penBanking informa

Confira as últimas atualizações da Estrutura de Governança

Liberação da Certificação Funcional Fase 3A - 1º Ciclo

Informamos que as certificações funcionais Fase 3A - 1º Ciclo (Pix manual, chave e recebedor) estão liberadas.

Está disponível a opção "Fase 3: Payments" para pedido de certificação pelo Service Desk. Para esse pedido de certificação, note que será necessário realizar um novo plano de testes que deverá estar na versão 403469206 ou superior.

Em especial, sugerimos a leitura relacionada à validação do *subject DN*, que pode ser encontrada no documento de DCR das especificações de Segurança. As principais alterações desse documento estão destacadas no próximo tópico desse mesmo informa.

Também alertamos que o documento de certificação de conformidade para a Fase 3 foi atualizado na última semana, sendo que todas as submissões devem conter a nova versão do documento, que se encontra no nosso github. A este documento foi incluído uma tabela onde a IF deve inserir todos os URIs de well-known referentes aos servidores de autorização em produção que serão objetos da certificação

Clique aqui para acessar o Service Desk

Clique aqui para acessar a especificação de DCR

Clique aqui para acessar a documentação no Github

Atualizações sobre formato do Subject DN

O item 7.1.2 da especificação de segurança foi atualizado conforme o texto abaixo e está disponível na integra no link.

Análise do Distinguished Name do Certificado {#Certificate}

A cláusula 3 do [Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names][RFC4514] define os OIDs obrigatórios cujas as strings do AttributeType (descritores) devem ser reconhecidos pelos implementadores. Esta lista obrigatória não inclui vários dos OIDs definidos em [Open Banking Brasil x.509 Certificate Standards][OBB-Cert-Standards], nem existe um mecanismo definido para os Servidores de Autorização publicarem informações sobre o formato que eles esperam de uma Solicitação Dinâmica de Registro do Cliente (Dynamic Client Registrarion) que inclui um tls_client_auth_subject_dn.

Para resolver essa ambiguidade, o Servidor de Autorização deve aceitar exclusivamente os AttributeType (descritores) definidas no último parágrafo da cláusula 3 [RFC4514] em formato string, também deve aceitar em formato OID, com seus valores em ASN.1, todos os AttributeTypes definidos no Distinguished Name [Open Banking Brasil x.509 Certificate Standards][OBB-Cert-Standards] ou adicionados pela Autoridade Certificadora.

Em caso de não atendimento destes requisitos o Servidor de Autorização deverá rejeitar o registro.

Segue na tabela abaixo como deve ser feita a decodificação:

Obtenha na ordem reversa os atributos do certificado

Concatene cada RDN (RelativeDistinguishedName) com uma virgula (',')

subject_dn	Issuer
UID=67c57882-043b-11ec-9a03-0242ac130003, 1.3.6.1.4.1.311.60.2.1.3=#13024252, 2.5.4.15=#1314507269766174652 04f7267616e697a6174696f6e, 2.5.4.5=#130d313333353332333630303139 39, CN= mycn.bank.gov.br,OU=497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Bank, L= BRASILIA, ST=DF, C=BR	issuer=CN=Open Banking SANDBOX Issuing CA - G1,OU=Open Banking,O=Open Banking Brasil,C=BR
UID=67c57882-043b-11ec-9a03-0242ac130003, 1.3.6.1.4.1.311.60.2.1.3=#13024252, 2.5.4.15=#1314507269766174652 04f7267616e697a6174696f6e, CN=mycn.bank.gov.br, 2.5.4.5=#130d313333353332333630303139 39, OU=497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Bank, L=BRASILIA, ST=DF, C=BR	issuer=CN=Autoridade Certificadora do SERPRO SSLv1,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-Brasil,C=BR
1.3.6.1.4.1.311.60.2.1.3=#13024252, 2.5.4.15=#1314507269766174652 04f7267616e697a6174696f6e, UID=67c57882-043b-11ec-9a03-0242ac130003, CN=openbanking.mybank.com.br, 2.5.4.5=#130d313333353332333630303139 39, OU=497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, L=Goiania, ST=GO, O=MyBank SA, C=BR	issuer=CN=AC SOLUTI SSL EV,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-Brasil,C=BR
CN=mycn.bank.com.br, UID=67c57882-043b-11ec-9a03-0242ac130003, OU=497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, L=Sao Paulo, ST=SP, O=MyBank SA, C=BR,2.5.4.5=#130d313333353332333630303139, 1.3.6.1.4.1.311.60.2.1.3=#13024252, 2.5.4.15=#1314507269766174652 04f7267616e697a6174696f6e	issuer=CN=AC SERASA SSL EV,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-Brasil,C=BR

Clique aqui para acessar a especificação de DCR

Certificações da Fase 2–Recertificação Funcional e Certificação de Segurança Relying Parties

Informamos que estão liberados os pedidos para:

- Recertificação Funcional Fase 2 (para todas APIs, exceto a API de Resources): obrigatória para todas instituições transmissoras de dados que aderiram à Fase 2. O documento de certificação de conformidade para a Fase 3 foi atualizado na última semana, sendo que todas as submissões devem conter a nova versão do documento, que se encontra no github . A este documento foi incluído uma tabela onde a IF deve inserir todos os URIs de well-known referentes aos servidores de autorização em produção que serão objetos da certificação

- Certificação de Segurança para Relying Parties Fase 2: obrigatória para todas instituições receptoras de dados que aderiram à Fase 2

A data limite para a emissão dos certificados listados acima é 30/11. Todos os pedidos de certificação enviados até o 19/11 serão processados até a data limite. Instituições que não se certificarem até essa data limite, poderão sofrer suspensão de seu cadastro no Diretório de Participantes do Open Banking Brasil.

Maiores detalhes sobre os pedidos de certificação estão disponíveis no Guia de Certificação de Conformidade.

Clique aqui para acessar a Documentação

Clique aqui para acessar o Guia de Certificação de Conformidade

OpenBanking