

**CONFIDENCIAL**

Especificação Plataforma de Open Banking

ÍNDICE

[1 Identificação do Documento 5](#_Toc65145360)

[2 Definições e Abreviaturas 5](#_Toc65145361)

[3 Visão Geral 6](#_Toc65145362)

[3.1 Plataforma de Open Banking 6](#_Toc65145363)

[6](#_Toc65145364)

[3.2 Arquitetura 7](#_Toc65145365)

[3.2.1 Visão de Serviços 8](#_Toc65145366)

[3.2.2 Arquitetura de Referência 8](#_Toc65145367)

[3.3 Integração com instituições financeiras 9](#_Toc65145368)

[3.4 Conectores Com a plataforma de Open Banking 9](#_Toc65145369)

[3.5 Conectores para gerenciamento do consentimento (Implementação TecBan) 9](#_Toc65145370)

[3.6 Conectores para o servidor de autorização (Implementação TecBan) 9](#_Toc65145371)

[3.7 Conectores para dados do cliente (2º Fase) (Implementação Banco) 10](#_Toc65145372)

[3.8 Conectores para iniciação de pagamentos (3º Fase) (Implementação Banco) 13](#_Toc65145373)

[14](#_Toc65145374)

[3.9 Relatórios e Logs 15](#_Toc65145375)

[3.10 Proposta Jornada do usuário 15](#_Toc65145376)

[3.11 Utilização do Swagger 15](#_Toc65145377)

[3.12 Esquema Swagger *Tecban* 15](#_Toc65145378)

[4 Monitoração 16](#_Toc65145379)

[5 Segurança 17](#_Toc65145380)

[5.1 Introdução 17](#_Toc65145381)

[5.2 Segurança nas APIs 18](#_Toc65145382)

[5.3 Geração do Token JWT 18](#_Toc65145383)

[5.4 Conectividade - Integração via internet ou API Gateway Privado (Link Dedicado ou VPN) 18](#_Toc65145384)

[5.5 Certificado Digital 21](#_Toc65145385)

[6 Ambiente Sandbox 21](#_Toc65145386)

[7 Premissas e Restrições 22](#_Toc65145387)

[8 Histórico de Alterações do Documento 22](#_Toc65145388)

[9 Documentos de apoio 22](#_Toc65145389)

**Importante: As informações deste documento são confidenciais, devendo circular somente entre os responsáveis pelo processo.**

# Identificação do Documento

Tabela – Identificação

|  |  |
| --- | --- |
| Nome do Documento: | **Especificação Plataforma de Open Banking** |
| Objetivo: | Esta especificação permite que as Instituições Financeiras conectem seus sistemas à Plataforma SaaS que disponibiliza as APIs em nome de seus clientes (White-Label);  Facilidade para o compliance com o Open Banking no Brasil;  Uma solução segura e economicamente eficiente para as instituições financeiras. |

# Definições e Abreviaturas

Tabela – Termos

| Termo | Descrição |
| --- | --- |
| API | Application Programming Interface: conjunto de definições de métodos e funções que fornece uma biblioteca para ser utilizada por outros programas (no caso desse projeto, para páginas Web). De modo geral, a API é composta por uma série de funções acessíveis somente por programação, e que permitem utilizar características do software menos evidentes ao usuário tradicional. |
| IF | Instituição Financeira, Banco Digital, Parceiro ou Fintech. |
| Sandbox | Ambiente para testes da aplicação. |
| APP | Aplicativo mobile transacional da Instituição Financeira. |
| Swagger | Traduzido do inglês – O Swagger é um framework open source que facilita os desenvolvedores a desenhar, especificar e documentar suas APIs. Ele segue a iniciativa [Open API](https://www.openapis.org/) que busca a padronização de APIs REST. Esse termo, descreve os recursos de suas APIs, como endpoints, parâmetros de entrada, objetos de retorno, códigos HTTP, métodos de autenticação, entre outros. |
| Certificado Digital | Arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele pode se fazer transações online com garantia de autenticidade e com toda proteção das informações trocadas. |

