# Roteiro de Integração do Login Único

**Higo**

**25 jan., 2021**

# Legislação e Conceitos

# CAPÍTULO 1

## Contexto

Decreto n° 8.936, de 19 de dezembro de 2016 ,pemititu o inicio do projeto da plataforma de cidadania digital, que contempla diversas diretrizes para a prestação de serviços públicos digitais, das quais fazem parte a convergência autoritativa e a federação dos processos de autenticação dos serviços digitais. Para essa diretriz foi concebido o conceito da Plataforma de Autenticação Digital do Cidadão, o projeto Login Único, tendo, como destaque no decreto, o mecanismo de acesso digital único.

Dentro deste contexto, podemos destacar as diversas dificuldades com múltiplas contas de acesso sob responsabilidade do cidadão e variados bancos de dados cadastrais, tais como a duplicidade e inconsistência de informações, falta de integração, dados dispersos e diversas formas de autenticação. Problemas enfrentados por cidadãos ao tentar consumir um serviço público digital oferecido pelo governo federal. Analisando essas dificuldades, o Ministério da Economia (ME), em parceria com o Serviço Federal de Processamento de Dados (Serpro), disponibilizou a plataforma central de autenticação digital do cidadão, o Login Único.

Essa é a nova proposta do Governo federal, para facilitar a identificação e autenticação do cidadão, privilegiando a governança e a convergência autoritativa, e finalmente o controle de acesso unificado. A Plataforma de Cidadania Digital chega para ampliar e simplificar o acesso dos cidadãos brasileiros aos serviços públicos digitais, inclusive por meio de dispositivos móveis.

CAPÍTULO 2

# Introdução

Este documento é o elemento para orientar a integração da Plataforma de Autenticação Digital do Cidadão – Login Único a qualquer ambiente. A partir de agora, será feita uma revisão sobre a arquitetura de serviço e alguns conceitos utilizados pela Plataforma, além de uma explicação sobre procedimentos administrativos essenciais para autorizar o acesso à Plataforma.

Este documento contém as formas de chamadas a operações, parâmetros e métodos de integração, e, por último, os procedimentos para permitir a conectividade entre os ambientes de implantação.

# CAPÍTULO 3

## Escopos de Atributos

São conjuntos de informações fornecidos a quem possui autorização.

Os escopos com atributos estão disponíveis no Login Único?

1. **openid, email, phone, profile** (CPF, Nome, e-mail, telefone, foto);
2. **govbr_empresa** (CNPJ, Nome Fantasia, CPF do Responsável, Nome do Responsável, Atuação no CNPJ)
3. **govbr_confiabilidades** (selos de confiabilidade).

CAPÍTULO 4

# Níveis de Autenticação, Selos e Catálogo de Confiabilidades

## 4.1 Níveis de Autenticação

Os Níveis de Autenticação tem como principal característica ser um recurso de segurança da informação da identidade, que permitem flexibilidade para realização do acesso.

## 4.2 Selos de Confiabilidade

Os Selos de Confiabilidade estão presentes em cada nível de autenticação e consistem em orientar para qualificação das contas com a obtenção dos atributos autoritativos do cidadão a partir das bases oficias de governo, por meio das quais permitirão a utilização da credencial de acesso em sistemas internos dos clientes e serviços providos diretamente ao cidadão.

Uso possível para os nívels e os selos é o aumento da confiança cadastral pelos serviços para aplicar controle de acesso às funcionalidades mais críticas.

## 4.3 Catálogo de Confiabilidades

O Catálogo de Confiabilidades permite ao Sistema requisitar a confiabilidade desejada e, de forma automática, redirecionar para aplicação integrada após o cidadão adquirir a confiabilidade permitida a aplicação.

O Catálogo trabalha com as estruturas:

### 4.3.1 Níveis

1. **Nível Básico**
2. **Nível Verificado**
3. **Nível Comprovado**

### 4.3.2 Categorias

Permitem manutenção mais facilitada da utilização dos níveis e confiabilidades (selos) do Login Único.

1. Nível Básico (**Cadastro via Carrossel de Perguntas;Confiabilidade adquirida por meio de validação de informações da Previdência Social**);
2. Nível Verificado (**Cadastro Presencial, Cadastro via validação biométrica, Cadastro via Internet Banking, Cadastro via Sigepe**);
3. Nível Comprovado (**Cadastro via validação biométrica do TSE, Cadastro via certificado digital**)

### 4.3.3 Confiabilidades

1. Nível Básico

- **Selo Cadastro Básico com Validação de Dados Pessoais**: Validação do cadastro do cidadão por meio da base de Cadastro de Pessoas Físicas (Ministério da Economia / Receita Federal). Orientações para aquisição do Selo Cadastro Básico com Validação de Dados Pessoais.
- **Selo Cadastro Básico com Validação de Dados Previdênciarios**: Validação do cadastro do cidadão por meio da base de Casdatro Nacional de Informações Sociais (CNIS / INSS). Orientações para aquisição do Selo Cadastro Básico com Validação de Dados Previdênciarios.

