IDP Fase 1

Arquitetura da solução

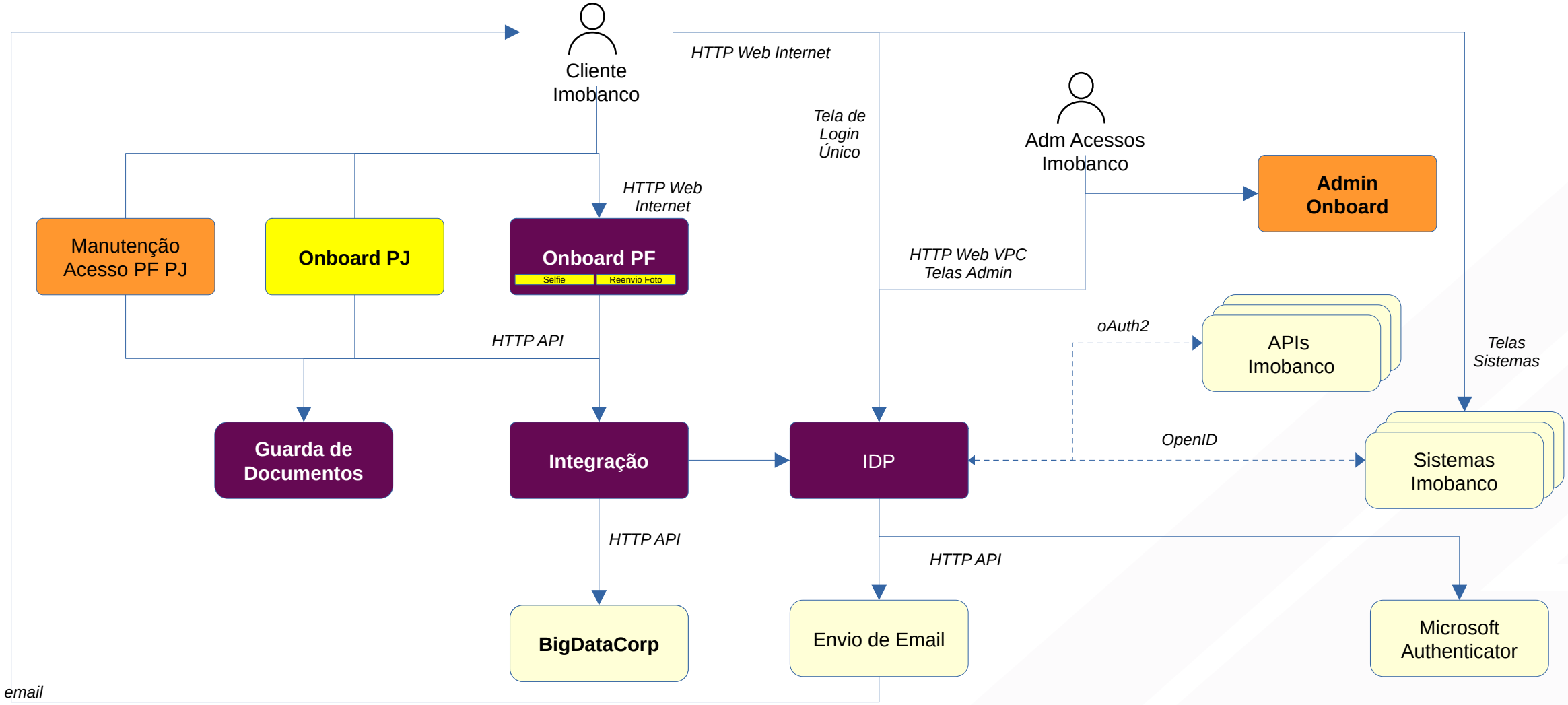
imo banco

Accurate SOFTWARE

OBJETIVO DO PROJETO IDP Fase 1

- Configurar um novo Identity Provider baseado em Keycloak para gestão de identidades de clientes e parceiros do Imobanco
- Configurar um módulo administrativo de identidades no IDP baseado em customização de telas do Keycloak
- Implementar uma nova aplicação web (Onboard PF) para o cadastramento *self service* de clientes PF que desejam uma identidade digital no novo IDP
- Implementar microsserviços de integração entre os sites de Onboard e a BigDataCorp para validação da identidades, antifraude e KYC
- Implementar upload e armazenamento de foto de documentos e comprovante de endereço dos clientes
- Configurar MFA
- Customizar a tela de login centralizado a partir dos templates do Keycloak
- Implantar em 2 ambientes: desenvolvimento e produção

