OpenInsurance

PERFIL FAPI ÚNICO

Perfil FAPI único

O ecossistema do Open Insurance aderirá ao perfil **Private Key + PAR** como perfil FAPI único

Quem irá aderir?

- Todos os participantes do Open Insurance.

Quando será a adesão?

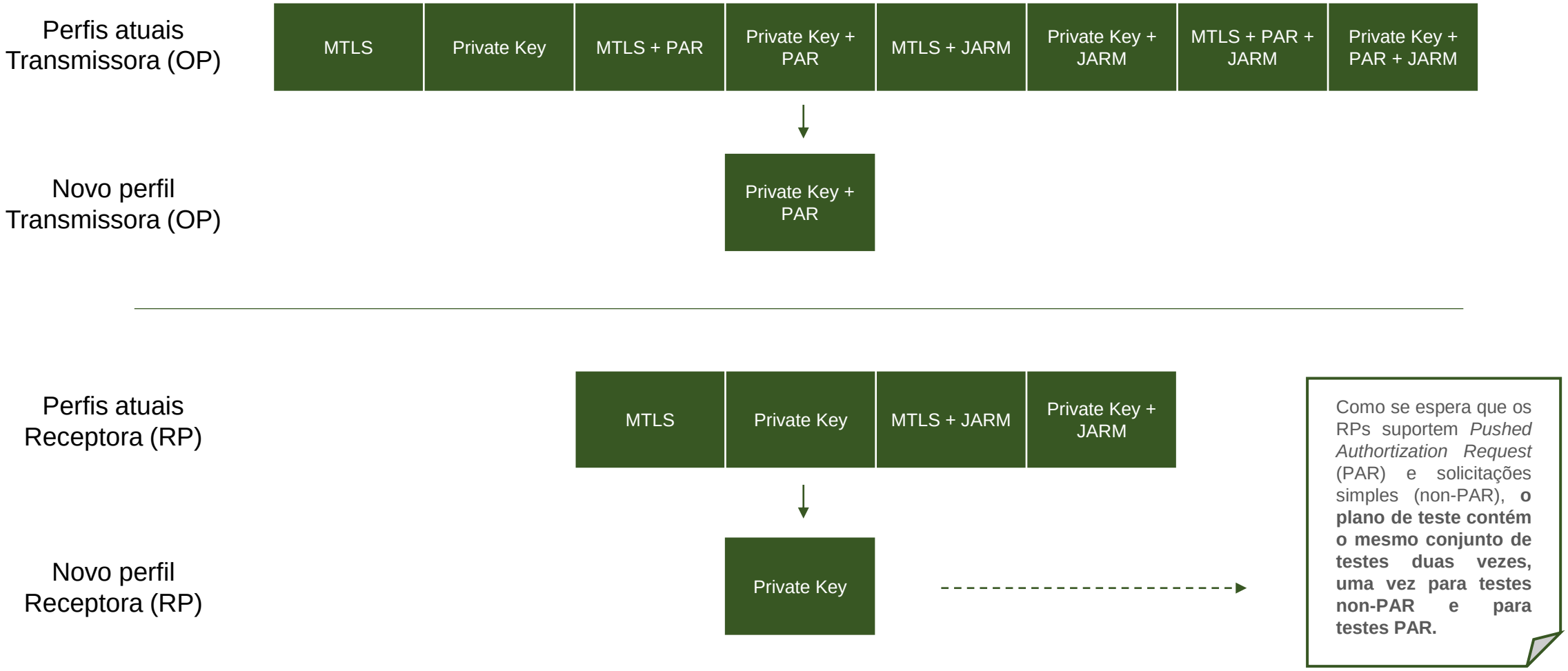
- Próximo ciclo – fim de 2024 e início de 2025
  - Isto é, o ciclo atual em andamento não será afetado

Benefícios do perfil único

- Menor complexidade de implementação
- Favorece a implementação de ecossistemas interoperáveis
- Favorece a implementação futura do FAPI 2.0

