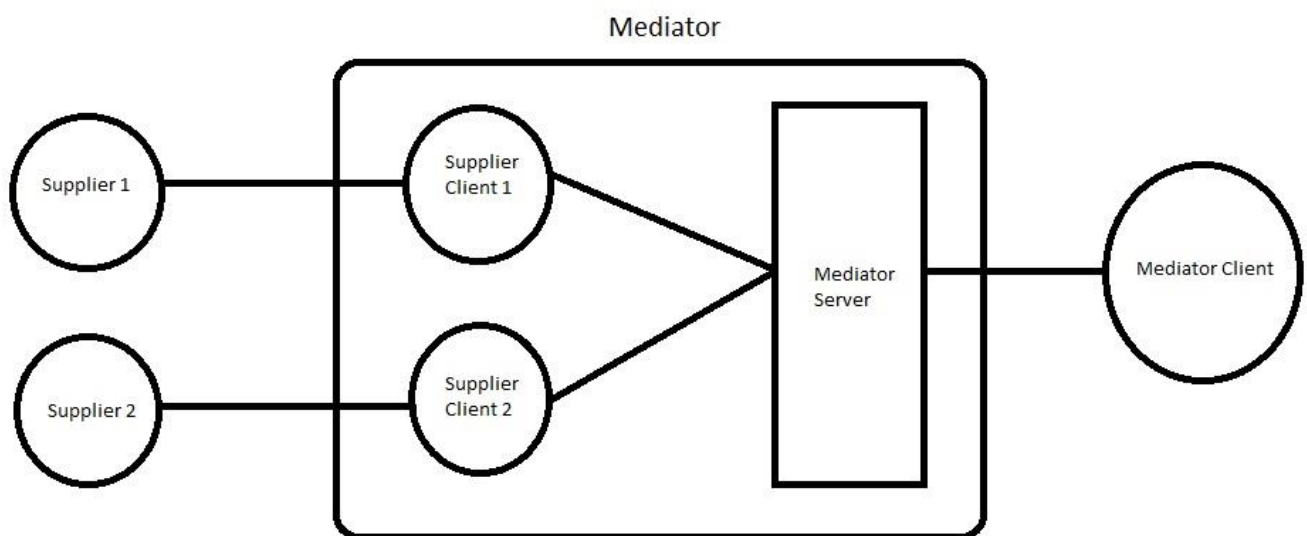




## *Relatório de Segurança*

### Diagrama de Segurança



#### **Grupo - T21:**

- Ruben Condesso - 81969
- Miguel Carreiro - 82012
- João Raimundo - 77064

## Envelopes e Processamento de Handlers

Tanto no Supplier como no Supplier Client há 3 handlers cada um com uma função específica.

De acordo com a Handler-Chain definida no Supplier e no Supplier Client é primeiramente executado o *LoggingHandler* seguido do *HeaderHandler*, depois o *SupplierSecurityHandler* e por fim é executado novamente o *LoggingHandler*. Os handlers têm as seguintes finalidades:

- O *LoggingHandler* tem como finalidade imprimir a mensagem no terminal.
- O *HeaderHandler* é responsável por adicionar um cabeçalho com a indicação do Timestamp (data e hora de criação da mensagem), garantindo assim a sua vivacidade.
- O *SupplierSecurityHandler* trata de garantir a autenticidade e integridade da mensagem adicionando um cabeçalho com uma assinatura gerada através do conteúdo da mensagem.

No canal de comunicação dos Mediators há 2 handlers, um do Client e um do Server. No cliente existe o *MediatorClientSecurityHandler*, unicamente responsável por processar mensagens de saída em que é chamada a função *BuyCart*, encriptando o número do cartão de crédito usando a chave pública do mediador.

No lado oposto (no servidor) apenas são processadas mensagens de chegada que contenham o método *buyCart*. Nesse caso o *MediatorServerSecurityHandler* é responsável por descriptar o número do cartão de crédito.

## Segurança

Quando a mensagem é recebida quer pelo Supplier quer pelo Supplier Client, este retira o cabeçalho da assinatura da mensagem e compara o conteúdo da mensagem final com o conteúdo presente na assinatura. Se for igual garante-se assim a autenticidade da mensagem.

Adicionalmente, antes de a mensagem ser enviada vai ser encriptada com a chave privada de quem envia. Quem recebe a mensagem não possui ainda a chave para descriptá-la. De seguida tem que ir à CA pedir a chave pública que necessita. Mas não podemos usar esta mesma chave sem antes assegurar que consultámos a CA autêntica então temos que comparar com a chave pública da CA que foi inserida em todos os módulos previamente, de maneira segura.