# Visão Geral

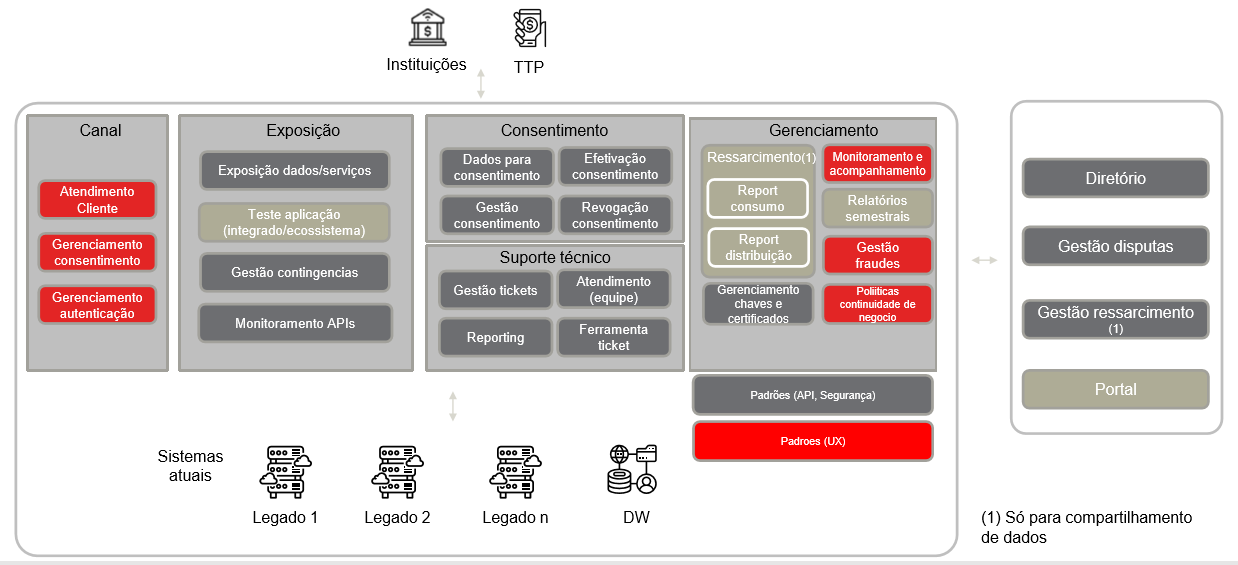
## Plataforma de Open Banking

Os bancos precisam de uma plataforma especializada para realizar a exposição de APIs, de maneira segura e fazer certo as coisas difíceis.

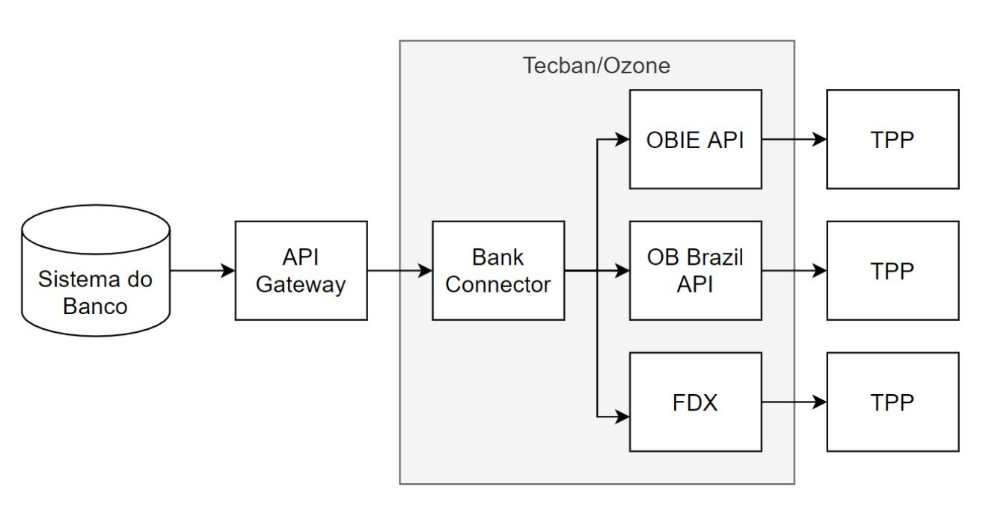
Os 6 pilares da Plataforma de Open Banking da TecBan, representam a solução para o problema acima.

