

Relatório de Segurança

Sistemas Distribuídos

<https://github.com/tecnico-distsys/A67-Komparator>

Grupo A67:



78982
Gonçalo Louro

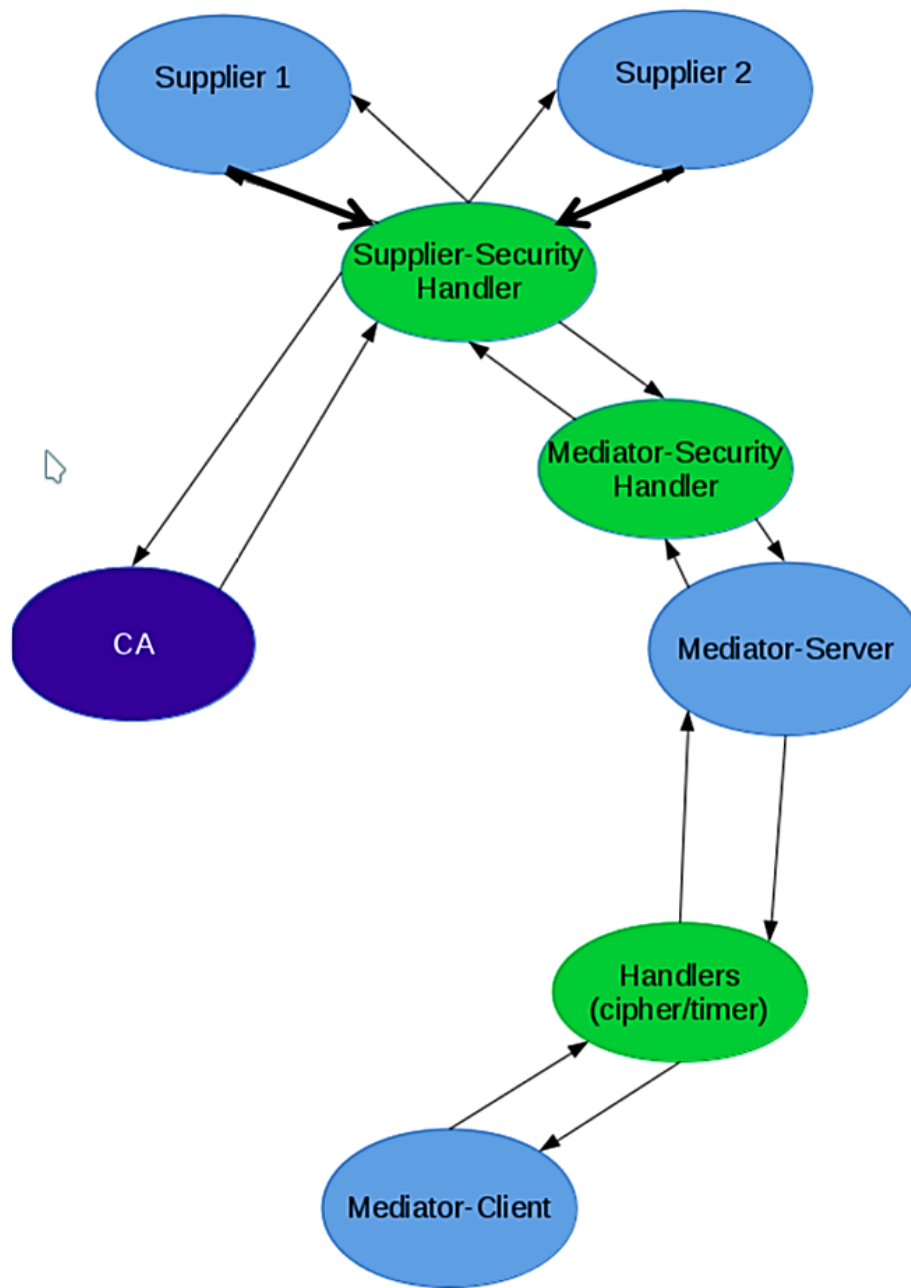


79601
Patrícia Lopes



81700
Sara Azinhal

Modelo de Segurança



A comunicação entre o cliente e o serviço Mediador é feita através de handlers, encarregados de cronometrar o tempo de transmissão das mensagens e cifrar o número de cartão de crédito.

A comunicação entre o Mediador e os Fornecedores é feita através dos handlers de segurança de cada uma das organizações. Estes handlers estão encarregados de assinar as mensagens enviadas por eles com a sua chave privada e também de garantir que as mensagens que lhes chegam vêm assinadas e se a assinatura é válida. Para isso é feita uma comunicação extra para o serviço de Autenticação de Certificados de modo a garantir que o certificado, de onde foram extraídas as chaves da assinatura, é válido.

Demonstração

1. Pedido do Mediator-client para o MediatorsServer e Pedido do Mediator-server para o Supplier

Teste – BuyCartIT#testInvalidCard

Apesar de não ser um pedido-resposta pareceu-nos relevante demonstrar a encriptação do número de cartão de crédito. Podemos verificar que o cartão de crédito é encriptado no handler de encriptação e é enviado encriptado para o fornecedor.

- ## 2. Pedido – Resposta entre o Mediator-ws e o Supplier1

Teste – BuyCartIT#testInvalidCard

Neste exemplo verificamos que o supplier recebe o pedido “getProduct” e devolve a resposta “getProductResponse”.

A nível de segurança verificamos que a mensagem vai assinada no campo <digest> e quando é interceptada pelo SecurityHandler a assinatura é verificada e validada.

[illegible][illegible]