Manual do Usuário - Autenticação

Plataforma de Integração

Histórico de Revisões

Data	Versão	Descrição
01/08/2014	1.0	Criação do documento
04/08/2014	1.1	Revisão

Índice

1. Introdução

Este documento tem como objetivo apresentar um guia para conexão e autenticação à Plataforma de Integração da CCEE. A Plataforma de Integração é baseada na troca de mensagens entre sistemas, utilizando a tecnologia web services SOAP. Para cada operação, as mensagens devem ser enviadas em conformidade com o documento WSDL específico. Além disso, os padrões de segurança estabelecidos pela CCEE devem ser observados, a saber:

- HTTPS com autenticação SSL mútua (*2-way SSL*)
- WS-Security com UsernameToken

2. Requisitos de segurança

Para garantir a integridade e segurança das transações enviadas para os web services da CCEE, o cliente deverá se preocupar com dois aspectos: a autenticação SSL mútua e a aplicação do WS-Security header na mensagem SOAP.

2.1. Autenticação SSL

O primeiro nível de segurança é aplicado no momento em que a comunicação entre o servidor do cliente e o servidor da Plataforma de Integração da CCEE. A transmissão é feita sobre o protocolo HTTPS, e uma autenticação SSL mútua é obrigatória. Isto significa que o cliente, no momento em que decide se comunicar com a CCEE, deve:

- Verificar e confiar no certificado público apresentado pelo servidor CCEE;
- Apresentar um certificado privado, sendo que a chave pública desse certificado foi previamente enviada à CCEE.

O certificado público do cliente, uma vez enviado à CCEE, é instalado nos servidores da Plataforma de Integração e será usado para validar se o certificado privado apresentado pelo cliente é o mesmo que está habilitado no lado da CCEE. Somente após a verificação e troca dos certificados a conexão HTTPS será estabelecida.

A figura abaixo descreve como a autenticação mútua SSL ocorre:

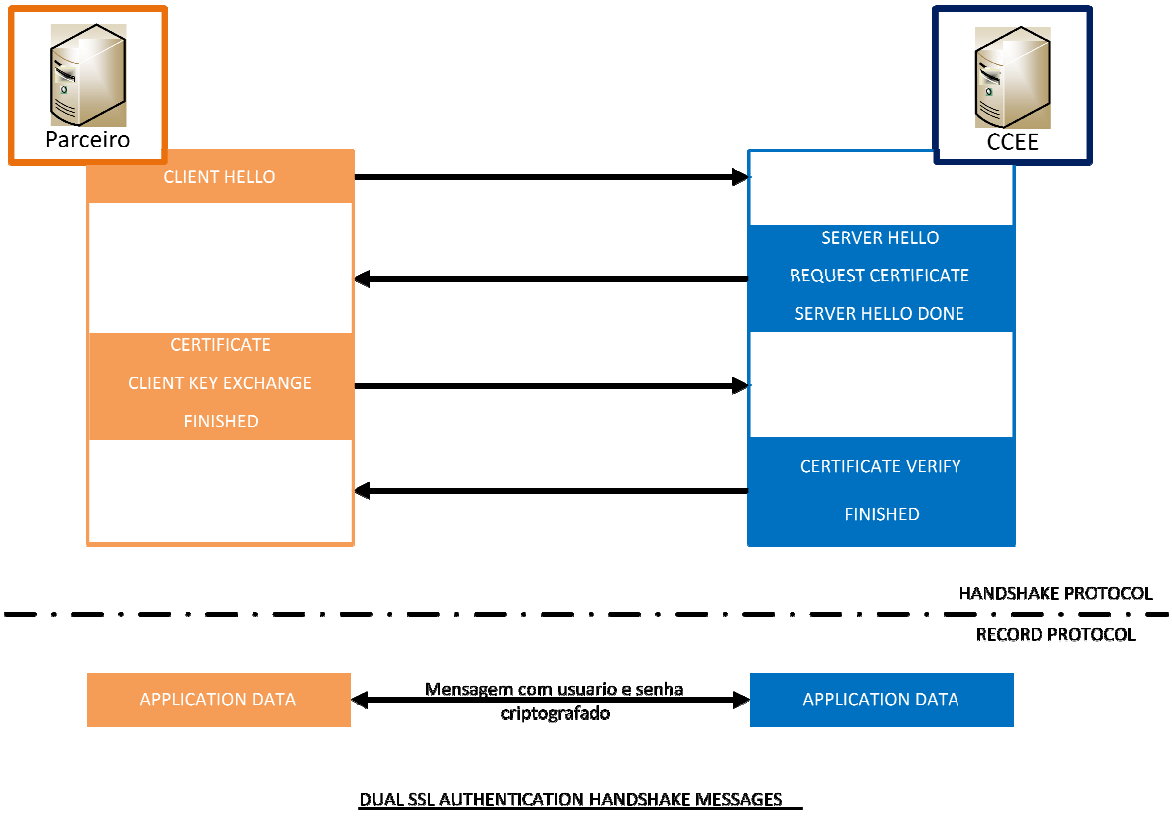

Figura 1 - Autenticação mútua SSL

A maneira como cada linguagem de programação ou software implementa soluções em SSL para o estabelecimento da conexão HTTPS irá variar. Para um melhor entendimento conceitual sobre o tema, recomendamos a leitura da especificação oficial do protocolo: http://tools.ietf.org/html/rfc2818 - Mais informações em como programar uma comunicação SSL com uma determinada linguagem poderão facilmente encontradas na internet.

