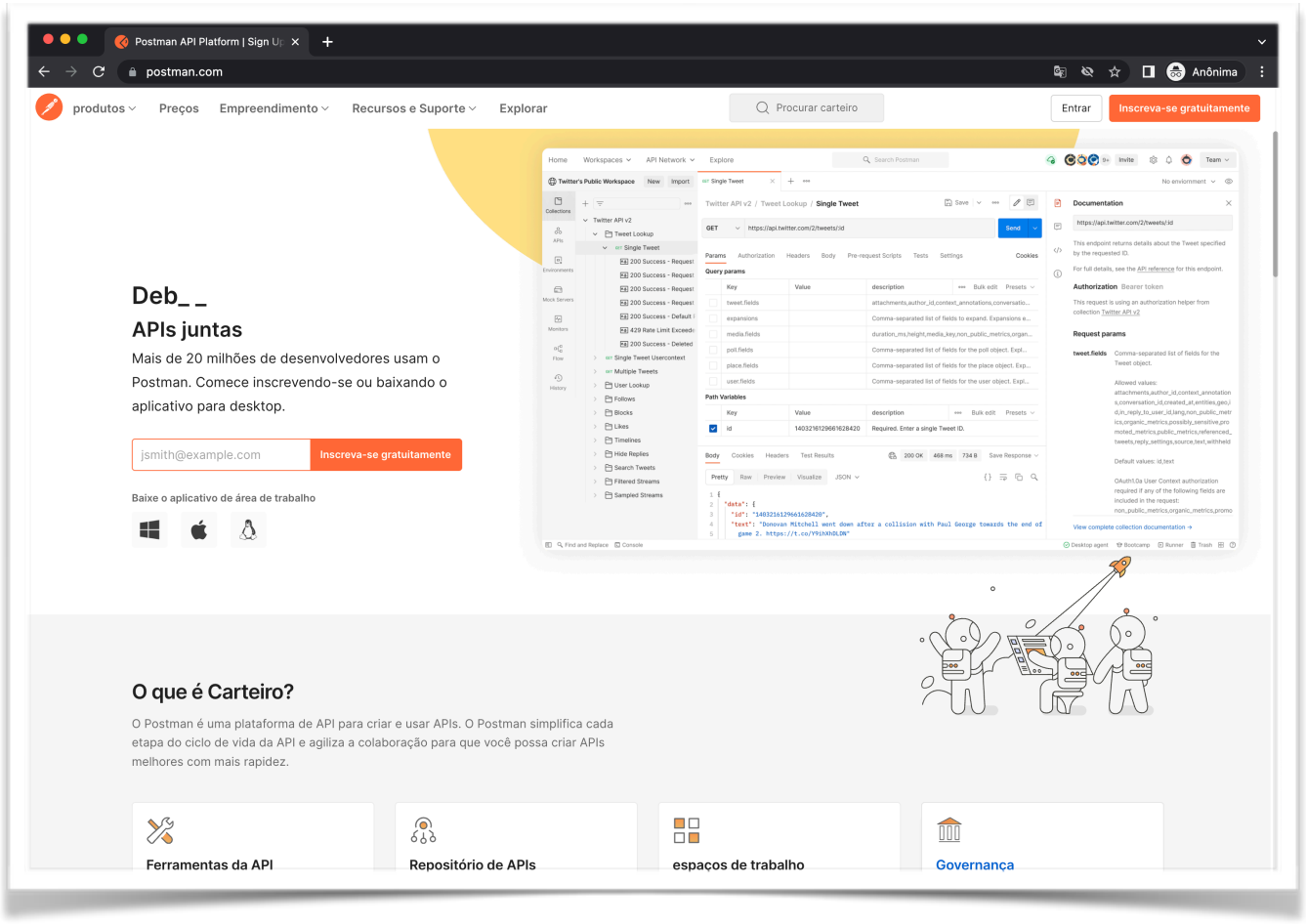

A autenticação com certificado digital da API utiliza a técnica chamada “Two-way SSL”, comunicação SSL de duas vías (cliente e servidor). No “Two- way SSL”, além do certificado do servidor, o cliente também deve utilizar um certificado válido. A validade do certificado digital será verificada no momento 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

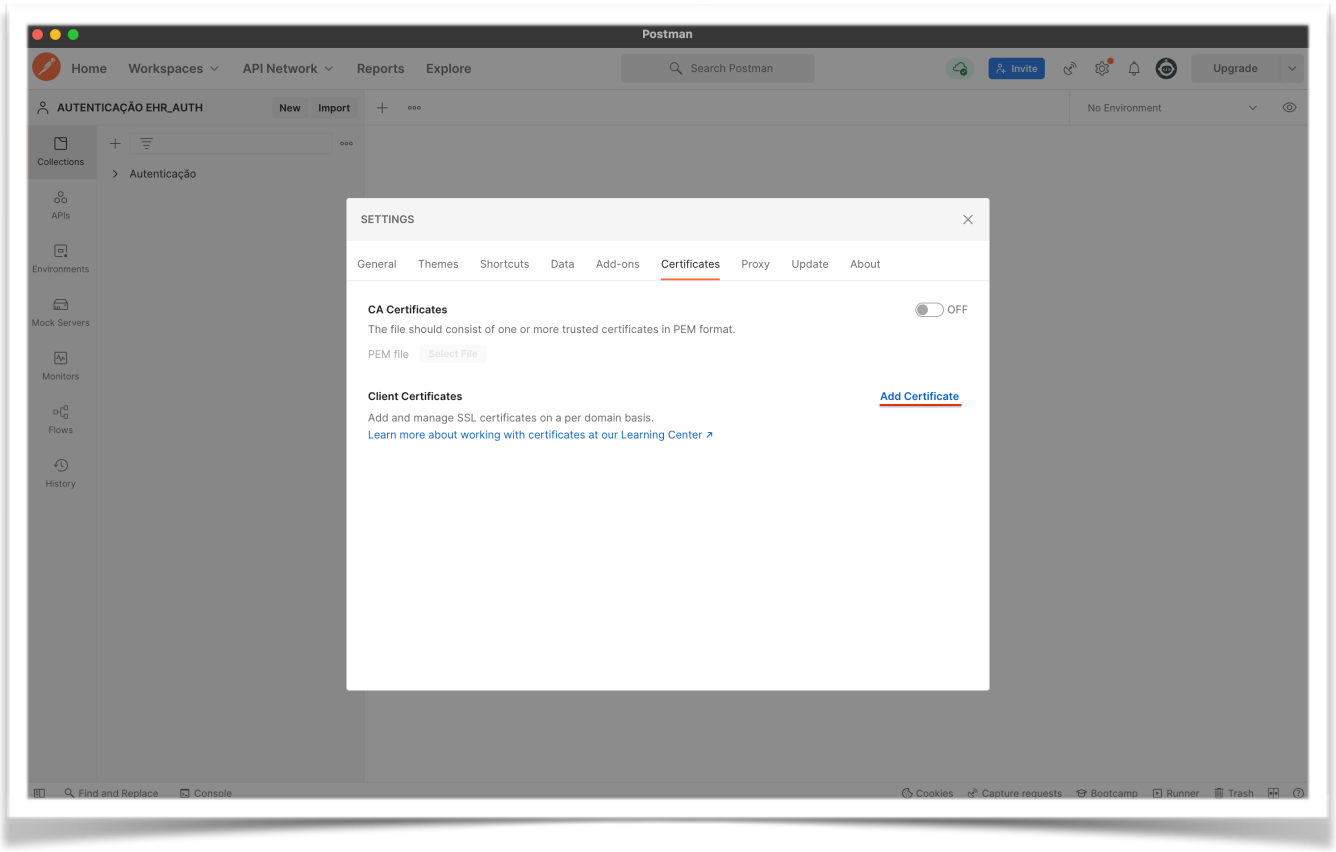
a. Faça o download do Postman, disponível no link: https://www.postman.com/