Consolidação dos Perfis

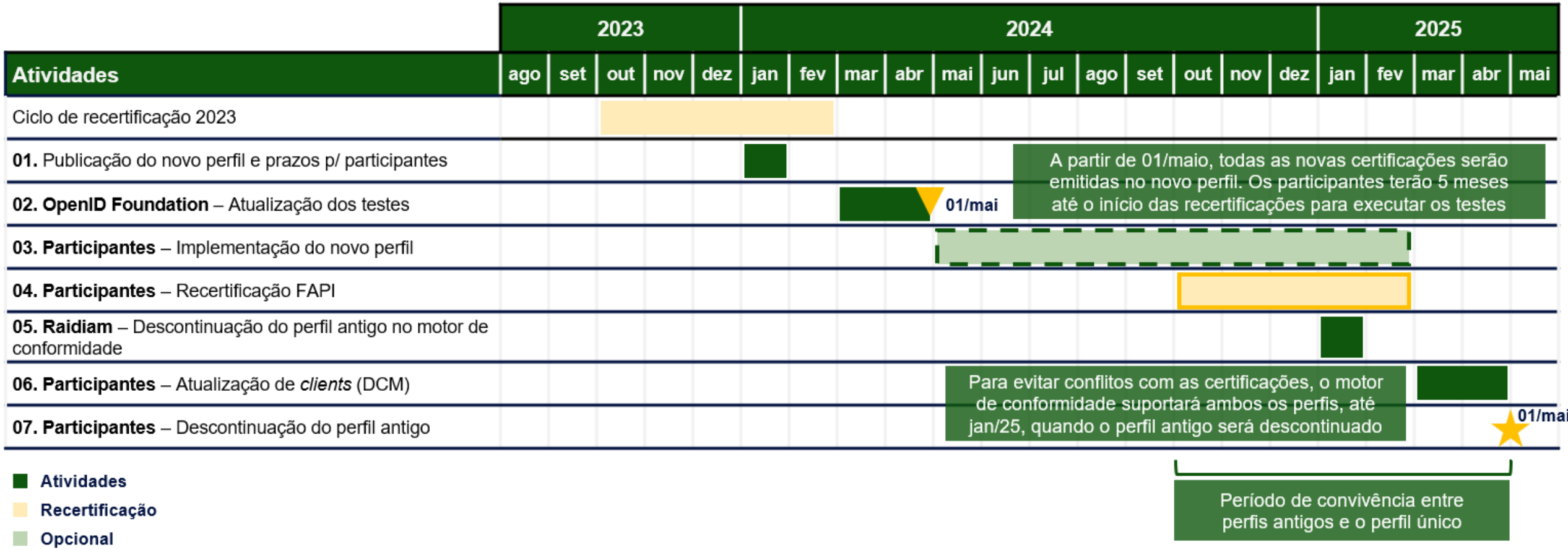
Tanto os perfis de transmissoras quanto receptoras serão consolidados em um único perfil



Calendário de implementação do FAPI único

Open Insurance

Apresenta-se abaixo como se dará a implementação do perfil único no ecossistema do Open Insurance:



Calendário de implementação do FAPI único

- **01. Publicação do novo perfil e calendário para os participantes:** Período de divulgação ao mercado do novo perfil FAPI único que será utilizado no Open Insurance, além da publicação deste calendário de implementação do FAPI único e realização de workshops.
- **02. OpenID Foundation – Atualização dos testes:** Período em que a OpenID Foundation irá utilizar para atualizar o motor de testes relacionados as certificações FAPI, para que os esses estejam adequados ao novo perfil de segurança.
- **03. Participantes – Implementação do novo perfil:** Nessa etapa do calendário, após atualização do motor de testes, as participantes podem opcionalmente testar a implementação do novo perfil. Visto que o motor é público e pode ser testado a qualquer momento, as participantes terão 5 meses para realizar seus testes até a submissão da recertificação.
- **04. Participantes – Recertificação FAPI:** Período no qual as participantes deverão submeter a recertificação FAPI no novo perfil único.
- **05. Raidiam – Descontinuação do perfil antigo no motor de conformidade:** A partir dessa data o motor de conformidade da Raidiam não aceitará mais testes relacionados aos perfis antigos.
- **06. Participantes – Atualização de *clients* (DCM):** Durante esse período, as receptoras devem informar aos servidores de autorização das transmissoras, via manutenção do *Client Registration*, que estão suportando somente o novo método de autenticação (Private Key + PAR).
- **07. Participantes – Descontinuação do perfil antigo:** Após a data de 01/05/2025, os servidores de autorização das transmissoras não devem mais aceitar pedidos de registro (DCR) e comunicações no perfil antigo.

