Dynamic Client Registration (DCR)

SN Owned by Suporte N2 •••
Jan. 09, 2024 • 13 min read

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.

O Perfil de Segurança Financial-grade API 1.0 do Open Insurance Brasil consiste nas seguintes partes:

- Open Finance Brasil Financial-grade API Security Profile 1.0
- Open Insurance Brasil Dynamic Client Registration Profile 1.0

Essas partes devem ser usadas com RFC6749, RFC6750, RFC7636, OIDC, OIDR, RFC7591, RFC7592, FAPI-1-Baseline e FAPI-1-Advanced

Introdução

O Perfil de Registro de Cliente Dinâmico (DCR - *Dynamic Client Registration*) do Financial-grade API (FAPI) do Open Insurance Brasil é um perfil de RFC7591, RFC7592 e OIDR que visa fornecer diretrizes de implementação específicas para segurança e interoperabilidade que podem ser aplicadas à identificação, registro e gerenciamento de *Clients OAuth* operando no ecossistema Open Insurance Brasil.

Embora seja possível codificar um *OpenID Provider* e *Relying Party* desde o princípio usando esta especificação, o principal público para esta especificação são as partes que já possuem uma implementação certificada do OpenID Connect e desejam obter a certificação para o Open Insurance Brasil.

Convenções Notacionais

Interpretadas conforme as diretrizes descritas em ISO Directive Part 2 observando 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 o método de

- aplicativos cadastrados no Diretorio de Participantes do Open Insurance para descobrir OpenID Providers que oferecem serviços no ecossistema Open Insurance Brasil;
- aplicativos para usar o OpenID Connect Registration para integrar seus aplicativos com OpenID Providers das seguradoras; e
- aplicativos para usar OAuth 2.0 Dynamic Client Registration Management Protocol para gerenciar seus aplicativos com OpenID Providers;

Este documento é aplicável a todos os participantes do Open Insurance no 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

- RFC6749 - The OAuth 2.0 Authorization Framework
- RFC6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage

- RFC6819 - OAuth 2.0 Threat Model and Security Considerations
- RFC7519 - JSON Web Token (JWT)
- 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)
- OIDC - OpenID Connect Core 1.0 incorporating errata set 1
- FAPI-CIBA - Financial-grade API: Client Initiated Backchannel Authentication Profile
- RFC4514 - Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
- RFC4517 - Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
- OIDD - OpenID Connect Discovery 1.0 incorporating errata set 1
- OIDR - OpenID Connect Registration 1.0 incorporating errata set 1
- RFC8705 - OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens
- JARM - Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)
- PAR - OAuth 2.0 Pushed Authorization Requests
- JAR - OAuth 2.0 JWT Secured Authorization Request
- FAPI-1-Baseline - Financial-grade API Security Profile 1.0 - Part 1: Baseline
- FAPI-1-Advanced - Financial-grade API Security Profile 1.0 - Part 2: Advanced
- OFB-FAPI - Open Finance Brasil Financial-grade API Security Profile 1.0
- OFB-Cert-Standards - Open Insurance Brasil x.509 Certificate Standards
- OFB-DCR/DCM-Swagger - DCR & DCM Swagger

3. Termos e definições

Para efeitos deste documento, aplicam-se os termos definidos em RFC6749, RFC6750, RFC7636, OpenID Connect Core e ISO29100.

4. Símbolos e Termos abreviados

API – Application Programming Interface (Interface de Programação de

- **DCR** – Dynamic Client Registration (Registro de Cliente Dinâmico)
- **FAPI** - Financial-grade API
- **HTTP** – Hyper Text Transfer Protocol
- **OIDF** - OpenID Foundation
- **REST** – Representational State Transfer
- **SS** – Software Statement (Declaração de Software)
- **SSA** – Software Statement Assertion (Afirmação de Declaração de Software)
- **TLS** – Transport Layer Security

5. Introdução

O ecossistema Open Insurance Brasil apoia-se em um provedor de confiança ou *diretório de participantes* como a fonte mais valiosa de informações sobre participantes credenciados e softwares que estão autorizados a participar do ecossistema Open Insurance Brasil.