Relativamente à frescura, é analisado o timestamp da mensagem e comparado com a hora em que foi recebida. De acordo com o que definimos, se ultrapassar os 3 segundos a mensagem é descartada.

```
[2017-05-05T13:51:30.458] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCar
t xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>xyz</cartId><creditCard
Nr>1234567890123452</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
AddHeaderHandler: Handling message.
Writing header in outbound SOAP message...
[2017-05-05T13:51:32.569] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCar
t xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>xyz</cartId><creditCard
Nr>d17/CrnuP7p63PButYk6lQp+Bq8qQVeGH+050ACN0x0PXThxR4AVM+vIJPZ3oqyRl+uhdyta54zHx
QTq7rmzm2yQZ3uMrmov2UZ//a1N1BQIp4/CmaROCDuLAVkdAzOKXWAFoI9mfcli9nAhDIzkwYfEKQzkU
Q6fCHZ5AE1PxRyLnIwqt+C0yJw3MLf5jjLDYtDGLewAYK056446rrgnWKnPV/5fcVDKuqXIC8XSAAJwn
n/mp63Ty0rweOFWfjwrnn8DyxuLZju0tL0JXvUt53WL1z/+UQH/aFo+vKF/Fg+MnwL4GES9F26GNVApB
tBuXzDb4926bQmKFFd73RWiTQ==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
```

Mensagem referente ao método buyCart, enviada do Mediator Client para o Mediator Server

```
[2017-05-05T13:50:20.552] intercepted INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCar
t xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>xyz</cartId><creditCard
Nr>H69JZVKg+pjkX3t/c05wMDpRSuLLyy5J0+gMGSTQHARWQ/ZFoEosGJk/sphqJY3Knv8j+R0S6809H
4jkGhIrH50KU9gkFEkFrX7VBPYaaCL8VUBBFuAE/oD8AgM6Pow44WaiPREwdG/5V/eB76mahARNwQ167
dFqjm6xjhHAbysNGgNT5uEEAaDw26wZTVUUsmXpk1jXVezix3mQElhx98z5/GQC1huq6YjuWwZa9Pl+
0j8J4BcD2Lw5DclbSPuW08akL/8GfU6ciJu7/kdvFD+8ySx9jBvNdVsPwAF/fvZsPmCJ811/LqewuYp6
l4rTPX2V2LVC3Apy9kTy910HA==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
AddHeaderHandler: Handling message.
Reading header in inbound SOAP message...
[2017-05-05T13:50:20.582] intercepted INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCar
t xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>xyz</cartId><creditCard
Nr>1234567890123452272828280228</creditCardNr></ns2:buyCart></S:Body></S:Envelop
e>
```

Mensagem referente ao método buyCart, enviada do Mediator Server para o Mediator Client

```
[2017-05-05T13:56:11.111] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:ping x
xmlns:ns2="http://ws.mediator.komparator.org/"><arg0>Mediator_client</arg0></ns2:
ping></S:Body></S:Envelope>
AddHeaderHandler: Handling message.
Writing header in outbound SOAP message...
[2017-05-05T13:56:11.182] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:ping x
xmlns:ns2="http://ws.mediator.komparator.org/"><arg0>Mediator_client</arg0></ns2:
ping></S:Body></S:Envelope>
[2017-05-05T13:56:11.946] intercepted INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:pingRe
sponse xmlns:ns2="http://ws.mediator.komparator.org/"><return>Ping with mediator
and all registered suppliers done</return></ns2:pingResponse></S:Body></S:Envel
ope>
AddHeaderHandler: Handling message.
[2017-05-05T13:56:11.948] intercepted INbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:pingRe
sponse xmlns:ns2="http://ws.mediator.komparator.org/"><return>Ping with mediator
and all registered suppliers done</return></ns2:pingResponse></S:Body></S:Envel
ope>
```

Mensagem referente ao método ping, enviada do Mediator Client para o Mediator Server

```
[2017-05-05T13:56:11.943] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:pingRe
sponse xmlns:ns2="http://ws.mediator.komparator.org/"><return>Ping with mediator
and all registered suppliers done</return></ns2:pingResponse></S:Body></S:Envel
ope>
AddHeaderHandler: Handling message.
[2017-05-05T13:56:11.943] intercepted OUTbound SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="
http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:pingRe
sponse xmlns:ns2="http://ws.mediator.komparator.org/"><return>Ping with mediator
and all registered suppliers done</return></ns2:pingResponse></S:Body></S:Envel
ope>
```

Mensagem referente ao método ping, enviada do Mediator Server para o Mediator Client