Visão Geral de Arquitetura



Escopo F1 | Escopo F2

Externo | Escopo F3

Jornada Onboard Pessoa Física

3 telas
- 10 informações
  - Nome
  - CPF
  - Data Nascimento
  - Gênero
  - Nome Mãe
  - Telefone
  - Email
  - Endereço
  - Flag Aceite PEP
  - Flag Aceite Termos

3 Arquivos de Imagem por Identidade
- 1 Foto identidade (CNH ou RG)
- 1 Foto Selfie
- 1 Foto Comprovante Endereço

API BigDataCorp Pessoas Basic
- Valida informações digitadas de CPF, Nome Completo, Data Nascimento e Nome da Mãe

API BigDataCorp Pessoas Adresses
- Consultar o histórico de endereços e validar contra o endereço digitado

API BigDataCorp Pessoas KYC
- Consulta sanções, restrições, protestos de diferentes órgãos incluindo Bacen e CVM

API BigDataCorp Documentoscopia
- Envio da foto identidade para OCR e autenticidade
- Identificação da foto selfie no documento
- OCR no comprovante de endereço e identidade

Keycloak 22 linux

E-mail com URL para cadastro

Microsoft Authenticator

Escopo F1 | Escopo F2 | Escopo F3

Validações CPF BigDataCorp

Lista de sanções analisadas pelo dataset

Campo
CVM - Alerta Suspensão
CVM - Penalidade Temporaria
CVM - Termo Compromisso
Banco Central - Inabilitados
Embargos do Ibama
OFAC
COAF
EU
GOVUK
FBI
INTERPOL
UNSC
CEAF
CNEP
MTE (Trabalho Escravo)

MTE (Trabalho Escravo)
Conselho Nacional de Justiça
CEIS
CEPIM
Inidôneos TCU (Tribunal de Contas da União)
Acordos de Leniência (Controladoria-Geral da União)
Processo Administrativo Disciplinar (BSM Supervisão)
Impedidos de Licitar e Contratar Banco
Tribunal de Contas do Estado de São Paulo
SEAPE-DF