2. Nível Verificado

- **Selo Balcão Presencial (INSS)**: Validação do cadastro do cidadão por meio do Balcão presencial localizado nas agências do INSS. Orientações para aquisição do Selo Balcão Presencial (INSS).
- **Selo Internet Banking**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking dos bancos conveniados. Orientações para aquisição do Selo Internet Banking.
- **Selo Cadastro Básico com Validação em Base de Dados de Servidores Públicos da União**: Validação do cadastro por meio de base de dados de Servidores Públicos da União. Orientações para aquisição do Selo Cadastro Básico com Validação em Base de Dados de Servidores Públicos da União.
- **Selo Validação Facial**: Validação do cadastro do cidadão por meio de biometria facial. A base utilizada para comparação é a da Carteira Nacional de Habilitação (Ministério da Infraestrutura / Denatran). Orientações para aquisição do Selo Validação Facial.
- **Selo Internet Banking (Banco do Brasil)**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking do Banco do Brasil. Orientações para aquisição do Selo Internet Banking do Bancos Credenciados.
- **Selo Internet Banking (Banrisul)**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking do Banco do Estado do Rio Grande do Sul (BANRISUL). Orientações para aquisição do Selo Internet Banking do Bancos Credenciados.
- **Selo Internet Banking (Bradesco)**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking do Bradesco. Orientações para aquisição do Selo Internet Banking do Bancos Credenciados.
- **Selo Internet Banking (BRB)**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking do Banco de Brasília (BRB). Orientações para aquisição do Selo Internet Banking do Bancos Credenciados.
- **Selo Internet Banking (CAIXA)**: Validação do cadastro do cidadão por meio da plataforma de Internet Banking da Caixa Econômica Federal (CAIXA). Orientações para aquisição do Selo Internet Banking do Bancos Credenciados.

3. Nível Comprovado

- **Selo de Certificado Digital de Pessoa Física**: Validação do cadastro do cidadão por meio da utilização de certificado digital de pessoal física. Orientações para aquisição do Selo de Certificado Digital de Pessoa Física.

- **Selo Validação Facial**: Validação do cadastro do cidadão por meio de biometria facial. A base utilizada para comparação é a da Justiça Eleitoral (Tribunal de Justiça Eleitoral). Orientações para aquisição do Selo Validação Facial.

CAPÍTULO 5

# Iniciando a Integração

## 5.1 Solicitação de Configuração

Para utilização do sistema Login Único, há necessidade de liberar os ambientes para aplicação cliente possa utilizar. Essa liberação ocorre por meio do preenchimento do Plano de Integração.

O formulário deverá ser encaminhado para os integrantes da Secretaria de Governança Digital (SGD) do Ministério da Economia (ME) para realizar configuração da utilização do Login Único.

## 5.2 Métodos e interfaces de integração (Passo-a-Passo para Integrar)

### 5.2.1 Autenticação

Para que a autenticação aconteça, todo o canal de comunicação deve ser realizado com o protocolo HTTPS. Será feito um redirecionamento para uma URL de autorização do Login Único e, após a autenticação ser concluída, retornará um código de autenticação para a aplicação cliente com intuito de adquirir um ticket de acesso para os serviços protegidos.

A utilização da autenticação do Login Único depende dos seguintes passos:

1. A chamada para autenticação deverá ocorrer pelo botão com o conteúdo **Entrar com GOV.BR**. Para o formato do botão, seguir as orientações do Design System do Governo Federal .
2. Ao requisitar autenticação via Provedor, o mesmo verifica se o usuário está logado. Caso o usuário não esteja logado o provedor redireciona para a página de login.
3. A requisição é feita através de um GET para o endereço https://sso.staging.acesso.gov.br/authorize passando as seguintes informações:

| Variavél | Descrição |
|---|---|
| **response_type** | Especifica para o provedor o tipo de autorização. Neste caso será **code** |
| **client_id** | Chave de acesso, que identifica o serviço consumidor fornecido pelo Login Único para a aplicação cadastrada |
| **scope** | Especifica os recursos que o serviço consumidor quer obter. Um ou mais escopos inseridos para a aplicação cadastrada. Informação a ser preenchida por padrão: **openid+email+phone+profile+govbr_confiabilidades**. |
| **redirect_uri** | URI de retorno cadastrada para a aplicação cliente no formato *URL Encode*. Este parâmetro não pode conter caracteres especiais conforme consta na especificação auth 2.0 Redirection Endpoint |
| **nonce** | Sequência de caracteres usado para associar uma sessão do serviço consumidor a um *Token* de ID e para atenuar os ataques de repetição. Pode ser um valor aleatório, mas que não seja de fácil dedução. Item obrigatório. |
| **state** | Valor usado para manter o estado entre a solicitação e o retorno de chamada. Item não obrigatório. |

Exemplo de requisição:

```
https://sso.staging.acesso.gov.br/authorize?response_type=code&client_id=ec4318d6-
↪f797-4d65-b4f7-39a33bf4d544&scope=openid+email+phone+profile&redirect_uri=http%3A%2F
↪%2Fappcliente.com.br%2Fphpcliente%2Floginecidadao.Php&nonce=3ed8657fd74c&
↪state=358578ce6728b
```

