Padrão de Certificados

Prefácio

A Estrutura Inicial do Open Insurance Brasil é responsável por criar os padrões e especificações necessários para atender aos requisitos e obrigações da Legislação do Open Insurance do Brasil, conforme originalmente delineado pela SUSEP. É possível que alguns dos elementos deste documento estejam sujeitos a direitos de patente. A Estrutura Inicial não se responsabiliza pela identificação de qualquer ou todos os direitos de patente.

Objetivo

Especificar o conjunto de certificados necessários que devem ser utilizados pelas entidades participantes do Open Insurance Brasil para garantir interoperabilidade para autenticação, confidencialidade, integridade e não repúdio entre os participantes, bem como para os usuários e consumidores destas entidades. O público desta especificação são entidades participantes do Open Insurance Brasil que necessitam fazer a emissão de certificados para se autenticar junto a outras entidades, bem como oferecer a seus clientes um canal de autenticação seguro.

Convenções Notacionais

As palavras-chave "*deve*" (shall), "*não deve*" (shall not), "*deveria*" (should), "*não deveria*" (should not) e "*pode*" (may) presentes nesse documento devem ser interpretadas conforme as diretrizes descritas em ISO Directive Part 2 observando a seguinte equivalência:

- "deve" ⇒ equivalente ao termo "shall" e expressa um requerimento definido no documento (nas traduções é similar ao termo "must", que pode denotar um requerimento externo ao documento);
- "não deve" ⇒ equivalente ao termo "shall not" e também expressa um requerimento definido no documento;
- "deveria" e "não deveria"⇒ equivalente ao termo "should" e "should not" e expressa uma recomendação
- "pode" ⇒ equivalente ao termo "may" indica uma permissão

Estas palavras-chave não são usadas como termos de dicionário, de modo que qualquer ocorrência deles deve ser interpretada como palavras-chave e não devem ser interpretados com seus significados de linguagem natural.

1. Escopo

Este documento especifica os tipos de certificados necessários para:

- Autenticar mutuamente (MTLS - Mutual TLS) as aplicações dos participantes;
- Assinatura de Mensagens (JWS - JSON Web Signature) de aplicações para garantir a autenticidade e não repúdio de mensagens entre os participantes;
- Apresentar um canal seguro e confiável para clientes do Open Insurance Brasil;
- Autenticar participantes no Diretório de participantes do Open Insurance Brasil.

2. Referências Normativas

Os seguintes documentos referenciados são indispensáveis para a aplicação deste documento. Para referências datadas, apenas a edição citada se aplica. Para referências não datadas, a última edição do documento referenciado (incluindo quaisquer emendas) se aplica.

- ISODIR2 - ISO/IEC Directives Part 2
- RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC7519 - JSON Web Token (JWT)
- RFC7515 - JSON Web Signature (JWS)
- RFC7591 - OAuth 2.0 Dynamic Client Registration Protocol
- RFC7592 - OAuth 2.0 Dynamic Client Registration Management Protocol
- BCP195 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
- RFC8705 - OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens
- OFB-FAPI - Open Finance Brasil Financial-grade API Security Profile 1.0
- OPIN-FAPI-DCR - Open Insurance Brasil Financial-grade API Dynamic Client Registration Profile 1.0
- DOC-ICP-01 - DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL
- RFC6749 - The OAuth 2.0 Authorization Framework
- RFC2818 - HTTP Over TLS
- RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2

3. Termos e Definições

Para o propósito deste documento os termos definidos na RFC5280, BCP195, RFC8705, e ISO29100 são aplicáveis.

4. Glossário

- **API** – Application Programming Interface

- **DCR** – Dynamic Client Registration
- **HTTP** – Hyper Text Transfer Protocol
- **ICP** - Infraestrutura de Chave Públicas Brasileira
- **SS** – Software Statement
- **SSA** – Software Statement Assertion
- **TLS** – Transport Layer Security
- **mTLS** – Mutual Transport Layer Security

5. Padrão de Certificados Open Insurance Brasil

5.1 Introdução

O ecossistema do Open Insurance Brasil faz uso de cadeias de certificados e protocolo TLS para garantir a confidencialidade, autenticação e integridade do canal de comunicação utilizado pelas APIs das instituições participantes, bem como dos clientes de cada um dos participantes.

Os certificados utilizados pelo Open Insurance Brasil também são necessários para autenticar as aplicações através do oAuth 2.0 mTLS ou private_key_jwt, além de também servirem para realizar a assinatura de *payloads* pelo uso de JWS. Outra atribuição importante dos certificados é autenticar e apresentar um canal seguro para o usuário final no ato de autenticação e uso dos serviços prestados pela entidade participante.

5.2 Certificados ICP-Brasil

Os certificados emitidos pelas Autoridades Certificadoras autorizadas pelo ICP-Brasil são utilizados apenas na comunicação entre as entidades participantes do ecossistema do Open Insurance Brasil.