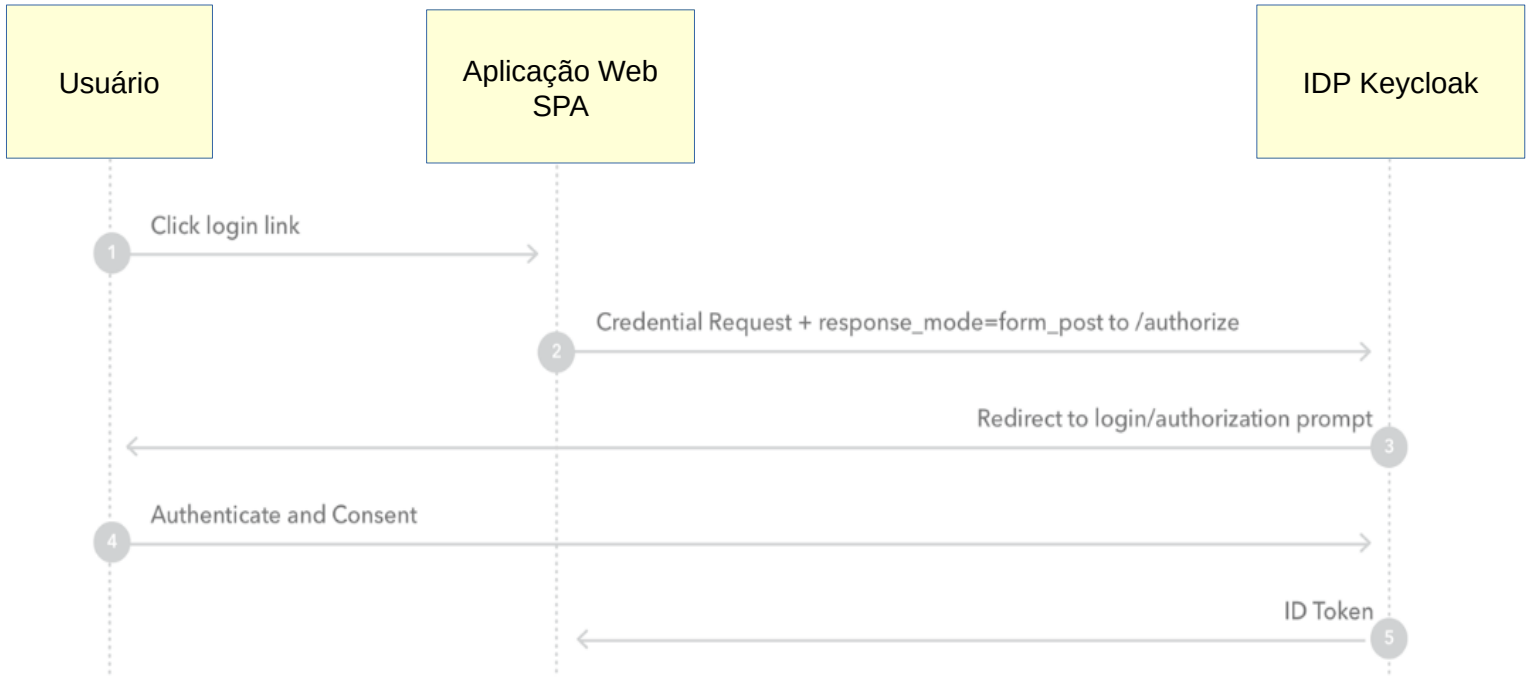
Modelos de Segurança

- OpenID Connector para a autenticação de pessoas utilizando um userid e senha do keycloak
  - Tela de Login centralizada no Keycloak
