Manual técnico para conectividade à plataforma de Pre-matching
Versão exclusiva para suporte aos testes em homologação

1. Objetivo deste documento

Este documento tem como base apresentar e detalhar todos os requisitos técnicos necessários para conectividade da instituição financeira à plataforma de Pre-matching **exclusivamente para o ambiente de homologação**. Novas versões deste manual e um novo para atendimento exclusivo ao ambiente de produção serão disponibilizados na medida em que o projeto evolua.

2. Descrição técnica

A API da plataforma de Pre-matching utiliza o protocolo HTTP REST para comunicação e estará acessível apenas através da Rede de Telecomunicações para o mercado (RTM). A API possui URLs que aceitam requisições pré-formatadas e retornam respostas no formato JSON com códigos de retorno HTTP padrão.

3. Conectividade – Requisitos técnicos e de infraestrutura para acesso à Plataforma

- Para ter acesso à API da plataforma e ao acesso WEB, sua instituição deverá possuir acesso a Rede de Telecomunicações para o mercado (RTM).
- Todas as solicitações à API e WEB devem ser realizadas através de conexão HTTPS com TLS 1.2.
- Nesta primeira versão que está sendo disponibilizada ainda **não está sendo exigido a autenticação mútua TLS**, isso será realizado em versões futuras da plataforma.
- A aplicação do Pre-matching permitirá acesso de duas maneiras: **WEB** e **HTTP REST API**.
- Acesso HTTP REST API (Este acesso exigirá um "**client_id**" e uma chave de acesso "**client_secret**"). Cada instituição financeira obrigatoriamente deverá obter seu "**client_id**" e sua chave de acesso "**client_secret**" através do portal do Selic através da aplicação "**Gerenciamento de Acesso**". Todos os detalhes encontram-se no documento "***Manual do gerenciamento de acesso do Selic.pdf***".

Definição:

client_id – Identificação da instituição financeira para acesso ao serviço.

client_secret – Credencial (senha) de acesso exclusiva da instituição financeira à plataforma.

- A instituição necessita conceder acesso a seguinte URL em suas regras de firewall/segurança:

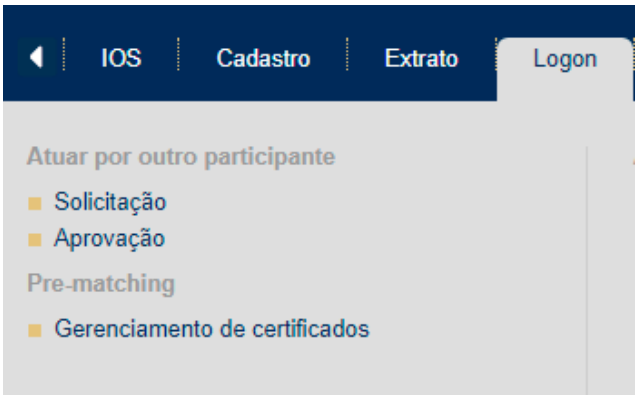
Ambiente de homologação (HML)

Host Origem: Rede da Instituição financeira
Hosts Destinos: https://pre-matching-hml.selic.rtm/***
https://api-pre-matching-hml.selic.rtm/***

Porta (TCP): 443 (TLS 1.2)

3.1. Acessando através da API (Server 2 Server)

O acesso à API da plataforma de Pre-matching exige a obtenção de um "**client_id**" e um "**client_secret**". Estes dados podem ser acessados diretamente por cada instituição através do portal do Selic. Para o acesso a esta funcionalidade a instituição deve ter acesso as funções do sistema Pre-matching. Caso seu perfil não seja de administrador você deve pedir para o responsável que as habilite no sistema Logon para o seu usuário. O Acesso é feito através do Portal Selic na RTM, menu Logon > Pre-matching.



OBS: Mais detalhes sobre este acesso podem ser obtidos no manual do Gerenciamento de acesso (Manual-Gerenciamento-de-Acesso_Mercado*.pdf)

3.2. Acessando através da WEB

O acesso pela interface WEB se dá exclusivamente através da URL abaixo:

https://pre-matching-hml.selic.rtm/pre-matching-web/

A autenticação do acesso web (iselic + usuário + senha) é a mesma utilizada atualmente pelos usuários do portal https://hml.selic.rtm.