Os processos de emissão e revogação dos certificados são de responsabilidade das próprias Autoridades Certificadores, sendo regulamentados por Declarações de Prática de Certificação, e supervisionadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira.

As práticas, processos, disponibilização e valores praticados pelas Autoridades Certificadoras não são de responsabilidade do Estrutura Inicial do Open Insurance Brasil.

Algoritmos

Todos os certificados emitidos junto ao ICP-Brasil devem possuir as seguintes características:

- Tipo A do ICP-Brasil;
- Algoritmo de Chaves: RSA 2048 bits;
- Message Digest: SHA 256 bits.

5.2.1 Certificado Servidor

O Certificado Servidor deve ser emitido para proteger e autenticar o canal TLS utilizado pelas APIs que serão consumidas pelas aplicações cliente de entidades participantes do Open Insurance.

O padrão de certificado utilizado deve seguir as práticas de emissão de certificados existentes de "CERTIFICADO PARA SERVIDOR WEB – ICP-Brasil".

O certificado de servidor precisa ser enviado com a cadeia intermediária, conforme RFC5246 (itens 7.4.2).

5.2.2 Certificado Cliente

Os Certificados de Aplicação Cliente (Transporte) são utilizados para autenticar o canal mTLS e para realizar a autenticação da aplicação cliente através de oAuth2.0 mTLS ou private_key_jwt, de acordo com o cadastro da aplicação realizado pelo processo de Dynamic Client Registration junto à entidade transmissora. Sobre o mTLS, o certificado cliente precisa ser enviado com a cadeia intermediária, conforme RFC5246 (itens 7.4.2 e 7.4.6). Caso a cadeia intermediária não for enviada, a entidade transmissora deve rejeitar a conexão.

Para emissão de Certificado Cliente é necessário que a instituição participante do Open Insurance Brasil tenha realizado o cadastro da aplicação no Serviço de Diretório, através do processo de emissão de Software Statement Assertion, e com isso já tenha obtido o valor de Software Statement ID.

5.2.2.1 Atributos Open Insurance Brasil

- **serialNumber:** Cadastro Nacional de Pessoal Jurídica (CNPJ) da pessoa jurídica titular do certificado e associado ao atributo UID e Software Statement ID, durante validação junto ao Serviço de Diretório do Open Insurance Brasil;
- **organizationIdentifier:** Código de Participante associado ao CNPJ listado no Serviço de Diretório do Open Insurance Brasil;
- **UID:** Software Statement ID cadastrado no Serviço de Diretório do Open Insurance Brasil e pertencente ao CNPJ e Código de Participante.

O Certificado Cliente deve ser emitido através de cadeia V10, e deve obrigatoriamente conter os seguintes atributos:

Distinguished Name

- **businessCategory (OID 2.5.4.15):** Tipo de categoria comercial, devendo conter: "Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity"
- **jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3):** BR

- **serialNumber (OID 2.5.4.5):** CNPJ
- **countryName (OID 2.5.4.6):** BR
- **organizationName (OID 2.5.4.10):** Razão Social
- **stateOrProvinceName (OID 2.5.4.8):** Unidade da federação do endereço físico do titular do certificado
- **localityName (OID 2.5.4.7):** Cidade do endereço físico do titular
- **organizationIdentifier (OID 2.5.4.97):** Código de Participante associado ao CNPJ listado no Serviço de Diretório do Open Insurance Brasil e prefixo de identificação do diretório
- **UID (OID 0.9.2342.19200300.100.1.1):** Software Statement ID gerado pelo Diretório do Open Insurance Brasil
- **commonName (OID 2.5.4.3):** FQDN ou Wildcard

Certificate Extensions

- **keyUsage:** critical,digitalSignature,keyEncipherment
- **extendedKeyUsage:** clientAuth

Subject Alternative Name

- **dNSName:** FQDN ou Wildcard

5.2.3 Certificado de Assinatura

Os Certificados de Assinatura são utilizados para realizar assinatura do *payload* através do uso de JWS (JSON Web Signature).

5.2.3.1 Atributos Open Insurance Brasil Presentes no Certificado

- **UID:** Código de Participante associado ao CNPJ listado no Serviço de Diretório do Open Insurance Brasil;
- **commonName:** Razão Social cadastrado no Serviço de Diretório do Open Insurance Brasil e pertencente ao CNPJ e Código de Participante.