  - Cada sistema participante terá um Client ID diferente

- OAuth2 Client Credential para autenticação sistêmica a partir de APIs

OpenID Connect

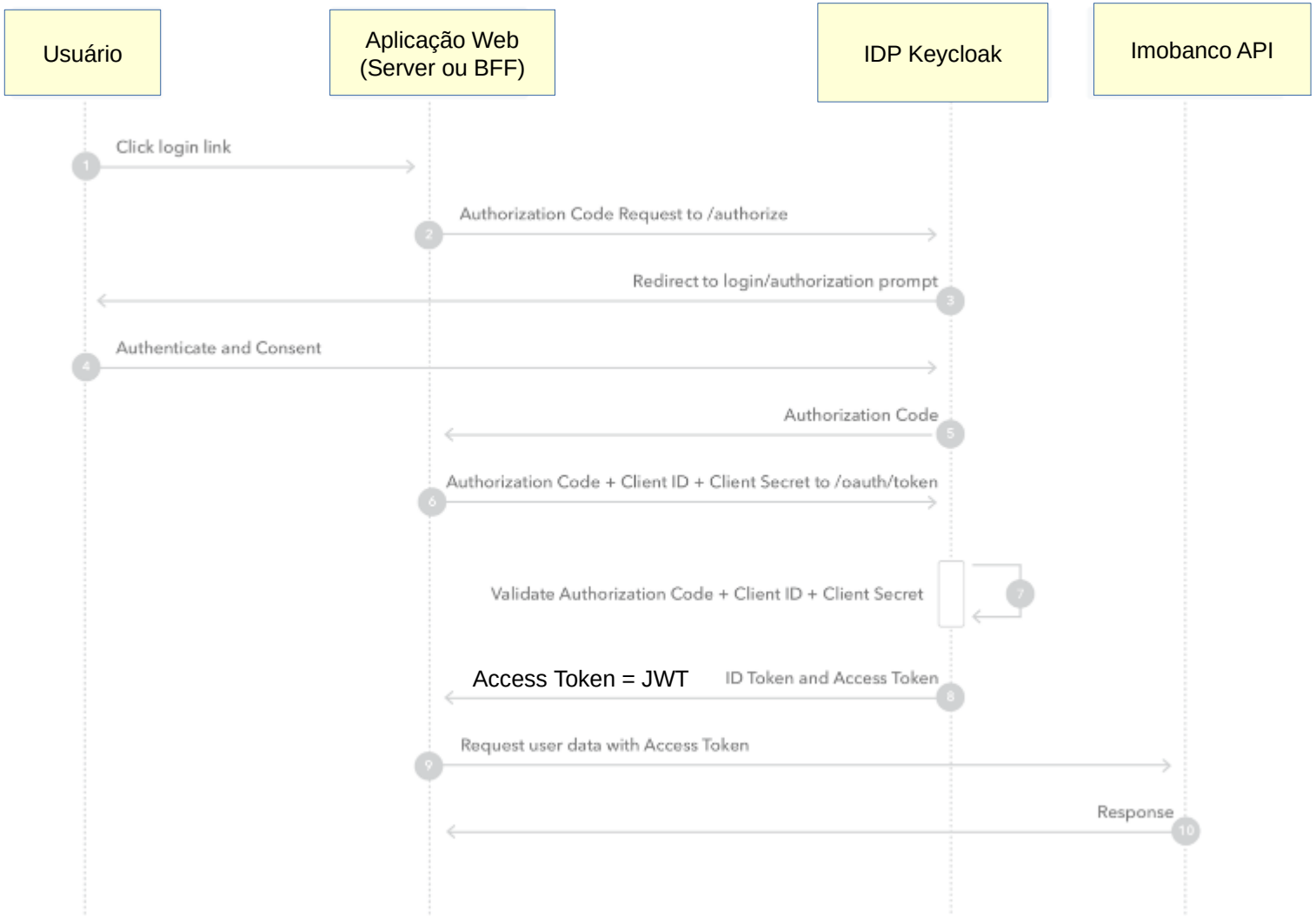
Grant Type Implicit flow – recomendado para aplicações SPA