Os serviços do Diretório incluem:

- Registro e gerenciamento de software
- Registro e gerenciamento de credenciais de software usando certificados ICP
- Geração de Software Statement Assertion (SSA)

Os participantes do ecossistema devem aproveitar esses serviços para facilitar o registro de cliente OAuth orientado por API usando o processo descrito na cláusula 3.1.1 do RFC7591 com metadados adicionais necessários para oferecer suporte ao OpenID Connect definido em OpenID Connect Registration.

É importante reforçar que o payload de registro de clientes possui a maior parte de seus atributos não obrigatórios, e que os atributos cujos valores conflitem com os presentes no software statement assertion *serão sobrepostos pelos valores do próprio software statement assertion emitido pelo diretório central*. Nem todos os metadados que um cliente deseja fornecer podem estar contidos em um *software statement*, por exemplo, alternativa Metadata Languages and Script values. Há casos ainda de metadados de cliente que são um subconjunto dos valores existentes no SSA, como por exemplo os redirect_URIs.

6. Provisionamentos do OpenID Connect Discovery do Open Insurance Brasil

O servidor de autorização deve suportar OpenID Connect Discovery conforme exigido pelo Financial-grade API Security Profile 1.0 - Part 1: Baseline. Este suporte deve estar explicito tanto na forma como o Servidor de Autorização está registrado no Diretório de Participantes quanto na declaração dos seus atributos no arquivo de Discovery (well-known), respeitando os mecanismos de autenticação certificados pela institição através dos testes de conformidade do Open Insurance Brasil.

Adicionalmente, o Servidor de Autorização:

1. deve anunciar sua presença no ecossistema Open Insurance Brasil, sendo listada no Diretório de Participantes;
2. deve anunciar todos os recursos API REST do Open Insurance Brasil protegidos pelo Provedor OpenID no Diretório de Participantes;
3. deve anunciar suporte para todos os mecanismos de assinatura, criptografia, autenticação e padrões necessários para suportar o Open Finance Brasil Financial API;
4. deve anunciar suporte para OpenID Dynamic Client Registration;
5. deve anunciar `mtls_endpoint_aliases` de acordo com a cláusula 5 RFC 8705 OAuth 2.0 Mutual-TLS Client Authentication e Certificate-Bound Access Tokens o `token_endpoint`, `registration_endpoint` e `userinfo_endpoint`;
6. se suportar OAuth 2.0 Pushed Authorisation Requests, deve anunciar por meio de OIDD `mtls_endpoint_aliases` o `push_authorization_request_endpoint`;
7. se suportar Financial API - Client Initiated Back Channel Authentication, deve anunciar através de OIDD `mtls_endpoint_aliases` o `backchannel_authentication_endpoint`;

6.2 Cliente

O cliente deve suportar OpenID Connect Discovery conforme exigido pelo Financial-grade API Security Profile 1.0 - Part 1: Baseline.

Além disso, o Cliente

1. deve contar com serviços de descoberta do ecossistemas fornecidos apenas pelo Diretório de Participantes;

2. deve derivar os metadados necessários do Authorization Server somente por meio do serviço OpenID Connect Discovery dos Authorization Servers;

Certificate-Bound Access Tokens;

7. Provisionamento de registro OpenID Connect do Open Insurance Brasil

7.1 Servidor de Autorização

O servidor de autorização deve suportar as RFCs de Dynamic Client Registration (DCR) RFC7591, Dynamic Client Management (DCM) RFC7592 e OpenID Registration

