Padrão de Certificado OpenBanking Brasil

Não
Corp
orati
vo

1. Representatividade dos membros

A convenção do OpenBanking Brasil, composta pelas associações https://www.ocb.org.br/ABBC (Associação Brasileira de Bancos - https://www.abbc.org.br), ABCD (Associação Brasileira de Crédito - https://creditodigital.org.br) /ABFintechs (Associação Brasileira de Fintechs - https://www.abfintechs.com.br), ABECS (Associação Brasileira das Empresas de Cartões de Crédito e Serviços - https://www.abecs.org.br) , Abipag (Associação Brasileira de Instituições de Pagamento - https://abipag.com.br)/ Abranet (Associação Brasileira de Internet - https://www.abranet.org.br) /Camara e-Net (Câmara Brasileira da Economia Digital - https://www.camara-e.net), Febraban (Federação Brasileira de Bancos - https://febraban.org.br), OCB (Organização das Cooperativas Brasileiras - https://www.ocb.org.br), representado pelos membros do Grupo de Trabalho de Segurança: Marcos Aurélio Rodrigues (marcos.aurelio-rodrigues@itau-unibanco.com.br), representante da FEBRABAN; Cleiton Soares de Moura (cleiton.moura@caixa.gov.br), FEBRABAN; Alexandre Siqueira (alexandre.siqueira@mercadolivre.com), Câmara e-Net, Gustavo Lichti Mendonça (gustavo@open-co.com), ABCD, Francisco Barciella (Francisco.barciella@nubank.com.br); Jose Michael Dias Henrique (jose.henrique@grupopan.com), ABBC, solicita ao ITI (Instituto Nacional de Tecnologia da Informação - https://www.gov.br/iti/pt-br) a criação de perfil de certificados necessários para a segurança do Open Banking Brasil.

Os perfis de certificados, incluindo atributos bem como suas necessidades podem ser encontradas na seção “Perfil de Certificados para o OpenBanking BR”.

2. Perfil de Certificados para o OpenBanking BR

Os certificados utilizados pela infraestrutura devem ser do tipo A, sendo os certificados de transportes emitidos utilizando cadeia v10 e os certificados de assinatura emitidos na cadeia v5.

2.1. Certificado de Aplicação Servidor

Certificados utilizados para expor os serviços de consumo de APIs e garantir a criptografia necessária para o canal. Os certificados utilizados devem seguir as diretrizes de emissão existente

e já adotada pelo ICP-Brasil, denominado “CERTIFICADO PARA SERVIDOR WEB – ICP-Brasil)”.

2.2. Certificado de Aplicação Cliente OpenBanking BR (Transporte)

Os certificados de Open Banking, denominados Certificado de Aplicação Cliente (Transporte) são utilizados para realizar autenticar o canal MTLS, e seguem o mesmo perfil para entidades cadastradas no serviço de diretório, bem como para entidades não cadastradas que venham a realizar contratos bilaterais com entidades transmissoras.

Sendo necessário o preenchimento de atributos já existentes na especificação:

- 2.16.76.1.3.2 Campo otherName em certificado de pessoa jurídica, contendo o nome do responsável pelo certificado;
- 2.16.76.1.3.3 (CNPJ) Campo otherName em certificado de pessoa jurídica, contendo o Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
- 2.16.76.1.3.4 Campo *otherName* em certificado de pessoa jurídica, contendo os dados do responsável pelo certificado de pessoa jurídica titular do certificado (data de nascimento, CPF, PIS/PASEP/CI, RG);
- 2.16.76.1.3.8 (razaoSocial) Campo *otherName* em certificado de pessoa jurídica, contendo nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações.

Identificação de Aplicação do OpenBanking

- Campo *CN,* no *DN* em certificado de pessoa jurídica, contendo identificação do Software Statement ID junto ao diretório do Open Banking ou emitido por empresa participante Transmissora.

Código de Participante do OpenBanking

- Campo *UID,* no *DN* em certificado de pessoa jurídica, contendo identificação do código de participante junto ao diretório do Open Banking. Caso a entidade não possua cadastro no diretório de OpenBanking, o valor deve ser preenchido com **0**.