O Certificado de Assinatura deve ser emitido através de cadeia V5, e deve obrigatoriamente conter os seguintes atributos:

Distinguished Name

- **UID (OID 0.9.2342.19200300.100.1.1):** Código de Participante associado ao CNPJ listado no Serviço de Diretório do Open Insurance Brasil
- **countryName (OID 2.5.4.6):** BR
- **organizationName (OID 2.5.4.10):** ICP-Brasil
- **organizationalUnitName (OID 2.5.4.11):** Nome da Autoridade Certificadora

- **organizationalUnitName (OID 2.5.4.11):** CNPJ da Autoridade de Registro
- **organizationalUnitName (OID 2.5.4.11):** Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)
- **commonName (OID 2.5.4.3):** Nome da Razão Social

Certificate Extensions

- **keyUsage:** critical,digitalSignature,nonRepudiation

Subject Alternative Name

- **otherName (OID 2.16.76.1.3.2 – ICP-Brasil):** Nome do responsável pelo certificado
- **otherName (OID 2.16.76.1.3.3 – ICP-Brasil):** Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
- **otherName (OID 2.16.76.1.3.4 – ICP-Brasil):** Responsável pelo certificado de pessoa jurídica titular do certificado (data de nascimento, CPF, PIS/PASEP/CI, RG);
- **otherName (OID 2.16.76.1.3.7 – ICP-Brasil):** Número do Cadastro Especifico do INSS (CEI) da pessoa jurídica titular do certificado.

5.2.3.2 Autoridades Certificadoras Participantes

As seguintes autoridades certificadoras realizaram o processo de onboarding ao Open Insurance Brasil e estão habilitadas para realizar a emissão de certificados do Open Insurance Brasil utilizando para tal os certificados nível 1 aqui listados:

- CertiSign (Cadeia v5 e v10)
- Serasa (Cadeia v5 e v10)
- Soluti (Cadeia v5 e v10)
- Valid (Cadeia v5 e v10)
- Serpro (Cadeia v5 e v10)

Apenas deverá ser aceito certificados indicados com "Situação: válido" nestes repositórios do ITI acima referenciados que são de Cadeia ICP-Brasil v5 e v10.

Além disso, os representantes das Autoridades Certificadoras estão convidados a participar das reuniões semanais de alinhamento do GT de Interfaces e Segurança do Open Insurance. Para obter mais informações e expressar interesse, favor contatar o Secretariado através do e-mail: secretariado@opinbrasil.com.br

5.2.4 Certificado para Front-End

Os certificados para Front-End são utilizados para disponibilizar serviços, em geral páginas Web, com uso de TLS, que são acessados pelo usuário final. Dado a sua finalidade, e para

garantir maior interoperabilidade, os certificados devem ser do tipo EV (Extended Validation) e devem ser ser gerados através de uma autoridade certificadora válida, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com os princípios e critérios WebTrust.

6. Apêndice

Modelo de Configuração de Certificado Cliente - OpenSSL

```
[req]
oid_section = OIDs

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

[ OIDs ]
organizationIdentifier = 2.5.4.97

[ client_distinguished_name ]
businessCategory = <tipo de organização>
jurisdictionCountryName = BR
serialNumber = <CNPJ>
countryName = BR
organizationName = <Razão Social>
stateOrProvinceName = <UF>
localityName = <Cidade>
organizationIdentifier = OPIBR-<Código de Participante>
UID = <Software Statement ID emitido pelo diretório>
commonName = <FQDN|Wildcard>

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

[ alt_name ]
DNS = <FQDN|Wildcard>

```

Modelo de Configuração de Certificado de Assinatura - 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 ]
```

```
UID = <Código de Participante>
countryName = BR
organizationName = ICP-Brasil
0.organizationalUnitName = <Certificate Authority>
1.organizationalUnitName = <CNPJ da Registration Authority>
2.organizationalUnitName = <Validation type>
commonName = <Company Name>

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

[ alt_name ]
otherName.0 = 2.16.76.1.3.2;UTF8:<Name of the person responsible for the organization>
otherName.1 = 2.16.76.1.3.3;UTF8:<CNPJ>
otherName.2 = 2.16.76.1.3.4;UTF8:<CPF/PIS/RF of responsible person>
otherName.3 = 2.16.76.1.3.7;UTF8:<INSS Number>

```

Tabela com Endpoints vs Tipo de Certificado e mTLS

Abaixo apresentamos quais endpoints podem ser publicados utilizando certificado EV como autenticação do consentimento e os endpoints de autenticação de APIs privadas/negócios que devem ser publicadas usando certificado ICP. Você também poderá verificar quais endpoints devem proteger suas conexões utilizando mTLS.

Fica a critério da instituição a escolha do certificado que deve ser adotado para os *endpoints* da Fase 1, os quais, por natureza, são de acesso público.

Fase	Grupo	APIs (em construção)	Certificado	mTLS
NA	OIDC	.well-known/openid-configuration	EV ou ICP WEB SSL	n/a
NA	OIDC	jwks_uri	EV ou ICP WEB SSL	n/a
NA	OIDC	authorization_endpoint	EV	n/a
NA	OIDC	token_endpoint	ICP WEB SSL	Obrigatório
NA	OIDC	userinfo_endpoint	ICP WEB SSL	Obrigatório
NA	OIDC	pushed_authorization_request_end	ICP WEB SSL	Obrigatório

		point		
NA	DCR	registration_endpoint	ICP WEB SSL	Obrigatório
NA	OIDC	revocation_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	Transacionais	/insurance-*/*	ICP WEB SSL	Obrigatório