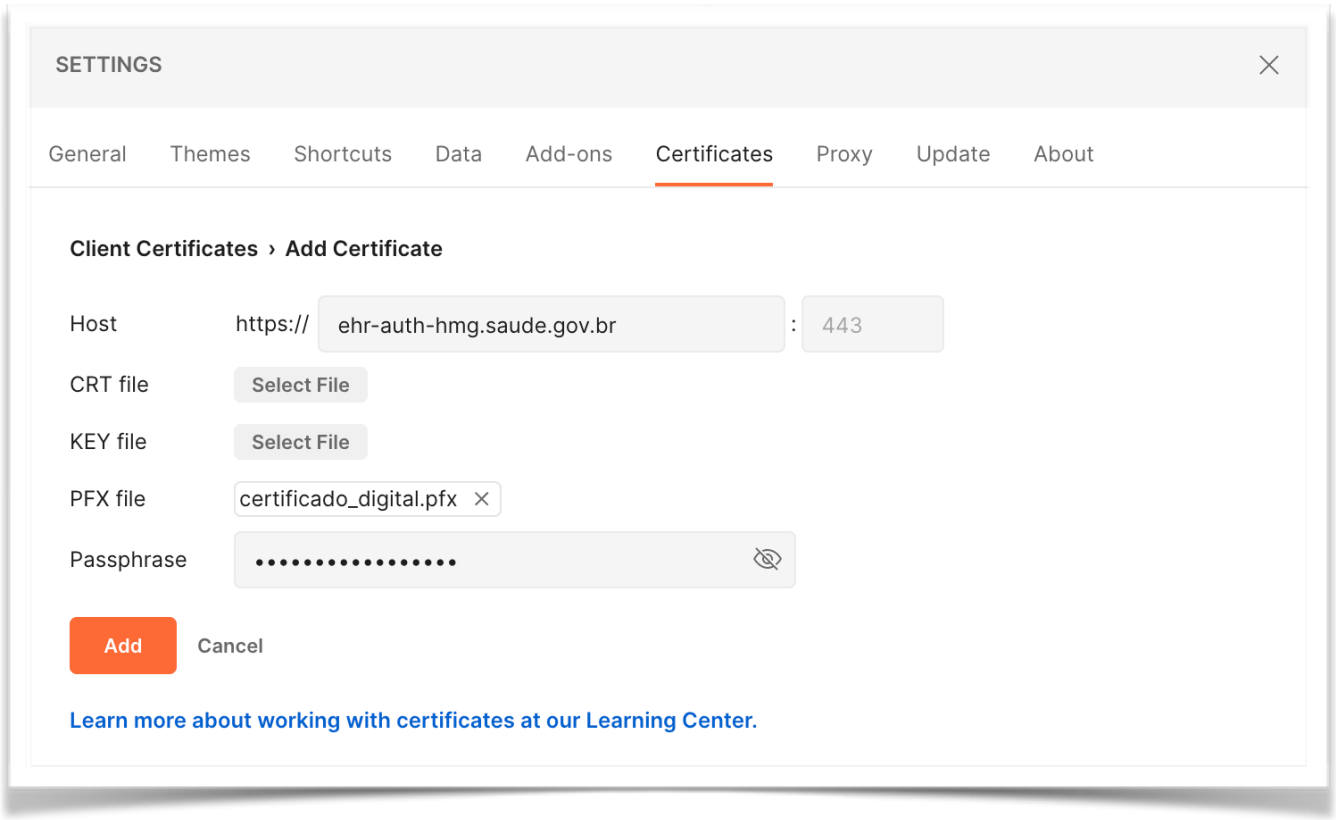
5. Configurar ambientes POSTMAN

5.1. Configurando o ambiente de homologação

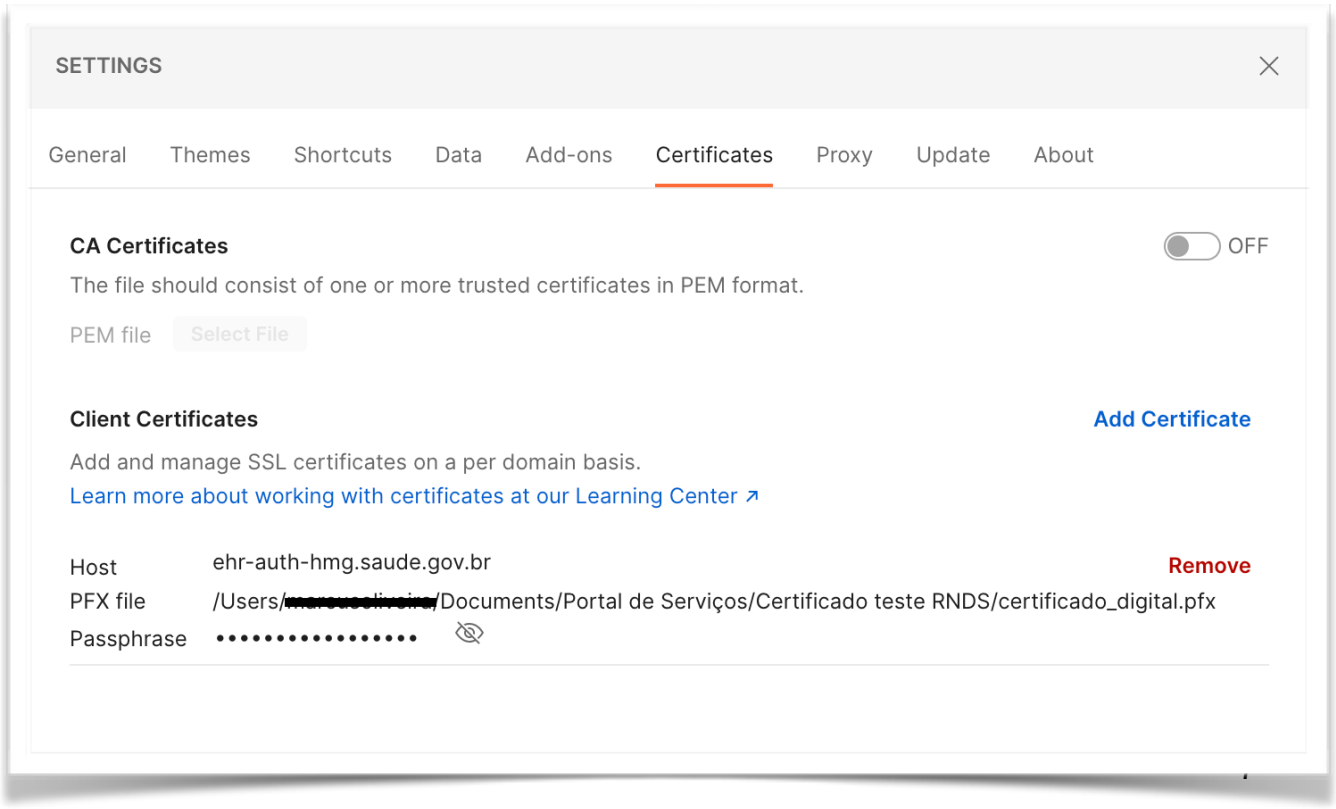
a. Abra o Postman, clique em Configurações (settings), na aba de opções, clique em Certificados (Certificates) e depois em Adicionar Certificado (Add Certificate).



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.

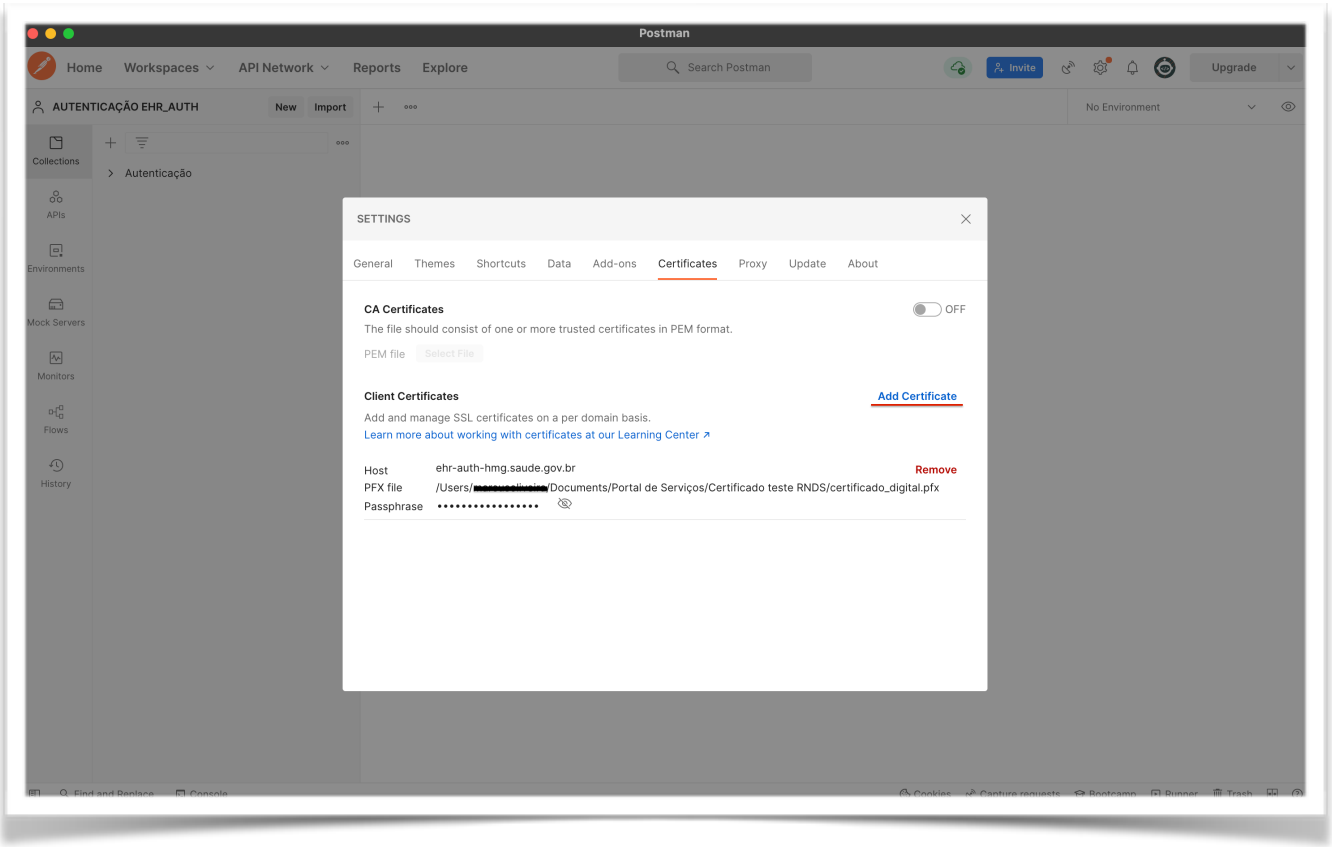


c. Depois que as configurações estiverem inseridas, clique em Adicionar (add). Na sequência, o certificado digital foi configurado para o ambiente de homologação.