## 

A figura abaixo representa em cinza os pontos do ecossistema do Open Banking que a Plataforma irá lhe apoiar:



## Arquitetura



### Visão de Serviços

Diagrama

Descrição gerada automaticamente

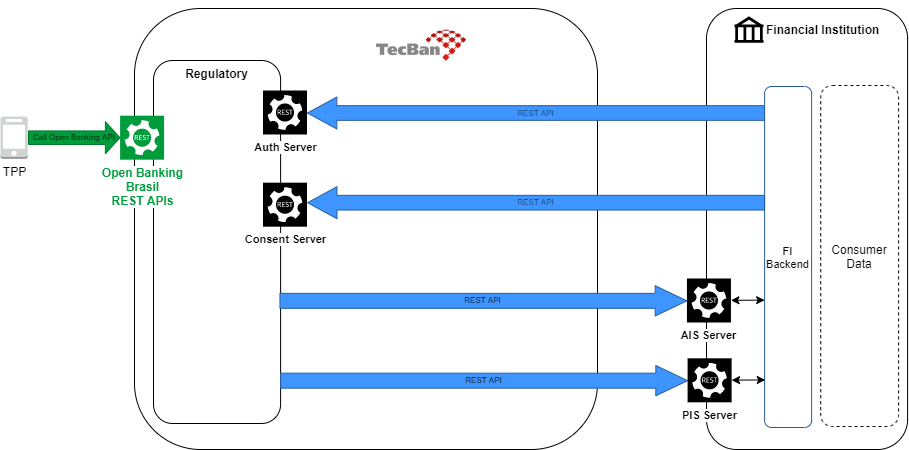
### Arquitetura de Referência

Uma imagem contendo Diagrama

Descrição gerada automaticamente

## Integração com instituições financeiras

O diagrama a seguir mostra as interfaces necessárias entre a Tecban e a IF.



É de responsabilidade da IF expor duas APIs:

**AIS Server** - Essa API deve ser implementada pela IF para que a Tecban possa expor esses serviços as TPPs. Devem estar de acordo com a especificação OpenAPI 3.0 disponibilizada pela Tecban. Vide seção xxx.

Funcionalidades:

* accounts
* balances
* transactions
* customer
* direct-debits
* scheduled-payments
* standing-orders
* offers
* beneficiaries

**PIS Server** - Essa API deve ser implementada pela IF para que a Tecban possa expor serviços de pagamento para TPPs. Devem estar de acordo com a especificação OpenAPI 3.0 disponibilidada pela Tecban. Vide seção xxx.

Funcionalidades:

* payments
* payments-consent

É de responsabilidade da IF chamar as APIs da Tecban de acordo com o fluxo definido nos diagramas de sequência em xxx.

Devem ser chamados dois serviços existentes na plataforma Open Banking da Tecban:

**Authorization Server** - devem ser chamados pela IF no final de suas viagens de autorização.

A interface permite que um ASPSP desenvolva a interface do usuário para PSUs sem ter que lidar com as complexidades de OIDC e FAPI e sem ter que obter um entendimento completo das restrições impostas pela FAPI.

