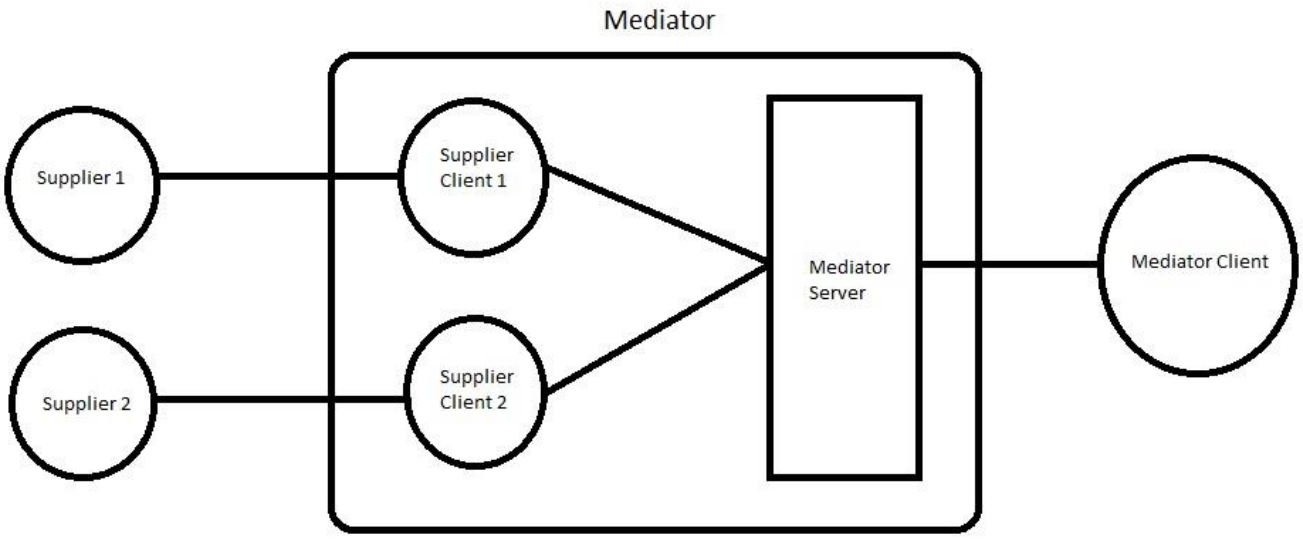
Instituto Superior Técnico – Taguspark

Sistemas Distribuídos

2016/2017 – 2º Semestre

Relatório de Segurança

Diagrama de Segurança



Grupo - T21:

- Ruben Condesso - 81969
- Miguel Carreiro - 82012
- João Raimundo - 77064

Envelopes e Processamento de Handlers

Tanto no Supplier como no Supplier Client há 3 handlers cada um com uma função específica.
De acordo com a Handler-Chain definida no Supplier e no Supplier Client é primeiramente executado o *LoggingHandler* seguido do *HeaderHandler*, depois o *SupplierSecurityHandler* e por fim é executado novamente o *LoggingHandler*. Os handlers têm as seguintes finalidades:

- O *LoggingHandler* tem como finalidade imprimir a mensagem no terminal.
- O HeaderHandler é responsável por adicionar um cabeçalho com a indicação do Timestamp (data e hora de criação da mensagem), garantindo assim a sua vivacidade.
- O *SupplierSecurityHandler* trata de garantir a autenticidade e integridade da mensagem adicionando um cabeçalho com uma assinatura gerada através do conteúdo da mensagem.

No canal de comunicação dos Mediators há 2 handlers, um do Client e um do Server.
No cliente existe o *MediatorClientSecurityHandler*, unicamente responsável por processar mensagens de saída em que é chamada a função BuyCart, encriptando o número do cartão de crédito usando a chave pública do mediador.

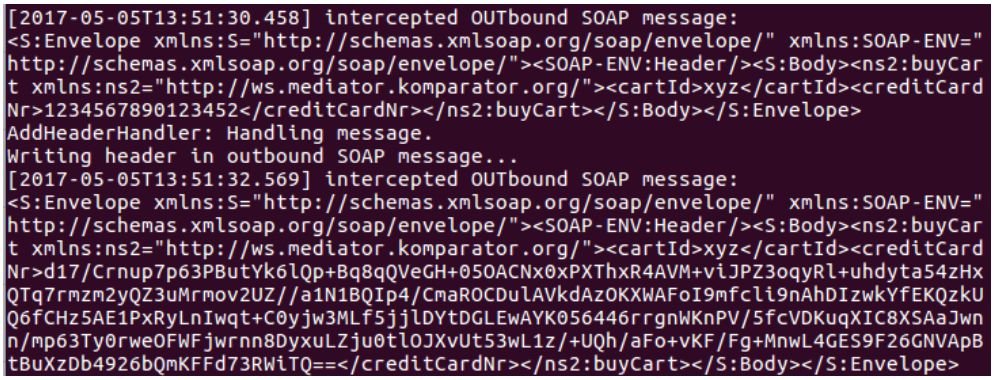
No lado oposto (no servidor) apenas são processadas mensagens de chegada que contenham o método buyCart. Nesse caso o *MediatorServerSecurityHandler* é responsável por desencriptar o número do cartão de crédito.