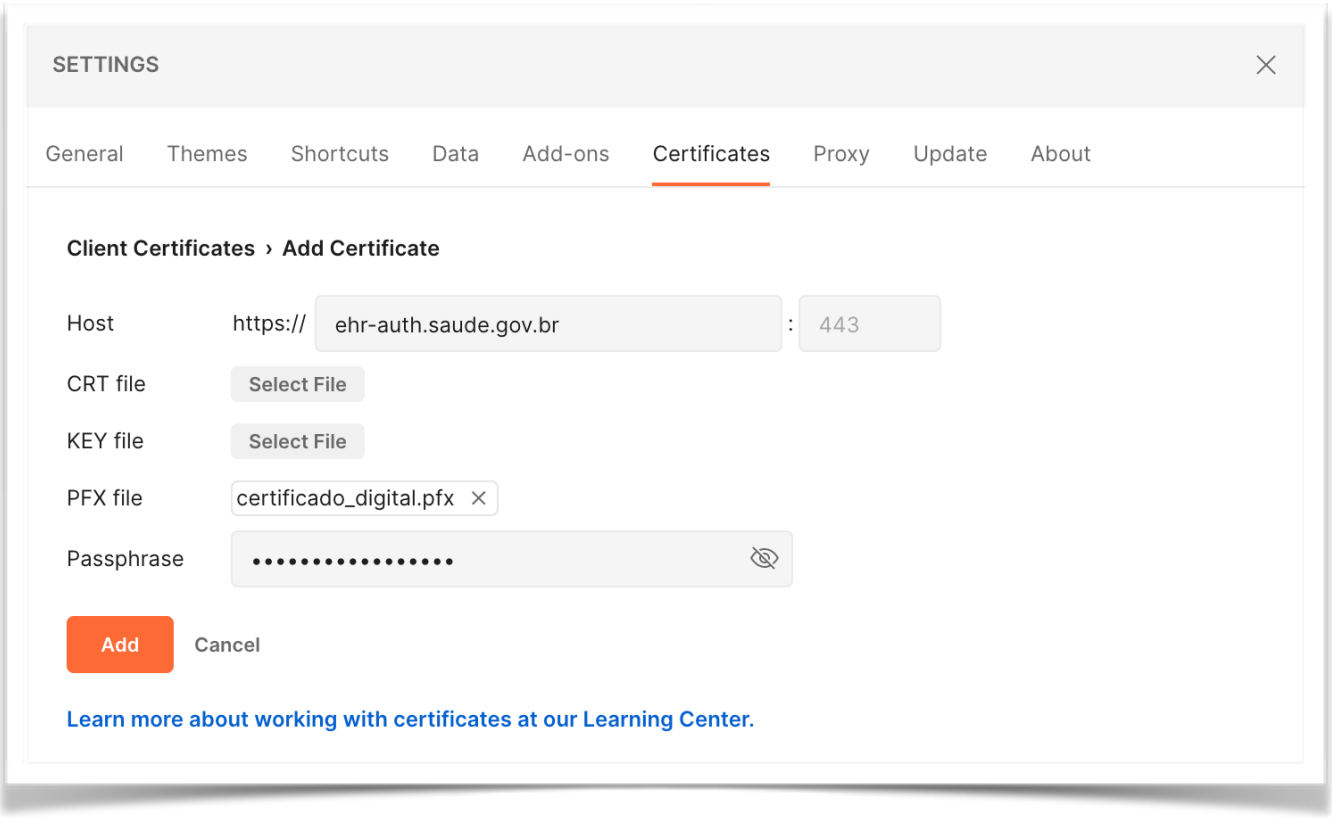


5.2. Configurando o ambiente de produção

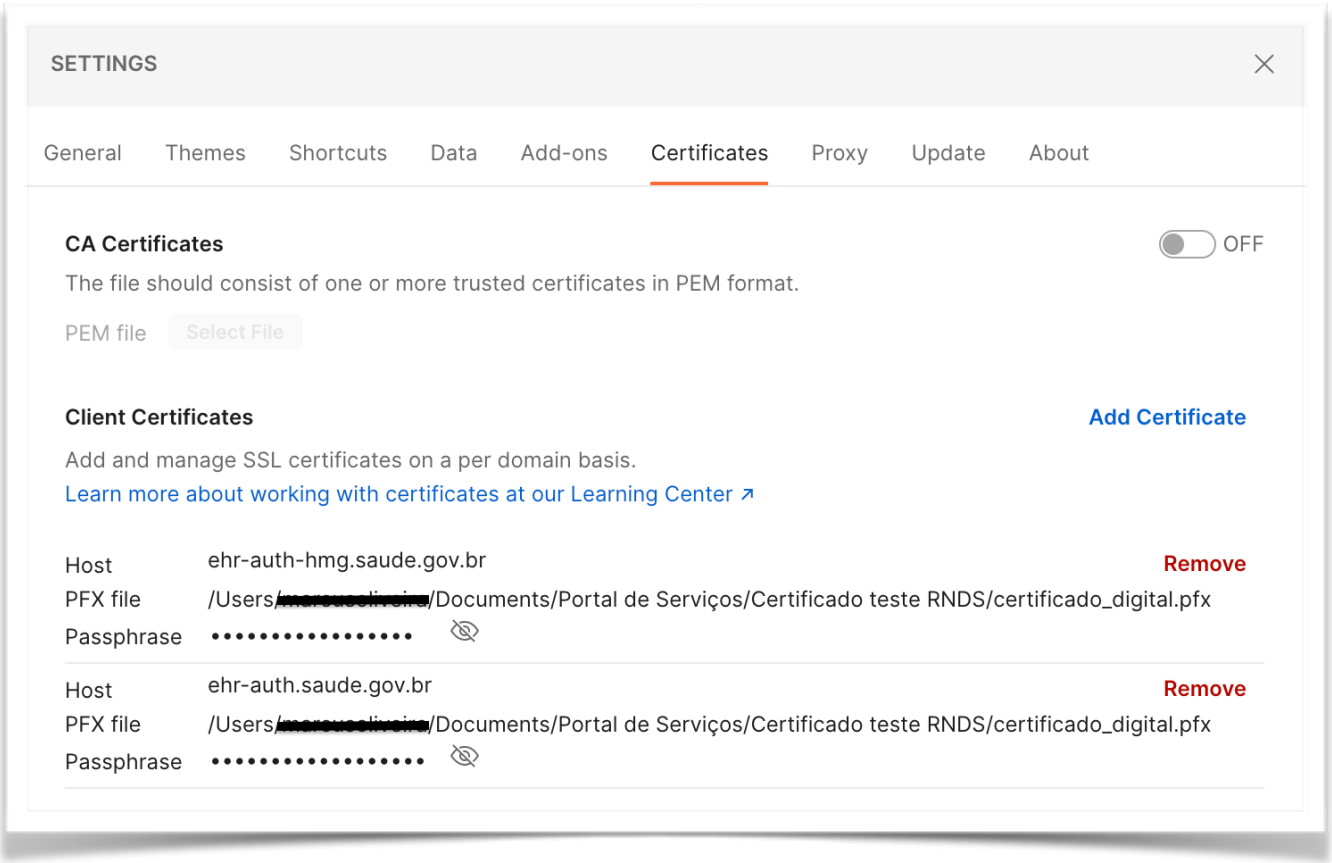
a. Abra o Postman, clique em Configurações (settings), na aba de opções, clique em Certificados (Certificates) e depois em Adicionar Certificado (Add Certificate).



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.



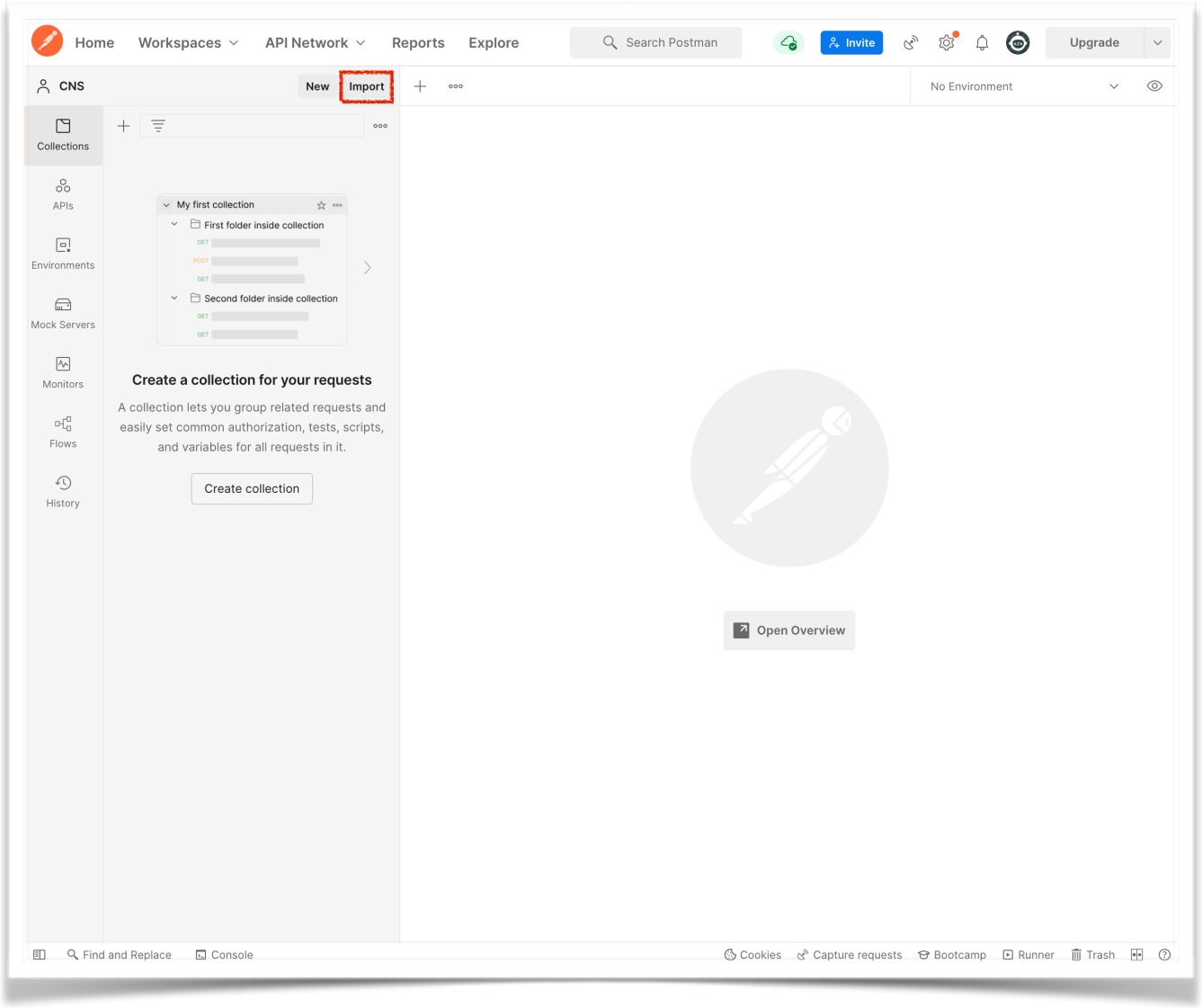
c. Depois que as configurações estiverem inseridas, clique em Adicionar (add). Pronto, o certificado digital foi configurado para o ambiente de produção.