Funcionalidades:

* auth
* auth-confirm
* auth-fail

**Consent Server** - deve ser chamado pela IF para localizar, modificar e excluir consentimentos.

Funcionalidades:

* consents
* psu

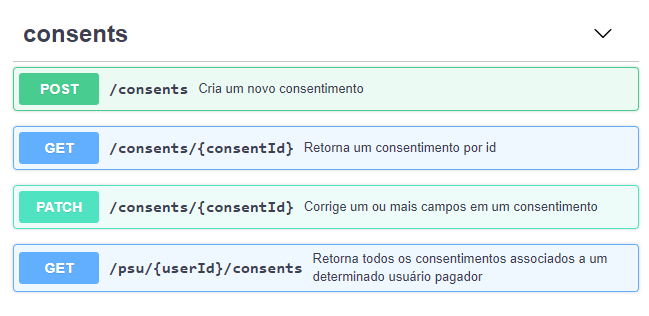
## Conectores Com a plataforma de Open Banking

A TecBan possui um padrão próprio para integração e oferece a possibilidade de customização do formato de troca de mensagens com as instituições financeiras.

## Conectores para gerenciamento do consentimento (Implementação TecBan)

Este seção fornece a especificação para as APIs fornecidas pela TecBan para gerenciamento de consentimento.

Essas APIs são implementadas pela TecBan e devem ser chamadas pelo banco para localizar, modificar e excluir consentimentos.

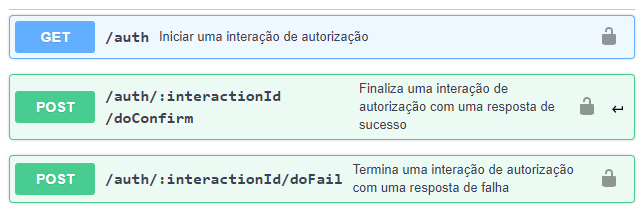


**\*Para detalhamento dos campos consultar arquivo Consent Manager APIs.yaml no formato OpenAPI 3**

## Conectores para o servidor de autorização (Implementação TecBan)

Este documento fornece a especificação para as APIs de autorização.

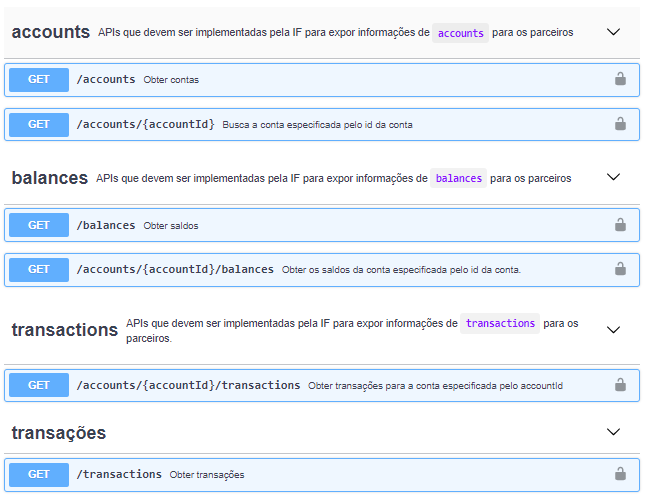
Essas APIs são implementadas pela TecBan e devem ser chamadas pelo banco no final de suas jornadas de autorização.