Para certificados de transporte, utilizados para MTLS:

- **Key Usage:** critical, digitalSignature, keyEncipherment
- **extendedKeyUsage:** clientAuth, serverAuth

Modelo de Configuração para emissão de certificados de Transporte utilizando OpenSSL

```
[ new_oids ]
businessCategory = 2.5.4.15
jurisdictionCountryName = 1.3.6.1.4.1.311.60.2.1.3
serialNumber = 2.5.4.5

[ req ]
default_bits = 2048
default_md = sha256
encrypt_key = yes
prompt = no
string_mask = utf8only
distinguished_name = client_distinguished_name
req_extensions = req_cert_extensions

[ client_distinguished_name ]
#Business Category
businessCategory = Private Organization
#Country
jurisdictionCountryName = BR
#serialNumber (CNPJ)
serialNumber = 000002222555
#Participant code
UID = 08568976899
countryName = BR
#Organization Name
organizationName = Exemplo S.A.
#State or Province
stateOrProvinceName = SP
#City
```

```
localityName = Sao Paulo
#Software Statement ID obtained at OpenBanking BR Directory
commonName = hvcg098gngjuhjgh9

[ req_cert_extensions ]
basicConstraints = CA:FALSE
subjectAltName = @alt_name
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = clientAuth,serverAuth

[ alt_name]
#Name of the person responsible by the Certificate (Company Representative)
otherName.0 = 2.16.76.1.3.2;UTF8:Joao Silva
#CNPJ
otherName.1 = 2.16.76.1.3.3;UTF8: 03093102000197
#Company Representative CPF/PIS/RG
otherName.2 = 2.16.76.1.3.4;UTF8:02365636544455000000000000000000
#Full Company Name
otherName.3 = 2.16.76.1.3.8;UTF8:Exemplo S.A.
```

2.3. Certificado de OpenBanking BR (Assinatura)

Os certificados de Open Banking, denominados Certificado de Assinatura (Assinatura) são utilizados para realizar assinatura do payload, e seguem o mesmo perfil para entidades cadastradas no serviço de diretório, bem como para entidades não cadastradas que venham a realizar contratos bilaterais com entidades transmissoras.

Sendo necessário o preenchimento de atributos já existentes na especificação:

- 2.16.76.1.3.2 Campo otherName em certificado de pessoa jurídica, contendo o nome do responsável pelo certificado;
- 2.16.76.1.3.3 (CNPJ) Campo otherName em certificado de pessoa jurídica, contendo o Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

- 2.16.76.1.3.4 Campo otherName em certificado de pessoa jurídica, contendo os dados do responsável pelo certificado de pessoa jurídica titular do certificado (data de nascimento, CPF, PIS/PASEP/CI, RG);
- 2.16.76.1.3.7 Campo otherName em certificado de pessoa jurídica, contendo o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

Código de Participante do OpenBanking

- Campo *UID,* no *DN* em certificado de pessoa jurídica, contendo identificação do código de participante junto ao diretório do Open Banking. Caso a entidade não possua cadastro no diretório de OpenBanking, o valor deve ser preenchido com **0**.

Para certificados de assinatura, utilizados para assinatura de payload:

