Sistemas Distribuídos 2016/2017

Relatório da 3º Parte do Projeto
Segurança

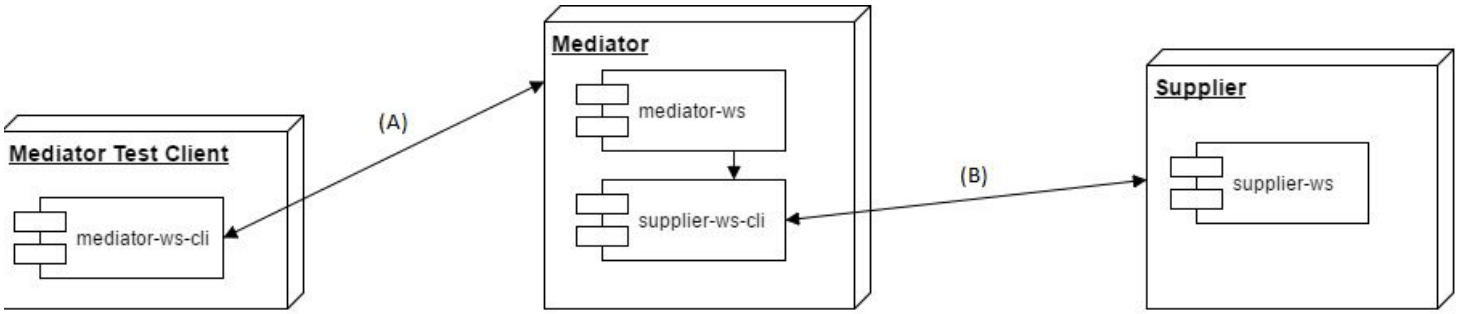
Grupo A50
Repositório Git: https://github.com/tecnico-distsys/A50-Komparator

77459 - Henrique Lourenço

78215 - José Touret

78579 - Pedro Cruz

Figura da Solução



Descrição da Solução

Foram criados handlers dentro dos pacotes da figura: mediator-ws-cli, mediator-ws, supplier-ws-cli e supplier-ws. As chaves e certificados estão todos no security.

- **Confidencialidade (A)**

Na ligação (A) entre mediator-ws-cli e mediator-ws assegura-se a confidencialidade do número de cartão de crédito. No outbound do MediatorClientHandler, vai ser percorrida a mensagem SOAP à procura do elemento que contém o número de cartão de crédito. Assim que o encontra, cifra esse número com a chave pública do A50_Mediator e atualiza a versão encriptada para dentro do envelope. No inbound do MediatorServerHandler, irá ser percorrida novamente a mensagem SOAP até encontrar o elemento do body do envelope que contém o número de cartão de crédito encriptado. Vai finalmente decifrar o número do cartão com a chave privada de A50_Mediator.

Esquema das mensagens SOAP:

```
[2017-05-05T21:53:43.002] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/enve
lope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><cr
editCardNr>4024007102923926</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
[2017-05-05T21:53:43.446] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/enve
lope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><cr
editCardNr>a5o0YkW7lsQVM6DmNRcQ2T489WMDeEhMh5B/jCvOJ+43un5eCvQcIvUcqTzsZsrNQ/3xWiodd272QkXHhbBCq1MGXAesPd1zhHJgyk7md
nTSmP9z2i71QhLSXP8SBCJYKYfgkAfVEVaVvzg4Lt8zoIKpuUufcGjQqb2jZzaqFr2qPw4mrbopuZXgG0lz9eFtV2nKE6FoeYE2IdxLdL2vAUiAGw+oJ
re/k04IFhM1nHpq9sMxf5gnk20e1Qj5vIBNLZ1v/zLQW0JE40UcEA8+CpNyK3+HSnpwKpC6naMqnVZ13//nJ0X0Y5qnstcuTJM6Id6Axrwf3f8nCVqvH
q/nng==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
```

Imagem 1 - MediatorSuppliertHandler - Possível verificar no elemento XML creditCardNr antes e depois de se cifrar

```
[2017-05-05T21:53:43.452] intercepted  INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/enve
lope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><cr
editCardNr>a5o0YkW7lsQVM6DmNRcQ2T489WMDeEhMh5B/jCvOJ+43un5eCvQcIvUcqTzsZsrNQ/3xWiodd272QkXHhbBCq1MGXAesPd1zhHJgyk7md
nTSmP9z2i71QhLSXP8SBCJYKYfgkAfVEVaVvzg4Lt8zoIKpuUufcGjQqb2jZzaqFr2qPw4mrbopuZXgG0lz9eFtV2nKE6FoeYE2IdxLdL2vAUiAGw+oJ
re/k04IFhM1nHpq9sMxf5gnk20e1Qj5vIBNLZ1v/zLQW0JE40UcEA8+CpNyK3+HSnpwKpC6naMqnVZ13//nJ0X0Y5qnstcuTJM6Id6Axrwf3f8nCVqvH
q/nng==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
[2017-05-05T21:53:43.860] intercepted  INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/enve
lope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><cr
editCardNr>4024007102923926</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
```

Imagem 2 - MediatorClientHandler - Possível verificar no elemento XML creditCardNr antes e depois de se decifrar.