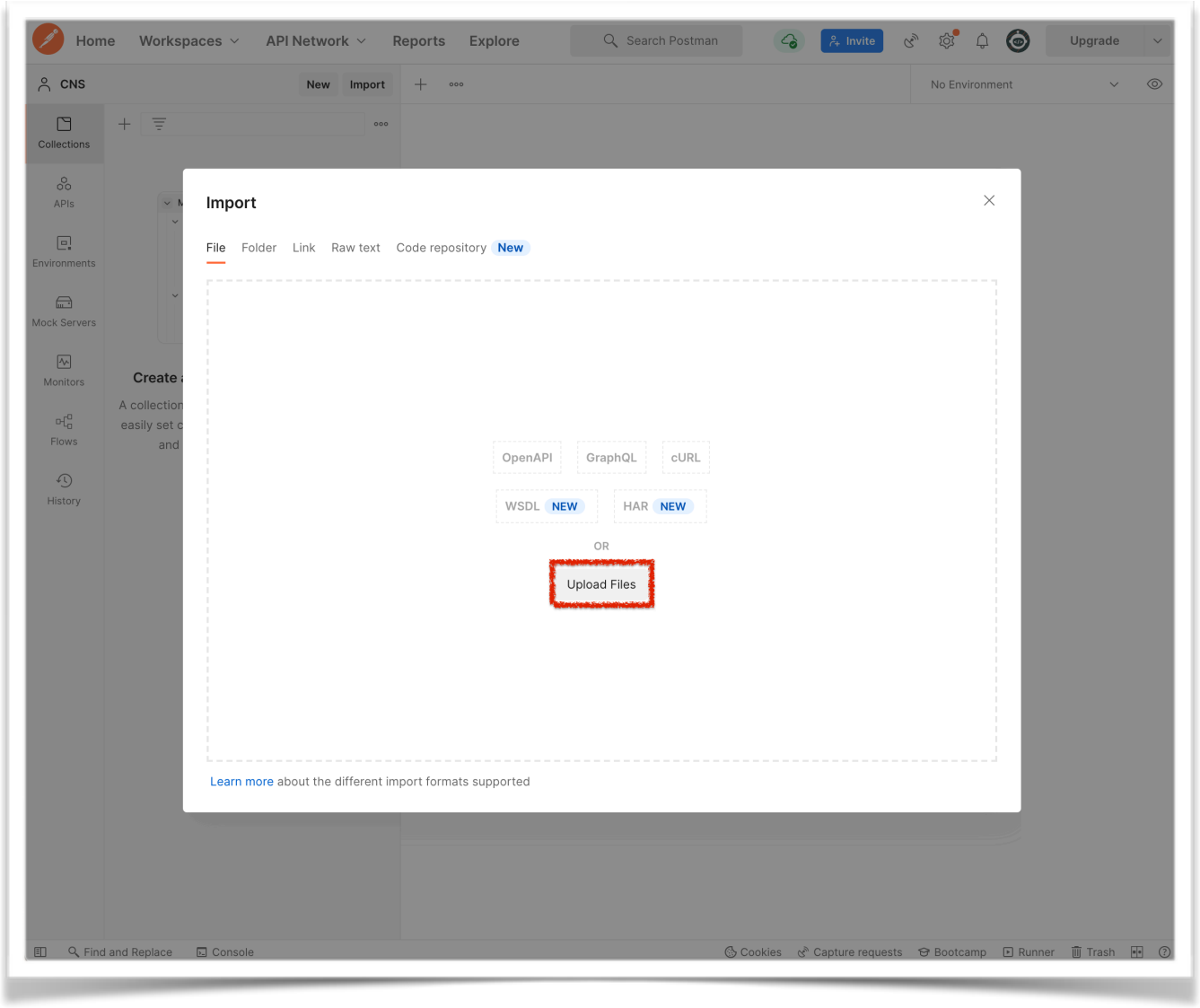
6. Configuração da Collection

a. 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.

b. Após o download da collection, clique em Import.

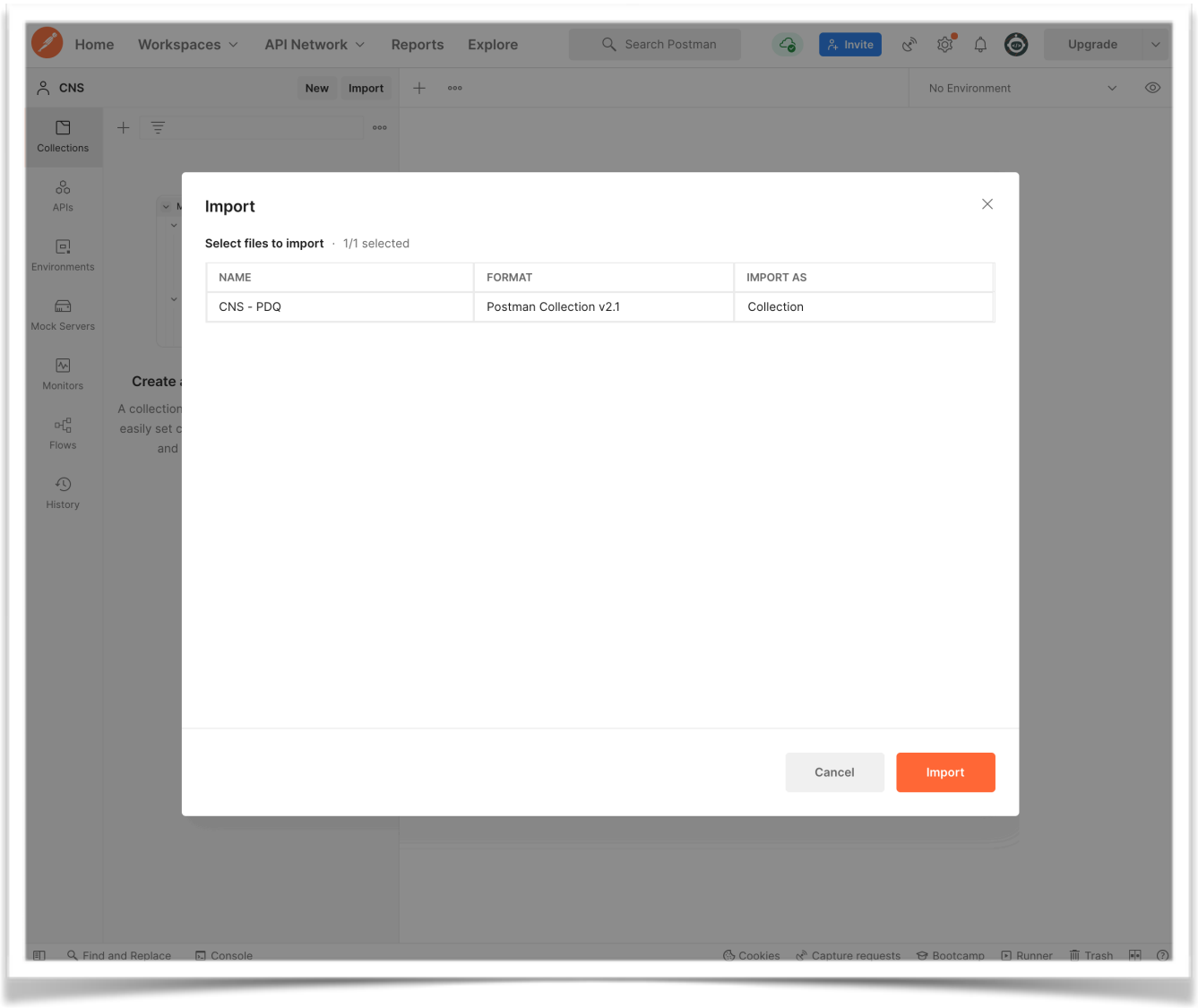


c. Após clicar em Import, apresenta-se uma tela para que seja localizado o arquivo da Collection baixada. Clique em Upload Files.

