Manual WS-Signer

Histórico da Revisão

Versão	Descrição	Autor	Aprovação	Data
1.0	Criação do documento	Késsia Barbosa		06/08/2013
1.1	Revisão do documento	Marcos Godinho		07/08/2013
1.2	Atualização do documento	Eduardo Soares		09/01/2015
1.3	Revisão do documento	Alex Oliveira		23/02/2015

Sumário

Table of Contents

1 Introdução

Este documento tem por objetivo auxiliar os desenvolvedores à realizarem a configuração do Web Service Signer (WS-Signer) para a integração com os serviços disponíveis. Este Web Service realiza a autenticação das requisições usando WS-Security aos servidores.

2 Terminologias

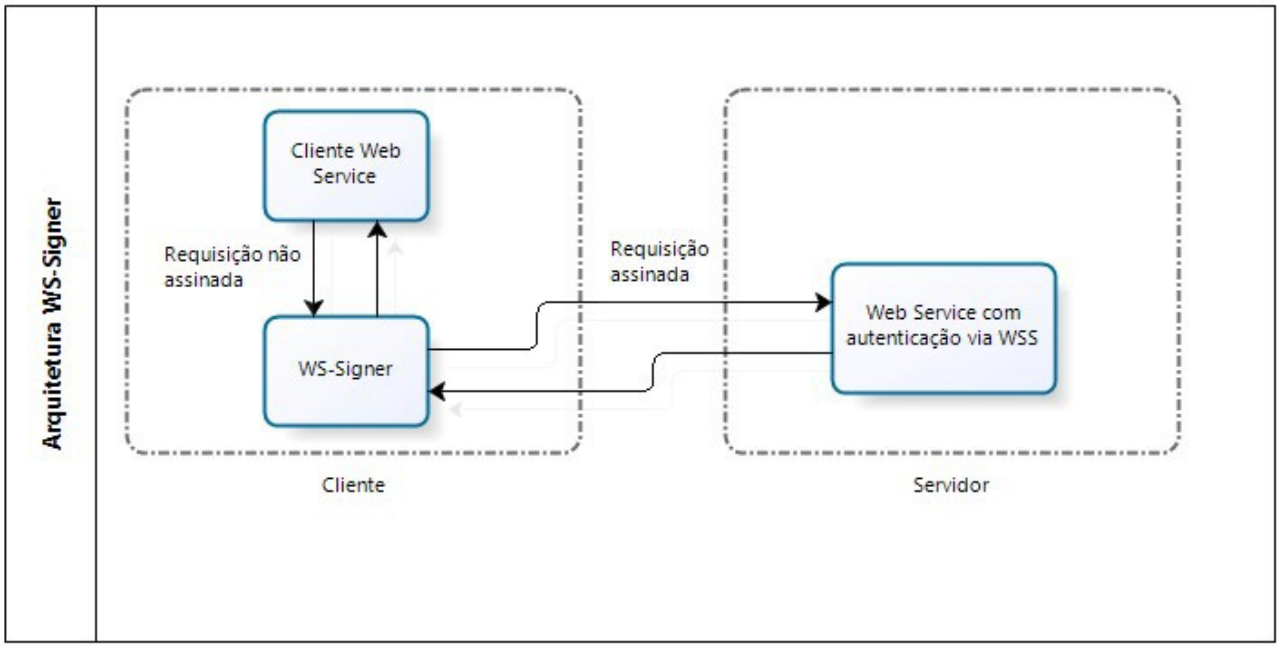
A fim de facilitar o entendimento deste documento, utilizaremos as seguintes siglas e terminologias:

- WS – Web Service;
- SOAP – Simple Object Access Protocol;
- WSS – Web Services Security;
- AR – Autoridade de Registro;
- AC – Autoridade Certificadora;
- MCC – Mobile Certificate Central;
- RS – Restful web-service;
- MSS – Mobile Signature Server;

3 Autenticação e o WS-Signer

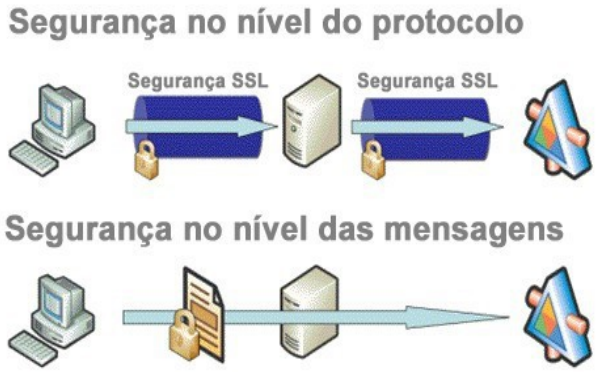
O processo de autenticação dos nossos serviços é realizado com um certificado digital ICPBrasil de equipamento, emitido em nome de uma pessoa jurídica. O certificado é utilizado para assinar todas as requisições SOAP utilizando o padrão WS-Security, para certificados X.509.

