penBanking informa

Confira as últimas atualizações da Estrutura de Governança

Indisponibilidade programada dos sistemas de email e Sharepoint (Secretariado e Camada administrativa) dos GTs e do Conselho

Informamos que, no período de sábado 02/10 00:01 até domingo 03/10 23:59, faremos a migração de alguns sistemas de informação, como parte da transição entre as empresas Mirow & Co. e Chicago Advisory Partners. Como consequência a comunicação por email do domínio openbankingbr.org (p.ex. secretariado@openbankingbr.org, gt-infraestrutura@openbankingbr.org) e o Sharepoint com arquivos dos GTs e Conselho Deliberativo não estarão disponíveis nesse período.

A abertura de tickets no *service desk* segue ativa sem nenhuma interrupção, assim como todo o restante da infraestrutura tecnológica do Open Banking Brasil (p.ex. diretório de participantes, portal em todas suas áreas).

Em caso de necessidade urgente de informações que não sejam supridas pelo Portal ou pelo service desk, favor contactar lara.aline@chicagoadvisory.com.br.

ENTRE EM CONTATO

Publicação da versão ID3 do documento Perfil de Segurança do OPB

Informamos a publicação da versão ID3 do documento Perfil de Segurança do Open Banking Brasil, onde foram contempladas as seguintes alterações:

- **Seção 5.2.2, item 11** – Remoção temporária da obrigatoriedade do CIBA para o escopo payments, de forma a não gerar dúvidas aos participantes até que o padrão de funcionamento seja definido pelo Squad CIBA;
- **Seção 5.2.2, item 14** – Orientação adicional sobre a claim “acr”;
- **Seção 5.2.2, itens 15 e 16** – Orientações adicionais sobre os atributos “response_type” e “response_mode”;
- **Seção 5.2.2.4** – Alteração nos padrões mínimos de nível de autenticação, conforme já divulgado no Informe 46;
- **Seção 5.2.3, itens 6 e 7** – Orientações adicionais sobre a claim “acr”;
- **Seção 5.2.3, item 8** – Orientação adicional sobre métodos de autenticação que devem ser suportados pelos TPPs;
- **Seção 7.2.2, itens 8 a 10** – Detalhamento dos requisitos para autenticação envolvendo dados do consentimento (CPF e CNPJ);
- **Seção 7.2.2, item 11** – Inclusão da informação do tempo de validade do refresh token, conforme já divulgado no Informe 46

VERSÃO ID3 DO PERFIL DE SEGURANÇA

Alteração na documentação Guia de Usuário para Instituição Transmissora (ASPSP User Guide)

Devido a dúvidas apresentadas por alguns participantes, informamos que foi incluída no documento Guia de Usuário para Instituição Transmissora (ASPSP User Guide) uma seção chamada “Sobre o uso de JARM”, com o objetivo de reforçar a seguinte informação:

“O suporte ao JARM é opcional aos transmissores e detentores de contas (ASPSP) e, portanto, as instituições que optarem pelo uso do JARM devem, no processo de certificação de segurança, atestar também o suporte a outro profile que não considere o uso do padrão JARM, ou seja, deve também se certificar com um dos profiles listados na tabela a seguir.”

Perfil da certificação OIDF
BR-OB Adv. OP w/ MTLS
BR-OB Adv. OP w/ Private Key
BR-OB Adv. OP w/ MTLS, PAR
BR-OB Adv. OP w/ Private Key, PAR

GUIA DE USUÁRIO — ASPSP

Alteração na documentação Guia de Usuário para Instituição Receptora ou Iniciadora de Pagamentos (TPP User Guide)

Devido a dúvidas apresentadas por alguns participantes, informamos que foram incluídas na seção 4.3.1 do documento Guia de Usuário para Instituição Receptora ou Iniciadora de Pagamentos (TPP User Guide) informações adicionais sobre a obrigatoriedade dos métodos de autenticação a serem suportados pelos TPPs, conforme apresentado abaixo:

“Diferentes métodos de autenticação (private_key_jwt e tls_client_auth) e de encaminhamento do Request Object (com e sem uso de PAR) podem ser suportados pelos Authorization Servers de acordo com a especificação FAPI-1.0 Part 2 - Advanced.

Portanto, como reforça o perfil de segurança para o Open Banking Brasil (item 8 da seção 5.2.3 dos requisitos de segurança para o cliente confidencial), todas as 4 combinações de métodos devem ser suportadas pelos clientes de API.

A tabela abaixo reflete os diferentes profiles de segurança e combinações que devem ser suportados por todos os clientes de API (conforme os profiles certificados pela OIDF para o Open Banking Brasil).”

Perfil da certificação OIDF
BR-OB Adv. OP w/ MTLS
BR-OB Adv. OP w/ Private Key
BR-OB Adv. OP w/ MTLS, PAR
BR-OB Adv. OP w/ Private Key, PAR

GUIA DE USUÁRIO — TPP

Alteração na documentação Padrão de Certificados

Informamos que foram incluídos dois novos esclarecimentos na documentação Padrão de Certificados, com o objetivo de evitar dúvidas aos participantes:

- **Seção 5.2.2** – Inclusão de orientação sobre o de envio da cadeia intermediária no mTLS, conforme RFC 5246;
- **Seção 8.3** – Inclusão de orientação sobre escolha de certificado a ser utilizado pelas instituições para os endpoints da Fase 1 que, por natureza, são de acesso público.

SEÇÃO PADRÃO DE CERTIFICADOS

Verificação de compatibilidade das informações publicadas no endpoint /.well-known das instituições com suas certificações

Foi identificado pelo Squad Operação Fase 2 um problema de interoperabilidade (e regulatório) causado pela divergência das informações publicadas pelas instituições no endpoint /.well-known que foi certificado no motor de conformidade de segurança com o endpoint que encontra-se publicado no Diretório.

Portanto, exortamos as instituições financeiras a checarem seus /.well-known de produção, publicados no Diretório, de forma a garantir que contenham apenas métodos previamente certificados pela instituição na OpenID Foundation.

OpenBanking