

## Gerenciamento de Acesso Sistema Pre-matching

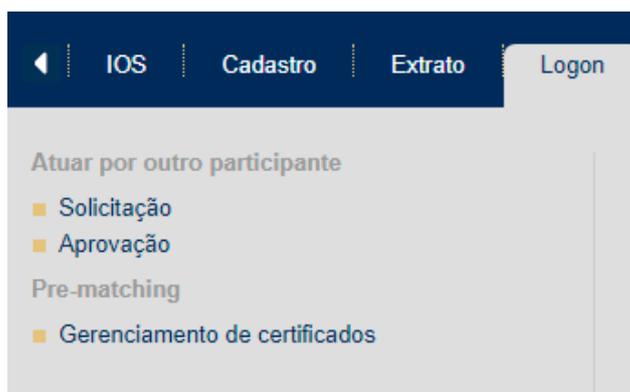
### 1. Objetivo

O objetivo do gerenciamento de acesso é incluir, ativar e desativar certificados digitais, necessários para autenticar a comunicação via API no sistema Pre-matching, e controlar as credenciais de acesso à API.

### 2. Acessando o sistema

Para acesso ao sistema 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 habilite as funções no sistema Logon para o seu usuário.

O Acesso é feito através do Portal Selic na RTM, menu Logon > Pre-matching.



### 3. Gerenciamento de certificados

Ao acessar o sistema você vai imediatamente para tela principal.

Gerenciar certificados digitais

Reincar

Nome do certificado:  Data de validade:

CONSULTAR

INCLUIR CERTIFICADO CREDENCIAIS DA API

	Nome	Status	Validade
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Teste	ATIVO	02/09/2022
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Teste	ATIVO	22/08/2020
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Teste	ATIVO	21/07/2020

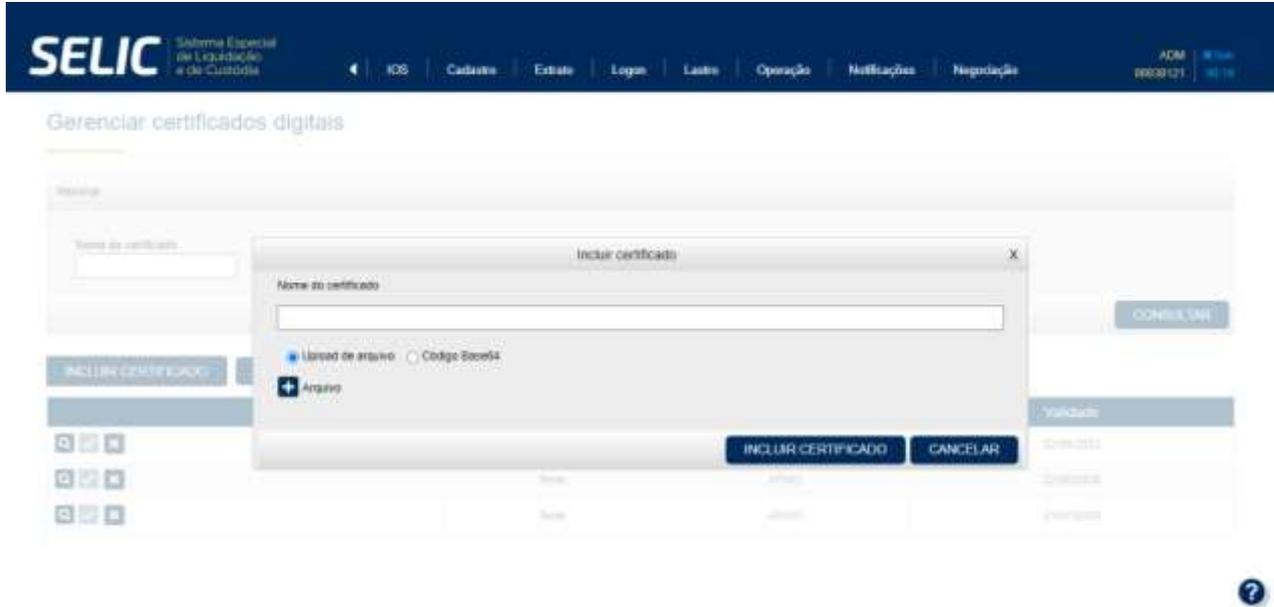
Ao acessar a tela o sistema fará automaticamente uma consulta dos certificados pertencentes a sua instituição. Caso queira buscar um certificado específico você pode alterar os filtros de Nome do certificado e / ou Data de validade.

Nesta tela temos também as opções de Incluir certificado e Credenciais da API, que veremos em detalhes mais adiante.

É possível também ver os detalhes dos certificados, ativá-los e desativá-los utilizando os botões da tabela de resultado da consulta, estas ações serão vistas em detalhes mais adiante.

### 3.1. Incluir certificado

Ao clicar no botão de Incluir certificado abaixo do filtro de busca o sistema abrirá uma janela pop-up para inclusão.