4. Autenticação à API

O método de autenticação disponível na API da plataforma de Pre-matching é o OAuth2 e HTTP padrão através de TOKEN JWT.

Para iniciar a comunicação com a plataforma e acessar as URLs protegidas da plataforma você necessitará recuperar um token de acesso válido. Nas seções seguintes seguem alguns exemplos utilizando a aplicação cURL para o envio da requisição autenticada para exemplificar a solicitação de um token.

> **Nota:** cURL é um aplicativo open source e não é suportado pelo Selic. Ele é citado apenas para demonstração das chamadas HTTP.

4.1. Recuperação/Solicitação de um token JWT para uso na API.

As variáveis são identificadas por ${}. Exemplo: ${client_id} é a variável que identifica o cliente da API da sua instituição, como por exemplo "desenv" nos ambientes de desenvolvimento. Ex.

```
curl -X POST \
https://pre-matching-hml.selic.rtm/auth/realms/logon/protocol/openid-connect/token \
  -H 'Accept: */*' \
  -H 'Accept-Encoding: gzip, deflate' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -H 'Host: pre-matching-hml.selic.rtm' \
  -d 'grant_type=client_credentials&client_id=${client_id}&client_secret=${client_secret}'
```

4.2. Simulação de envio (Request)

```
curl -X POST \
  https://pre-matching-hml.selic.rtm/auth/realms/logon/protocol/openid-connect/token \
  -H 'Accept: */*' \
  -H 'Accept-Encoding: gzip, deflate' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -H 'Host: pre-matching-hml.selic.rtm' \
  -d 'grant_type=client_credentials&client_id=desenv&client_secret=secret'
```

Simulação de resposta (Response)

```
{
    "access_token": "eyJhbGciOiJ...ctSsFxQ",
    "expires_in": 300,
    "refresh_expires_in": 1800,
    "refresh_token": "eyJhbGciOiJIUzI1...obc_iKm00YandA",
    "token_type": "bearer",
    "not-before-policy": 1593542949,
    "session_state": "62f8d7c7-c25f-4d7d-8892-24dbb775e4db",
    "scope": "email profile"
}
```

4.3. Simulação de comunicação à API

Após recuperação do TOKEN válido, você deve utilizá-lo nas chamadas à API, seguindo o exemplo abaixo.

```
curl -X GET \
  https://api-pre-matching-hml.selic.rtm/pre-matching/api/v1/negocios/202004010000001 \
  -H "accept: application/json" \
  -H 'Accept-Encoding: gzip, deflate' \
  -H 'Authorization: Bearer eyJhbGciOiJ...ctSsFxQ' \
  -H 'Host: api-pre-matching-hml.selic.rtm'
```

4.4. Simulação de renovação do Token (Refresh - Timeout)

Atualmente durante os testes em homologação o tempo limite do token será de 300 segundos (5 minutos), como pode-se observar no atributo de retorno "expires_in", para o caso de um token expirar seu uso, é necessário solicitar um novo token utilizando o token de refresh, esse token mantem a sessão do usuário no contexto do acesso utilizando o serviço de autenticação via token ou reiniciar a solicitação de um novo token, mas essa segunda opção necessita de mais recursos de processamento sendo, portanto, mais custosa tanta para o requisitante quanto para a plataforma.

```
curl -X POST \
  https://pre-matching-hml.selic.rtm/auth/realms/logon/protocol/openid-connect/token \
  -H 'Accept: */*' \
  -H 'Accept-Encoding: gzip, deflate' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -H 'Host: pre-matching-hml.selic.rtm' \
 -d 'grant_type=refresh_token&client_id=${client_id}&refresh_token=${refresh_token}&client_secret=${client_secret}'
```

Onde ${refresh_token} é o valor recuperado na primeira autenticação.

5. Rate Limiting – Limitação de requisições

A política de limitação (rate-limiting) funciona com base em cabeçalhos enviados na requisição. **Todas as requisições de consulta, geração e atualização de TOKENS serão limitadas**. Portanto, atente-se a configuração do seu cliente da API evitando bloqueios de acesso à plataforma causada por excesso de requisições.

