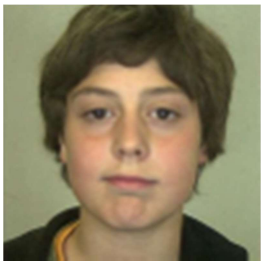
Licenciatura em Engenharia Informática e de Computadores

Relatório de Segurança

Grupo A54

Repositório GitHub: https://github.com/tecnico-distsys/A54-Komparator

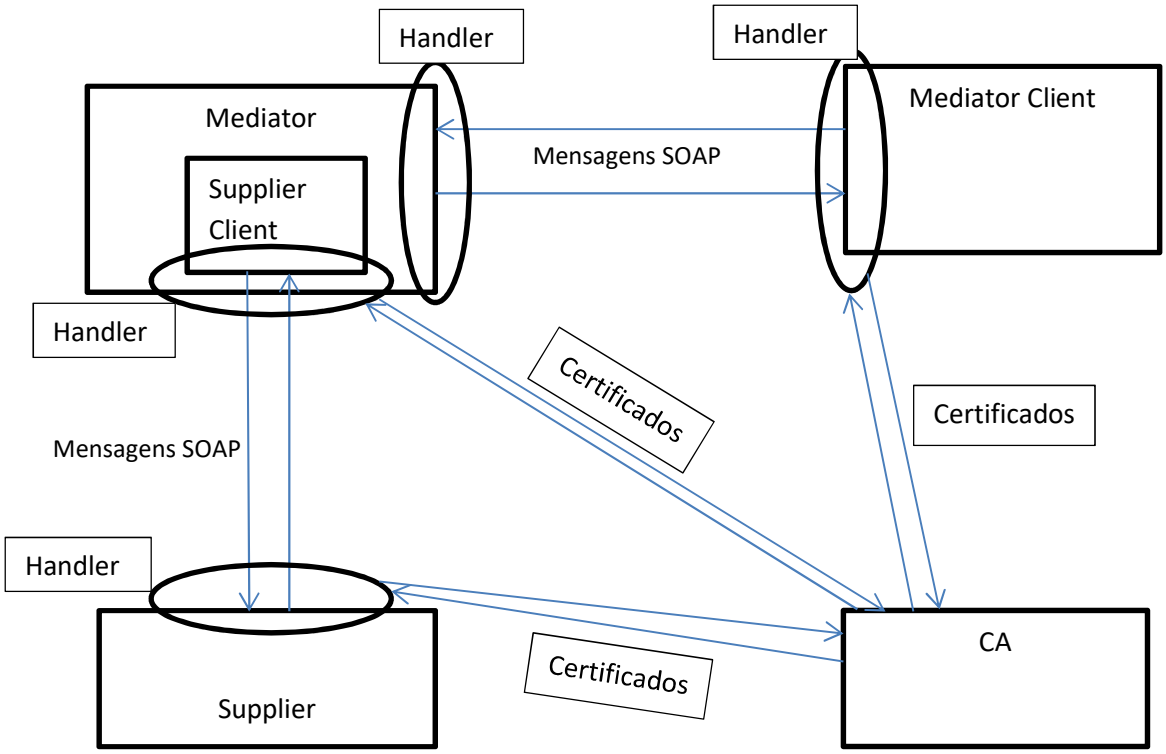
Pedro Lindeza, nº80831



Filipe Azevedo, nº82468

Martim Silva, nº82517

Esquema Ilustrativo



Com este pequeno esquema tentamos, de maneira sucinta, explicar a funcionalidade do nosso projeto, e das ligações entre os vários módulos.

O Mediator Client comunica com o Mediator através de mensagens SOAP. No entanto, os handlers interceptam as mensagens e, no caso de ser chamada a função buyCart, cifram/decifram as mesmas.

O Mediator cria depois um Supplier Client que comunica com um Supplier. Mais uma vez, os handlers interceptam estas mensagens SOAP e, neste caso, assinam as messagens e encriptam a assinatura de forma a manter a autenticidade e integridade, colocando também um timer de forma a manter a frescura das mesmas. Mais uma vez, estes handlers pedem os certificados ao CA.

Para cifrar, os handlers pedem ao CA os certificados que contém as chaves públicas e privadas.

