penBanking informa

Confira as últimas atualizações da Estrutura de Governança

Início da Certificação de Conformidade de Segurança Fase 3

A partir de hoje, dia 27/08, estará aberto o envio do pedido de certificação dos testes de segurança FAPI Brasil e DCR para instituições Fase 3.

Lembramos que o teste deverá ser realizado na plataforma da OIDF.

ACESSE A PLATAFORMA OIDF

Tipo de certificado de servidor a ser utilizado em cada *endpoint*

Com o objetivo de dar mais clareza aos requisitos de segurança para acesso aos *endpoints*, tanto de negócio quanto do *authorisation server*, o GT Segurança preparou a tabela abaixo, que explicita o tipo de certificado de servidor a ser utilizado em cada *endpoint*, bem com a indicação dos *endpoints* cujo acesso deve ser realizado exclusivamente por meio de autenticação mTLS.

Esta tabela será refletida nas especificações de segurança do Open Banking Brasil futuramente.

Fase	Grupo	API	Certificado	mTLS
NA	OIDC	.well-known/openid-configuration	EV ou ICP Web SSL	
NA	OIDC	jwks_uri	EV ou ICP Web SSL	
NA	OIDC	authorization_endpoint	EV	
NA	OIDC	token_endpoint	ICP Web SSL	Obrigatório
NA	OIDC	userinfo_endpoint	ICP Web SSL	Obrigatório
NA	OIDC	pushed_authorization_request_endpoint	ICP Web SSL	Obrigatório
NA	DCR	registration_endpoint	ICP Web SSL	Obrigatório
NA	OIDC	revocation_endpoint	ICP Web SSL	Obrigatório
NA	OIDC	introspection_endpoint	ICP Web SSL	Obrigatório
2	Consentimentos	/consents/*	ICP Web SSL	Obrigatório
2	Resources	/resources/*	ICP Web SSL	Obrigatório
2	Dados	/customers/*	ICP Web SSL	Obrigatório
2	Cartão	/credit-cards-accounts/*	ICP Web SSL	Obrigatório
2	Contas	/accounts/*	ICP Web SSL	Obrigatório
2	Empréstimos	/loans/*	ICP Web SSL	Obrigatório
2	Financiamentos	/financings/*	ICP Web SSL	Obrigatório
2	Adiantamento	/unarranged-accounts-overdraft/*	ICP Web SSL	Obrigatório
2	Direitos Creditórios	/invoice-financings/*	ICP Web SSL	Obrigatório
3	Pagamentos	/payments/*	ICP Web SSL	Obrigatório

Tempo de validade do *refresh token*

Com o objetivo de dar publicidade à deliberação realizada pelo Conselho Deliberativo em 31/05, informamos que a validade do *refresh token* deve ser igual à validade do consentimento. Este ajuste será explicitado na próxima versão do Perfil de Segurança do Open Banking Brasil.

Padrões mínimos de nível de autenticação

Informamos uma alteração na documentação do Perfil de Segurança do Open Banking Brasil, no que diz respeito aos padrões mínimos de nível de autenticação. Foi identificado que as exigências contidas neste documento não estavam aderentes às exigências contidas na Resolução Conjunta nº 1 de 2020 (art. 17, caput e art. 17 § 1º Inciso I).

Portanto, a seção 5.2.2.4 do Perfil de Segurança do Open Banking Brasil será atualizada, de forma a contemplar a seguinte orientação:

"A seguinte orientação deve ser observada para o mecanismo de autenticação:

- *De acordo com o Art. 17 da Resolução Conjunta nº 01, as instituições devem adotar procedimentos e controles para autenticação de cliente* ***compatíveis com os aplicáveis ao acesso a seus canais de atendimento eletrônicos.***
- *Em observância à regulação em vigor, sugere-se que:*
  - ***Para a autenticação do usuário em autorizações de acessos às APIs de compartilhamento de dados (Fase 2),*** *os Authorization Servers* ***deveriam*** *adotar, no mínimo, método compatível com LoA2; e*
  - ***Para a autenticação do usuário em autorizações de acessos às APIs das fases subsequentes,*** *os Authorization Servers* ***deveriam*** *adotar método de autenticação compatível com LoA3 ou superior.*

Em todos os casos, a adoção de mecanismo de autenticação mais rigoroso (LoA3 ou superior) fica a critério da instituição transmissora ou detentora de conta, de acordo com sua avaliação de riscos e de forma compatível com os mecanismos habitualmente utilizados. Portanto, o cliente de API ***não deve*** *estabelecer na claim acr qualquer método a ser exigido, mas o método adotado pelo ASPSP deve ser retornado pelo Authorization Server na claim acr conforme estabelecido nesta definição."*

OpenBanking