- **Autenticidade, integridade e frescura das mensagens (B)**

Na ligação (B) entre supplier-ws-cli e supplier-ws pretende-se garantir autenticidade, integridade e frescura nas mensagens. No outbound de SupplierClientHandler, é primeiro adicionado um novo elemento com a data do envio da mensagem ao header e seguidamente assina-se a mensagem SOAP com a chave privada A50_Mediator e adiciona-se essa assinatura também ao header. No inbound do SupplierServerHandler, recebe-se os envelopes provenientes do cliente. Primeiro, através da data recebida, verifica se o envio da mensagem foi feito à mais de 3 segundos, se sim lança uma exceção e desta maneira garante-se a frescura das mensagens. De seguida, verifica se a assinatura está correta, usando a chave pública de A50_Mediator, garantindo-se desta maneira a autenticidade e integridade das mensagens. No outbound do SupplierServerHandler vai realizar o mesmo processo adicionando a data, o nome do servidor respetivo e ainda a assinatura ao header, assinando neste caso usando a chave privada do supplier respetivo. No inbound do SupplierClientHandler, analisa-se a mensagem proveniente do supplier e verifica-se a assinatura da mesma maneira, usando a chave pública do supplier respetivo.

Esquema das mensagens SOAP:

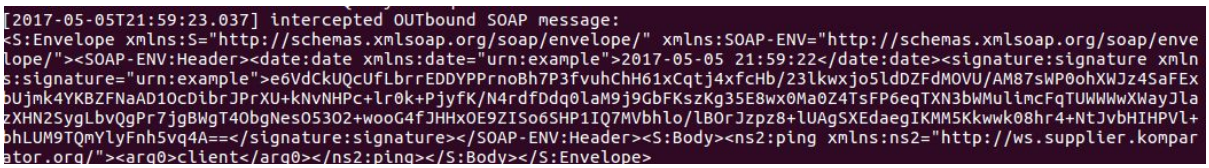


Imagem 3 - SupplierClientHandler - Envelope enviado com a data e a assinatura adicionada ao header do envelope

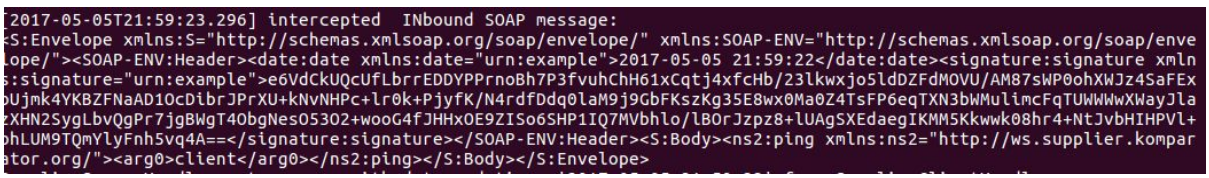


Imagem 4- SupplierServertHandler - Envelope recebido com a data e a assinatura do SupplierClientHandler

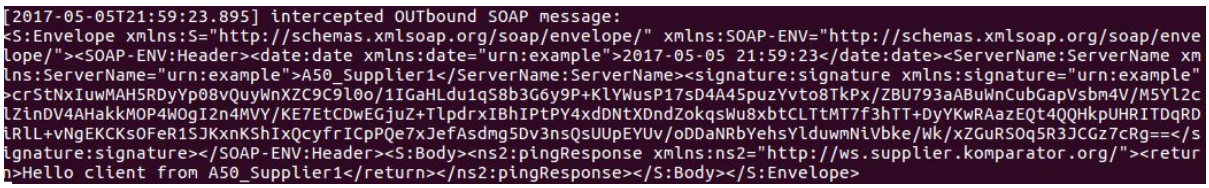


Imagem 5- SupplierServertHandler - Envelope enviado com a data, nome do supplier e assinatura

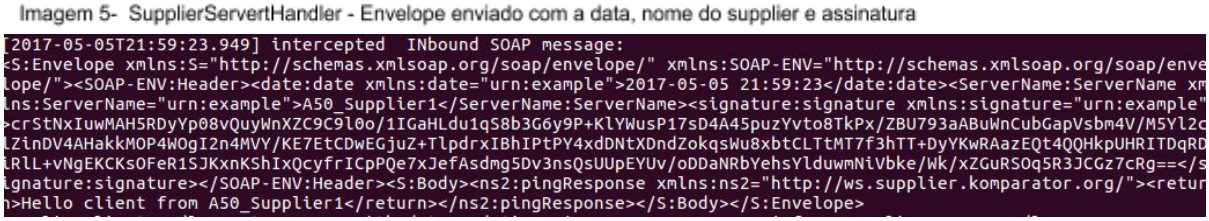


Imagem 6- SupplierClientHandler - Envelope recebido com a data, nome do supplier e a assinatura