Segurança

Quando a mensagem é recebida quer pelo Supplier quer pelo Supplier Client, este retira o cabeçalho da assinatura da mensagem e compara o conteúdo da mensagem final com o conteúdo presente na assinatura. Se for igual garante-se assim a autenticidade da mensagem.

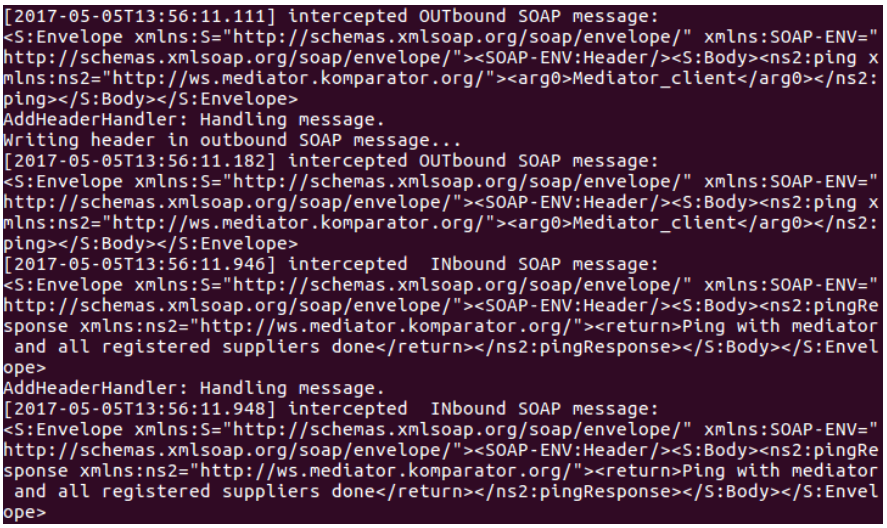
Adicionalmente, antes de a mensagem ser enviada vai ser encriptada com a chave privada de quem envia. Quem recebe a mensagem não possui ainda a chave para desencriptá-la. De seguida tem que ir à CA pedir a chave pública que necessita. Mas não podemos usar esta mesma chave sem antes assegurar que consultámos a CA autêntica então temos que comparar com a chave pública da CA que foi inserida em todos os módulos previamente, de maneira segura.

Relativamente à frescura, é analisado o timestamp da mensagem e comparado com a hora em que foi recebida. De acordo com o que definimos, se ultrapassar os 3 segundos a mensagem é descartada.

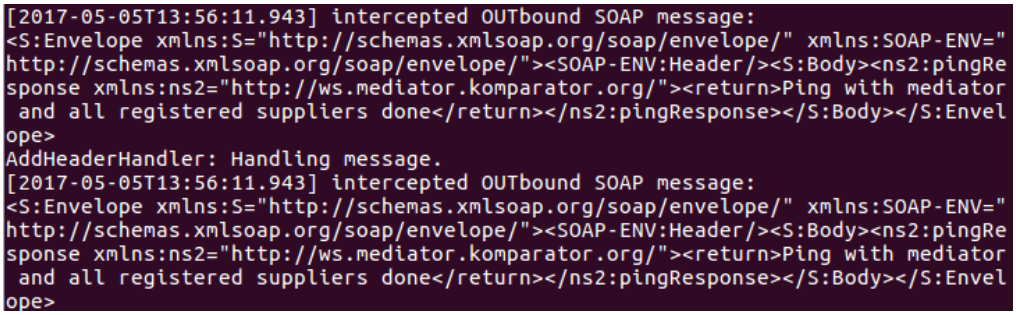


Mensagem referente ao método buyCart, enviada do Mediator Client para o Mediator Server

Mensagem referente ao método buyCart, enviada do Mediator Server para o Mediator Client



Mensagem referente ao método ping, enviada do Mediator Client para o Mediator Server



Mensagem referente ao método ping, enviada do Mediator Server para o Mediator Client

Imagens alta qualidade: https://goo.gl/sYsxyw | click na fotografia