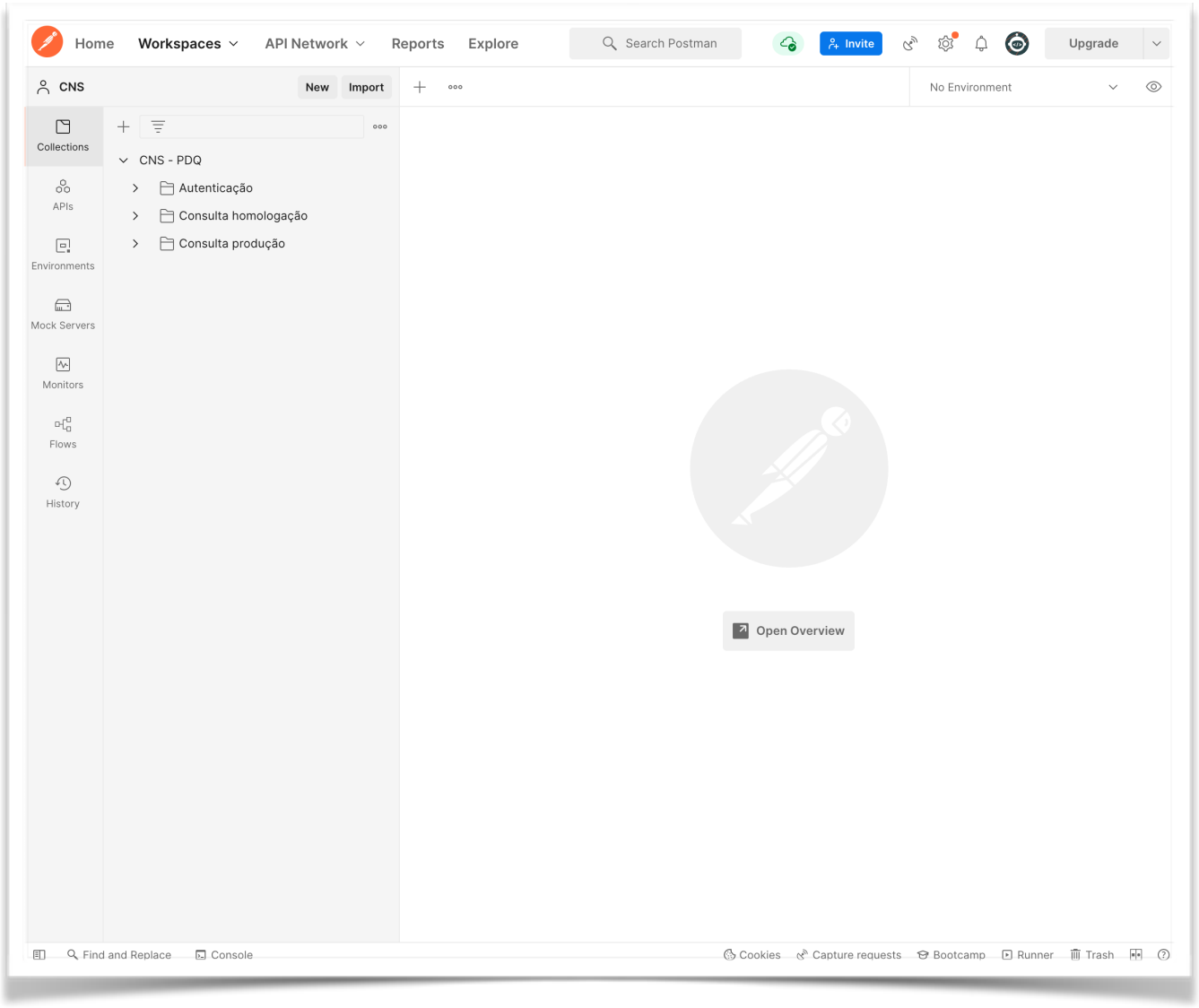


d. Após clicar Upload Files, apresenta-se uma tela para que seja localizado o arquivo da Collection baixada. Localize o arquivo e clique em Open (abrir).

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



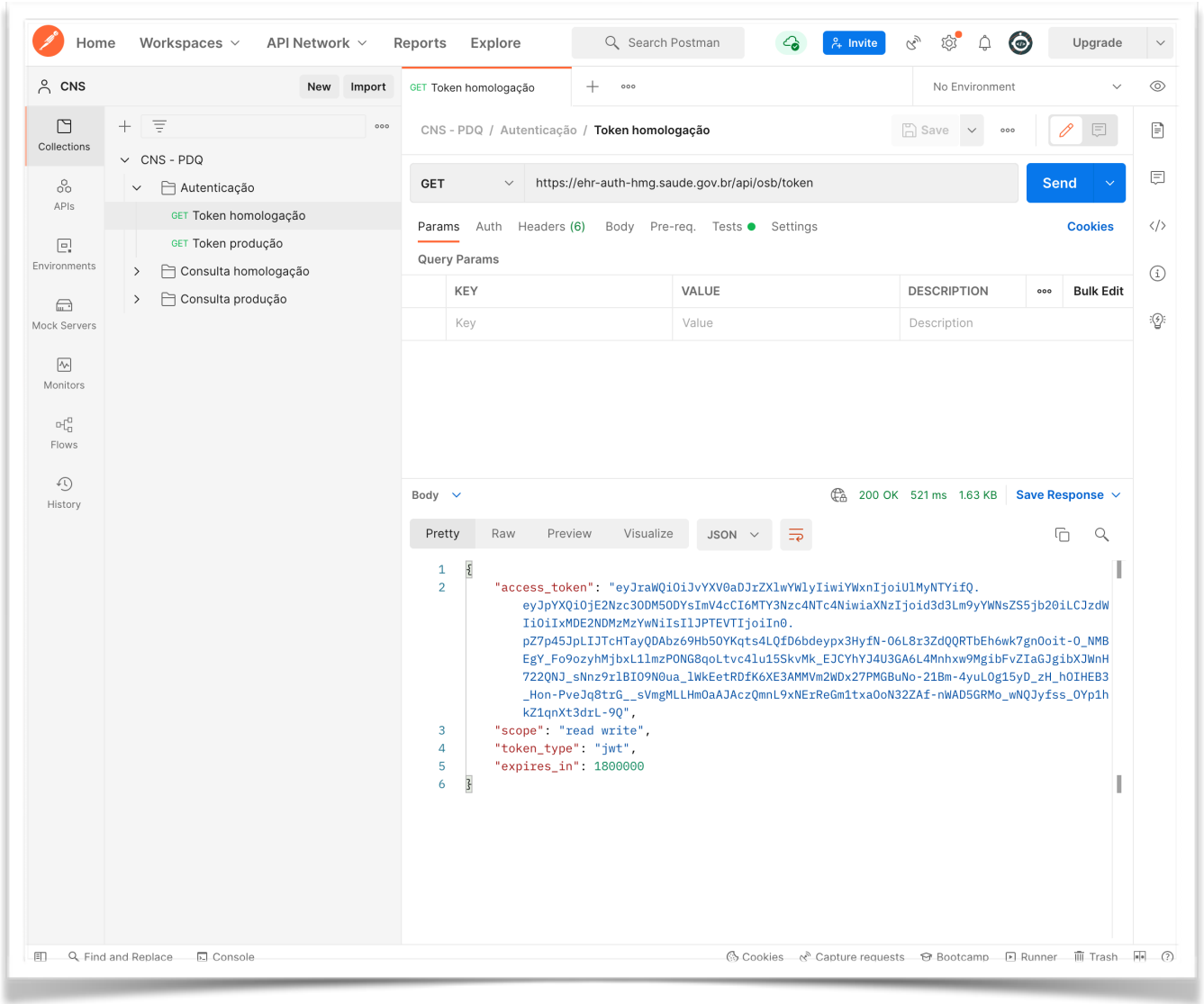
f. Após clicar em Importar, a Collection estará pronta para ser usada.



7. Realizar consultas em ambiente de homologação

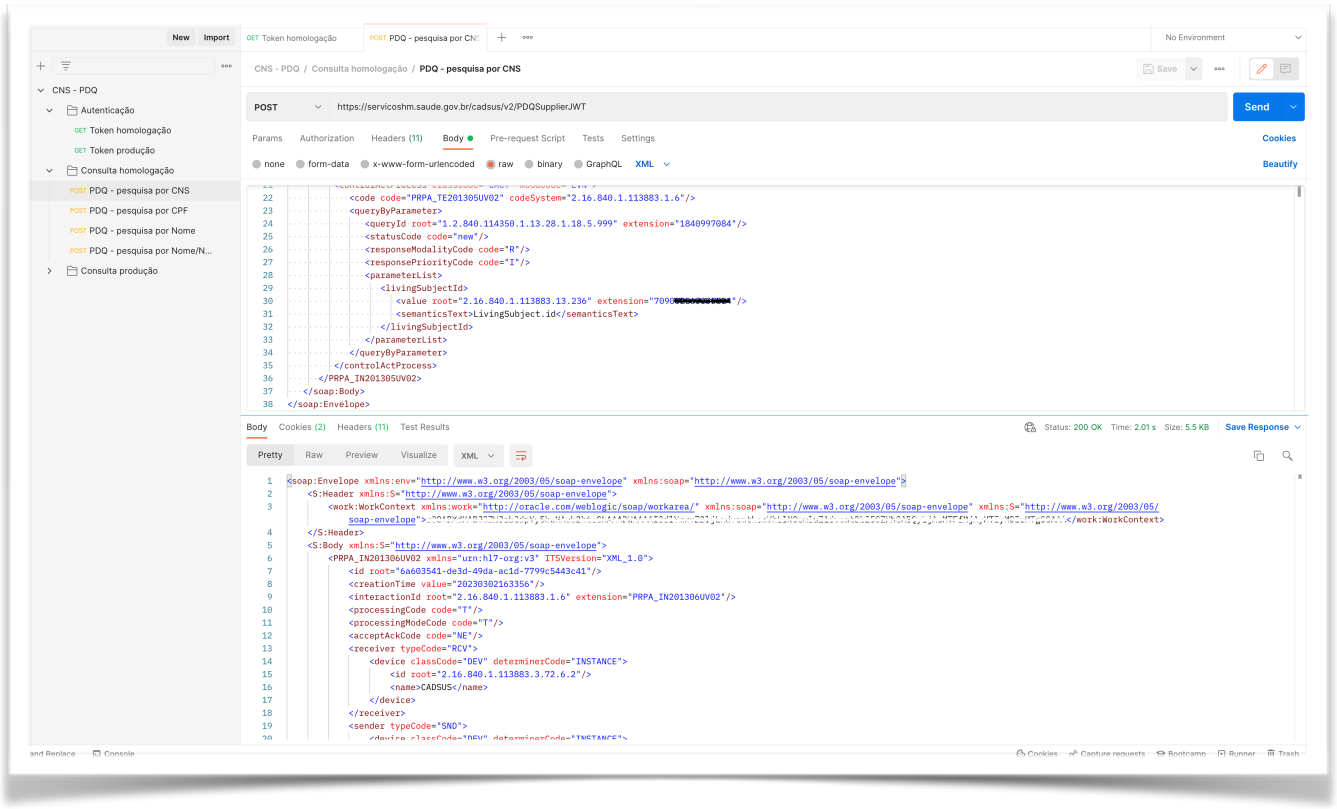
7.1. Gerar token em ambiente de homologação