ID Token = JWT

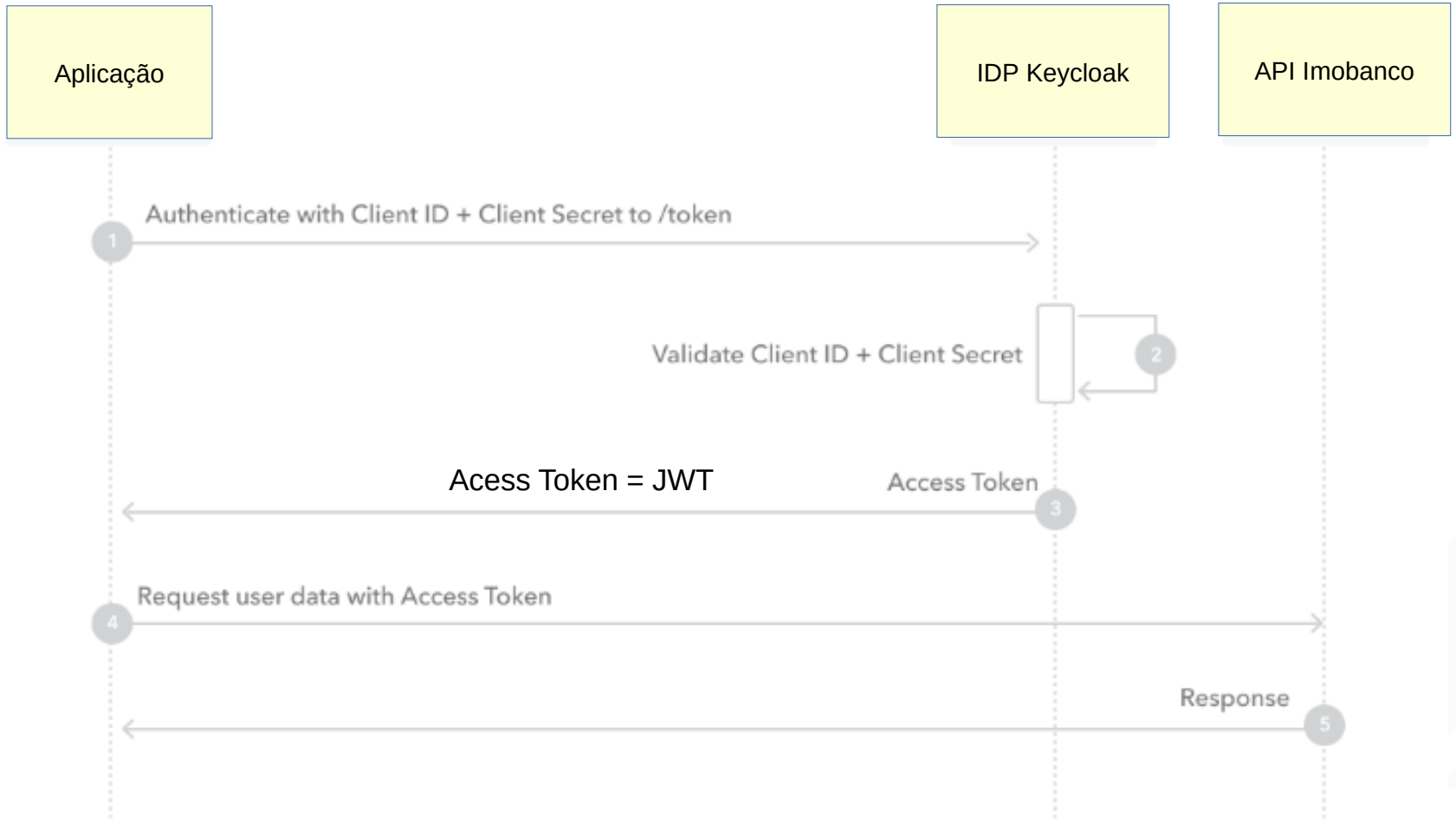
OpenID Connect

Authorization Code flow – recomendado para aplicações com backend em servidor ou com BFF