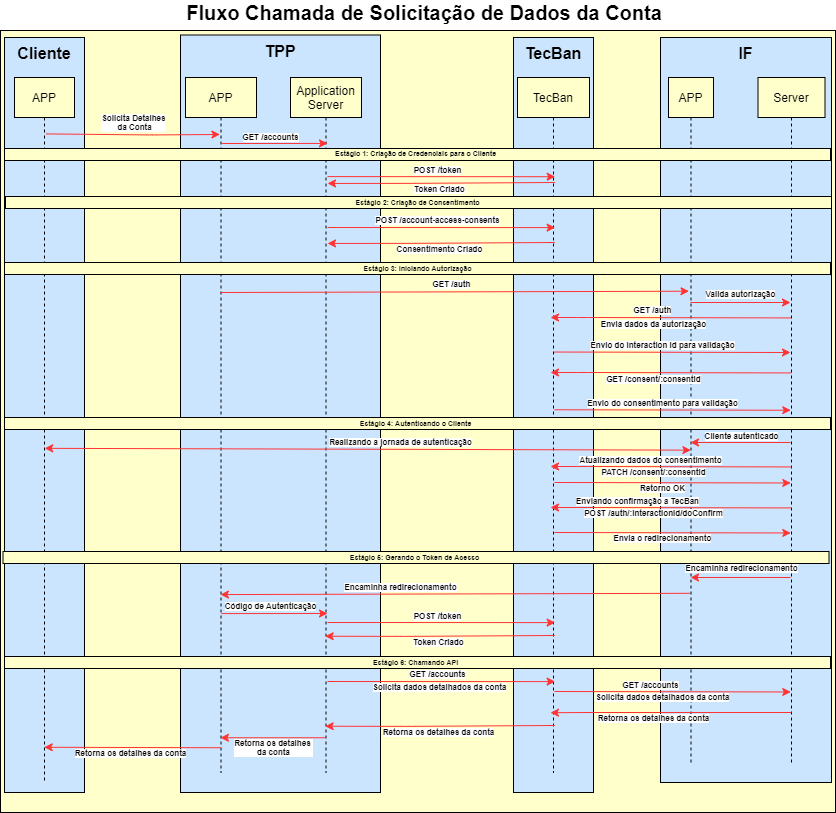
**\*Para detalhamento dos campos consultar o arquivo Headless Heimdall APIs.yaml no formato OpenAPI 3**

## Conectores para dados do cliente (2º Fase) (Implementação Banco)

APIs que devem ser implementadas pelos bancos para expor informações de contas os parceiros.



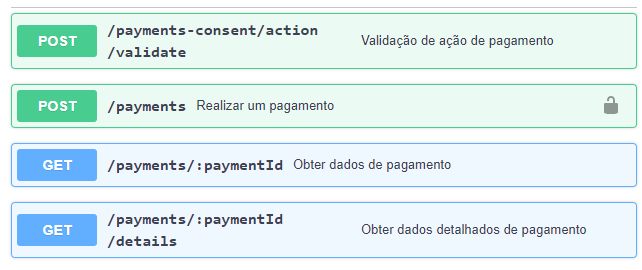
**\*Para detalhamento dos campos consultar o arquivo Bank\_Connect\_AIS\_APIs.yaml no formato OpenAPI 3**



## Conectores para iniciação de pagamentos (3º Fase) (Implementação Banco)

Este documento fornece as especificações para que as instituições iniciadoras de pagamento possam utilizer a plataforma

Essas APIs devem ser implementadas pelos bancos para que a TecBan possa fornecer recursos de iniciação de pagamento para os Terceiros,



**\*Para detalhamento dos campos consultar o arquivo Bank\_Connect \_PIS.yaml no formato OpenAPI 3**

## 

## Relatórios e Logs

A ser especificado.

## Proposta Jornada do usuário

Consultar o Guia em anexo a este documento (Jornadas de usuário.pdf), produzido pelo Grupo de Trabalho do Open Banking e aprovado pelo Banco Central.

## Utilização do Swagger (OpenAPI 3)

Para visualizar o detalhamento dos campos que deseja consultar no swagger, basta acessar no link <https://editor.swagger.io/>

Selecione “File/Import File” para importar os arquivos yml disponíveis juntamente com essa Especificação Técnica Funcional.

## Esquema Swagger *Tecban*

* **Formato date-time ( GMT +0 )**

Os swaggers da TecBan utilizam o padrão GMT + 0 nos campos com o formato “date-time”.

Dessa forma, ao consumir as APIs da TecBan utilizar esse esquema definido no swagger.

