WEB-Service para Gestão de Credencial de Acesso

Informações Gerais

Serviço

Nome:	Web Service para gestão de credencial de acesso aos serviços
Nome na interface:	WSCredencial
Início da operação:	31/05/2017
Endereço do WSDL - Testes	https://testews.siop.gov.br/services/credencial/WSCredencial?wsdl
Endereço do WSDL - Produção	https://webservice.siop.gov.br/services/credencial/WSCredencial?wsdl

Objetivo

Fornecer uma interface que possibilite a interoperabilidade entre os sistemas governamentais e o SIOP para recuperação de acesso e, quando aplicável, troca de senha da credencial utilizada pelos web services.

Além das operações SOAP do `WSCredencial`, usuários de web service já migrados para o novo modelo de autenticação utilizam a interface GraphQL do módulo de login para obtenção de token, que deve ser enviado no cabeçalho `Authorization` das chamadas aos demais web services.

Como Identificar Seu Fluxo

Antes de implementar ou consumir o serviço, identifique em qual situação sua credencial se encontra.

Siga o fluxo MD5 se:

- seu sistema autentica enviando a credencial no corpo XML da requisição SOAP;
- sua credencial ainda utiliza hash MD5;
- a operação `gerarNovaSenha` envia uma senha provisória em texto pleno para o e-mail cadastrado;
- a operação `trocarSenha` ainda é utilizada no seu processo.

Siga o fluxo Argon2Id + Token se:

- sua autenticação já é feita obtendo token na interface GraphQL do módulo de login;
- suas chamadas aos web services usam o cabeçalho `Authorization: Bearer [token]`;
- a recuperação de acesso envia uma URL token para definição de nova senha;
- sua credencial já foi migrada para o novo padrão de autenticação.

Importante: após a migração para `Argon2Id + token`, a credencial deixa de utilizar autenticação por hash MD5 no XML.

Fluxo 1 - Usuário de Web Service Ainda em MD5

Neste fluxo, a autenticação continua sendo feita da forma tradicional, com envio da estrutura `CredencialDTO` no corpo XML da requisição SOAP.

Cadastro e uso inicial

1. O administrador do SIOP cadastra a credencial no sistema. 2. O SIOP cria a credencial com marcação para exigir troca de senha. 3. O SIOP envia uma senha provisória para o e-mail cadastrado. 4. O cliente cria sua senha definitiva por meio da operação `WSCredencial.trocarSenha(CredencialDTO credencial, String novaSenha)`. 5. Depois disso, a credencial continua sendo usada nas requisições SOAP com hash MD5 no campo `senha`.

Regras da operação trocarSenha

Na operação `trocarSenha`:

- o campo `credencial.usuario` deve conter o login cadastrado para a credencial;
- o campo `credencial.senha` deve conter o hash MD5 da senha atual;
- o campo `novaSenha` deve conter a nova senha em texto puro;
- a nova senha deve atender às regras vigentes de segurança.

Exemplo de requisição:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://servicoweb.siop.sof.planejamento.gov.br/">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:trocarSenha>
         <credencial>
            <senha>[hash md5 da senha atual]</senha>
            <usuario>[login credencial]</usuario>
         </credencial>
         <novaSenha>[nova senha em texto puro]</novaSenha>
      </ser:trocarSenha>
   </soapenv:Body>
</soapenv:Envelope>
```

Regras da operação gerarNovaSenha

Na operação `gerarNovaSenha`:

- informar apenas os atributos `email` e `usuario` da credencial;
- o sistema envia uma senha provisória em texto pleno para o e-mail cadastrado;
- após o recebimento da senha, o cliente deve utilizar novamente a operação `trocarSenha` para definir a senha desejada.

Exemplo de requisição:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://servicoweb.siop.sof.planejamento.gov.br/">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:gerarNovaSenha>
         <credencial>
            <email>[e-mail da credencial]</email>
            <usuario>[login da credencial]</usuario>
         </credencial>
      </ser:gerarNovaSenha>
   </soapenv:Body>
</soapenv:Envelope>
```

Como autenticar nos demais web services neste fluxo

Enquanto a credencial estiver neste fluxo, a autenticação aos demais web services continua sendo feita com envio de `CredencialDTO` no XML da operação, contendo:

- `usuario`: login da credencial;
- `senha`: hash MD5 da senha da credencial.

Fluxo 2 - Usuário de Web Service Migrado para Argon2Id + Token

Neste fluxo, a autenticação deixa de ser feita por hash MD5 no XML e passa a usar token obtido na interface GraphQL do módulo de login.

Como funciona

1. O cliente autentica com login e senha em texto puro na interface GraphQL do módulo de login. 2. O sistema retorna `tokenSiop` e `refreshToken`. 3. O cliente passa a enviar o token no cabeçalho `Authorization` das chamadas aos demais web services. 4. A credencial deixa de usar autenticação por hash MD5 no XML.