Para facilitar a implementação da assinatura das requisições, é disponibilizado um proxy de assinaturas, chamado WS-Signer, que recebe as requisições do cliente SOAP, as assina, e repassa as requisições para o servidor.



4 O padrão WS-Security

O WS-Security padroniza autorização, criptografia e processamento de assinaturas digitais em Web Services. Ele, ao contrário dos modelos de segurança de transporte, como o SSL, aplica segurança diretamente aos elementos da mensagem do Web Service.



O WS-Security aumenta a flexibilidade de seus Web Services, mantendo a segurança do sistema independe da camada de transporte. Uma das formas de realizar a autenticação é pela assinatura do corpo da mensagem e a assinatura gerada é inserida no header da mensagem.

Para mais informações sobre esse procedimento ler a especificação da biblioteca no endereço: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf.

5 Configurações do WS-Signer

Esta seção descreve as configurações necessárias para utilizar o WS-Signer.

5.1 Configuração inicial

A comunicação do WS-Signer com os nossos servidores deve ser configurada no arquivo config.xml na pasta config. Esse arquivo já vem com as configurações para servidores locais (hostname localhost).

O primeiro bloco do arquivo declara o certificado usado para assinar as requisições e os certificados confiáveis para autenticar os servidores MCC e MSS. Esses campos devem ser alterados com os dados do certificado a ser utilizado para a assinatura. Este bloco contém:

- O nome do arquivo, relativo à pasta home do WS-Signer;
- O tipo da keystore – normalmente PKCS12 é o formato exportado pelo browser;
- O alias de identificação do certificado dentro da keystore.

Exemplo:

```
<certificates>
  <signing-certificate>
        <keystore-file>40784776000164.p12</keystore-file>
        <keystore-type>PKCS12</keystore-type>
        <key-alias>40784776000164</key-alias>
  </signing-certificate>
</certificates>
```

O segundo bloco declara os servidores a serem comunicados com o serviço. Nesta parte são feitas as configurações do próprio WS-Signer (proxy), do MCC e do MSS. No exemplo abaixo o WS-Signer responde por requisições no endereço localhost:8280:

```
<servers>
  <local-server name="proxy">
        <host-name>localhost</host-name>
        <port-number>8280</port-number>
  </local-server>
</servers>
```

O último bloco não precisa ser alterado. Ele define as configurações de redirecionamento dos serviços. Cada soap-redirect cria um SOAP web service no servidor local (WS-Signer) que recebe requisições, assina-as e envia-as ao servidor remoto (MCC ou MSS). A configuração rest-redirect cria um REST web service que recebe requisições HTTP e reenvia usando HTTPS com autenticação de cliente.

5.2 Inicialização do serviço

A inicialização do WS-Signer é feita através do script ws-signer.sh (ou .bat) localizado na pasta raiz do WS-Signer. Ao inicializar o arquivo deverá ser infomado a senha do certificado a ser utilizado. Nesse caso o serviço deve ser inicializado manualmente.

Uma alternativa para inicialização automática do serviço é a configuração da senha do certificado em uma variável de ambiente denominada “WS_SIGNER_PASSWORD”. Dessa forma a senha será lida da variável e não será requisitada durante a execução do script de início.

5.3 Utilizando o serviço

Durante a realização de requições aos serviços deve adicionar um endpoint apontando para o WS-Signer que foi configurado no config.xml.

O WSDL do endpoint do MCC, disponibilizado pelo proxy, é acessível em:

http://<hostname-ws-signer>:<port-number-ws-signer >/mcc/serviceRa.wsdl

O WSDL do endpoint do MSS, disponibilizado pelo proxy, é acessível em:

http://<hostname-ws-signer>:<port-number-ws-signer>/mss/serviceAp.wsdl