4. Após a autorização, a requisição é retornada para a URL especificada no redirect_uri do serviço https://sso.staging.acesso.gov.br/authorize, enviando os parâmetros:

| Variavél | Descrição |
|---|---|
| **code** | Código de autenticação gerado pelo provedor. Será utilizado para obtenção do Token de Resposta. Possui tempo de expiração e só pode ser utilizado uma única vez. |
| **state** | *State* passado anteriormente do https://sso.staging.acesso.gov.br/authorize que pode ser utilizado para controle da aplicação cliente. Pode correlacionar com o *code* gerado. |

5. Após autenticado, o provedor redireciona para a página de autorização. O usuário habilitará o consumidor no sistema para os escopos solicitados. Caso o usuário da solicitação autorize o acesso, é gerado um "ticket de acesso", conforme demonstra na especificação OpenID Connect ;

6. Para obter o *ticket de acesso*, o consumidor deve fazer uma requisição POST para o endereço https://sso.staging.acesso.gov.br/token passando as seguintes informações:

Parâmetros do Header para requisição Post https://sso.staging.acesso.gov.br/token

| Variavél | Descrição |
|---|---|
| **Content-Type** | Tipo do conteúdo da requisição que está sendo enviada. Nesse caso estamos enviando como um formulário |
| **Authorization** | Informação codificada em *Base64*, no seguinte formato: CLIENT_ID:CLIENT_SECRET (senha de acesso do serviço consumidor)(utilizar codificador para Base64 para gerar codificação). A palavra Basic deve está antes da informação. |

Exemplo de *header*:

```
Content-Type:application/x-www-form-urlencoded
Authorization: Basic
ZWM0MzE4ZDYtZjc5Ny00ZDY1LWI0ZjctMzlhMzNiZjRkNTQ0OkFJSDRoaXBfTUJYcVJkWEVQSVJkWkdBX2dRdjdWRWZqYlRFT2NWN
```

Parâmetros da Query para requisição Post https://sso.staging.acesso.gov.br/token

| Variavél | Descrição |
|---|---|
| **grant_type** | Especifica para o provedor o tipo de autorização. Neste caso será **authorization_code** |
| **code** | Código retornado pela requisição anterior (exemplo: Z85qv1) |
| **redirect_uri** | URI de retorno cadastrada para a aplicação cliente no formato *URL Encode*. Este parâmetro não pode conter caracteres especiais conforme consta na especificação auth 2.0 Redirection Endpoint |

Exemplo de *query*

```
https://sso.staging.acesso.gov.br/token?grant_type=authorization_code&code=Z85qv1&
↪redirect_uri=http%3A%2F%2Fappcliente.com.br%2Fphpcliente%2Floginecidadao.Php
```

O serviço retornará, em caso de sucesso, no formato JSON, as informações conforme exemplo:

```
{
        "access_token": "(Token de acesso a recursos protegidos do autenticador, bem␣
↪como serviços do Login Único.)",
        "id_token": "(Token de autenticação com informações básicas do usuário.)",
        "token_type": "(O tipo do token gerado. Padrão: Bearer)",
        "expires_in": "(Tempo de vida do token em segundos.)"
}
```

7. De posse das informações do json anterior, a aplicação consumidora está habilitada para consultar dados de recursos protegidos, que são as informações e método de acesso do usuário ou serviços externos do Login Único.

8. Antes de utilizar as informações do JSON anterior, de forma especifica os **ACCESS_TOKEN** e **ID_TOKEN**, para buscar informações referente ao método de acesso e cadastro básico do usuário, há necessidade da aplicação consumidora validar se as informações foram geradas pelos serviços do Login Único. Esta validação ocorrerá por meio da consulta da chave pública disponível no serviço https://sso.staging.acesso.gov.br/jwk. Para isso, verificar o método **processToClaims** dos Exemplos de Integração.

9. A utilização das informações do **ACCESS_TOKEN** e **ID_TOKEN** ocorrerá ao extrair do JSON codificado os seguintes parâmetros:

**JSON do ACCESS_TOKEN**

```
{
        "sub": "(CPF do usuário autenticado)",
        "aud": "Client ID da aplicação onde o usuário se autenticou",
        "scope": ["(Escopos autorizados pelo provedor de autenticação.)"],
        "amr": ["(Listagem dos fatores de autenticação do usuário. Pode ser “passwd”␣
↪se o mesmo logou fornecendo a senha, “x509” se o mesmo utilizou certificado digital␣
↪ou certificado em nuvem, ou “bank” para indicar utilização de conta bancária para␣
↪autenticar. Esse último seguirá com número de identificação do banco, conforme␣
↪código de compensação do Bacen presente ao final da explicação.)"],
        "iss": "(URL do provedor de autenticação que emitiu o token.)",
        "exp": "(Data/hora de expiração do token)",
        "iat": "(Data/hora em que o token foi emitido.)",
        "jti": "(Identificador único do token, reconhecido internamente pelo provedor␣
↪de autenticação.)",
```

(continues on next page)

(continuação da página anterior)

```
        "cnpj": "CNPJ vinculado ao usuário autenticado. Atributo será preenchido␣
↪quando autenticação ocorrer por certificado digital de pessoal jurídica."
}
```

**Observações para ACCESS_TOKEN:**

- Caso conta do cidadão esteja com segundo fator de autenticação ativado, quando o atributo *AMR* vier com *passwd*, aparecerão os conteúdos *mfa* (indica presença de segundo fator) e *otp* (forma de segundo fator com código encaminhado pelo aplicativo gov.br).
- Documento para verificação do Código de Compensação dos possíveis bancos integrados ao Login Único:Documento verificar Código de Compensação dos Bancos.