a. 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.



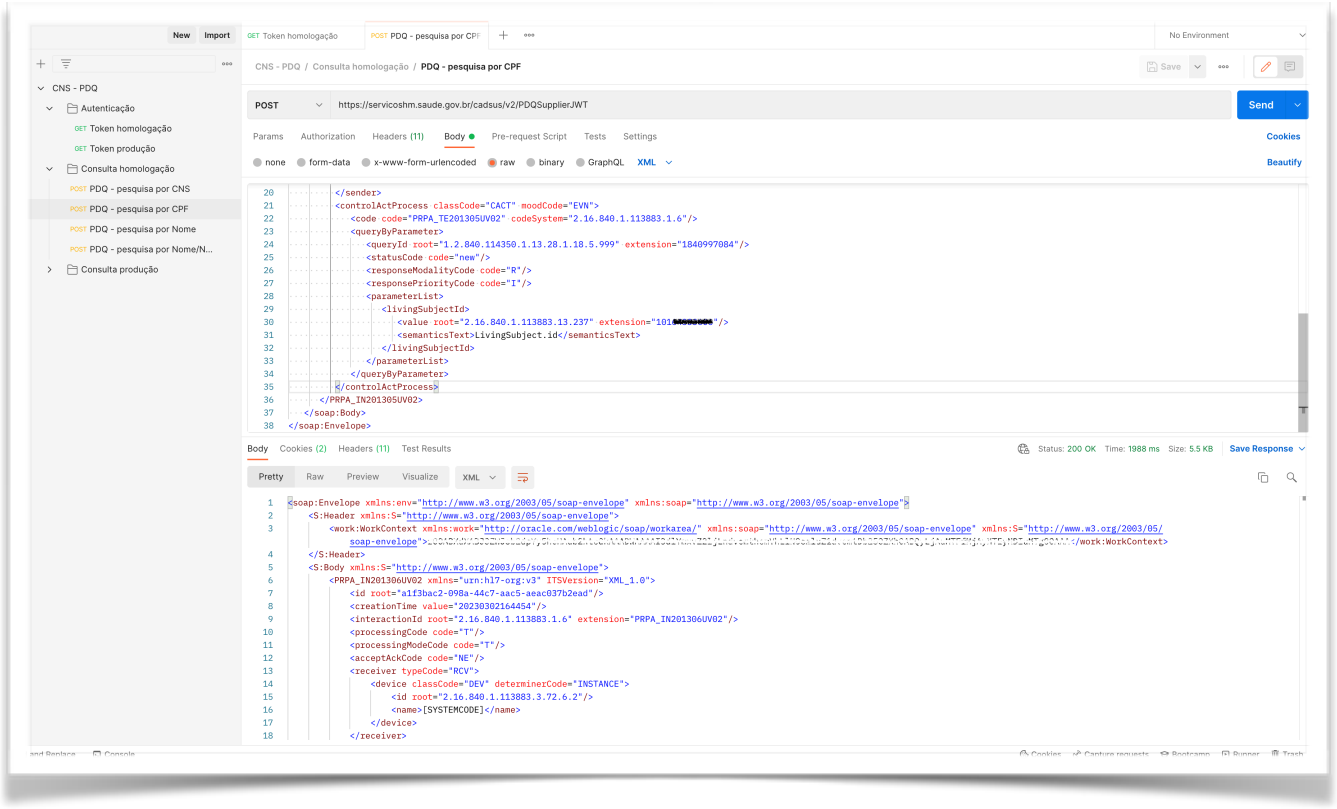
7.2. Consulta por número CNS

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="**xxxxxxxxxxxxxxx**"/>". Na sequência, deve-se inserir o número do CNS, clicar em **S**end, e serão retornados os dados do cidadão pertencente ao número do CNS passado.



7.3. Consulta por número CPF

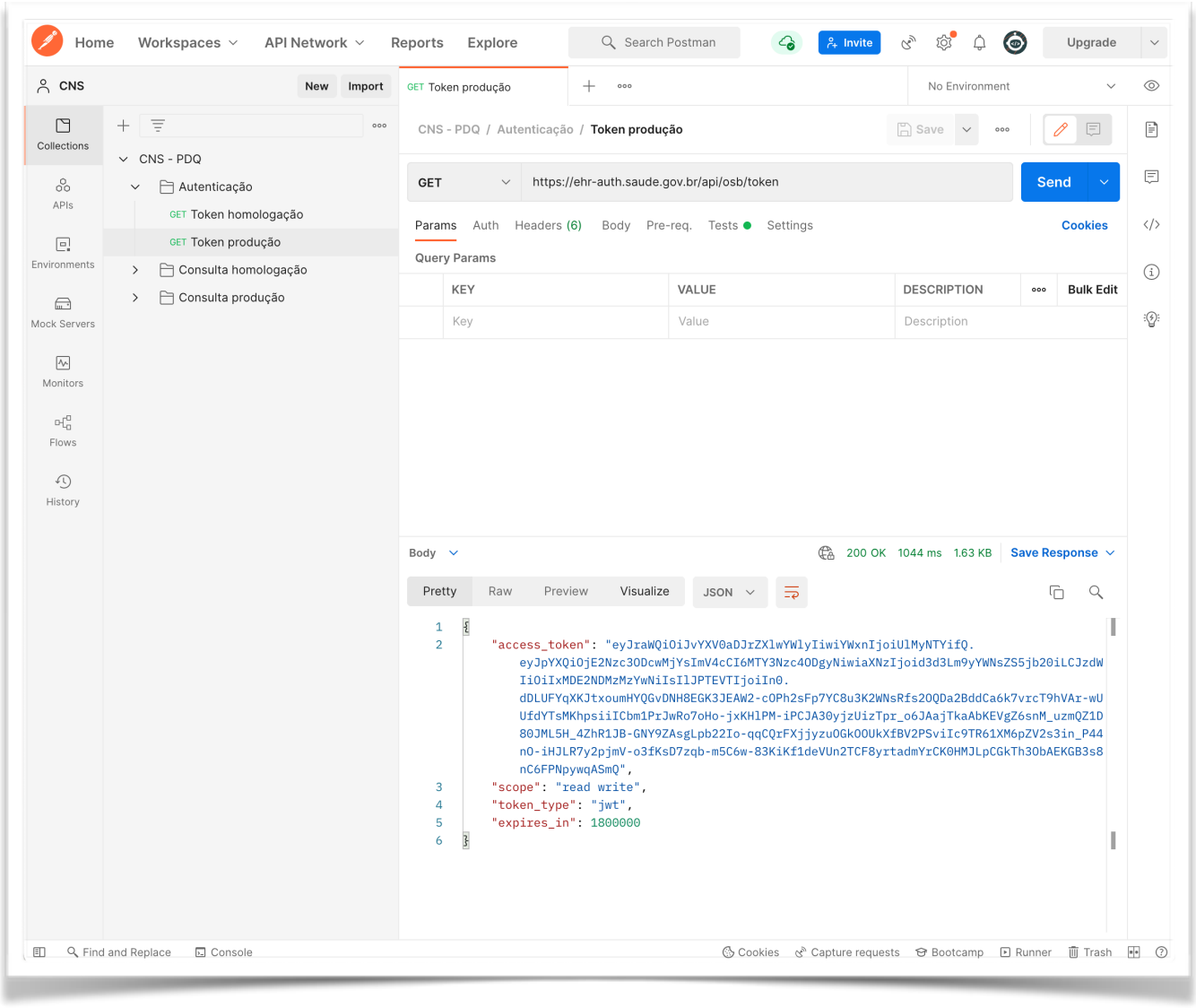
a. Após ter gerado o Token homologação, clique na pasta Consulta homologação e na sequência em PDQ - Pesquisa por CPF. Após abrir a tela de request, clique na aba Body e insira o número de CPF na tag "<value root="2.16.840.1.113883.13.236" extension="**xxxxxxxxxxx**"/>". Em seguida, ao inserir o número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