Além disso, o servidor de autorização

1. deve rejeitar as solicitações de registro de cliente dinâmico não realizadas em uma conexão protegida com mTLS usando certificados emitidos pelo Brasil ICP (produção) ou o Diretório de Participantes (sandbox);
2. deve validar que a solicitação contém *software_statement* JWT assinado usando o algoritmo `PS256` emitido pelo Diretório de Participantes do Open Insurance Brasil;
3. deve validar que o *software_statement* foi emitido (iat - *issued at*) não mais de 5 minutos antes do pedido ser recebido;
4. deve validar que um atributo `jwks` (definida por valor) **não** foi incluído, e sim declarado como referência no atributo `jwks_uri` ;
5. deve, quando informado, validar que o `jwks_uri` corresponda ao `software_jwks_uri` fornecido na declaração do software;
6. deve exigir e validar que o `redirect_uris` corresponda ou contenha um subconjunto dos valores de `software_redirect_uris` fornecidos no *software_statement*;
7. deve exigir e validar que todos os mecanismos de autenticação de cliente cumpram os requisitos definidos nas RFC7591 e RFC7592, através da validação do `registration_access_token` e, como conexão segura, da cadeia de certificados confiáveis ICP-Brasil.
8. deve validar se os escopos solicitados são adequados para as permissões regulatórias autorizadas da instituição e contidas no *software_statement*. A relação de permissões regulatórias e os escopos correspondentes está descrita nas seções a seguir.

9. deve, sempre que possível, validar os metadados declarados pelo cliente em relação aos metadados fornecidos no *software_statement*, adotando os valores

10. deve aceitar todos os nomes X.520 AttributeType definidos no Distinguished *Name* dos Perfis de Certificado x.509 definidos em Open Insurance Brasil x.509 Certificate Standards;
11. se for compatível com o mecanismo de autenticação do cliente `tls_client_auth` , conforme definido em RFC8705, somente deve aceitar `tls_client_auth_subject_dn` como uma indicação do valor do atributo *subject* do certificado, conforme definido na cláusula 2.1.2 RFC8705;
12. o valor do campo *UID* do certificado deve coincidir com o enviado no SSA, onde o campo *UID* deve conter o valor do campo *software_id* do SSA.
13. o valor do campo *organizationIdentifier* do certificado deve conter o prefixo correspondente ao Registration Reference *OPIBR-* seguido do valor do campo *org_id* do SSA.
14. deve, durante o processo de handshake TLS, usar a regra `distinguishedNameMatch` para comparar os valores DN conforme definido na RFC4517.
15. deve garantir a integridade do estoque de consentimentos ativos, mesmo após eventuais mudanças sistêmicas, para que taís alterações sejam transparentes para as instituições receptora de dados.
16. deve realizar recertificação FAPI e DCR da OIDF após eventuais mudanças sistêmicas.

Estas disposições aplicam-se igualmente ao processamento de pedidos RFC7591, RFC7592 e OpenID Registration

7.1.1 Aplicando Server Defaults

Quando as propriedades de uma solicitação DCR não estão incluídas e não são obrigatórias na especificação, o Authorization Server deve aplicar os padrões do cliente da seguinte maneira:

1. deve selecionar e aplicar o algoritmo de criptografia e a escolha da cifra a partir dos conjuntos mais recomendados de cifra da IANA que são suportados pelo Servidor de Autorização;
2. deve preencher *defaults* a partir de valores da afirmação de *software_statement*, sempre que possível;

3. deve conceder ao cliente permissão para o conjunto completo de escopos potenciais com base nas permissões regulatórias de softwares incluídas no

7.1.2 Análise do Distinguished Name do Certificado

A cláusula 3 do Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names 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 Insurance Brasil x.509 Certificate 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 Insurance Brasil x.509 Certificate 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 (',')
- Use as strings da RFC (CN, L, ST, O, OU, C, Street, DC, UID) com o valor dos seus atributos legível para humanos
- Use os OIDs dos atributos definidos nesta especificação para uso no OFB (businessCategory = OID 2.5.4.15, jurisdictionCountryName = OID 1.3.6.1.4.1.311.60.2.1.3, serialNumber = OID 2.5.4.5) com o valor dos seus atributos em formato ASN.1 seguindo a RFC4514, sendo que:
  - Os nomes dos atributos devem ser definidos seguindo a notação ponto-decimal, sem adição de prefixo “OID”, ex. “2.5.4.15”, seguido dos sinais de (‘=#’) mais o valor hexadecimal do atributo, exemplo final: 2.5.4.15=#0C1450726976617465204F7267616E697A6174696F6E