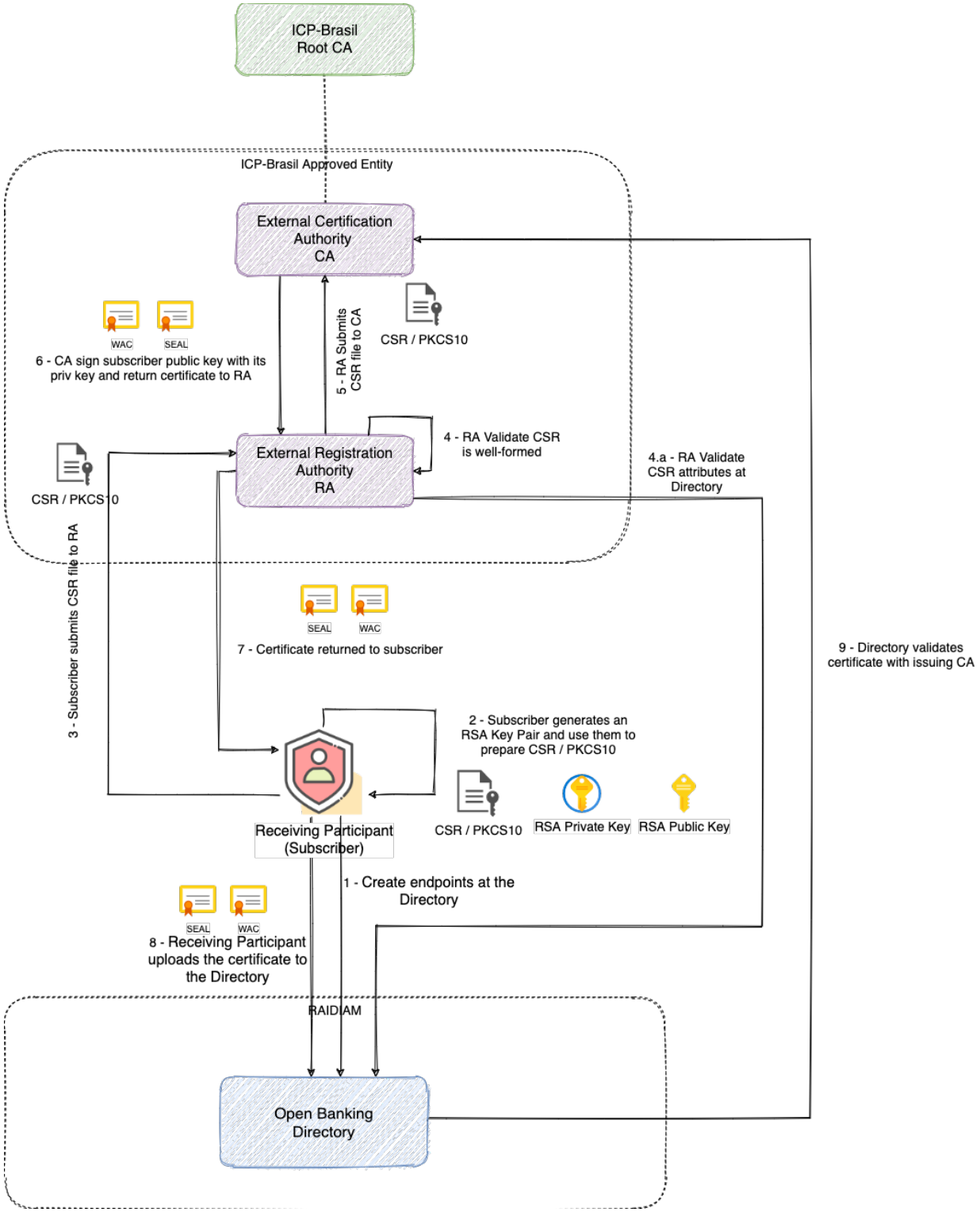
Key Usage: critical, digitalSignature, nonRepudiation

Modelo de Configuração para emissão de certificados de Assinatura utilizando OpenSSL

```
[ req ]
default_bits = 2048
default_md = sha256
encrypt_key = yes
prompt = no
string_mask = utf8only
distinguished_name = client_distinguished_name
req_extensions = req_cert_extensions

[ client_distinguished_name ]
#Participant code
UID = 08568976899
countryName = BR
#Root Identification
organizationName = ICP-Brasil
#Identificacao da AC
0.organizationalUnitName = Diretorio OpenBanking BR AC
#AR CNPJ
1.organizationalUnitName = 000002222555
```

```
#Validation Type
2.organizationalUnitName = certificado digital
#Organization Name
commonName = Exemplo S.A.

[ req_cert_extensions ]
basicConstraints = CA:FALSE
subjectAltName = @alt_name
keyUsage = critical,digitalSignature,nonRepudiation

[ alt_name]
#Name of the person responsible by the Certificate (Company Representative)
otherName.0 = 2.16.76.1.3.2;UTF8:Joao Silva
#CNPJ
otherName.1 = 2.16.76.1.3.3;UTF8: 03093102000197
#Company Representative CPF/PIS/RG
otherName.2 = 2.16.76.1.3.4;UTF8:023656365444550000000000000000
#INSS (CEI)
otherName.3 = 2.16.76.1.3.7;UTF8:0055895959595959
```