**JSON do ID_TOKEN**

```
{
        "sub": "(CPF do usuário autenticado.)",
        "amr": ["(Listagem dos fatores de autenticação do usuário. Pode ser "passwd"␣
↪se o mesmo logou fornecendo a senha, "x509" se o mesmo utilizou certificado digital␣
↪ou certificado em nuvem, ou "bank" para indicar utilização de conta bancária para␣
↪autenticar. Esse último seguirá com número de identificação do banco, conforme␣
↪código de compensação do Bacen presente ao final da explicação.)"],
        "picture": "(URL de acesso à foto do usuário cadastrada no Gov.br. A mesma é␣
↪protegida e pode ser acessada passando o access token recebido.)",
        "name": "(Nome cadastrado no Gov.br do usuário autenticado.)",
        "phone_number_verified": "(Confirma se o telefone foi validado no cadastro do␣
↪Gov.br. Poderá ter o valor "true" ou "false")",
        "phone_number": "(Número de telefone cadastrado no Gov.br do usuário␣
↪autenticado. Caso o atributo phone_number_verified do ID_TOKEN tiver o valor false,␣
↪o atributo phone_number não virá no ID_TOKEN)",
        "email_verified": "(Confirma se o email foi validado no cadastro do Gov.br.␣
↪Poderá ter o valor "true" ou "false")",
        "email": "(Endereço de e-mail cadastrado no Gov.br do usuário autenticado.␣
↪Caso o atributo email_verified do ID_TOKEN tiver o valor false, o atributo email␣
↪não virá no ID_TOKEN)",
        "cnpj": "(CNPJ vinculado ao usuário autenticado. Atributo será preenchido␣
↪quando autenticação ocorrer por certificado digital de pessoal jurídica.)"
}
```

**Observações para ID_TOKEN:**

- Os paramêtros email,phone_number,picture não são obrigatórios. Ambos podem estar preenchidos ou não.
- Caso conta do cidadão esteja com segundo fator de autenticação ativado, quando o atributo *AMR* vier com *passwd*, aparecerão os conteúdos *mfa* (indica presença de segundo fator) e *otp* (forma de segundo fator com código encaminhado pelo aplicativo gov.br).
- Documento para verificação do Código de Compensação dos possíveis bancos integrados ao Login Único:Documento verificar Código de Compensação dos Bancos.

10. Para solicitação do conteúdo da foto salva no cadastro do cidadão, deverá acessar, pelo método GET, o serviço https://sso.staging.acesso.gov.br/userinfo/picture e acrescentar o atributo Authorization ao header do HTTP da requisição:

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |

O serviço retornará, em caso de sucesso a informação em formato Base64

11. Para verificar quais níveis da conta do cidadão está localizada, deverá acessar, pelo método GET, o serviço https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/niveis?response-type=ids

Parâmetros para requisição GET https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/niveis?response-type=ids

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |
| **cpf** | CPF do cidadão (sem ponto, barra etc). |

A resposta em caso de sucesso retorna sempre um **array** de objetos JSON no seguinte formato:

```
[
        {
        "id": "(Identificação para reconhecer o nível)",
        "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização do nível na␣
↪conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

Verificar quais níveis estão disponíveis, acesse *Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Níveis)*

12. Para verificar quais catagorias da conta do cidadão está localizado, deverá acessar, pelo método GET, o serviço https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/categorias?response-type=ids

Parâmetros para requisição GET https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/categorias?response-type=ids

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |
| **cpf** | CPF do cidadão (sem ponto, barra etc). |

A resposta em caso de sucesso retorna sempre um **array** de objetos JSON no seguinte formato:

```
[
        {
        "id": "(Identificação para reconhecer a categoria)",
        "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

Verificar quais categorias estão disponíveis, acesse Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Categorias)

13. Para verificar quais selos de confiabilidade a conta do cidadão possui, deverá acessar, pelo método GET, o serviço https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/confiabilidades?response-type=ids

Parâmetros para requisição GET https://api.staging.acesso.gov.br/confiabilidades/v3/contas/**cpf**/confiabilidades?response-type=ids

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |
| **cpf** | CPF do cidadão (sem ponto, barra etc). |

A resposta em caso de sucesso retorna sempre um **array** de objetos JSON no seguinte formato:

```
[
        {
        "id": "(Identificação para reconhecer a confiabilidade)",
        "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

Verificar quais selos de confiabilidade estão disponíveis, acesse Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Selos)

### 5.2.2 Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Níveis)

As categorias existentes no Login Único são:

```
[
        {
                "id": "1 (conta_basica)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "2 (verificada)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "3 (comprovada)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

