

2015

Sistema Protocolo Integrado

Manual do Cliente Web Service

Manual com a descrição do Cliente Web Service do Sistema Protocolo Integrado.

Versão 1.0 –Vigência a partir de 01/01/2015



Presidenta da República

Dilma Rousseff

Ministério do Planejamento, Orçamento e Gestão – MP

Nelson Barbosa

Ministério da Justiça - MJ

José Eduardo Cardozo

Secretaria de Logística e Tecnologia da Informação – SLTI

Loreni F. Foresti

Arquivo Nacional – AN/MJ

Jaime Antunes da Silva

Departamento de Logística – DELOG/SLTI/MP

Ana Maria Vieira Neto

Sumário

INTRODUÇÃO.....	4
CAPÍTULO I – O CLIENTE WEB SERVICE.....	5
1.1 INTRODUÇÃO.....	5
1.2 INSTALAÇÃO DO CERTIFICADO DIGITAL.....	5
1.2 ARQUIVO DE CONFIGURAÇÃO DO CLIENTE.....	6
1.3 UTILIZAÇÃO DO CLIENTE.....	7
1.4 ARQUIVO DE ENTRADA.....	7
CAPÍTULO II – SOLUÇÃO DE PROBLEMAS.....	9

INTRODUÇÃO

O Sistema Protocolo Integrado consolida uma base de dados com informações sobre processos e documentos oriundas dos diversos sistemas de protocolo dos órgãos e entidades da Administração Pública Federal. Oferece à sociedade mais um canal de consultas dessas informações, além de serviços como envio de informes sobre andamento de documentos, avulsos ou processos, via correio eletrônico (e-mail).

A iniciativa permite que o Governo Federal promova a melhoria da prestação de informações e serviços à sociedade, principalmente em um momento onde a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) tem grande visibilidade e a celeridade na identificação e no resgate de dados é crucial para sua efetividade. Além disso, o projeto está em conformidade com a simplificação do atendimento ao cidadão prevista no Decreto Cidadão (Decreto nº 6.932, de 11 de agosto de 2009).

Este documento apresenta o manual técnico de uso do Cliente Web Service do Sistema Protocolo Integrado. Dadas as informações extraídas no formato esperado pelo Sistema Protocolo Integrado, a ferramenta realiza o envio das informações via Web Service e pode ser reutilizada pelos órgãos e entidades para que haja maior economicidade na implementação da integração ao referido sistema.

ANA MARIA VIEIRA NETO

Diretora

CAPÍTULO I – O CLIENTE WEB SERVICE

1.1 INTRODUÇÃO

Este documento apresenta um manual de utilização do cliente Web Service do Sistema Protocolo Integrado. A tabela 1 contém as URLs dos ambientes do Web Service do Sistema Protocolo Integrado.

Ambiente	URL
Homologação	https\://homologa.protocolointegrado.gov.br/ProtocoloWS/integrad orService?wsdl
Produção	https\://protocolointegrado.gov.br/ProtocoloWS/integradorService ?wsdl

Tabela 1: URL dos WebServices

Obs.: O caracter “\” antes do “:” nas URLs deve estar presente no arquivo de configuração do cliente, para que haja a leitura correta da URL de conexão pelo sistema operacional.

O cliente utiliza o método **getQuantidadeMaximaDocumentosPorRequisicao** para obter o tamanho máximo do lote de documentos que o Web Service aceita. Depois disso, irá fazer quantas requisições forem necessárias ao método **enviarListaDocumentos** para enviar as informações de todos os documentos, em lotes contendo a quantidade máxima de documentos aceita, existentes no arquivo de entrada. Essas chamadas ao método **enviarListaDocumentos** são feitas em paralelo.

Ao final do processamento, um arquivo de log é gerado, contendo os resultados do processamento das informações de cada um dos documentos. Caso algum documento seja rejeitado pelo Web Service, um arquivo contendo esses documentos é gerado para análise, correção e reenvio.

1.2 INSTALAÇÃO DO CERTIFICADO DIGITAL

A comunicação com o Web Service é feita através do protocolo HTTPS e por isso, é necessário instalar o certificado do Protocolo Integrado. Para instalar o certificado, é necessário importar o certificado para um arquivo Keystore do Java que contém os certificados confiáveis (trust store).

Para instalar o certificado em uma trust store, é necessário executar o seguinte comando:

```
keytool -import -trustcacerts -alias protocolo -file certificado-protocolo.cer -keypass  
PASSWORD -keystore CAMINHO
```

Onde:

1. keytool – ferramenta de administração de chaves e certificados. Localizado em: \$JAVA_HOME\bin
2. CAMINHO - localização da trust store do java, por ex.: "C:\Program Files (x86)\Java\jdk1.6.0_45\jre\lib\security\cacerts"
3. certificado-protocolo.cer - certificado do Protocolo Integrado. A versão para o ambiente de homologação encontra-se em:
http://comprasgovernamentais.gov.br/arquivos/certificado_homologacao.cer.
A versão para ambiente de produção encontra-se em:
http://comprasgovernamentais.gov.br/arquivos/certificado_producao.cer.
4. PASSWORD – senha para adicionar certificados. Caso ninguém tenha alterado, a senha padrão é **changeit**.