- Não há qualquer restrição para as codificações/formatações utilizadas nos valores dos atributos. Deve ser respeitado o uso em hexadecimal apresentado

frente aos normativos ICP e ao itens 2.3, 2.4 e 5.2 da RFC4514.

Seguem abaixo exemplos para os atributos obrigatórios da CAs atualmente ativas:

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=#131450726976617465204f7267616e697a6174696f6e, 2.5.4.5=#130e31333335333233363030303139313839, CN=mycn.insurance.gov.br,2.5.4.97=OPIBR-497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Insurance, L=BRASILIA, ST=DF, C=BR	issuer=CN=Open Insurance SANDBOX Issuing CA - G1,OU=Open Insurance,O=Open Insurance 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=#131450726976617465204f7267616e697a6174696f6e, 2.5.4.5=#130e31333335333233363030303139313839, CN=mycn.insurance.gov.br,2.5.4.97=OPIBR-497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Insurance, L=BRASILIA, ST=DF, C=BR	issuer=CN=Autoridade Certificadora do SERPRO SSLv1,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-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=#131450726976617465204f7267616e697a6174696f6e,	issuer=CN=AC SOLUTI SSL EV,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-Brasil,C=BR

2.5.4.5=#130e31333335333233363030 30313839,	

70633fd11b59, O=My Public Insurance, L=BRASILIA, ST=DF, C=BR	
UID=67c57882-043b-11ec-9a03-0242ac130003, 1.3.6.1.4.1.311.60.2.1.3=#13024252, 2.5.4.15=#1314507269766174652O4f72 67616e697a6174696f6e, 2.5.4.5=#130e31333335333233363030 30313839, CN=mycn.insurance.gov.br,2.5.4.97=OP IBR-497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Insurance, L=BRASILIA, ST=DF, C=BR	issuer=CN=AC SERASA SSL EV,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-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=#1314507269766174652O4f72 67616e697a6174696f6e, 2.5.4.5=#130e31333335333233363030 30313839, CN=mycn.insurance.gov.br,2.5.4.97=OP IBR-497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Insurance, L=BRASILIA, ST=DF, C=BR	issuer=CN=AC Certisign ICP-Brasil SSL G2,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-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=#1314507269766174652O4f72 67616e697a6174696f6e, 2.5.4.5=#130e31333335333233363030 30313839, CN=mycn.insurance.gov.br,2.5.4.97=OP	issuer=CN=AC VALID SSL EV,OU=Autoridade Certificadora Raiz Brasileira v10,O=ICP-Brasil,C=BR

IBR-497e1ffe-b2a2-4a4e-8ef0-70633fd11b59, O=My Public Insurance,

7.2 Funções regulatórias para mapeamentos OpenID e OAuth 2.0

Para participar do ecossistema do Open Insurance, as instituições credenciadas devem se cadastrar no Diretório de Participantes de acordo com seus papéis regulatórios. Essas funções refletem a autorização do SUSEP para as instituições e, consequentemente, as APIs que podem utilizar.

A tabela a seguir descreve as funções regulatórias do Open Insurance e o mapeamento de escopos do OAuth 2.0 relacionado. Se os escopos forem omitidos durante o processo de DCR, o Servidor de Autorização deve conceder o conjunto completo de escopos potenciais com base nas funções regulatórias registradas par a seguradora, conforme descrito na seção Server Defaults.