Mudanças técnicas

Além da consolidação dos perfis, certas restrições e alterações que visam reduzir o número de possibilidades e facilitar a implementação serão adotadas:

- Criptografar o id_token por padrão, sem a necessidade de validação do PII em seu conteúdo
- Tornar o Proof Key for Code Exchange (PKCE) obrigatório
- Remover claims CPF e CNPJ
- Proibir a rotação de registration_access_token no processo de DCR/DCM

- Restringir os parâmetros do atributo response_type
- Restringir os parâmetros do atributo response_mode
- Restringir os parâmetros do atributo subject_type
- Implementar refresh_tokens opacos sem data de validade nos cenários onde o mesmo é necessário
- Cadastrar um enc_key no diretório de participantes

As documentações atualizadas estão disponíveis na seção de Segurança do Portal do Desenvolvedor.

Os documentos alterados foram: Dynamic Client Registration (DCR), FAPI Security Profile e a seção 4.3.1 do documento Guia do Usuário para Instituições Receptores de Dados

Lembrete: O que será testado – **Certificação FAPI OP**

Essa certificação garante que as transmissoras do ecossistema estão aderentes a esse padrão, de modo que é primordial para assegurar a privacidade dos dados de clientes e resguardar a imagem do ecossistema.

Validações das mensagens de requisição

Testes exaustivos que verificam a conformidade das requisições com o padrão FAPI, como:

- Validação de assinaturas
- Tratamento correto de parâmetros ausentes/inválidos

Teste de autorização e autenticação segura

Avaliações profundas de variados cenários como:

- Manipulação correta de tokens
- Manipulação de consentIds por diferentes clientes
- Uso correto de assinaturas de clientes
- Entre outros...

Validação de comportamento de erro e fluxo de exceção

Testes com escopos específicos:

- Simulação de situações de erro para verificar a capacidade do Authorization Server em direcionar as mensagens corretas de erro e;
- Simulação da capacidade de orientar corretamente o usuário quanto a lidar da maneira correta em cenários que o id_token não corresponde ao esperado.

Lembrete: O que será testado – **Certificação FAPI RP**

OpenInsurance

FAPI RP garante que as aplicações receptoras estão em consonância com os padrões estabelecidos assegurando confiabilidade, interoperabilidade e segurança em ambientes de autorização e autenticação

Testes de validação

Verifica se os id_tokens estão corretamente emitidos pelo AS, verificando valores, como:

- C_hash
- Aud
- Exp
- Iss
- S_hash
- Entre outros...

Fluxo de autenticação

Testa variados fluxos de autenticação/autorização de clientes, casos de uso de refresh_token e fluxo com escopos específicos para atender a conformidade com as especificações

Segurança e conformidade

Assegura que os clientes sigam as práticas e os padrões de segurança estabelecidos pela regulamentação FAPI, garantido os pilares de segurança da informação nas interações realizadas entre clientes e servidores

Lembrete: O que será testado – **DCR/DCM**

OpenInsurance

DCR e **DCM** são processos no qual o **Clients** e os **Authorization Servers** se identificam e estabelecem os padrões de segurança que serão utilizados no consumo das APIs. Dessa maneira, certifica que a transmissora implementou este processo nos padrões de segurança e funcionando de forma adequada.

DCR – Dinamic Client Registration

- Verificação da eficácia na criação e deleção de registro de clientes
- Validação dos requisitos de segurança como:
  - Certificados TLS
  - Assinaturas JWT
  - Cadeia de certificados ICP-Brasil
  - Não rotação de token de registro
  - Transmissão de dados adequada

DCM – Dinamic Client Management

- Garantia da manutenção do access_token durante as atualizações além da verificação de segurança no que se refere a dados inválidos
- Atualização da configuração de cliente como
  - URLs de redirecionamento
  - JWKS URI
  - redirect_uri

FICOU COM ALGUMA DÚVIDA?

Abra um chamado no portal do *Service Desk*

OpenInsurance