2.1.1. WS-Security

Web Services Security (também conhecido como WS-Security ou WSS), é uma especificação oficial para Web Services, sendo o padrão para aplicação de padrões de segurança em mensagens SOAP.

A especificação do WSS é publicada pela OASIS (*Organization for the Advancement of Structured Information Standards*). A *feature* adotada pela CCEE, dentro do WSS, será o *UsernameToken*. Isto significa que, em cada mensagem SOAP enviada para a CCEE, o cliente deverá apresentar uma credencial (usuário e senha), que serão adicionados aos elementos seguindo o padrão WSS. A transação só será aceita pela plataforma de Integração após a validação destas credenciais.

O exemplo abaixo mostra os elementos de WS-Security contendo o UsernameToken:

```
<wsse:Security
   soapenv:mustUnderstand = "0"
   xmlns:wsse = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
   xmlns:wsu = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <wsse:UsernameToken wsu:Id = "UsernameToken-1">
      <wsse:Username>usuario123</wsse:Username>
      <wsse:Password Type = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
profile-1.0#PasswordText">senha123</wsse:Password>
   </wsse:UsernameToken>
</wsse:Security>
```

Figura 2 - Os elementos do WS-Security com UsernameToken

Considerando a operação helloWorld presente no web service PingService (mais detalhes sobre o serviço mais adiante), a mensagem de request ficaria assim (adicionando o UsernameToken):

```
<soapenv:Envelope
   xmlns:soapenv = "http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:mes = "http://integration.CCEE.org.br/ws/common/MessageHeader"
   xmlns:hel = "http://integration.CCEE.org.br/ws/operation/HelloWorld">
   <soapenv:Header>
      <wsse:Security
         soapenv:mustUnderstand = "0"
         xmlns:wsse = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
         xmlns:wsu = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
         <wsse:UsernameToken wsu:Id = "UsernameToken-1">
            <wsse:Username>usuario123</wsse:Username>
            <wsse:Password Type = "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
profile-1.0#PasswordText">senha123</wsse:Password>
         </wsse:UsernameToken>
      </wsse:Security>
      <mes:messageHeader>
         <mes:codigoPerfilAgente >1234</mes:codigoPerfilAgente >
      </mes:messageHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hel:helloWorld>
         <hel:nome>Meu Nome</hel:nome>
      </hel:helloWorld>
```

```
  </soapenv:Body>
</soapenv:Envelope>
```

Figura 3 - Mensagem SOAP com o WS-Security Header e UsernameToken

Para ler a especificação oficial desta biblioteca, acesse o site da OASIS com a definição do WS-Security com UsernameToken: https://www.oasis-open.org/committees/download.php/13392/wss-v1.1-spec-pr-UsernameTokenProfile-01.htm

3. Conclusão

Após o estabelecimento da conexão segura SSL e do envio da mensagem com as credenciais de acesso, a Plataforma de Integração validará as credenciais informadas e também se o certificado utilizado para estabelecer a conexão é válido e pertence ao cliente que efetuou a conexão. Em caso positivo, a mensagem será consumida. Caso contrário, a mensagem será rejeitada.

Concluímos então que para utilização dos serviços disponíveis na Plataforma de Integração, é necessário estabelecer a conexão segura SSL entre os servidores e enviar as credenciais de acesso à Plataforma de Integração em cada mensagem trocada.

4. Abreviações, siglas e acrônimos

Sigla	Definição
XML	eXtensible Markup Language
SOAP	Simple Object Access Protocol
WSDL	Web Service Description Language
XSD	Xml Schema Definition
CCEE	Câmara de Comercialização de Energia Elétrica
HTTPS	HyperText Transfer Protocol Secure
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
JDK	Java Development Kit
WSS	Web Service Security
JKS	Java Keystore
HTML	HyperText Markup Language
JAR	Java ARchive
IDE	Integrated Development Environment

5. Referências

Sigla	Definição
Apache Axis 1.x, 2.x	http://ws.apache.org/axis/
HTTP	http://www.w3.org/Protocols/rfc2616/rfc2616.htm
SOAP 1.1	http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
WSDL 1.1	http://www.w3.org/TR/2001/NOTE-wsdl-20010315
Web Services Security 1.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
XML 1.1	http://www.w3.org/TR/xml11/
XML Schema 1.1	http://www.w3.org/XML/Schema
XML Schema Definition	http://www.w3.org/2001/XMLSchema.xsd
SSL	http://www.ssl.com/
HTTPS	http://tools.ietf.org/html/rfc2818