A lista abaixo contém as localizações normalmente utilizadas pelo Java para armazenar a trust store padrão:

1. \$JAVA_HOME/lib/security/jssecacerts
2. \$JAVA_HOME/lib/security/cacerts

Dependendo das configurações de instalação é possível que o Java utilize outra trust store como padrão. Para maiores detalhes, verifique

1.2 ARQUIVO DE CONFIGURAÇÃO DO CLIENTE

Para configurar o cliente, basta editar o arquivo config.properties, que fica no mesmo diretório do pacote .jar da aplicação cliente.

Configuração	Descrição
wSDL	Localização do arquivo de descrição(wSDL) do webservice a ser chamado pelo cliente. Ver Tabela 1.
codsiorg	Código siorg do órgão que deseja enviar as informações para o Protocolo Integrado.

senha	Senha de integração do órgão que deseja enviar as informações para o Protocolo Integrado.
numero-tentativas	Quantidade de tentativas de reenvio que será feita em caso de falha de conexão.
segundos-entre-tentativas	Intervalo, em segundos, aguardado antes da realização de uma nova tentativa de envio em caso de erro. O Valor mínimo para este parâmetro é de 10 segundos. O sistema utilizará este valor caso um valor inferior seja informado.

Tabela 2: Configurações do Cliente

1.3 UTILIZAÇÃO DO CLIENTE

Os seguintes passos são necessários para executar o cliente:

1. Iniciar o terminal de comando;
2. Navegar até o diretório onde esta localizado o cliente.jar;
3. Executar o seguinte comando: `java -jar cliente.jar arquivo.xml`. Onde “arquivo.xml” é o arquivo que contém os documentos a serem enviados para o Web Service.

Para informações sobre o arquivo.xml, consultar a seção 1.4 ARQUIVO DE ENTRADA

Após a execução, o arquivo “arquivo.log” possuirá um relatório sobre a execução. Os documentos que porventura tiverem sido rejeitados pelo webservice estarão em “arquivo-rejeitados.xml”.

1.4 ARQUIVO DE ENTRADA

O arquivo .xml deve conter uma lista de documentos na forma:

```

<ListaDocumentos>

    <Documento>...</Documento>

    <Documento>...</Documento>

    <Documento>...</Documento>

    ...

</ListaDocumentos>

```

O conteúdo dentro das tags <Documento></Documento> deve estar em conformidade com o padrão de dados do Sistema Protocolo Integrado.

A lista pode conter quantos documentos forem desejados, porém pode ser necessário aumentar a oferta de memória para o Java de forma que o cliente consiga ler todo o arquivo (ver Problema 2, na seção CAPÍTULO II – SOLUÇÃO DE PROBLEMAS).

O arquivo deve estar codificado em UTF-8 para que não ocorram problemas de codificação de caracteres.

CAPÍTULO II – SOLUÇÃO DE PROBLEMAS

Problema 1: Ao utilizar o cliente, a seguinte mensagem é exibida no terminal:

```
com.sun.xml.internal.messaging.saaj.client.p2p.HttpSOAPConnection      post
Grave: SAAJ0009: Message send failed
```

Solução: Esse problema está relacionado com a instalação do certificado em uma trust store diferente da que o Java está utilizando por padrão. Existem duas formas de solucionar:

1. Indicar, na hora de executar o cliente, a localização da trust store que deseja utilizar:

```
java -jar -Djavax.net.ssl.trustStore=CAMINHO cliente.jar arquivo.xml
```

Onde, CAMINHO, é a localização da trust store em que o certificado foi instalado.

2. Outra solução, é verificar qual trust store está sendo utilizada pelo sistema e então, instalar o certificado nesta. Uma das formas de verificar a localização da trust store é executar o cliente com o seguinte argumento `-Djavax.net.debug=all` e direcionar a saída da execução para um arquivo de texto. Ou seja, executar o seguinte comando:

```
java -jar -Djavax.net.debug=all cliente.jar teste.xml > saida.txt
```

Ao inspecionar o arquivo `saida.txt`, procurar pela linha que começa com “trustStore is: “. Nesta linha está a localização da trust store que está sendo utilizada pelo sistema. Deve-se então, repetir a instalação do certificado nesta trust store.

Problema 2: Ao executar o cliente é exibido um erro de memória Heap insuficiente.

Solução: Existem duas soluções possíveis:

1. Aumentar a memória Heap disponível para a JVM por meio do parâmetro `-Xmx`. Por exemplo, executar o cliente da seguinte forma:

```
java -jar -Xmx1024m cliente.jar arquivo.xml
```

O valor 1024m indica que serão disponibilizados até 1GB de memória para a Heap da JVM.

2. Reduzir o tamanho do arquivo a ser carregado pelo cliente até que o mesmo possa ser carregado no cliente.