Exemplos de Mensagens Capturadas

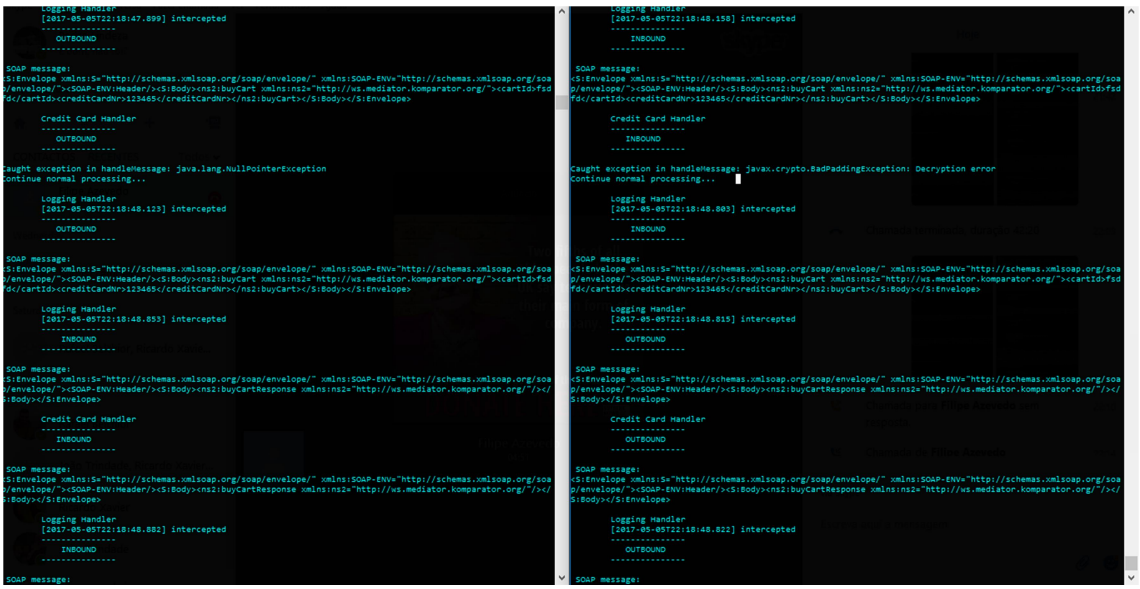


Ilustração 1: Mensagens capturadas entre o Mediator e o MediatorClient.

O XML que se encontra na Ilustração 1 refere-se aos Logging Handlers e ao CreditCardHandler, este último serve para encriptar e desencriptar o número do cartão de crédito.

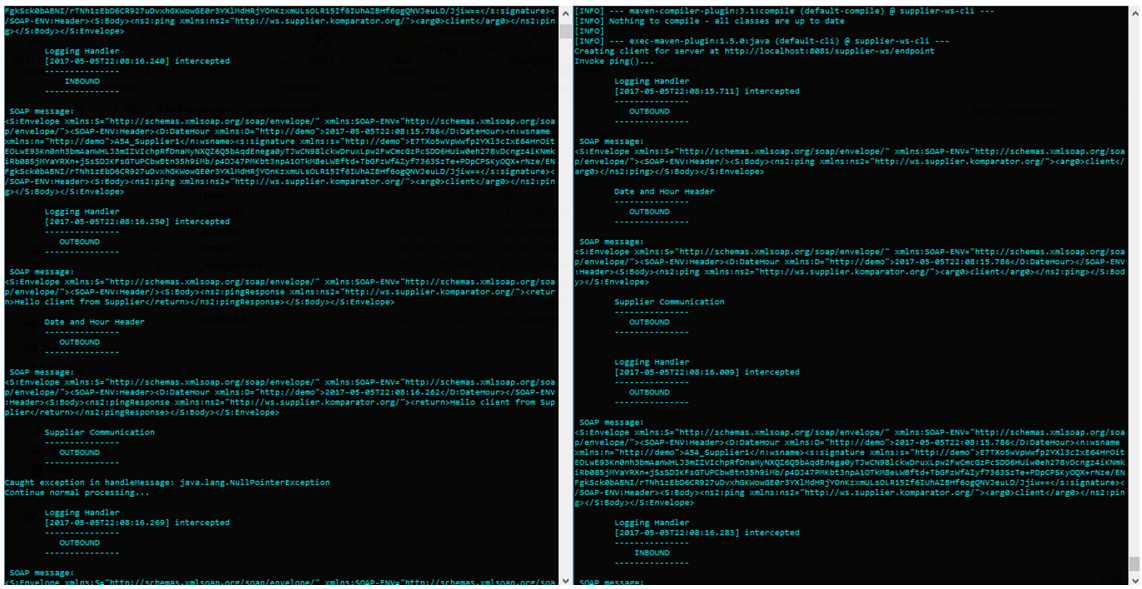


Ilustração 2: Mensagens capturadas entre o Supplier e o SupplierClient.

O XML que se encontra na Ilustração 2 refere-se aos Logging Handlers, ao DateandHour Handler, que contém um timestamp no Header, e ao Supplier Handler, responsável por assinar digitalemente a mensagem.