Exemplo:

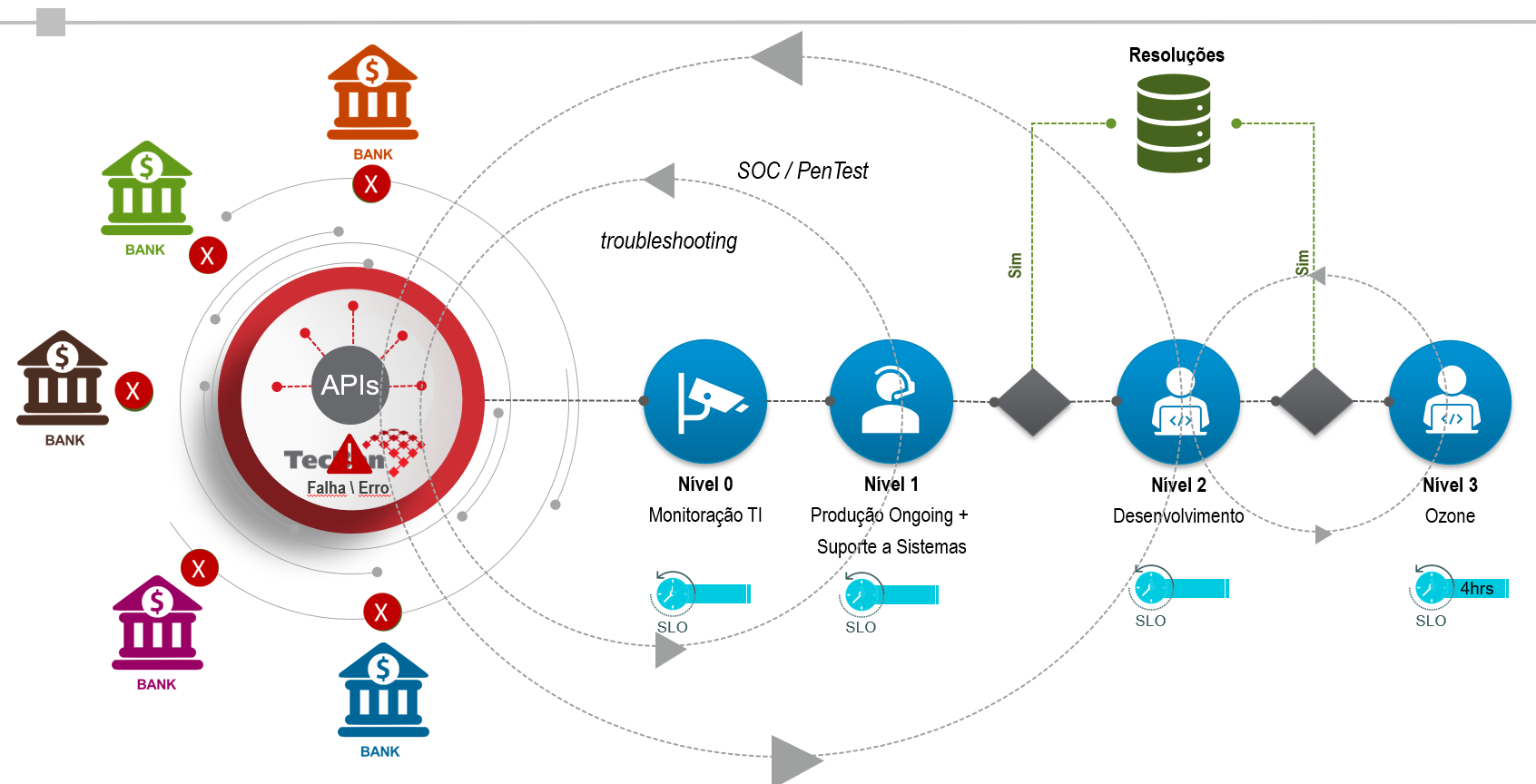


# Monitoração

Os ambientes produtivos são monitorados 24x7 por ferramentas de última geração que avisam imediatamente os operadores do centro de controle que conta com uma equipe técnica especializada para o pronto atendimento.