### 5.2.3 Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Categorias)

As categorias existentes no Login Único são:

```
[
        {
                "id": "101 (carrosel_perguntas_previdencia)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
```

(continues on next page)

(continuação da página anterior)

```
        },

        {
                "id": "102 (carrosel_perguntas)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "201 (servidor_publico)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },
        {
                "id": "202 (biometria_facial)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "203 (balcao_presencial)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "204 (internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },
        {
                "id": "301 (biometria_individualizada)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": " 302 (certificado_digital)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪categoria na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }

]
```

### 5.2.4 Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Selos)

Os selos existentes no Login Único são:

```
[
        {
                "id": "101 (kba_previdencia)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
```

(continues on next page)

(continuação da página anterior)

```
        },

        {
                "id": "201 (cadastro_basico)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "301 (servidor_publico)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },
        {
                "id": "401 (biovalid_facial)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "501 (balcao_sat_previdencia)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "502 (balcao_denatran)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },
        {
                "id": "503 (balcao_correios)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "601 (balcao_nai_previdencia)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "602 (bb_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "603 (banrisul_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "604 (bradesco_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
```

(continues on next page)

(continuação da página anterior)

```
        },

        {
                "id": "605 (caixa_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "606 (brb_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "607 (sicoob_internet_banking)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "701 (tse_facial)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        },

        {
                "id": "801 (certificado_digital)",
                "dataAtualizacao": "(Mostra a data e hora que ocorreu atualização da␣
↪confiabilidade na conta do usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

### 5.2.5 Acesso ao serviço de Catálogo de Confiabilidades (Selos)

1. Com usuário autenticado, deverá acessar, por meio do método GET ou POST, a URL https://confiabilidades.staging.acesso.gov.br/

Parâmetros da Query para requisição GET https://confiabilidades.staging.acesso.gov.br/

| Variável | Descrição |
|---|---|
| **client_id** | Chave de acesso, que identifica o serviço consumidor fornecido pelo Login Único para a aplicação cadastrada |
| **niveis** | Recurso de segurança da informação da identidade, que permitem flexibilidade para realização do acesso. **Atributo opcional** |
| **categorias** | Permitem manutenção mais facilitada da utilização dos níveis e confiabilidades (selos) do Login Único. **Atributo obrigatório** |
| **confiabilidades** | Consistem em orientar para qualificação das contas com a obtenção dos atributos autoritativos do cidadão a partir das bases oficias de governo, por meio das quais permitirão a utilização da credencial de acesso em sistemas internos dos clientes e serviços providos diretamente ao cidadão. **Atributo obrigatório** |

2. O resultado será o Catálogo apresentado com as configurações solicitadas. Após atendido as configurações, o Login Único devolverá o fluxo para aplicação por meio da URL de Lançador de Serviços, conforme Plano de Integração.

**Observações sobre as variáveis do serviço de catálogo**

1. Conteúdo para variável *niveis* : Será a informação do atributo id presente em cada nível no *Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Níveis)*
2. Conteúdo para variável *categorias* : Será a informação do atributo id presente em cada categoria no Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Categorias)
3. Contéudo para variável *confiabilidades*: Será a informação do atributo id presentes em cada confiabilidade no Resultado Esperado do Acesso ao Serviço de Confiabilidade Cadastral (Selos)
4. Tratamento do conteúdo para cada variável:

- Todos são obrigatórios, deve-se separá-los por vírgula. **Exemplo (categorias=102,101)**
- Apenas um é obrigatório, deve-se separar por barra invertida. **Exemplo (confiabilidades=(301/801)**

### 5.2.6 Acesso ao Serviço de Log Out

1. Com usuário autenticado, deverá acessar, por meio do método GET ou POST, a URL: https://sso.staging.acesso.gov.br/logout. O acesso ao Log Out deverá ser pelo **Front End** da aplicação a ser integrada com Login Único.

Parâmetros da Query para requisição GET https://sso.staging.acesso.gov.br/logout

| Variavél | Descrição |
|---|---|
| **post_logout_redirect_uri** | URL que direciona ao Login Único qual página deverá ser aberta quando o token for inválidado. A URL deverá ser previamente liberada por meio do preenchimento do campo **URL de Log Out** presente no Plano de Integração. |

Exemplo 1 de **execução** no front end em javascript

```
    var form = document.createElement("form");
    form.setAttribute("method", "post");
form.setAttribute("action", "https://sso.staging.acesso.gov.br/logout?post_logout_
↪redirect_uri=https://www.minha-aplicacao.gov.br/retorno.html");
document.body.appendChild(form);
    form.submit();
```

Exemplo 2 de **execução** no front end em javascript

```
window.location.href='https://sso.staging.acesso.gov.br/logout?post_logout_redirect_
↪uri=https://www.minha-aplicacao.gov.br/retorno.html';
```

### 5.2.7 Acesso ao Serviço de Cadastro de Pessoas Jurídicas

O Login Único disponibiliza dois serviços para acesso a informações de Pessoa Jurídica. O primeiro apresenta todos os CNPJs cadastrados para um determinado usuário. O segundo, utiliza desse CNPJ para extrair informações cadastradas no Login Único para aquela pessoa e empresa.

Para acessar o serviço que disponibiliza os CNPJs vinculados a um determinado usuário, é necessário o seguinte:

1. Na requisição de autenticação, adicionar o escopo "govbr_empresa", conforme exemplo:

Exemplo de requisição