Endpoint para obtenção do token

Testes: https://testews.siop.gov.br/modulo/login/api

Produção: https://www1.siop.planejamento.gov.br/modulo/login/api

Mutation GraphQL para autenticação

```
{
  "query": "mutation { autenticarUsuarioSenha(login: \"SEU_LOGIN\", senha:
\"SUA_SENHA_EM_TEXTO_PLANO\") { tokenSiop, refreshToken } }"
}
```

Exemplo de resposta:

```
{
  "data": {
    "autenticarUsuarioSenha": {
      "tokenSiop": "eyJhbGciOi...",
      "refreshToken": "eyJhbGciOi..."
    }
  }
}
```

Como autenticar nos demais web services neste fluxo

As chamadas aos demais web services devem enviar o token no cabeçalho `Authorization`:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header>
      <Authorization>Bearer [tokenSiop]</Authorization>
   </soapenv:Header>
   <soapenv:Body>
      <!-- XML normal da operação -->
   </soapenv:Body>
</soapenv:Envelope>
```

Recuperação de acesso neste fluxo

Para usuários já migrados:

- a operação `gerarNovaSenha` continua existindo;
- porém, em vez de enviar senha provisória em texto pleno, ela envia uma URL token para definição de nova senha;
- a definição da nova senha ocorre pela interface web;
- a operação `trocarSenha` deixa de ser o fluxo aplicável para a credencial já migrada.

Observações importantes

- se a credencial ainda estiver em MD5 e a senha atual não atender aos critérios mínimos de segurança, pode ser necessário usar `trocarSenha` antes da primeira autenticação GraphQL;
- após migrada para `Argon2Id + token`, a credencial não deve mais usar hash MD5 no XML;
- o `tokenSiop` possui validade temporária;

- quando necessário, deve-se usar o `refreshToken` para renovação do acesso.

Operações SOAP

2.1 Trocar Senha

Operação para troca de senha da credencial de acesso.

Nome da operação na interface do serviço: `trocarSenha`

Parâmetro(s) de entrada:

Parâmetro	Tipo (tamanho)	Observações
credencial	CredencialDTO	Credencial do usuário
novaSenha	String	Nova senha em texto puro, conforme regras vigentes de segurança

Tipo de Retorno: `RetornoDTO`

Observação: esta operação é aplicável ao fluxo de usuários que ainda utilizam autenticação por MD5. Para usuários já migrados para `Argon2Id + token`, a redefinição de senha ocorre por URL token enviada por e-mail.

Exemplo:

Requisição:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://servicoweb.siop.sof.planejamento.gov.br/">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:trocarSenha>
         <credencial>
            <senha>[hash md5 da senha]</senha>
            <usuario>[login credencial]</usuario>
         </credencial>
         <novaSenha>[nova senha em texto puro]</novaSenha>
      </ser:trocarSenha>
   </soapenv:Body>
</soapenv:Envelope>
```

2.2 Gerar Nova Senha

Operação de obtenção de novo acesso por e-mail.

Nome da operação na interface do serviço: `gerarNovaSenha`

Parâmetro(s) de entrada:

Parâmetro	Tipo (tamanho)	Observações
credencial	CredencialDTO	Para essa operação é necessário preencher apenas os atributos `email` e `usuario`.

Tipo de Retorno: `RetornoCaptacaoDetalheBaseExternaDTO`

Observação: o comportamento desta operação depende do fluxo da credencial:

- no fluxo MD5, o sistema envia senha provisória em texto pleno;
- no fluxo `Argon2Id + token`, o sistema envia URL token para definição de nova senha.

Exemplo:

Requisição:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://servicoweb.siop.sof.planejamento.gov.br/">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:gerarNovaSenha>
         <credencial>
            <email>[e-mail da credencial]</email>
            <usuario>[login da credencial]</usuario>
         </credencial>
      </ser:gerarNovaSenha>
   </soapenv:Body>
</soapenv:Envelope>
```

Estruturas de Entrada/Saída e Retorno

As informações que trafegam pelo serviço são organizadas em estruturas de dados que atuam como entrada e retorno das operações.

CredencialDTO

Esta estrutura é composta pelas informações necessárias para que a aplicação cliente se identifique junto ao serviço quando estiver utilizando o fluxo de autenticação por credencial no XML. A credencial utilizada nos web services do SIOP é específica para esse fim e não é válida para acessar a aplicação web.

Atributo	Tipo(tamanho)	Aceita Nulo?	Observações
usuario	Texto	Não	Login do usuário no SIOP
senha	Texto	Não	Hash MD5 da senha do usuário no SIOP. Campo aplicável ao fluxo de autenticação por MD5
perfil	Inteiro	Sim	Perfil com o qual o usuário deseja realizar determinada operação, quando aplicável

Observação: para usuários já migrados para `Argon2Id + token`, a autenticação dos demais web services não é feita pelo campo `senha` do `CredencialDTO`, mas pelo envio do token no cabeçalho `Authorization`.

RetornoDTO

Atributo	Tipo(tamanho)	Observações
sucesso	boolean	Indica se a requisição foi processada com sucesso
mensagensErro	List<String>	Contém a lista de mensagens de erro nos casos em que `sucesso` retornar valor igual a `false`