Inicialmente a pltaforma permitirá **até 30 requisições por minuto** nos tipos de requisições citadas acima. Acompanharemos o comportamento e utilização da plataforma pelo mercado durante os primeiros testes efetivos da plataforma para confirmar o seu valor definitivo que deverá ser divulgado na versão final deste manual.

As respostas do cabeçalho HTTP de qualquer requisição à API mostrarão o status atual do seu limite de requisições permitidas. Exemplo:

```
curl -X GET \
  https://api-pre-matching-hml.selic.rtm/pre-matching/api/v1/negocios/202004010000001 \
  -H "accept: application/json" \
  -H 'Accept-Encoding: gzip, deflate' \
  -H 'Authorization: Bearer eyJhbGciOiJ...ctSsFxQ' \
  -H 'Host: api-pre-matching-hml.selic.rtm'
HTTP/1.1 200 OK
Date: Mon, 13 Jul 2020 09:27:06 GMT
Status: 200 OK
RateLimit-Limit: 30
RateLimit-Remaining: 10
RateLimit-Reset: 60
```

Descrição:

RateLimit-Limit = O número máximo de requisições por minuto.
RateLimit-Remaining = O número de requisições restantes dentro da janela de limite atual.
RateLimit-Reset = O tempo em que o limite de requisições atual será reiniciado. (Em segundos).

Caso sua aplicação cliente exceda este limite, ela receberá um **HTTP STATUS 429** informando que o limite máximo permitido foi ultrapassado. Exemplo:

```
GET /obter-status/123

Response:

  HTTP/1.1 429 Too Many Requests
  Content-Type: application/json
  Date: Mon, 13 Jul 2020 09:27:40 GMT
```

```
Retry-After: Mon, 13 Jul 2020 09:27:40 GMT

RateLimit-Limit: 30
Ratelimit-Remaining: 0
RateLimit-Reset: 60

{
  "title": "Too Many Requests",
  "status": 429,
  "detail": "Você ultrapassou o número de requisições permitidas"
}
```

Dica: Você pode adequar seu cliente de API para que verifique cada requisição os campos RateLimit-Limit ou Ratelimit-Remaining enviados no cabeçalho HTTP das respostas evitando o bloqueio temporário na plataforma.

Checklist de acesso ao ambiente de homologação

O que minha instituição deve verificar antes de iniciar a comunicação com a API do Pre-matching?

☐ Minha instituição possui acesso à rede RTM?

☐ O firewall de minha instituição já permite acesso as URLs do ambiente de HML indicados pelo Selic?

URL(s) de Homologação: https://pre-matching-hml.selic.rtm/*
https://api-pre-matching-hml.selic.rtm/*

☐ Conseguimos acessar as URLs abaixo?

Descrição	URL
Autenticação da API/Token (Well-Known)	https://pre-matching-hml.selic.rtm/auth/realms/logon/.well-known/openid-configuration
Acesso WEB	https://pre-matching-hml.selic.rtm/pre-matching-web/
Acesso API – Testes	https://api-pre-matching-hml.selic.rtm/pre-matching/
Acesso API – Contrato OpenAPI 3	https://pre-matching-hml.selic.rtm/pre-matching/api/openapi

☐ Minha instituição já obteve o "**client_id**" e a chave de acesso "**client_secret**" através do portal do selic?

☐ O time técnico da minha instituição já compreende como devem ser realizadas as comunicações e autenticação à plataforma?

☐ **Rate Limiting** – Já configuramos nosso cliente da API para realizar **apenas 30 requisições por minuto** à plataforma? Esse valor é limitado e contabilizado automaticamente pela plataforma de segurança.

Importante: Em caso de excesso de requisições os sistemas de segurança do Selic realizam um bloqueio do IP de origem da instituição automaticamente impedindo o acesso à plataforma de Pre-matching por **1 minuto**.

Histórico de Revisão

Data	Descrição	Autor
13/07/2020	Elaboração da versão 1.0	Irwim Scott
15/09/2020	Atualização das URLs de acesso	Irwim Scott
28/09/2020	Adição das explicações para acesso WEB e geração de chaves da api (client_secret) através do portal do Selic.	Irwim Scott