Nesta janela você pode escolher entre fazer a inclusão do arquivo ou colar o texto em formato de código Base64, pois o sistema não aceita certificados no formato binário. Após a inclusão do arquivo ou texto você deve selecionar a opção Incluir certificado para finalizar a operação. O sistema exibirá uma mensagem de sucesso e o novo certificado irá aparecer na lista. O certificado recém-incluído entra com o status de Ativo.

### 3.2. Detalhes do certificado

Na lista de resultados você pode ver cada um dos certificados que pertencem a sua instituição, seu Status e sua Validade.

	Nome	Status	Validade
	Teste	ATIVO	83/08/2022
	Teste	ATIVO	22/06/2022
	Teste	ATIVO	21/07/2022

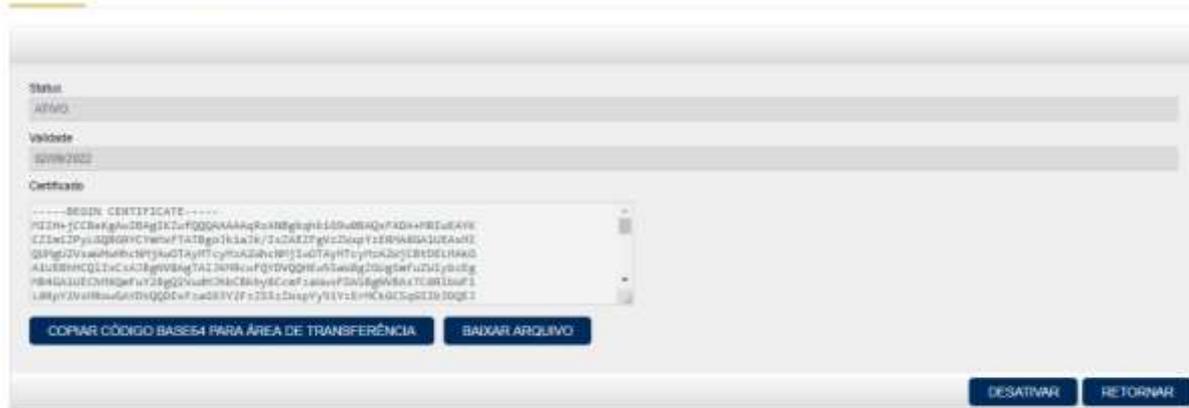
Na tabela de resultado temos também a opção de interagir com os certificados, vendo seus detalhes, ativando e desativando diretamente pelos botões na primeira coluna.

Um certificado INATIVO pode ser reativado a qualquer momento enquanto estiver válido. A instituição pode ter múltiplos certificados ATIVOS e INATIVOS em qualquer momento, e essa gestão é de responsabilidade da própria instituição.

Ao clicar na lupa você vai ver a tela de detalhes.



Detalhes do certificado digital - Teste



Nesta tela temos os detalhes do certificado incluindo seu Status, sua Validade e o certificado em Base64 que pode ser copiado para a área de transferência ou baixado como arquivo. Temos também a opção de Ativar / Desativar o certificado dependendo do seu Status atual.

Ao clicar nas opções de Ativar e Desativar o certificado na tabela o sistema exibirá uma mensagem indicando a efetivação e o Status será alterado.

### 3.3. Credenciais da API

Ao clicar no botão Credenciais da API abaixo do filtro de busca o sistema abrirá uma janela pop-up para criação de um Secret para a sua instituição.

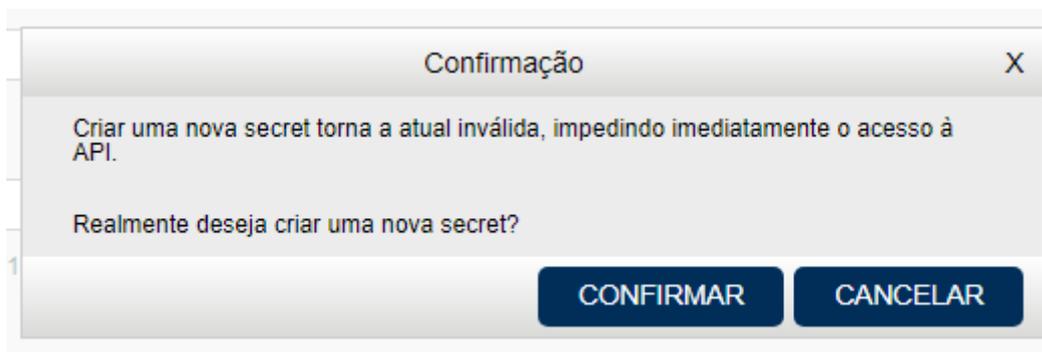


Gerenciar certificados digitais



O campo Cliente ID - ISelic virá preenchido e caso já exista uma Secret para a ID escolhida o sistema irá gerar um aviso quanto a inutilização da Secret antiga ao gerar uma nova, conforme no exemplo acima.

Criar uma nova Secret automaticamente inutilizará a anterior, impossibilitando a solicitação de um novo token JWT para uso da API com a Secret antiga. Para isso toda solicitação de Secret deve ser confirmada, em uma tela de confirmação, exemplo abaixo:



## Histórico de Revisão

Data	Descrição	Autor
24/09/2020	Elaboração da versão 1.0	Filipe Villanova