

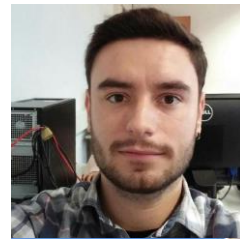
# Sistemas Distribuídos 2016/2017

## Relatório de Segurança (Parte 3 do Projeto)

### Grupo 35

76479

Miguel Marques



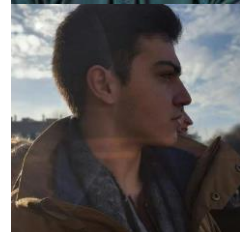
77915

Goncalo Santos



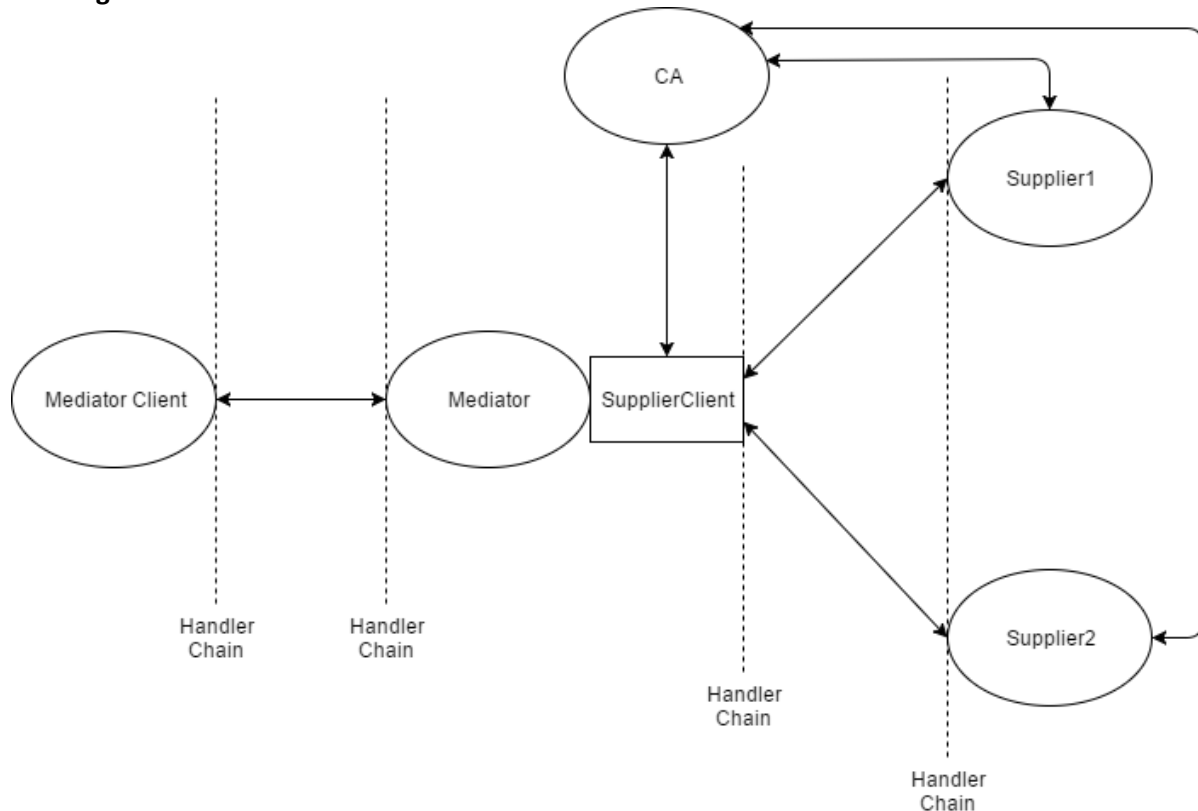
78029

Vasco Pombo



Projeto no website do GitHub: <https://github.com/tecnico-distsys/T35-Komparator>

**Diagrama:**



**Descrição da Figura:**

A comunicação entre as várias aplicações disponíveis na nossa solução é feita com SOAPMessages. Estas mensagens são interceptadas antes do seu envio e/ou recepção pelos Handlers especificados nas handler-chains de cada aplicação.

Estes handlers têm a seguinte funcionalidade:

- Mediator client <-> Mediator:  
Se existir um número de cartão de crédito à saída de uma mensagem, um handler chamado CCHandler encripta-o com a chave pública do Mediator.  
Se existir um número de cartão de crédito encriptado à entrada de uma mensagem, o mesmo handler desencripta-o com a chave privada do Mediator.
- Mediator/SupplierClient <-> Supplier1/Supplier2:  
Existem 3 Handlers em funcionamento:
  - IDHandler  
Adiciona, no Header de uma mensagem de saída, o nome do serviço que a envia, permitindo o acesso às chaves desta.
  - TokenHandler  
Garante a frescura de uma mensagem ao atribuir-lhe um número aleatório. Este número é verificado à chegada da mensagem. Se já tiver sido lido pela aplicação antes, a mensagem é rejeitada.
  - SignHandler  
Se a mensagem for de saída, gera uma assinatura com base no body, token e identificador, encripta-a com a chave privada da aplicação e insere-a no header. Se a mensagem for de entrada, desencripta esta assinatura com a

chave pública da aplicação que a encriptou e verifica-a. Se não forem iguais, rejeita a mensagem.