Papel Regulador	Descrição	Escopos Permitidos (em construção)	Fase-alvo
DADOS	Instituição transmissora / receptora de dados	openid consents resources customers insurance-acceptance-and-branches-abroad insurance-auto insurance-financial-risk insurance-housing insurance-patrimonial insurance-rural insurance-responsibility insurance-transport	Fase 2

ICS	Iniciadora de Compartilhamento	openid claim-notification quote-patrimonial-lead quote-patrimonial-home quote-patrimonial-condominium quote-patrimonial-business quote-patrimonial-diverse-risks	Fase 3
TCS	Transmissora de Compartilhamento	openid	Fase 3

É necessário validar as *roles* ativas no *software_statement* da aplicação. Na validação dessa informação deve ser utilizado o campo *software_statement_roles*, e deve ser verificado se as *roles* listadas estão ativas.

7.3 Registro do Cliente

No processo de registro do cliente, utilizando-se o método de autenticação *tls_client_auth*, o cliente deve encaminhar o campo *tls_client_auth_subject_dn* com os AttibuteTypes(Descritores) em formato definido no item 7.1.2 Análise do Distinguished Name do Certificado. Em caso de não aderencia a este padrão o registro será rejeitado.

8. Declaração de Software

Uma declaração de software (*software_statement*) é um JSON Web Token (JWT) que afirma valores de metadados sobre o software cliente como um todo. Na estrutura do Open Insurance Brasil, esse *software_statement* é assinado pelo Diretório de Participantes, e sua assinatura DEVE ser validada pelos Servidores de Autorizacao usando as chaves públicas disponíveis na seção a seguir.

