



**TÉCNICO**  
LISBOA

# Sistemas Distribuídos 2016/2017

## Relatório da 3º Parte do Projeto Segurança

Grupo A50

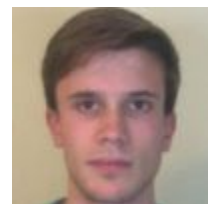
Repositório Git: <https://github.com/tecnico-distsys/A50-Komparator>



77459 - Henrique Lourenço

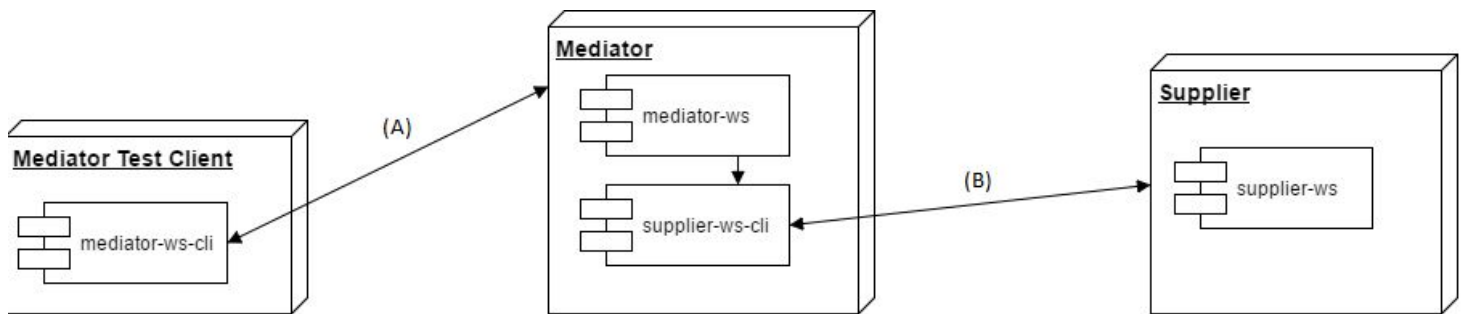


78215 - José Touret



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/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><creditCardNr>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/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><creditCardNr>a500Yk7l5QVM6DmNRcQ2T489WMDDeEhMh5B/jCv0J+43un5eCvQcIvUcQTzsZsrNQ/3xWlodd272QkXHhBBCq1MGXAesPd1zhHJgyk7mdnTSMp9z2i710hLSXP8SBCJYKfGkAFVEVaVvzg4Lt8zoIKpuUufcGjQqb2jZzaqFr2qPw4mrBopuZXgG0lz9eFtV2nKE6FoeYE2IdxLDL2vAUiAGw+oJre/k04IFhM1nHpq9sMxf5gnk20e1Qj5vIBNLZ1v/zLQW0JE40UcEA8+CpNyK3+HSnpwKpC6naMqnVZ13//nJ0X0Y5qnstcuTJM6Id6Axrwf3f8nCVqvHq/nng==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
```

Imagem 1 - MediatorSupplierHandler - 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/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><creditCardNr>a500Yk7l5QVM6DmNRcQ2T489WMDDeEhMh5B/jCv0J+43un5eCvQcIvUcQTzsZsrNQ/3xWlodd272QkXHhBBCq1MGXAesPd1zhHJgyk7mdnTSMp9z2i710hLSXP8SBCJYKfGkAFVEVaVvzg4Lt8zoIKpuUufcGjQqb2jZzaqFr2qPw4mrBopuZXgG0lz9eFtV2nKE6FoeYE2IdxLDL2vAUiAGw+oJre/k04IFhM1nHpq9sMxf5gnk20e1Qj5vIBNLZ1v/zLQW0JE40UcEA8+CpNyK3+HSnpwKpC6naMqnVZ13//nJ0X0Y5qnstcuTJM6Id6Axrwf3f8nCVqvHq/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/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/"><cartId>cid</cartId><creditCardNr>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:

```
[2017-05-05T21:59:23.037] 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><date:date xmlns:date="urn:example">2017-05-05 21:59:22</date:date><signature:signature xmlns:signature="urn:example">e6VdCkUqCfLbrrEDDYPPrnoBh7P3fvuhChH61xQtj4xfChB/23lkwxjo5ldDZFdMOVU/AM87sWP0ohXWJz4SaFExbUjmk4YKBZFNAD10cDibrJPXU+kNvNHPC+Lr0k+Pjyfk/N4rdfDdQ0laM9j9GbfKszKg35E8wx0Ma0Z4TsFP6eqTXN3bWmUlinCfQTUWWWWXWayJLaZxHN2SylLbvQgPr7jgBWgT40bgNes05302+woog4fJHHx0E9ZISo6SHP1IQ7MVBhlo/LB0rJzpz8+LUAgSXEdaegIKMM5Kkwwk08hr4+NtJvbHIHPVl+phLUM9TQmYlyFnh5vq4A==</signature:signature></SOAP-ENV:Header><S:Body><ns2:ping xmlns:ns2="http://ws.supplier.komparator.org/"><arg0>client</arg0></ns2:ping></S:Body></S:Envelope>
```

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

```
[2017-05-05T21:59:23.296] 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><date:date xmlns:date="urn:example">2017-05-05 21:59:22</date:date><signature:signature xmlns:signature="urn:example">e6VdCkUqCfLbrrEDDYPPrnoBh7P3fvuhChH61xQtj4xfChB/23lkwxjo5ldDZFdMOVU/AM87sWP0ohXWJz4SaFExbUjmk4YKBZFNAD10cDibrJPXU+kNvNHPC+Lr0k+Pjyfk/N4rdfDdQ0laM9j9GbfKszKg35E8wx0Ma0Z4TsFP6eqTXN3bWmUlinCfQTUWWWWXWayJLaZxHN2SylLbvQgPr7jgBWgT40bgNes05302+woog4fJHHx0E9ZISo6SHP1IQ7MVBhlo/LB0rJzpz8+LUAgSXEdaegIKMM5Kkwwk08hr4+NtJvbHIHPVl+phLUM9TQmYlyFnh5vq4A==</signature:signature></SOAP-ENV:Header><S:Body><ns2:ping xmlns:ns2="http://ws.supplier.komparator.org/"><arg0>client</arg0></ns2:ping></S:Body></S:Envelope>
```

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

```
[2017-05-05T21:59:23.895] 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><date:date xmlns:date="urn:example">2017-05-05 21:59:23</date:date><ServerName:ServerName xmlns:ServerName="urn:example">A50_Supplier1</ServerName:ServerName><signature:signature xmlns:signature="urn:example">crStNxIuwMAH5RDyYp08vQuyWnXZC9C9l0o/1IGaHLduiqS8b3G6y9P+KLYWusP17sD4A4SpuzYvto8TkPx/ZBU793aABuWnCubGapVsbm4V/M5Yl2cLZindV4AHakkMOP4WogI2n4MVV/KE7EtCDWEGjuZ+TlPdrxIBhIPtPY4xdDntXNdZokqswu8xbtCLTtMT7f3hTT+DyYKwRAazEQ4Q0HkpUHRITDqRDRL+VnGEKCKSoFeR15JXknKShIXqcyfRiCpPQe7xJefAsdmg5Dv3nsQsUUpEYUv/oDDANRbYehsYlduwmNiVbke/wk/xZGuRSQ5R3JCgZ7cRg==</signature:signature></SOAP-ENV:Header><S:Body><ns2:pingResponse xmlns:ns2="http://ws.supplier.komparator.org/"><returnHello client from A50_Supplier1</return></ns2:pingResponse></S:Body></S:Envelope>
```

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

```
[2017-05-05T21:59:23.949] 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><date:date xmlns:date="urn:example">2017-05-05 21:59:23</date:date><ServerName:ServerName xmlns:ServerName="urn:example">A50_Supplier1</ServerName:ServerName><signature:signature xmlns:signature="urn:example">crStNxIuwMAH5RDyYp08vQuyWnXZC9C9l0o/1IGaHLduiqS8b3G6y9P+KLYWusP17sD4A4SpuzYvto8TkPx/ZBU793aABuWnCubGapVsbm4V/M5Yl2cLZindV4AHakkMOP4WogI2n4MVV/KE7EtCDWEGjuZ+TlPdrxIBhIPtPY4xdDntXNdZokqswu8xbtCLTtMT7f3hTT+DyYKwRAazEQ4Q0HkpUHRITDqRDRL+VnGEKCKSoFeR15JXknKShIXqcyfRiCpPQe7xJefAsdmg5Dv3nsQsUUpEYUv/oDDANRbYehsYlduwmNiVbke/wk/xZGuRSQ5R3JCgZ7cRg==</signature:signature></SOAP-ENV:Header><S:Body><ns2:pingResponse xmlns:ns2="http://ws.supplier.komparator.org/"><returnHello client from A50_Supplier1</return></ns2:pingResponse></S:Body></S:Envelope>
```

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