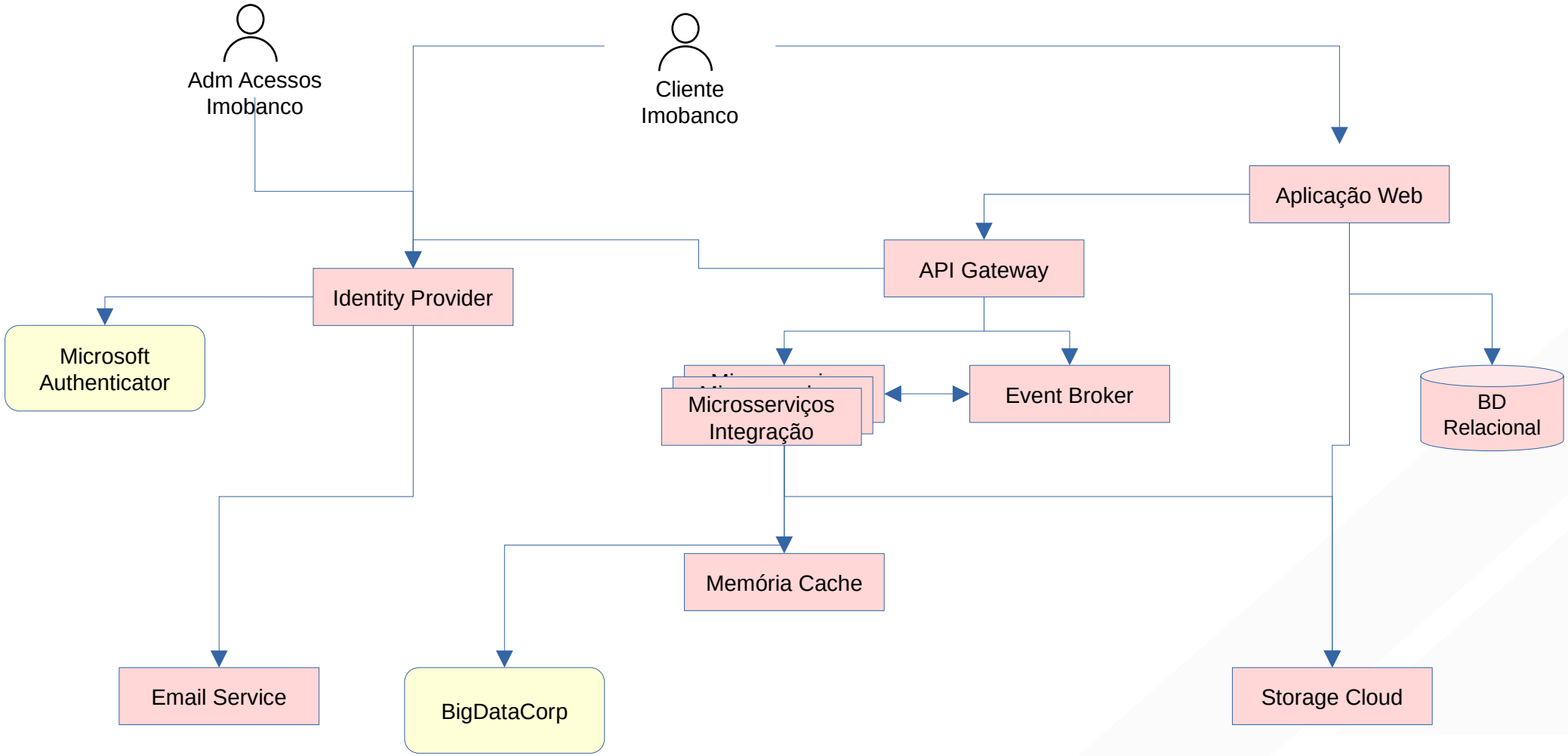


OAuth2 Client Credential

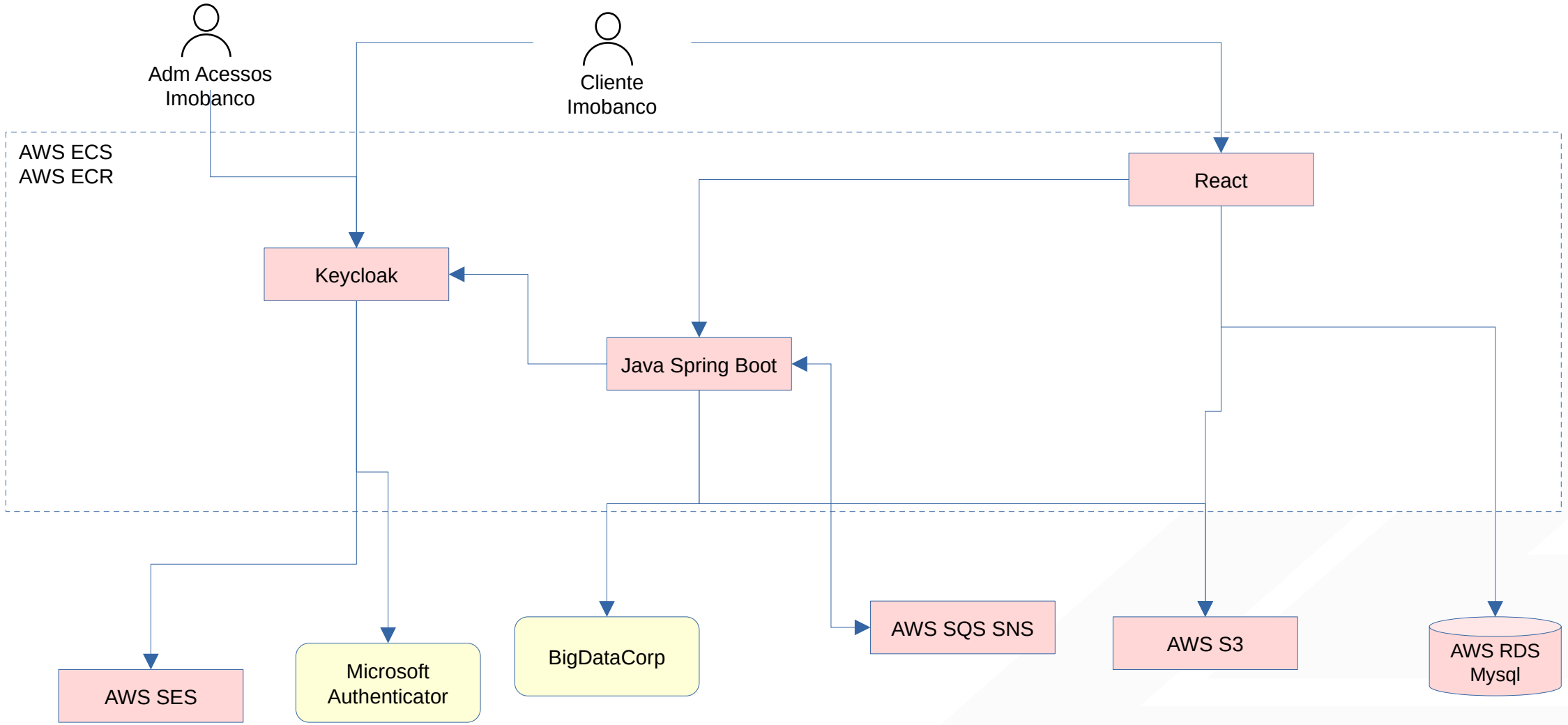
Recomendado para aplicações consumidoras de API