8. Realizar consultas em ambiente de produção

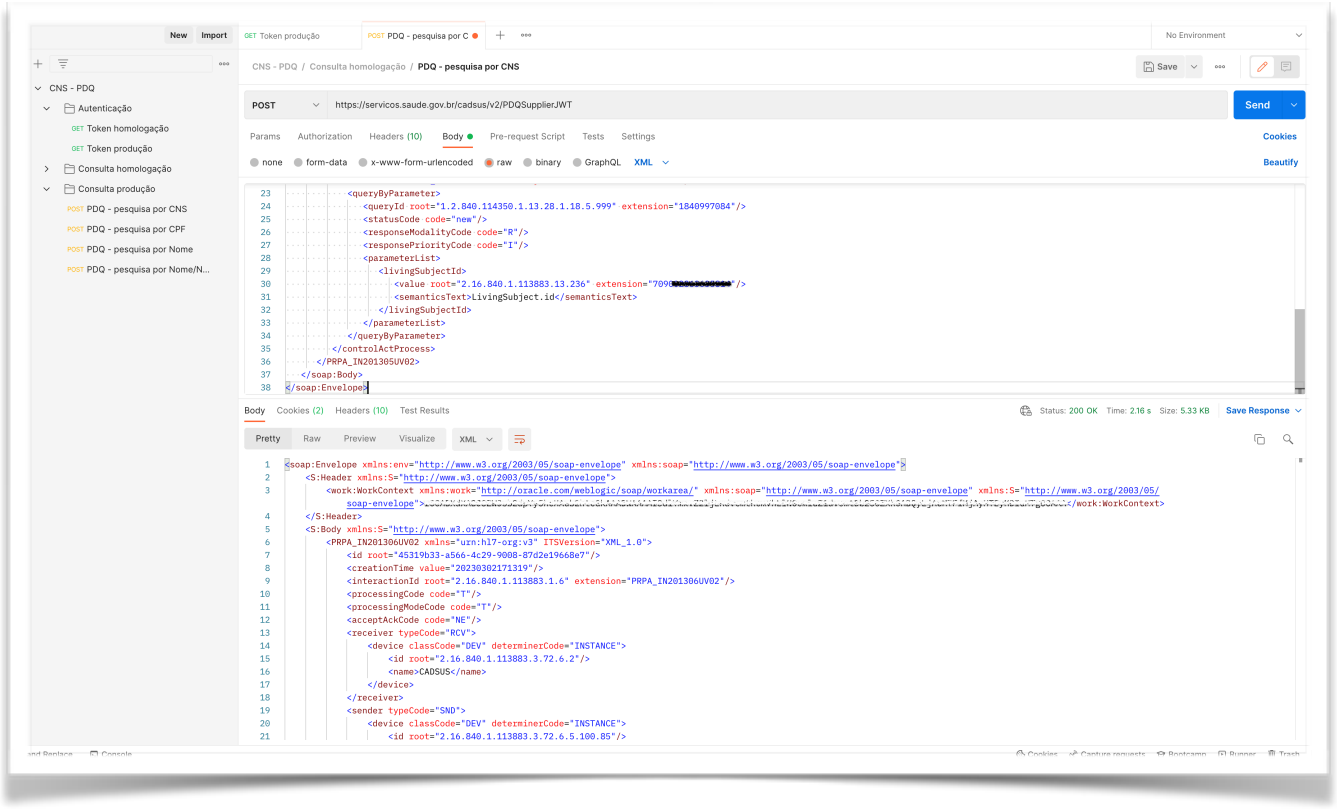
8.1. Gerar token em ambiente de produção

a. 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.



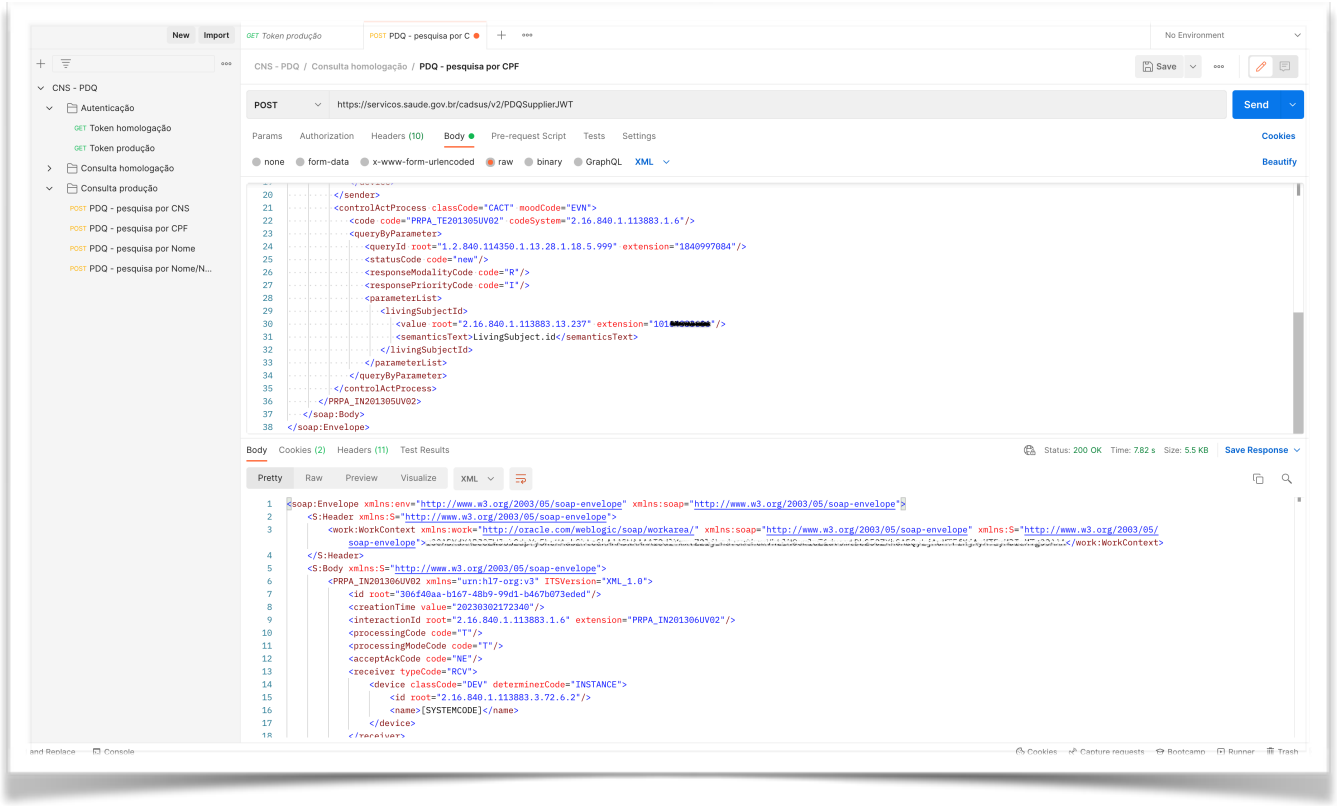
8.2.Consulta por número CNS

a. Após ter gerado o Token produção, clique na pasta Consulta produção e na sequência 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="**xxxxxxxxxxxxxxx**"/>". Em seguida, clicar em Send que serão retornados os dados do cidadão pertencente ao número do CNS passado.



8.3.Consulta por número CPF

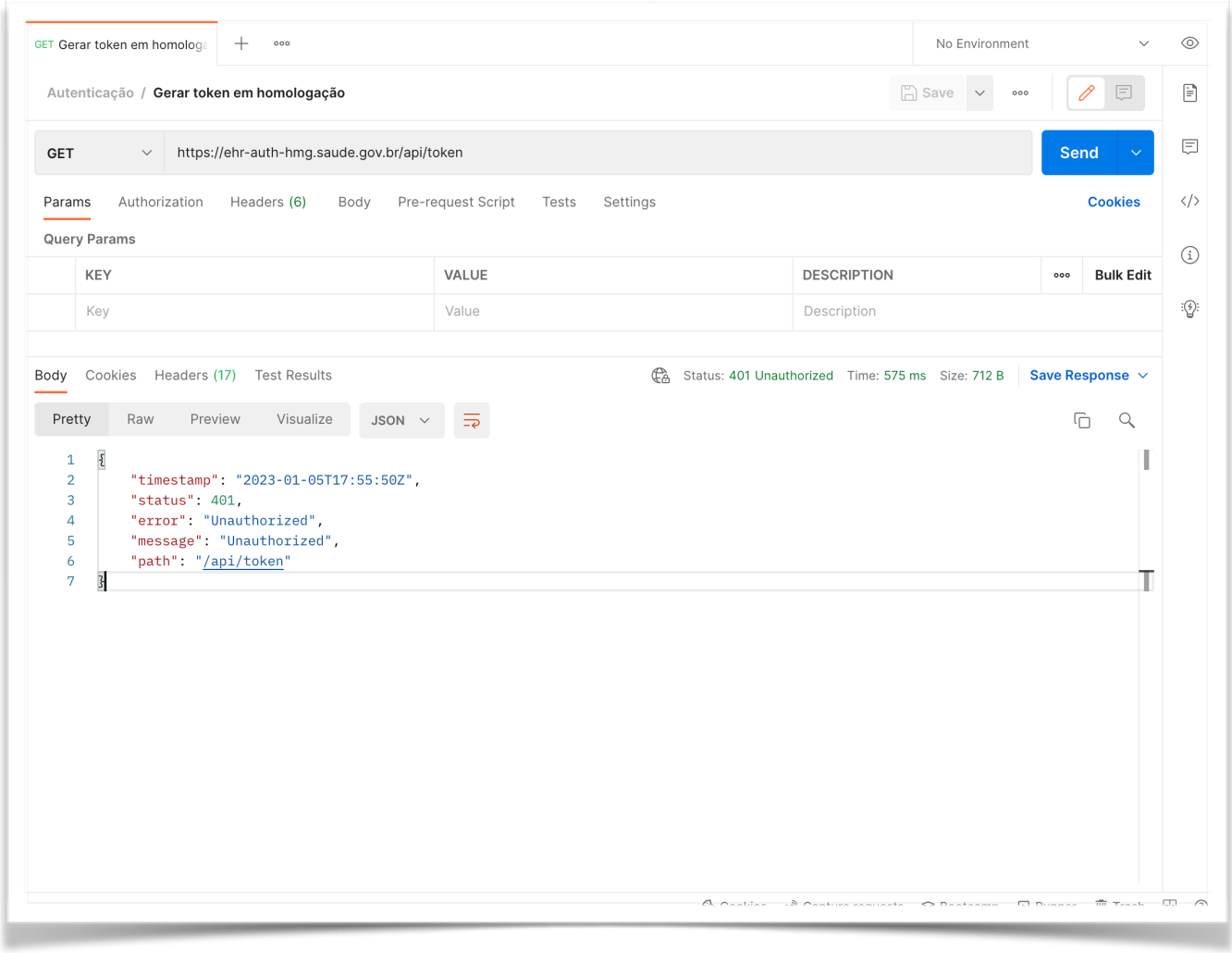
a. Após ter gerado o Token produção**,** clique na pasta **Consulta produção** e após clique em PDQ - pesquisa por CPF. Após abrir a tela de request, clique na aba Body e insira o número de CPF na tag "<value root="2.16.840.1.113883.13.236" extension="**xxxxxxxxxxx**"/>". Em seguida, basta clicar em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