```
https://sso.staging.acesso.gov.br/authorize?response_type=code&client_id=minha-
↪aplicacao&scope=openid+email+phone+profile+govbr_empresa&redirect_uri=http%3A%2F
↪%2Fappcliente.com.br%2Fphpcliente%2Floginecidadao.Php&nonce=3ed8657fd74c&
↪state=358578ce6728b
```

2. Com o usuário autenticado, a aplicação deverá realizar uma requisição por meio do método GET a URL https://api.staging.acesso.gov.br/empresas/v2/empresas?ltrar-por-participante=**cpf** enviando as seguintes informações:

Parâmetros para requisição GET https://api.staging.acesso.gov.br/empresas/v2/empresas?ltrar-por-participante=cpf

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |
| **cpf** | CPF do cidadão (sem ponto, barra etc). |

3. O resultado em formato JSON é a lista de CNPJs do CPF autenticado, conforme o exemplo abaixo:

Exemplo de requisição

```
[
        {
        "cnpj": "(Número de CNPJ da empresa vinculada)",
        "razaoSocial": "(Razão Social (Nome da empresa) cadastrada na Receita Federal)
↪",
        "dataCriacao": "(Mostra a data e hora da vinculação do CNPJ a conta do␣
↪usuário. A mascará será YYYY-MM-DD HH:MM:SS)"
        }
]
```

4. Com o usuário autenticado, a aplicação cliente deverá acessar, por meio do método GET, a URL https://api.staging.acesso.gov.br/empresas/v2/empresas/**cnpj**/participantes/**cpf** enviando as seguintes informações:

Parâmetros para requisição GET https://api.staging.acesso.gov.br/empresas/v2/empresas/**cnpj**/participantes/**cpf**

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |
| **cpf** | CPF do cidadão (sem ponto, barra etc). |
| **cnpj** | CNPJ da empresa (sem ponto, barra etc). |

5. O resultado em formato JSON é o detalhamento do CNPJ do CPF autenticado, conforme o exemplo abaixo:

Exemplo de requisição

```
{
"cpf": "(Número do CPF que pode atuar com empresa)",
"atuacao": "(Papel do CPF na empresa na Receita Federal. O conteúdo será SOCIO,␣
↪CONTADOR, REPRESENTANTE_LEGAL ou NAO_ATUANTE. O NAO_ATUANTE representa CPF possui␣
↪certificado digital de pessoa jurídica, porém não possui um papel na empresa na␣
↪base da Receita Federal. Se CPF for colaborador, atributo atuacao não aparecerá)",
"cadastrador": "(Identifica se o CPF pode realizar cadastro de colaboradores para␣
↪CNPJ. O conteúdo false determinar que o CPF é um colaborador da empresa. O conteúdo␣
↪true determina CPF é representante da empresa com certificado digital de pessoal␣
↪jurídica)",
"cpfCadastrador": "(CPF responsável por realizar cadastro do Colaborador. Se CPF␣
↪apresentar atributo cadastrador com conteúdo true, o atributo cpfCadastrador não␣
↪aparecerá)",
```

(continues on next page)

(continuação da página anterior)

```
"dataCriacao": "(Mostra a data e hora da vinculação do CPF ao CNPJ. A mascará será␣
↪YYYY-MM-DD HH:MM:SS)",
"dataExpiracao": "(Mostra a data e hora que o CPF poderá atuar com CNPJ. A mascará␣
↪será YYYY-MM-DD HH:MM:SS)"
}
```

### 5.2.8 Acesso ao Serviço de Revalidação de Senha

Para que a revalidação aconteça, todo o canal de comunicação deve ser realizado com o protocolo HTTPS. Será feito um redirecionamento para URL de autorização especifica do Login Único e, após a revalidação ser concluída, retornará um código de autenticação para a aplicação cliente com intuito de adquirir um ticket de acesso para revalidação da senha e continuação do fluxo do sistema.

Esta estrutura precisará autorização específica a ser solicitada para Ministério da Economia.

Passos para processo:

1. Requisição GET para endereço https://oauth.staging.acesso.gov.br/v1/authorize passando as seguintes informações:

| Variável | Descrição |
|---|---|
| **response_type** | Especifica para o provedor o tipo de autorização. Neste caso será **code** |
| **client_id** | Chave de acesso, que identifica o serviço consumidor fornecido pelo Login Único para a aplicação cadastrada |
| **scope** | Informação ser preenchida: **password-validation**. |
| **redirect_uri** | URL de retorno cadastrada para a aplicação cliente continuar o processo após a revalidação da senha no formato *URL Encode*. Este parâmetro não pode conter caracteres especiais conforme consta na especificação auth 2.0 Redirection Endpoint |
| **state** | Valor usado para manter o estado entre a solicitação e o retorno de chamada. Item não obrigatório. |

Exemplo de requisição:

```
https://oauth.staging.acesso.gov.br/v1/authorize?response_type=code&client_
↪id=ec4318d6-f797-4d65-b4f7-39a33bf4d544&redirect_uri=http%3A%2F%2Fappcliente.com.br
↪%2Fphpcliente%2Floginecidadao.Php&scope=password-validationstate=exASJANS12sa
```

2. Após a autorização, a requisição é retornada para a URL especificada no redirect_uri do serviço https://oauth.staging.acesso.gov.br/v1/authorize, enviando os parâmetros:

| Variável | Descrição |
|---|---|
| **code** | Código de autenticação gerado pelo provedor. Será utilizado para obtenção do Token de Resposta. Possui tempo de expiração de 2 minutos e só pode ser utilizado uma única vez. |
| **state** | *State* passado anteriormente do https://oauth.staging.acesso.gov.br/v1/authorize que pode ser utilizado para controle da aplicação cliente. Pode correlacionar com o *code* gerado. |

3. Para obter o novo *ticket de acesso*, o consumidor deve fazer uma requisição POST para o endereço https://oauth.staging.acesso.gov.br/v1/token passando as seguintes informações:

Parâmetros do Header para requisição Post https://oauth.staging.acesso.gov.br/v1/token

| Variavél | Descrição |
|---|---|
| **Content-Type** | Tipo do conteúdo da requisição que está sendo enviada. Nesse caso estamos enviando como um formulário (**application/x-www-form-urlencoded**) |
| **Authorization** | Informação codificada em *Base64*, no seguinte formato: CLIENT_ID:CLIENT_SECRET (senha de acesso do serviço consumidor)(utilizar codificador para Base64 para gerar codificação). A palavra Basic deve está antes da informação. |

Exemplo de *header*:

```
Content-Type:application/x-www-form-urlencoded
Authorization: Basic
ZWM0MzE4ZDYtZjc5Ny00ZDY1LWI0ZjctMzlhMzNiZjRkNTQ0OkFJSDRoaXBfTUJYcVJkWEVQSVJkWkdBX2dRdjdWRWZqYlRFT2NWN
```

Parâmetros da Query para requisição Post https://oauth.staging.acesso.gov.br/v1/token

| Variavél | Descrição |
|---|---|
| **grant_type** | Especifica para o provedor o tipo de autorização. Neste caso será **authorization_code** |
| **code** | Código retornado pela requisição anterior (exemplo: 8bfac143-c4ca-daf-8ea8-517f0d93db7a) |
| **redirect_uri** | URI de retorno cadastrada para a aplicação cliente no formato *URL Encode*. Este parâmetro não pode conter caracteres especiais conforme consta na especificação auth 2.0 Redirection Endpoint |
| **state** | Valor usado para manter o estado entre a solicitação e o retorno de chamada. Item não obrigatório. |

Exemplo de *query*

```
https://oauth.staging.acesso.gov.br/v1/token?grant_type=authorization_code&
↪code=8bfac143-c4ca-daf-8ea8-517f0d93db7a&redirect_uri=http%3A%2F%2Fappcliente.com.br
↪%2Fphpcliente%2Floginecidadao.Php&client_id=ec4318d6-f797-4d65-b4f7-39a33bf4d544
```

O serviço retornará, em caso de sucesso, no formato JSON, as informações conforme exemplo:

```
{
        "access_token": "(Token de acesso a recursos protegidos do autenticador, bem␣
↪como serviços do Login Único.)",
        "token_type": "(O tipo do token gerado. Padrão: Bearer)",
        "expires_in": "(Tempo de vida do token em segundos.)"
}
```

4. De posse das informações do json anterior, a aplicação consumidora está habilitada para concluir revalidação da senha.
5. Antes de utilizar as informações do JSON anterior, de forma especifica o **ACCESS_TOKEN**, para revalidação da senha, há necessidade da aplicação consumidora validar se as informações foram geradas pelos serviços do Login Único. Esta validação ocorrerá por meio da consulta da chave pública disponível no serviço https://oauth.staging.acesso.gov.br/v1/jwks. Para isso, verificar o método **processToClaims** dos Exemplos de Integração.
6. Verificado o access token, a aplicação cliente consegue, através do atributo **sub**, saber qual usuário confirmou sua identidade gov.br com sucesso e continuar o processo no sistema integrado.

### 5.2.9 Acesso ao Serviço de Recuperação do Tipo de Certificado

1. Na requisição de autenticação, adicionar o escopo "govbr_recupera_certificadox509", conforme exemplo:

Exemplo de requisição

```
https://sso.staging.acesso.gov.br/authorize?response_type=code&client_id=minha-
↪aplicacao&scope=openid+email+phone+profile+govbr_recupera_certificadox509&redirect_
↪uri=http%3A%2F%2Fappcliente.com.br%2Fphpcliente%2Floginecidadao.Php&
↪nonce=3ed8657fd74c&state=358578ce6728b
```

2. Com o usuário autenticado, a aplicação deverá realizar uma requisição por meio do método GET a URL https://sso.staging.acesso.gov.br/api/x509/info enviando as seguintes informações:

Parâmetros para requisição GET https://sso.staging.acesso.gov.br/api/x509/info

| Variavél | Descrição |
|---|---|
| **Authorization** | palavra **Bearer** e o *ACCESS_TOKEN* da requisição POST do https://sso.staging.acesso.gov.br/token |

3. O resultado em formato JSON é tipo de certificado da autenticação, conforme o exemplo abaixo:

Exemplo de requisição