O processo de monitoria conta com 4 níveis de suporte em caso de falha ou erro das API´s



# Segurança

## Introdução

A segurança é um item primordial para garantir a viabilidade da solução. A partir disso, os requisitos abaixo devem tratar as possíveis ameaças relacionadas:

**Especificação de utilização de comunicação cifrada via HTTPs TLS1.2 com cifras fortes** (TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 ou

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 ou superiores).

**Repetição de mensagem –** deve garantir que mensagens repetidas não sejam aceitas pelo Host TecBan

* Mesmo que os dados sejam capturados, o mesmo comando não deve funcionar com tentativas de reenvio. (Possível fraude)
* Mensagens duplicadas enviadas por bug do sistema não devem ser processadas. (Erro de programação)

**Acesso não autorizado –** a segurança deve garantir que o acesso só seja concedido se o usuário (IF) possuir credenciais válidas e permissão de acordo com as politicas de segurança definidas pela TecBan.

**Garantia de origem –** as aplicações deverão garantir a origem através de validação de assinatura digital.

## Segurança nas APIs

Segurança é fundamental para integração com nossas APIs, utilizamos elementos de segurança como autenticação e autorização.

Para autorização será necessário que o parceiro gere um token no padrão JWT (JSON Web Tokens).

## Geração do Token JWT

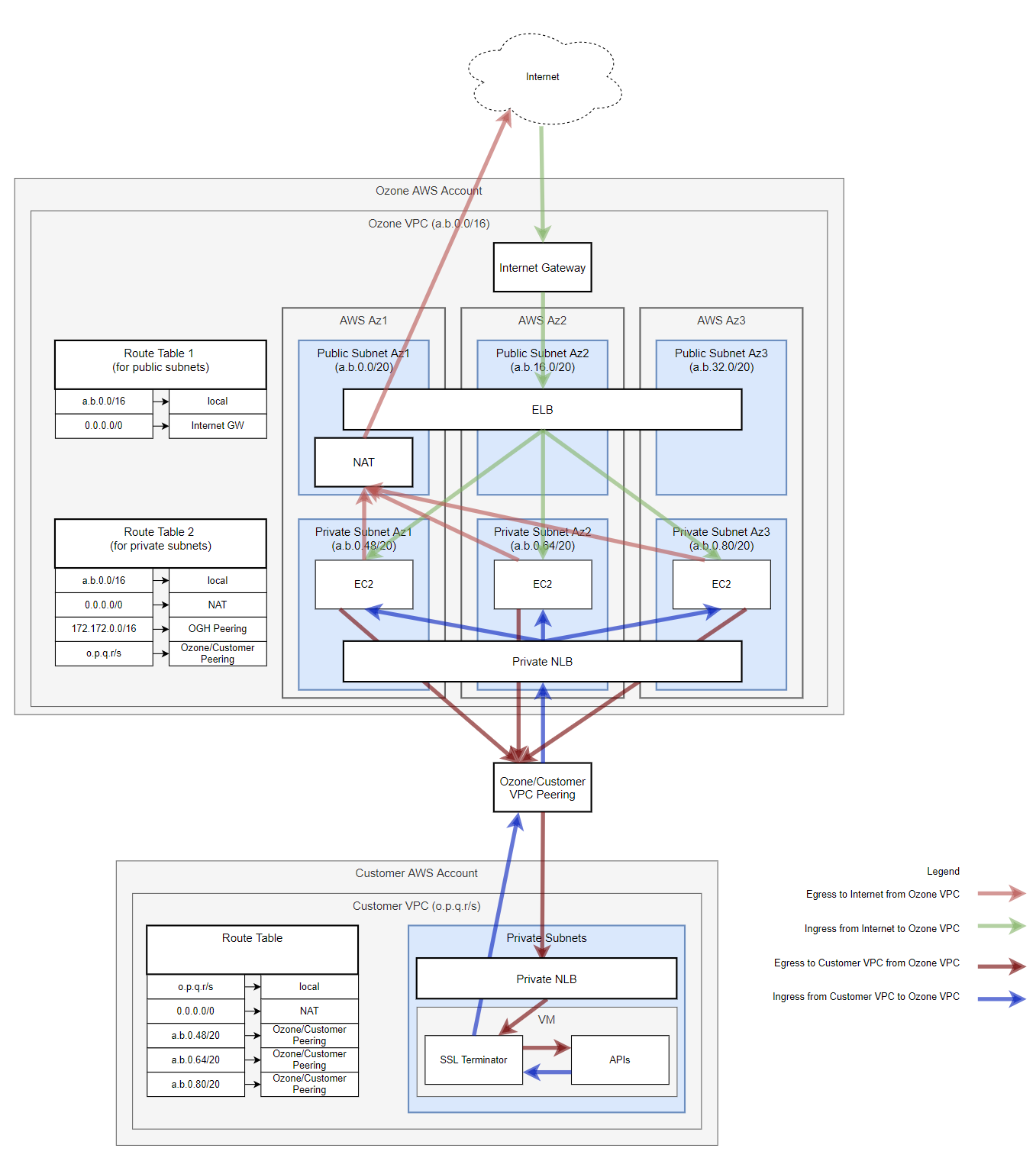
Em breve iremos divulgar a documentação da geração do token.

