Camada de Integração
Serviços Prova de Vida

Orientação sobre como fazer as chamadas de serviços do SIGEPE - Camada de Integração que atendem ao SIGEPE - Benefícios Previdenciários (Prova de Vida).

Cadastro de consumidores

Cada banco que for acessar o serviço, precisa nos informar o nome e código do banco, além da CN (Common Name) do certificado que será utilizado para realizar as chamadas. Estes dados serão cadastrados no SIGEPE - Camada de integração e será disponibilizado um hash individual para cada banco. Cada consumidor estará autorizado a acessar um serviço específico e este hash é utilizado para determinar isso.

É necessário que nos enviem:
- o IP da máquina que estará realizando o acesso ao serviço para que seja pedida liberação de regra de firewall no nosso ambiente de homologação;
- as cadeias de certificado utilizadas para que sejam cadastradas no servidor da nossa aplicação.

URL de acesso

https://hom.integracao.sigepe.gov.br/sigepe-camadaintegracao-servicos/camadaIntegracao/{serviço}

Envio de variáveis

A maioria das chamadas dos serviços do camada de integração são POST,

No serviço de consultar, as variáveis devem ser enviadas em um form.

Nos serviços de realizar prova de vida (positiva/negativa), esperamos um JSON de entrada. O modelo pode ser encontrado no swagger.

Variáveis de autorização

Estas variáveis obrigatórias são usadas no header de cada serviço e são utilizadas para identificar o consumidor e o certificado.

Consumidor do serviço (X-AUTH-CONSUMIDOR)

Ao ser realizado o cadastro de um banco como consumidor do serviço, será disponibilizado um hash individual. Este valor do hash deve ser enviado no header da chamada, na variável X-AUTH-CONSUMIDOR.

Certificado

O certificado da máquina que está chamando o serviço também deve ser incluído no header da chamada. O CN deste certificado deve ser o mesmo que foi cadastrado como um consumidor do serviço.

Cliente de acesso

Enviamos junto um cliente feito em java com resteasy, como exemplo de como deve ser feita a chamada para os serviços do SIGEPE - Camada de Integração. Cada banco pode implementar o cliente da maneira que preferir, somente precisam ser obedecidos os critérios de envio de dados mencionados anteriormente.

https://drive.google.com/file/d/1ir7tB3ZHTHBv8RX9cF3rU7atoLI7_8TX/view?usp=sharing

Serviços

Os serviços disponíveis e mais detalhes com exemplos podem ser encontrados na url https://hom.integracao.sigepe.gov.br/sigepe-camadaintegracao-servicos/swagger/index.html?url=https://hom.integracao.sigepe.gov.br/sigepe-camadaintegracao-servicos/camadaIntegracao/swagger.json (Caso seja solicitado autenticação via certificado, clicar em cancelar)

Resposta dos serviços

Por padrão, sempre é retornada uma resposta http 200 e um json de retorno com o seguinte formato


```
{
        "dataCarga": null,
        "retorno": 0,
        "motivoErro": null,
        "ultimaProvaVida": {
        "nomeBeneficiario": "NADIR DEMARCHI RAMOS",
        "cpf": "17475465187",
        "dataNascimento": "30/03/1956",
        "nomeMaeBeneficiario": "MAE SERVIDOR",
        "situacao": "REGULAR",
        "mensagemErro": null
        },
        "dataCargaFormatado": ""
}
```


Campo retorno

0 = sucesso na comunicação com o Camada de Integração
1 = quando ocorre algum problema interno do sistema
2 = quando ocorrem outros erros relacionados a camada de autorização/autenticação (por exemplo, erro de acesso negado)

Campo motivoErro

mensagem de erro do Camada de Integração

Campos dataCarga, dataCargaFormatado

podem ser ignorados, são utilizados por outros serviços

Campo ultimaProvaVida

Quando realizada com sucesso, traz os dados da consulta.
Quando ocorre algum erro de negócio, o campo mensagemErro trará a mensagem de erro de negócio pertinente. Por exemplo: CPF que não seja de beneficiário.

Campo provaVida

Quando realizada com sucesso, todos campos devem vir nulos.
Quando ocorre algum erro de negócio, o campo mensagem trará a mensagem de erro de negócio pertinente. Por exemplo: CPF que não seja de beneficiário.

No momento estamos retornando os campos nulos na resposta dos serviços por causa da maneira como o Camada de Integração foi implementado inicialmente, podendo ser ignorados.

FAQ

1. Será utilizado o método de autenticação mútua TLS?
Sim, será utilizado o método de autenticação mútua TLS.

2. Podemos optar pelo uso de outro método de autenticação (ex.: OAuth 2.0)?
A aplicação não está preparada para utilização de outros métodos de autenticação.

3. Há alguma definição quanto a cadeia de certificação (AC internacional ou ICP-Brasil)?
Se o emissor for a ICP-Brasil, já temos a cadeia instalada no nosso servidor. Caso seja outro emissor será necessário o envio das cadeias do certificado para que sejam adicionadas na nossa aplicação.

4. Podemos utilizar certificados emitidos pela nossa PKI Interna (ao menos para o ambiente de homologação)?
Sim, desde que enviem as cadeias do certificado para que sejam adicionadas na nossa aplicação.

5. Há alguma definição de características mínimas para o certificado TLS (composição do Common Name, tamanho de chave, etc.)?
O Common Name deverá corresponder com o DNS da aplicação cliente. Tamanho da chave com 2048 bits.

6. Há alguma definição quanto ao tipo de certificado permitido (validação de domínio, e-CNPJ, etc.)?
Certificado de equipamento A1 (validação de domínio).