8.1 Atributos da Declaração de Software (Claims)

Área do / **Dynamic Client Registration (DCR)**

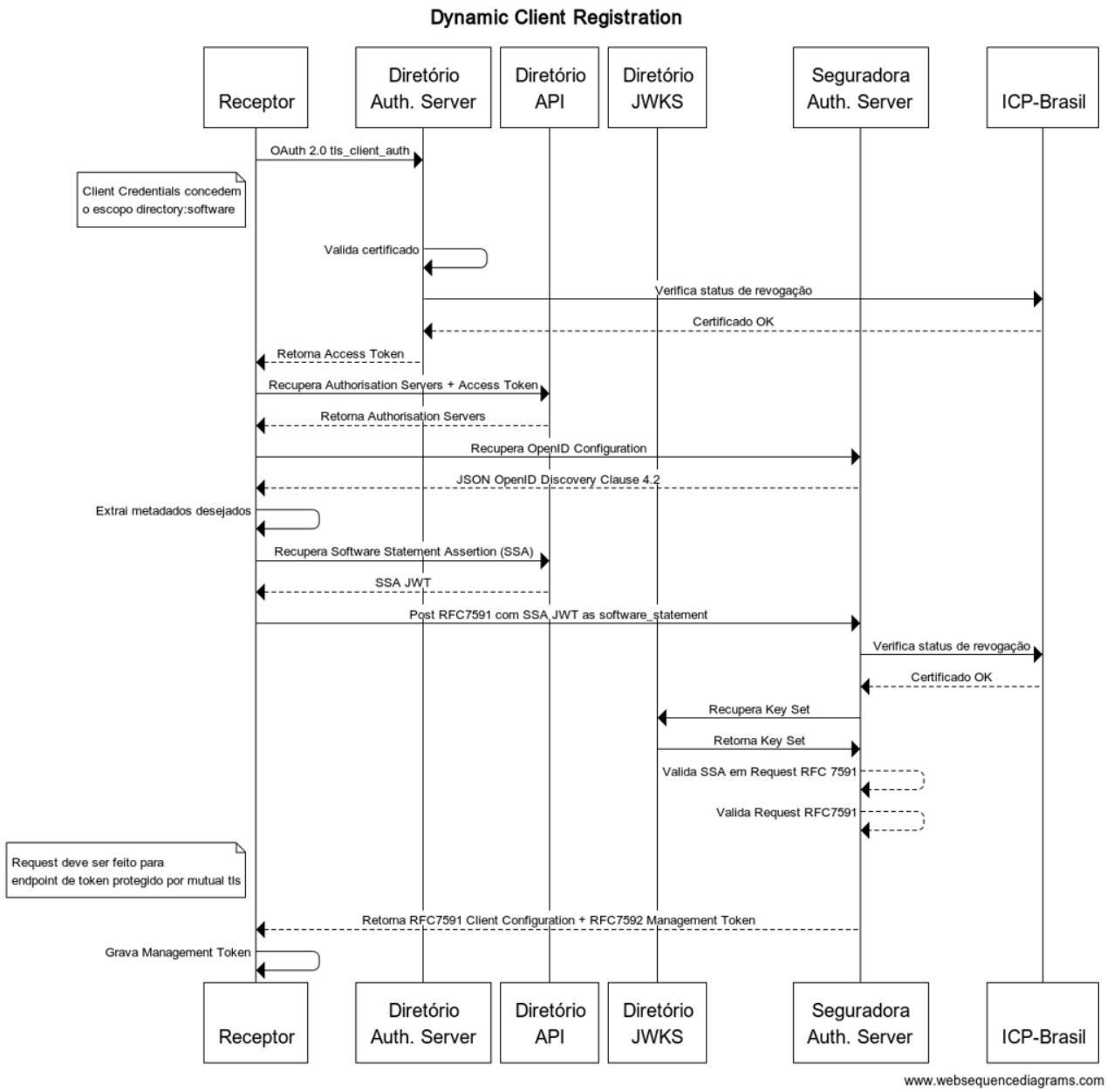

```
{
  "software_mode": "Live",
  "software_redirect_uris": [
    "https://www.raidiam.com/insurance/cb"
  ],
  "software_statement_roles": [
    {
      "role": "DADOS",
      "authorisation_domain": "Open Insurance",
      "status": "Active"
    }
  ],
  "software_client_name": "Raidiam Insurance",
  "org_status": "Active",
  "software_client_id": "Cki1EbvjwyhPB12NGLlz2",
  "iss": "Open Insurance Brasil prod SSA issuer",
  "software_tos_uri": "https://www.raidiam.com/insurance/tos.html",
  "software_client_description": "Raidiam Insurance leverage cutting ed
  "software_jwks_uri": "https://keystore.directory.opinbrasil.com.br/b9
  "software_policy_uri": "https://www.raidiam.com/insurance/policy.html
  "software_id": "25556d5a-b9dd-4e27-aa1a-cce732fe74de",
  "software_client_uri": "https://www.raidiam.com/insurance.html",
  "software_jwks_inactive_uri": "https://keystore.directory.opinbrasil.
  "software_jwks_transport_inactive_uri": "https://keystore.directory.o
  "software_jwks_transport_uri": "https://keystore.directory.opinbrasil
  "software_logo_uri": "https://www.raidiam.com/insurance/logo.png",
  "org_id": "b961c4eb-509d-4edf-afeb-35642b38185d",
  "org_number": "112233445566",
  "software_environment": "production",
  "software_version": "1.1",
  "software_roles": [
    "DADOS"
  ],
  "org_name": "Open Insurance Brasil",
  "iat": 1620060821,
  "organisation_competent_authority_claims": [
    {
      "authorisation_domain": "Open Insurance",
```

```
39        "authorisations": [],
40        "registration_id": "13353236-OIB-DADOS",
```



```
43        "authorisation_role": "DADOS",
44        "authority_code": "SUSEP",
45        "status": "Active"
46      }
47    ]
48  }
49
```

