Relatório de Segurança

Grupo : A53

URL GitHub: https://github.com/tecnico-distsys/A53-Komparator

Nº Aluno: 68199

Nome: Tiago Santos

Nº aluno: 73522

Nome: Hugo Afilhado

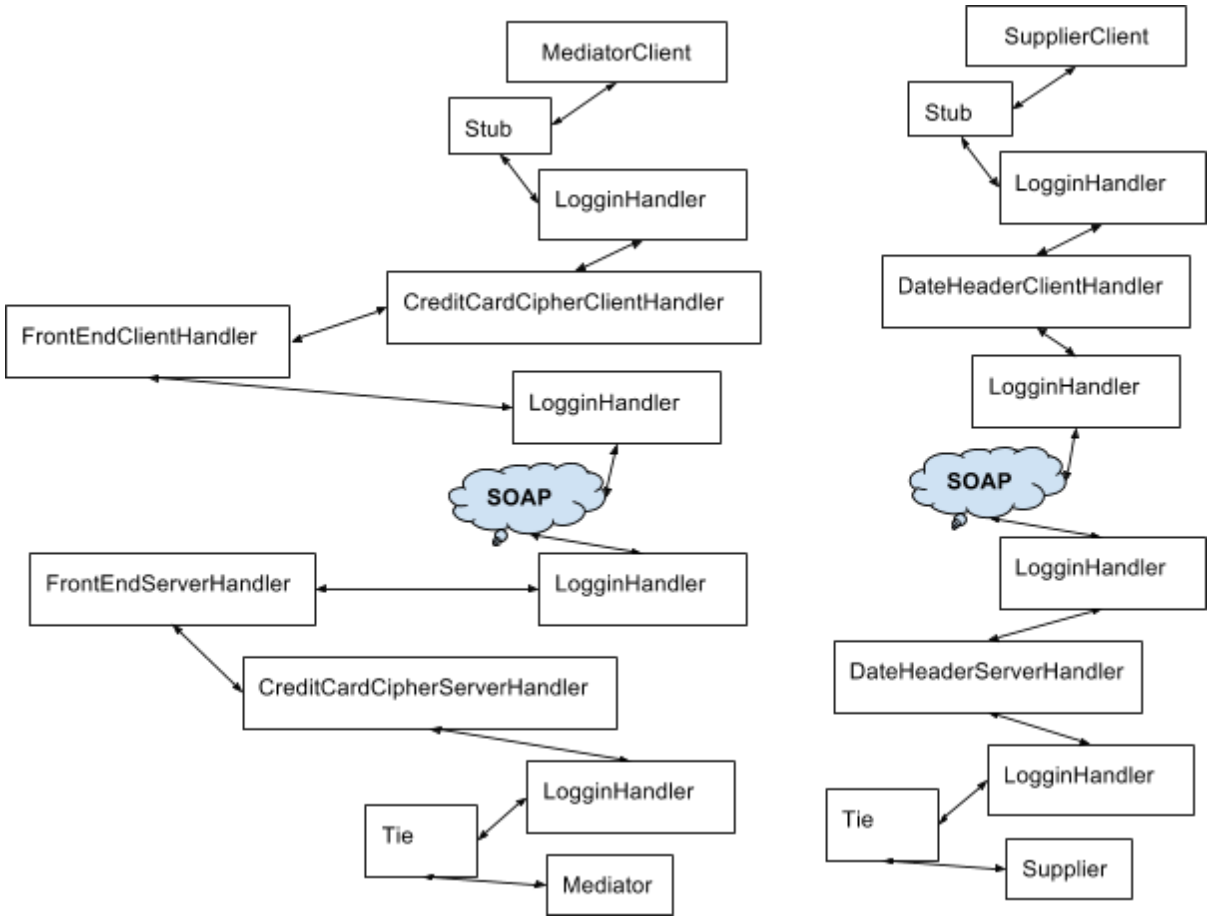

Fig.1 - Figura ilustrativa Modelo de Segurança e Tolerância a Faltas

A Fig.1 representa a comunicação entre serviços e o processamento e tratamento da troca de mensagens entre os mesmos através de handlers, assume-se na figura que supplier e mediator representa, todos os suppliers e mediadores presentes no projecto, visto que o seu funcionamento é igual.

Segurança:

LogginHandler responsável pelo tratamento das mensagens soap tanto no envio como receção de mensagens.

DateHeaderClientHandler que acrescenta uma data ao Header da mensagem enviada pelo cliente do supplier de forma a garantir a integridade.

DateHeaderServerHandler que tem uma condição em que se à mensagem recebida pelo servidor do supplier já tiver sido enviada à mais de 3 segundos pelo cliente esta é rejeitada de forma a garantir a frescura .

CreditCardCipherClientHandler que cifra o valor do cartão de crédito para ser enviado na mensagem do cliente do mediador de forma a que este só possa ser lido pelo mediador garantido a confidencialidade.

CreditCardCipherServerHandler que decifra o valor do cartão de crédito recebido na mensagem do cliente do mediador de forma a que este só possa ser lida pelo mediador garantido a confidencialidade.

FrontEndServerHandler gere a repetição de mensagens com base nos identificadores dos pedidos dos clientes.

FrontEndClientHandler adiciona um valor identificador único do pedido ao cabeçalho da mensagem.

Tolerância a Faltas

Aplica-se um método de replicação passiva ao mediador em que existe um servidor secundário que funciona como backup do servidor primário. As mensagens são recebidas pelo servidor primário e executadas, este actualiza o estado do servidor secundário com o resultado dessa operação, por fim responde ao cliente.

Para tal ser possível, o servidor primário dispõe de um mecanismo cíclico (LifeProof) encarregue de sinalizar ao servidor secundário que ainda se mantém vivo, enviando uma mensagem unidirecional. Se passados mais que 5 segundos (valor configurável) em que o servidor secundário não recebe essa mensagem, assume o lugar de servidor primário publicando-se ao serviço de nomes (UDDI) ficando disponível para os clientes.

A comunicação do cliente do mediador passa por uma camada (FrontEnd), esta será responsável por comunicar os pedidos do cliente ao servidor, passando por um handler da parte do cliente que atribui um identificador único a cada pedido para que se controle os pedidos repetidos. Se o pedido recebido pelo handler do servidor, for detectado como repetido este vai devolver a resposta que estava guardada. Caso contrário, o servidor efetua as operações na ordem de chegada, guarda a resposta de cada pedido e responde ao cliente.