Arquitetura Técnica



Arquitetura Técnica



Arquitetura Técnica - Detalhamento

- 1 aplicação Web React

  - 1 site de Onboard PF com aproximadamente 4 telas/funcionalidades
    - Cadastro (2)
    - Upload dos documentos (1)
    - MFA (1)

- Microsserviços
  - Validação Cadastral CPF
  - Endereços
  - Autenticidade documento PF
  - Restrições e Sanções PF
  - Identidade
  - Upload

- Integração com API BigDataCorp para bureau e validação de PF e PJ
  - Cadastral PF
  - Endereço PF
  - Restrições Sanções PF
  - Autenticidade Foto Identidade PF
  - OCR Comprovante de Endereço PF

Arquitetura Técnica - Detalhamento

- Banco de dados relacional mysql gerenciado por AWS RDS para armazenamento dos dados de cadastro dos cliente PF
- Event Broker AWS SQS para controle dos fluxos de onboard e integrações
- AWS SES como serviço de disparo de e-mails
- AWS S3 como serviço de storage cloud para armazenamento das fotos do onboard

Arquitetura Técnica - Detalhamento

- Keycloak versão 21 em imagem docker sobre Java Quarks
- Customização das telas nativas do Keycloak para o módulo administrativo de login e credenciais
- Customização da tela de login do Keycloak conforme template do produto
- Uso de Java OpenJDK
- IDP MFA baseado em Microsoft Authenticator
- Utilizar o GitHub do Imobanco

Arquitetura Técnica - Detalhamento

Eventos:

2 filas para tratamento de documento

- dev_fila_documento_pf
- dev_fila_documento_pf_dlq

2 filas para validação cadastral

- dev_fila_cadastro_pf
- dev_fila_cadastro_pf_dlq

2 filas para validação de endereço

- dev_fila_endereco_pf
- dev_fila_endereco_pf_dlq

2 filas para validação de restrições

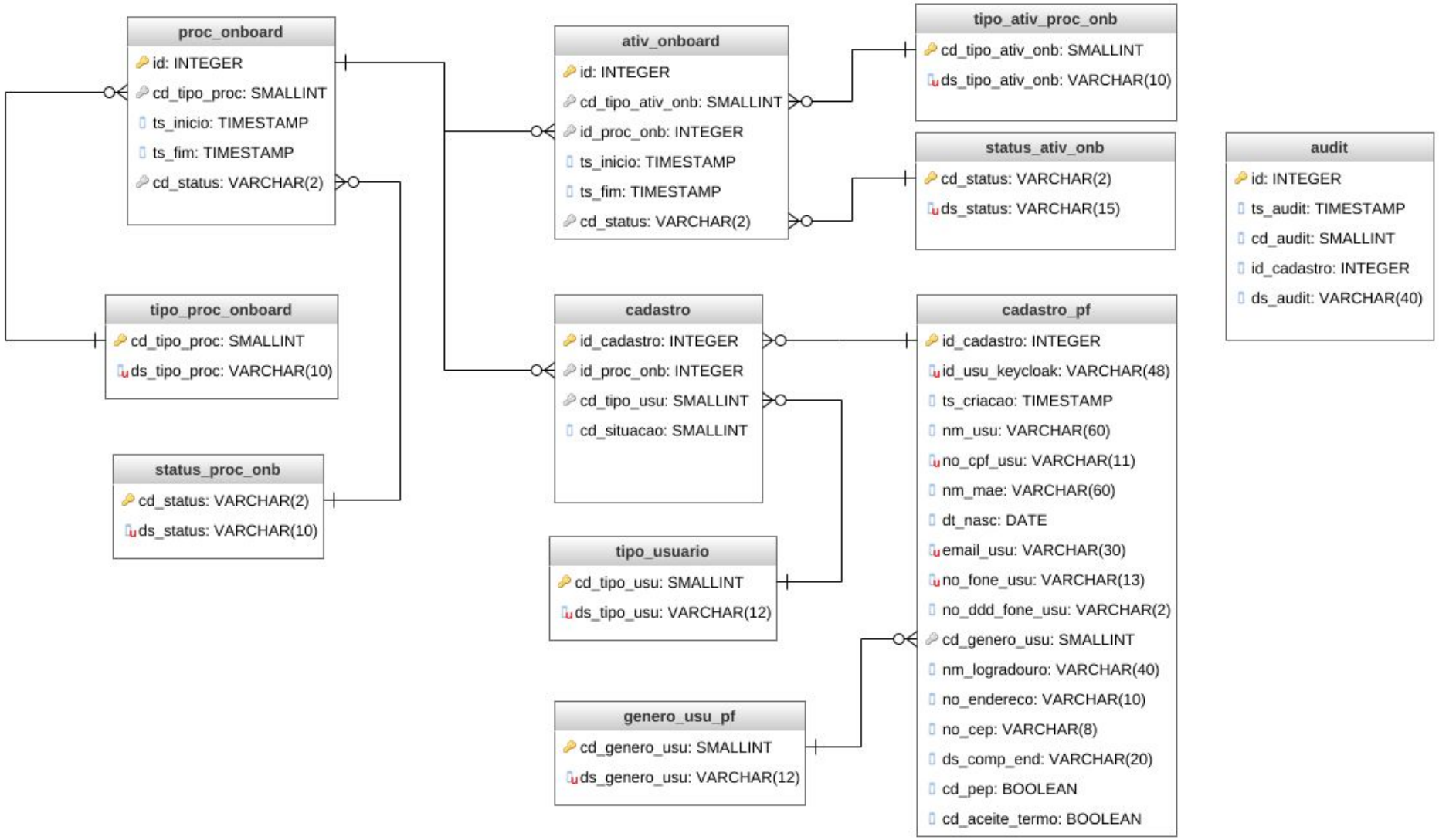
- dev_fila_restricao_pf
- dev_fila_restricao_pf_dlq

