# Relatório
# Sistemas Distribuídos 2016/17

## Grupo A42:

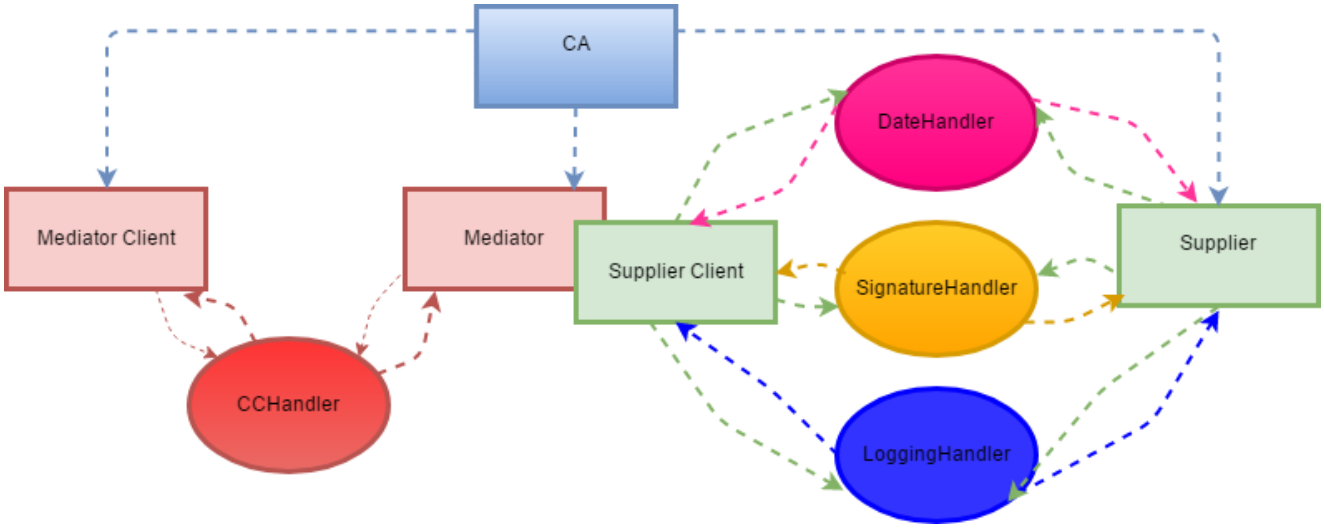
**Github**: https://github.com/tecnico-distsys/A42-Komparator.git


81172
Carolina Xavier

81186
Stéphane Duarte

81328
Inês Leite

# Segurança




**Comunicação entre Supplier e SupplierClient**

A nossa comunicação entre o Supplier Client e o Supplier é feita através de suporte a Handlers (DateHandler, SignatureHandler, LoogingHandler) que garantem a segurança da ligação Supplier-SupplierClient recorrendo a um modelo de certificação que é garantido através da existência da entidade Certificate Authority (CA).

O CA emite um certificado através do qual é possível gerar chaves públicas.

Cada vez que uma mensagem chega duma entidade que está ligada a um destes handlers estes vão provocar alterações nas mensagens SOAP trocadas entre as duas entidades:

- O **LoggingHandler** imprime a SOAPMessage actual;

- O **DateHandler** acrescenta um cabeçalho simples (header) à saída do cliente (outbound message) com a data e hora atual. Caso a diferença temporal seja maior do que 3 segundos, deve rejeitar a mensagem. Este handler vai garantir a frescura da comunicação;

- O **SignatureHandler** acrescenta um cabeçalho simples com o nome da entidade que envia e mensagem e uma assinatura digital forma pelo texto do SOAPBody e o tempo de criação da assinatura (timestamp). Este handler vai garantir a integridade e autenticidade da comunicação.

**Comunicação entre Mediator e MediatorClient**

Cada vez que uma mensagem chega duma entidade que está ligada ao CCHandler este vai provocar alterações nas mensagens SOAP trocadas entre as duas entidades:

- O **CCHandler** permite ao MediatorClient encriptar o número de cartão de crédito na mensagem SOAP enviada para o Mediator de forma a que apenas o Mediator consiga ler esta informação.