9. Processamento de solicitação de registro de cliente dinâmico



9.1 Enviar uma solicitação com uma declaração de software

obrigatoriedade, consultar o Swagger DCR. A quebra de linha dentro dos valores são apenas para fins de exibição.

```
POST /reg HTTP/1.1
Host: auth.raidiam.com
Content-Type: application/json
{
"application_type": "web",
"grant_types": [
    "client_credentials",
    "authorization_code",
    "refresh_token",
    "implicit"
],
"id_token_signed_response_alg": "PS256",
"require_auth_time": false,
"response_types": [
    "code id_token",
    "id_token"
],
"software_statement": "eyJraWQiOiJzaWduZXIiLCJ0eXAiOiJKV1QiLCJhbGciOiJQ
"subject_type": "public",
"token_endpoint_auth_method": "private_key_jwt",
"request_object_signing_alg": "PS256",
"require_signed_request_object": true,
"require_pushed_authorization_requests": false,
"tls_client_certificate_bound_access_tokens": true,
"client_id": "aCnBHjZBvD6ku3KVBaslL",
"client_name": "Raidiam Insurance",
"client_uri": "https://www.raidiam.com/insurance.html",
"request_object_encryption_alg": "RSA-OAEP",
"request_object_encryption_enc": "A256GCM"
"jwks_uri": "https://keystore.directory.opinbrasil.com.br/b961c4eb-509d
"redirect_uris": [
    "https://www.raidiam.com/insurance/cb"
]
}

```

9.2 Open Insurance Brasil SSA Key Store e detalhes do emissor

apresentados durante o processo de registro de cliente.

Producão

https://keystore.directory.opinbrasil.com.br/openinsurance.jwks

Emissor do Open Insurance Open Insurance Brasil SSA de produção

Sandbox

https://keystore.sandbox.directory.opinbrasil.com.br/openinsurance.jwks

Emissor do Open Insurance Open Insurance Brasil SSA de sandbox

9.3 Sobre os mecanismos de autenticação e autorização dos serviços de DCR e DCM

Por serem serviços auxiliares ao fluxo principal do Open Insurance Brasil, os serviços de registro e manutenção dinâmica de clientes não utilizam os mesmos mecanismos de controle de acesso. Por exemplo: não é possível exigir um *access_token* OAuth 2.0 de uma aplicação cliente que ainda não está registrada na instituição transmissora. Para estender as RFC7591 e RFC7592, que recomendam mecanismos mínimos para autenticação dos seus serviços, as instituições que suportam os fluxos de registro e manutenção dinâmica de clientes devem implementar em seus Servidores de Autorização os controles a seguir:

9.3.1 Registro de cliente - POST /register

1. validar que o certificado apresentado pela aplicação cliente é subordinado às cadeias do ICP-Brasil definidas no Padrão de Certificados do Open Insurance Brasil;
2. assegurar que a assinatura do *software_statement* apresentado pela aplicação cliente durante o registro tenha sido feita pelo Diretório de Participantes através das chaves públicas descritas na seção anterior;
3. assegurar que o *software_statement* apresentado pela aplicação cliente durante o registro corresponda à mesma instituição do certificado de cliente apresentado, validando-o através dos atributos que trazem `organization_id` no certificado X.509.

4. emitir, na resposta do registro, um `registration_access_token` para ser usado como token de autenticação nas operações de manutenção da aplicação cliente

Statement, de forma que em caso de tentativa de novo registro para um Software Statement já cadastrado, deve se utilizar o procedimento de Error Response definido no item 3.2.2 da RFC7591.

9.3.2 Manutenção de cliente - GET /register - PUT /register - DELETE /register

1. validar que o certificado apresentado pela aplicação cliente é subordinado às cadeias do ICP-Brasil definidas no Padrão de Certificados do Open Insurance Brasil;
2. validar a presença e a correspondência do header Bearer `Authorization` contendo o valor do atributo `registration_access_token` retornado durante o registro do cliente correspondente.

Observação: A RFC7592 prevê a possibilidade de rotação do `registration_access_token` emitido pelo Servidor de Autorização a cada uso, tornando-o um token de uso único. As instituições devem considerar esse aspecto no registro de suas aplicações cliente para receber e atualizar o `registration_access_token` pelo novo valor recebido nas chamadas de manutenção de cliente.