```
[
        {
          "provider":"(Indicará qual o provedor disponibilizará o certificado.␣
↪Aparecerá para certificado em nuvem)",
          "amr":["(Lista de forma de certificados autenticados. Padrão é x509)"],
          "certificate":"(Demonstra o nome do cerficado da autenticação)",
          "type":"(Informa qual tipo de certificado utilizado para autenticação. O␣
↪contéudo será <device> para certificados A1 e A3 e <cloud> para indicar certificado␣
↪em núvem)"
        }
]
```

### 5.2.10 Resultados Esperados ou Erros do Acesso ao Serviços do Login Único

Os acessos aos serviços do Login Único ocorrem por meio de chamadas de URLs e as respostas são códigos presentes conforme padrão do protocolo http por meio do retorno JSON, conforme exemplo:

```
{
      "codigo": "(Código HTTP do erro)",
      "descricao": "(Descrição detalhada do erro ocorrido. )"
}
```

# CAPÍTULO 6

# Exemplo de implementação

Os exemplos são básicos da forma de realizar as requisições para Login Único. Cabe ao desenvolvedor realizar a organização e aplicação da segurança necessária na aplicação consumidora.

## 6.1 JAVA

Exemplo para download em JAVA

### 6.1.1 Observações para executar o exemplo JAVA

Link para biblioteca jose4j .

CAPÍTULO 7

# Execução dos Exemplos de Integração

## 7.1 JAVA

Caso você queira ver o exemplo JAVA funcionando execute com o Docker instalado:

```
$ docker run -it \
  --name meu-login-teste govbr/login-java-exemplo
```

**Aviso:** Siga os passos que vão aparecer no terminal.

Gif mostrando como executa o exemplo:

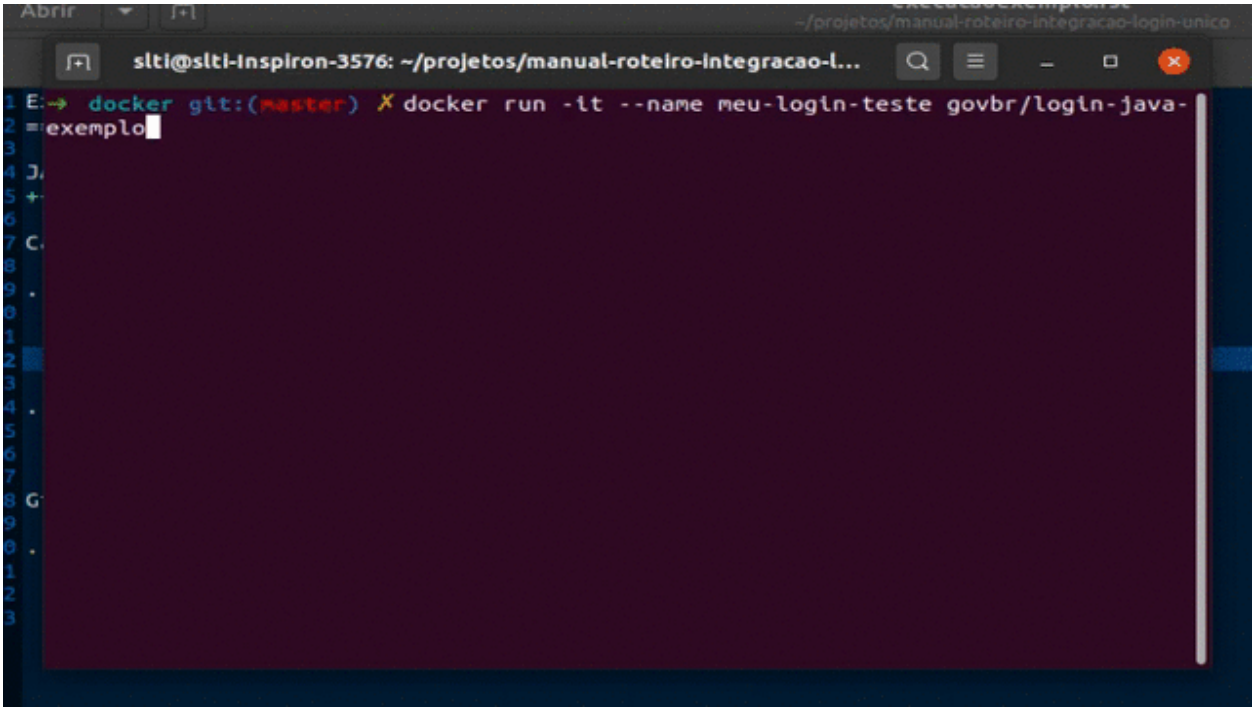


Fig. 1: Exemplo com o comando docker em JAVA.