9. Erros possíveis

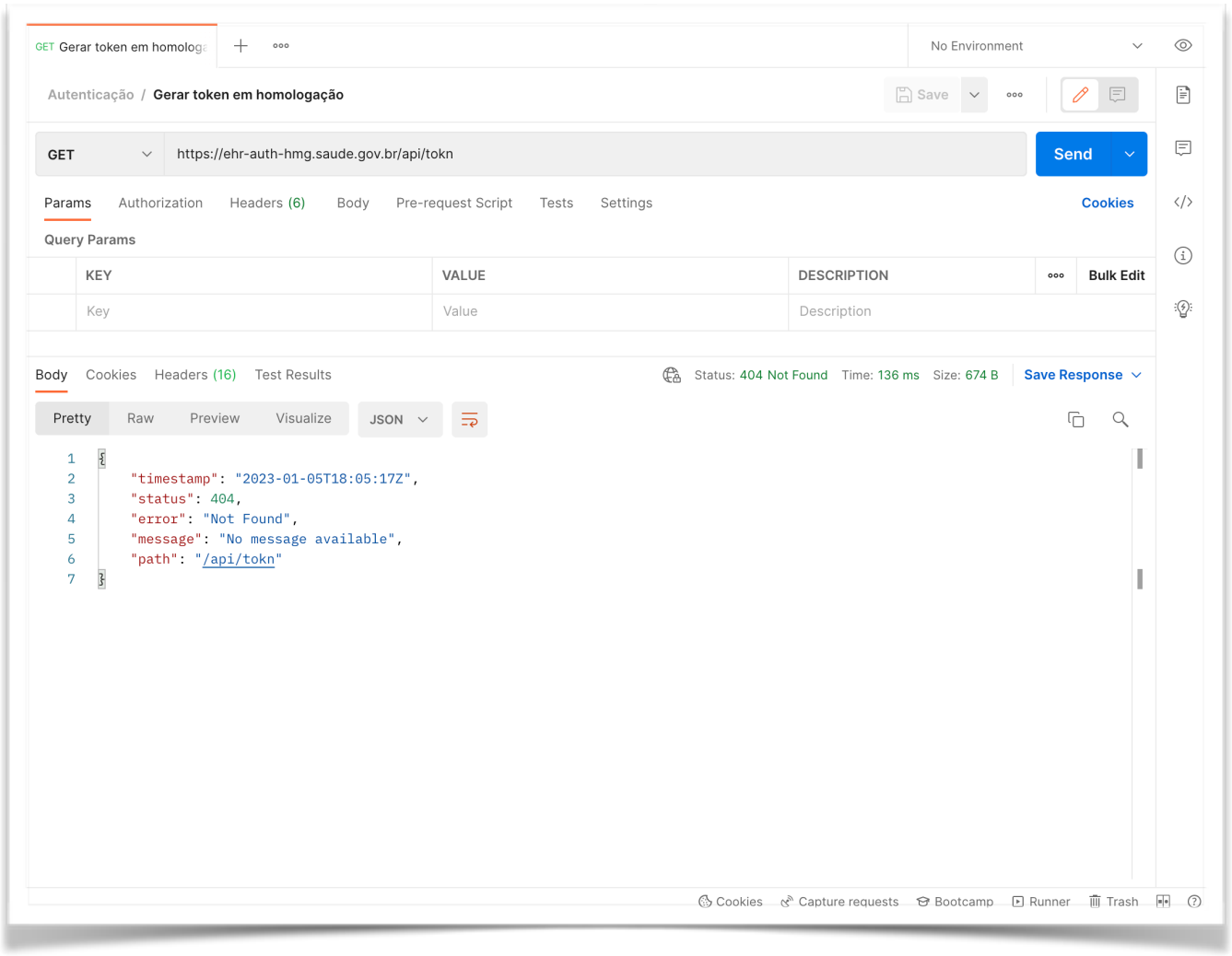
9.1. Erro 401 Unauthorized

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



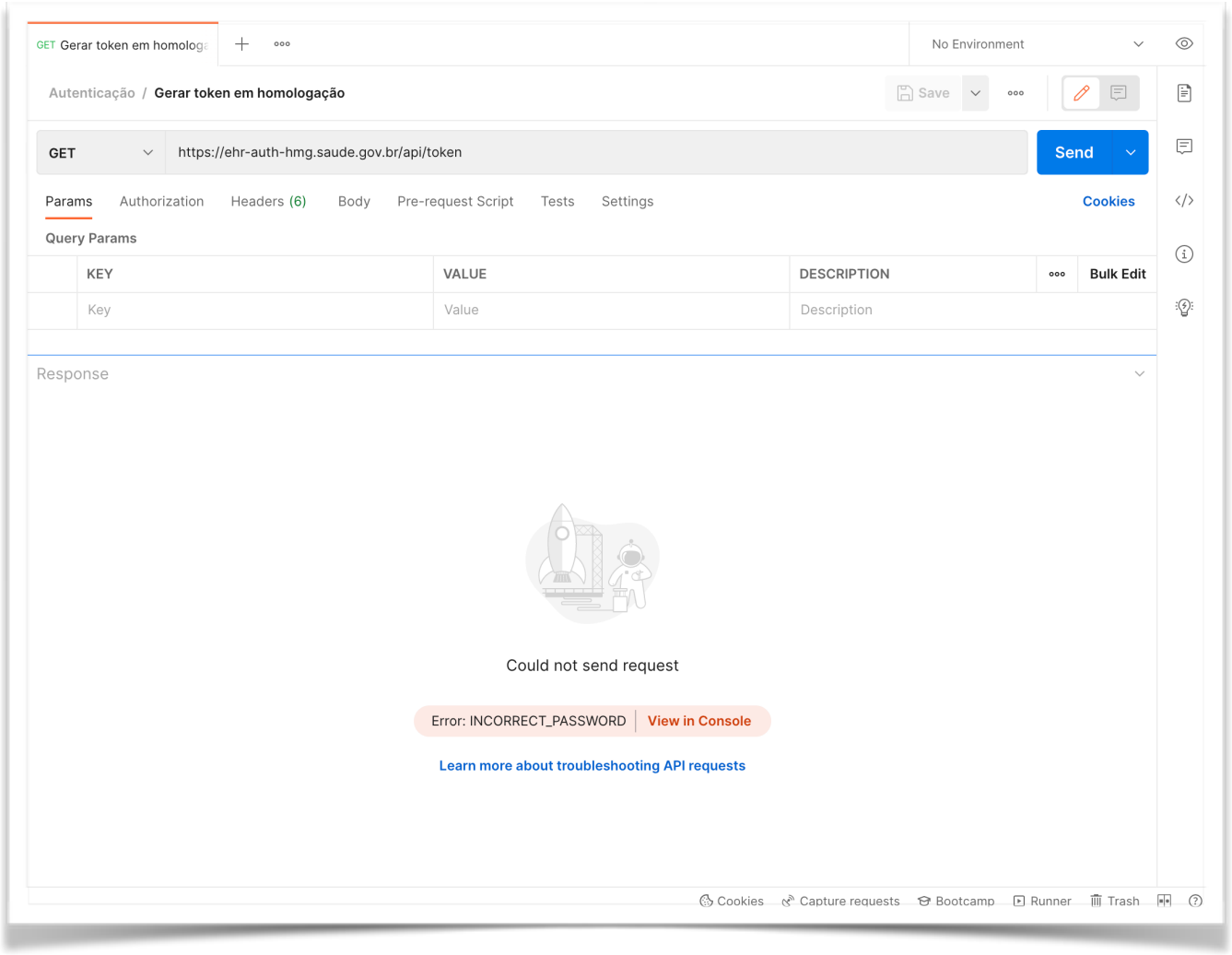
9.2. Erro 404 Not Found

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.



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.



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 API´s 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