## Conectividade - Integração via internet ou API Gateway Privado (Link Dedicado ou VPN)

Para as Instituições Financeiras que ingressarem na rede Banco24Horas® será analisado o modelo de conectividade com a TecBan, que poderá envolver a contratação de link físico dedicado ou utilização de VPN.

Durante o projeto deverá ser compartilhado com a TecBan os IPs que irão chamar as APIs para para autorização das chamadas.

Para as Instituições Financeiras que já ingressaram no Banco24Horas® haverá uma avaliação sobre o uso do link já existente.



## Certificado Digital

O parceiro deve gerar dois certificados, sendo um para o ambiente de homologação e outro para o ambiente de produção. A chave pública do certificado deve ser compartilhada com a TecBan da seguinte forma: A chave de homologação pode ser enviada para a equipe do projeto, e a chave de Produção deve ser enviada pelo e-mail de um representante cadastrado da IF para a área de relacionamento da TecBan.

Nossa recomendação para geração do certificado digital, é utilizar certificados com data de validade máxima de 1 ano e padrão RSA 2048.

As mensagens sem assinatura digital do seu conteúdo ou cuja a assinatura não corresponda ao certificado supracitado devem ser desconsideradas.

# Ambiente Sandbox

Para auxiliar nos fluxos iniciais de testes, disponibilizaremos um ambiente de Sandbox no decorrer do projeto.

Este ambiente é completamente separado do ambiente de Produção. Nenhum dado é compartilhado entre os ambientes.

O ambiente Sandbox permite exercitar as chamadas sem as validações de segurança como certificado e assinatura, sendo um contato inicial com as APIs.

# Premissas e Restrições

Ao cosumir as APIs da TecBan, a IF deverá enviar todos os campos respectivos ao date-time no padrão GMT+0.

# Histórico de Alterações do Documento

Tabela – Histórico

| Versão | Data | Autor | Alteração |
| --- | --- | --- | --- |
| 1.0 | 23/02/2021 | Josué Jofre e Luiz Bonnarder | Criação do documento |
| 1.1 | 15/03/2021 | Josué Jofre | Adicionado referência ao documento |

# Documentos de apoio

| Versão | Descrição |
| --- | --- |
| Versão 2.2 Lançamento 26.4 | Bank\_Connect \_PIS.yaml |
| Versão 2.2 Lançamento 30.1 | Bank\_Connect\_AIS\_APIs.yaml |
| Versão 2.2 Lançamento 26.4 | Consent Manager APIs.yaml |
| Versão 2.2 Lançamento 26.4 | Headless Heimdall APIs.yaml |
| Versão 1.0 | Plano de disaster recovery, nome do documento Open\_Banking\_DR.doc |
| Versão 1.01.01 - 05/03/2021 | Jornadas de usuário.pdf |