






**TÉCNICO**  
**LISBOA**

## **Sistemas Distribuídos**

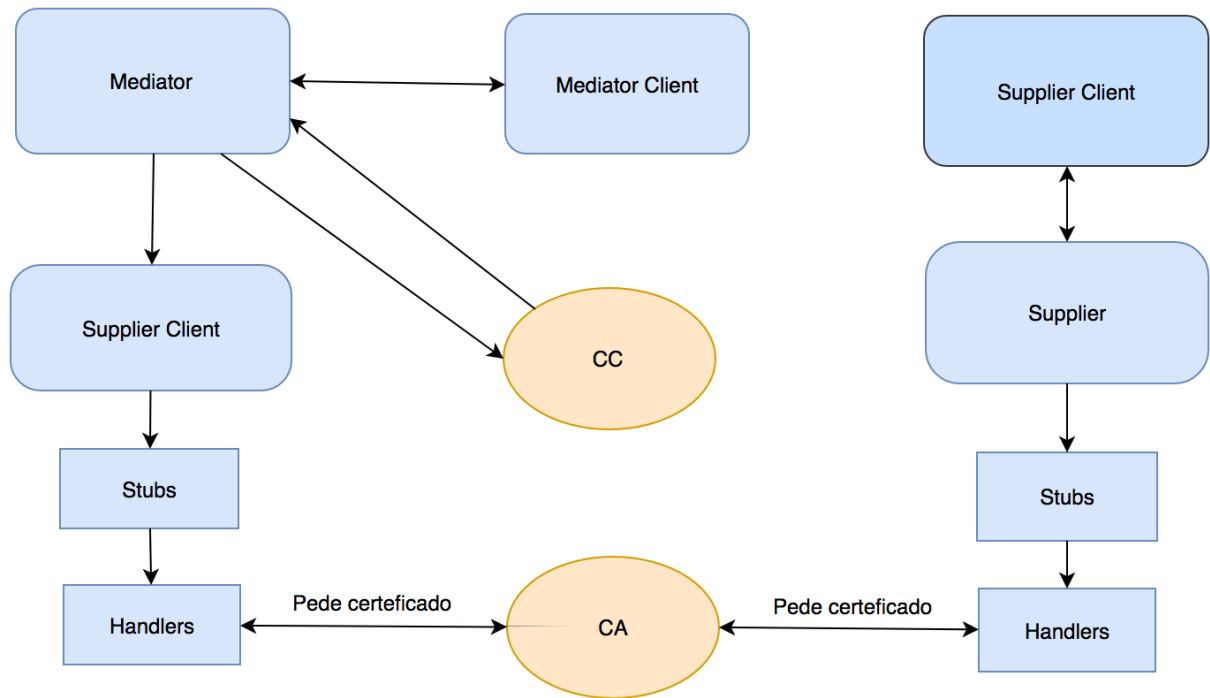
**2016/2017**

**Grupo A65**

		
<b>Pedro Sousa</b>	<b>João Ramos</b>	<b>João Silvestre</b>
<b>78024</b>	<b>80915</b>	<b>80996</b>

<https://github.com/tecnico-distsys/A65-Komparator>

## Segurança



## Autenticidade

- O Supplier Client pede o certificado através do handler.
- O Supplier pede o certificado através do handler.
- A comunicação entre mediator-ws-cli e mediator-ws deve ocultar o número do cartão de crédito da seguinte forma: a mensagem é encriptada com uma public key e desencriptada com uma private key.
- A comunicação entre supplier-ws-cli e supplier-ws é feita através da Digital Signature

## Frescura

Foi possível introduzir frescura nas mensagens com a introdução do timestamp (3 segundos). No entanto têm um ponto fraco que são os replay attacks. É possível um atacante interceptar a mensagem e enviar cópias dela, enviar mais que mensagem igual nesse intervalo podendo comprometer o estado do sistema.

# Esquema das Mensagens SOAP

## Mensagem SOAP com o número do Credit Card não encriptado

```
<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/">
      <creditCardNr>4024007102923926</creditCardNr>
    </ns2:buyCart>
  </S:Body>
</S:Envelope>
```

## Mensagem SOAP com o número do Credit Card encriptado

```
<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/">
      <creditCardNr>o0TRZkFqE87F1UT/sgR4HgQhY5b7q86mXk67hYobZ5s5fsk0bo/
        vWaLaTUPfyBiHTC/1iARrfAF6kgHD0pUUD9UtlmMabaUr49RqZFP/
        oqru1xmpe0kNv8xJcvTD5CL3uE1ZbVpQBqreTsLg+8jdhY1fX3mf8AGSzyBrLlLdyTgu0/
        AEjEtEPLA4eVSs9bu6MMXHoEZ20k+BQa0rka3LGgSNC1+eUfPr6pFI1zvMcgESgT3h02RagI+
        repMmrcJv+
        qJd34PqybB3ENpYbRVPFcRXnD2TVgyK3JQkK1TqFHoMr5zoyVgRgC1LBryihaPelUpLBtdK/
        fPz4FNsZQn3fw==
      </creditCardNr>
    </ns2:buyCart>
  </S:Body>
</S:Envelope>
```

## Mensagem SOAP com a Digital Signature encriptada

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <e:uniqueTime xmlns:e="ut">05/05/2017 22:59:40</e:uniqueTime>
    <e:servicename xmlns:e="sn">A65_Supplier2</e:servicename>
    <e:signature xmlns:e="sg">
      KsLCEfQlvjdsG3bujuxrlqz1FF26B062SsK uXMzx1Qw+xKbubYHoxbZjvkGfqZAo03sU8pT+0
      VNyn1Ey5THEpApE6gD9NqeCvPdxXmkXaz2Q3f7IFcj 45vXEetj7wCQ/sWDJHFsB4BxWkhD3okmXo1/cWjI1jggmDbunBKxhIn+
      cQvaJiDV3RHVkm02UJsc7umB 1BISRXWg+XhtgfkAMFaJL3lX4tr/r3ThDH48iQnJFSuHt9KcepEC8yeCIKMa7OowEP0+
      XxDusf5sq3xQ IWLzsXrxUGHNK9e5ipX81izDm4giiDF5UQkONp/
      hwhvnnizisCFqdVFSAgk4HZKQZQ==</e:signature>
    </SOAP-ENV:Header>
  <S:Body>
    <ns2:createProductResponse xmlns:ns2="http://ws.supplier.komparator.org/" />
  </S:Body>
</S:Envelope>
```

As mensagens SOAP são feitas pela seguinte ordem: primeiro imprime a mensagem SOAP, o handler que verifica a frescura, o handler que adiciona/verifica a assinatura digital (poderá também ter um handler para a encriptação do número de Cartão de Crédito), e por último tem o handler que verifica que a mensagem foi atacada ou não

```
<handler-chains xmlns="http://java.sun.com/xml/ns/javaee">
  <handler-chain>
    <handler>
      <handler-class>org.komparator.security.handler.LoggingHandler</handler-class>
    </handler>
    <handler>
      <handler-class>org.komparator.security.handler.FreshnessHandler</handler-class>
    </handler>
    <handler>
      <handler-class>org.komparator.security.handler.DigitalSignatureHandler</handler-class>
    </handler>
    <handler>
      <handler-class>org.komparator.security.handler.MaliciousAttackHandler</handler-class>
    </handler>
    <handler>
      <handler-class>org.komparator.security.handler.LoggingHandler</handler-class>
    </handler>
  </handler-chain>
</handler-chains>
```