# Esquema Mensagens SOAP

Mensagem no supplier com o DateHandler:

Data encontra-se na *tag* de nome 'timestamp':

2017-05-06T21:22:28.886

```
DateHandler: Handling message.
Reading header in inbound SOAP message...
Header date is 2017-05-05T21:22:28.886
[2017-05-05T21:22:29.082] 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><timestamp:timestamp
        xmlns:timestamp="http://timestamp.komparator.org/">2017-05-05T21:22:28.886</timestamp:timestamp></SOAP-ENV:Header><S:Body><ns2:ping
        xmlns:ns2="http://ws.supplier.komparator.org/"><arg0>client</arg0></ns2:ping></S:Body></S:Envelope>
```

Mensagem no supplier com o SignatureHandler

Nome de remetente da mensagem encontra-se na *tag* de nome 'name'

Assinatura digital do remetente da mensagem encontra-se na *tag* de nome 'signature'.

```
SignatureHandler: Handling message.
Reading header in inbound SOAP message...
Mensagem verificada e recebida com sucesso.
[2017-05-05T21:26:45.887] 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><timestamp:timestamp
        xmlns:timestamp="http://timestamp.komparator.org/">2017-05-05T21:26:44.932</timestamp:timestamp><name:name
        xmlns:name="http://name.komparator.org/">A42_Mediator</name:name><sig:signature
        xmlns:sig="http://signature.komparator.org/">DAwNethxYGplDjQZZ62fpz7gdOwlqvlXqjpHclU1Dur0Q184i8am1iGhQ4m4eOoi2+Idp95PkebiiFo
        E6egWFow3Var7pil4py2MljTn2DbSn73iknSOiUvzChIov1tVGEiZcvXYKNZYTHGtfXW7nVIDdH2vAyjX+xCBhneDyB+LaYb8CMe35eDDQjPgJPztssYSf6m5q5J
        lvAf4910LDwrc5XzQ5msMtpxcOQFjDATgqVBRMps9PxeVOvHAVeIy41acKNP8wWhdme3u51szzlU1WCQci6Go0TAvYqvUWYpbYGacH8PR1iZ6hekr/P9YlxCddkq
        4JK9RCxDgCnnL4Q==</sig:signature></SOAP-ENV:Header><S:Body><ns2:ping
        xmlns:ns2="http://ws.supplier.komparator.org/"><arg0>client</arg0></ns2:ping></S:Body></S:Envelope>
```

Mensagem no mediator com o CCHandler:

Na inbound SOAP message o mediator recebe o número de cartão de credito encriptado pelo mediator cliente, encontra-se na *tag* de nome 'creditCardNr'

De seguida o mediator desencripta a o número de cartão de crédito. Encontra-se na *tag* 'creditCardNr'

```
[2017-05-05T23:05:46.430] 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:buyCart
        xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>Cart2</cartId><creditCardNr>fMvcbawqFogm4bJBbvZJV3s7Q5iawRlw/sAhkBNegUV/0dEeusvKhf6U7HuCofO2lYMnvQZCaPCbaLP
            D5v4VDXUCJdilVuWBmUTRg+pqTzAFMArfMlCU1OE2hr53E5ZFzbLBTDMUCK+fBXWDnEVmIG0xIZvxdXexdxIa4mXQqOi4qQN5+h4hasZB/E6lw+Qt/mkhlJWRao93LRPYjqBbw2NmcpCxc8+s6YBNHKRG+Rm2F
            2qOfkk6gfWFyI9gwsJTr+9m8fcoiXMK+mY4wjHJF0BfDPsMX/UGD3BIudmuYCSVLe+Et5GG8uLS5L5qFOQAQmR/IwUhayw7lBSQNqTHKA==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
CreditCardHandler: Handling message.
Reading header in inbound SOAP message...
Numero de cartao de credito desencriptado.
[2017-05-05T23:05:46.476] 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:buyCart
        xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>Cart2</cartId><creditCardNr>4024007102923926</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
```

**AttackHandler-** Criámos um handler de forma a testar as vulnerabilidades do nosso projecto. No AttackTest simulámos a alteração não autorizada de mensagem. Para tal procuramos por um produto com o id "ATTACK" e mudamos o valor de um preço devolvido por um fornecedor.

No entanto não conseguimos finalizar com sucesso esta ideia, mas deixamos o código disponível para consulta.