3. Processo de validação de certificados



1) A entidade participante realiza a criação de um endpoint (Aplicação) junto ao serviço de diretório.
2) A entidade participante gera a criação de um par de chaves (privada/pública) que será associada ao certificado, e realiza a geração do CSR.
3) A entidade participante submete o CSR para a RA.
4) A RA valida os campos presentes no CSR enviado pela entidade participante.
   4.a) Validar os campos associados ao OpenBanking junto ao diretório.
5) A RA submete o CSR para a CA.
6) A CA realiza assinatura do CSR com sua chave privada e disponibiliza para a RA.
7) O Certificado assinado é disponibilizado para a entidade participante,
8) A entidade participante realiza o upload e associação do certificado no diretório do OpenBanking BR.
9) O serviço de diretório do OpenBankingBR realiza a validação dos certificados junto a CA.

3.1. Validações

Os processos de validação de atributos dos certificados do OpenBanking seguem os mesmos procedimentos já implementados de acordo com práticas definindas junto ao ICP-Brasil.

Adicionalmente aos processos existentes, dois novos campos são necessários de serem validados utilizando a infraestrutura do serviço de diretório do OpenBanking Brasil.

Os mecanismos necessários para validação ainda precisam ser desenvolvidos e possuem as características abaixo.

Certificados de transporte

- Software Statement ID preenchido do campo CN do Distinguished Name validado junto ao serviço de diretório do OpenBanking Brasil.
- Código de Participante preenchido no campo UID do do Distinguished Name validado junto ao serviço de diretório do OpenBanking Brasil.

Certificados de assinatura

- Participant Code preenchido no campo UID do do Distinguished Name validado junto ao serviço de diretório do OpenBanking Brasil.

3.1.1. Validação Manual

Certificados de transporte

Serão disponibilizadas credenciais de acesso ao portal do serviço de diretório do OpenBanking BR, onde o profissional responsável pela validação do certificado conseguirá listar os códigos de OpenBanking, CNPJ e Razão Social, confirmando:

- Código de Participante, CNPJ e Razão Social presentes no certificado são os mesmos listados no Portal do Diretório OpenBanking BR.
- Software Statement ID está corretamente associado ao Participant Code, CNPJ, Razão Social conforme listados no Portal do Diretório do OpenBanking BR.

Certificados de assinatura

Serão disponibilizadas credenciais de acesso ao portal do serviço de diretório do OpenBanking BR, onde o profissional responsável pela validação do certificado conseguirá listar os códigos de OpenBanking, CNPJ e Razão Social, confirmando:

- Código de Participante, CNPJ e Razão Social presentes no certificado são os mesmos listados no Portal do Diretório OpenBanking BR.

3.1.2. Validação via API

Certificados de transporte

Serão disponibilizadas APIs do serviço de diretório do OpenBanking BR, onde a RA realiza uma chamada via API fornecendo Código de Participante, CNPJ, Razão Social e Software Statement ID, sendo retornado:

- Positivo – Para confirmação que os dados enviados para consulta estão corretamente associados.
- Negativo – Caso os dados enviados para consulta não estejam corretamente associados.

Certificados de assinatura

Serão disponibilizadas APIs do serviço de diretório do OpenBanking BR, onde a RA realiza uma chamada via API fornecendo Código de Participante, CNPJ, Razão Social, sendo retornado:

- Positivo – Para confirmação que os dados enviados para consulta estão corretamente associados.
- Negativo – Caso os dados enviados para consulta não estejam corretamente associados.

3.2. Validações de Certificados para Entidades não cadastradas no diretório

É possível a uma entidade não cadastrada no serviço de diretório realizar a emissão de certificados do tipo OpenBanking para realização de parceiras Bilateral.

Os processos de validação de atributos dos certificados do OpenBanking seguem os mesmos procedimentos já implementados de acordo com práticas definidas junto ao ICP-Brasil.

Certificados de participantes não cadastrados no diretório devem possuir seus atributos identificados da maneira abaixo, não sendo necessários suas validações junto ao serviço de diretório Open Banking:

Sendo para certificados de assinatura:

- Código de Participante preenchido no campo UID do do Distinguished Name com valor 0.

Sendo para certificados de transporte:

- Software Statement ID preenchido do campo CN do Distinguished Name.
- Código de Participante preenchido no campo UID do do Distinguished Name com valor 0.