- 2 filas para documentoscopia
- dev_fila_documentoscopia_pf
- dev_fila_documentoscopia_pf_dlq

2 filas para processamento da identidade

- dev_fila_identidade_pf
- dev_fila_identidade_pf_dlq

Modelo de Dados ER



Modelo de Dados ER

Entidade	Descrição
cadastro_pf	Cadastro de usuário PF. Especialização da entidade “cadastro”
cadastro	Cadastro de usuários PF ou PJ
proc_onboard	Processos de onboard realizados (PF ou PJ)
tipo_proc_onboard	Tipo do processo de onboard (PF ou PJ)
status_proc_onboard	Status do processo de onboard, ie, concluido, em andamento etc
ativ_onboard	Atividades relacionadas a um processo de onboard
tipo_ativ_proc_onb	Tipo da atividade do processo de onboard, por exemplo, validação cadastral, validação de endereço etc
status_ativ_onb	Status das atividades de onboard, ie, em andamento, pendente, concluido, erro, sucesso etc.
tipo_usuario	Tipo de usuario pertencente ao cadastro, ie, PF ou PJ
genero_usu_pf	Generos de um usuário PF, ie, masculino, feminino e outros
audit	Tabela de registro de transações estilo Quem, Quando, O que

Implementação em 3 Fases

- **Fase 1 - PF**
  IDP
  - Login Único
  - Modulo Administrativo
  - MFA
  - Cadastro CPF

  Onboard PF
  - Upload de Identidade + Comprovante de Endereço
  - Validação Cadastral
  - Restrições e Sanções
  - Autenticidade e OCR da CNH ou RG
  - Validação histórico de Endereços vs digitado

- **Fase 2 – PJ e Melhorias PF**
  Onboard PJ
  - Validação Cadastral
  - Restrições e Sanções
  - Identificação de sociedade pelo Bureau

  Onboard PF
  - Validação Selfie vs foto identidade
  - OCR Comprovante de Endereço
  - Reenvio de fotos

- **Fase 3 – Vinculos e Gestão do Processo**
  Manutenção Acessos PF PJ
  Administração Processos

Fora do escopo

- Migração dos sistemas atuais do Imobanco para terem login integrado ao novo IDP
- Migração de identidades existentes em outros Realms em uso pelos atuais sistemas IDP

Paulo Renato Licciardi

paulo.renato@accurate.com.br

07/08/2023

/company/accurate-br/

/accuratesoftwareLTDA

/accurateSoftware

@accurate.br

Obrigado!