

# Sistemas Distribuidos 2015-2016

Grupo A44

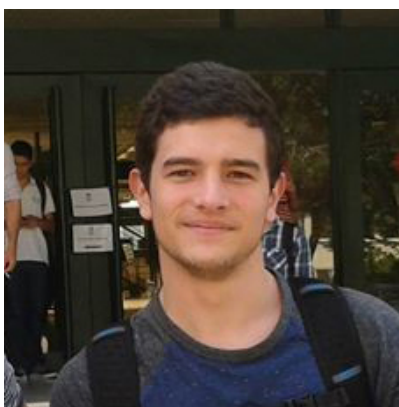
12 de Maio de 2016

[https://github.com/tecnico-distsys/A\\_44-project](https://github.com/tecnico-distsys/A_44-project)



Lídia Freitas

78559



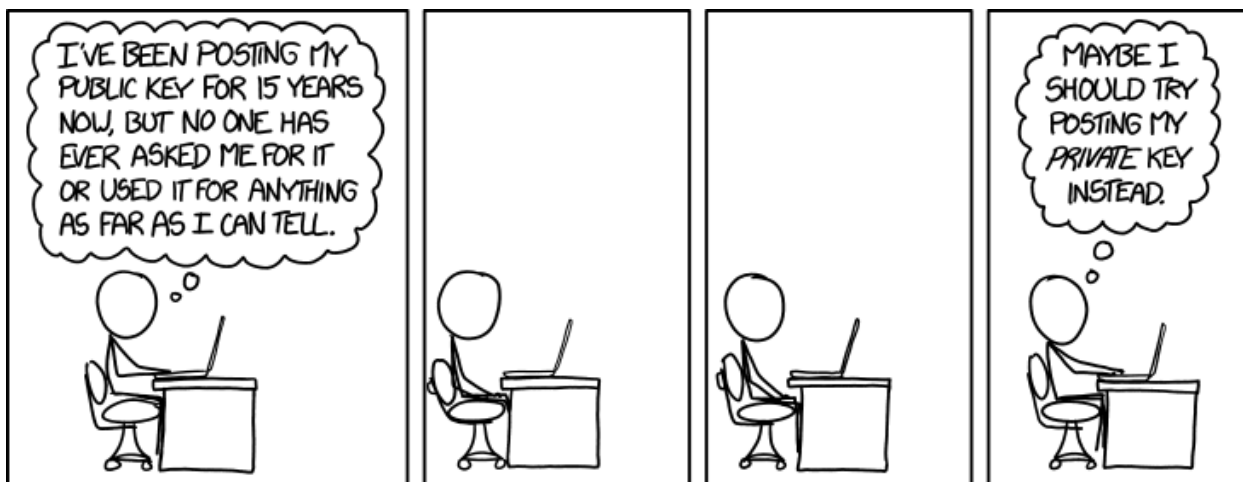
João Marçal

78471



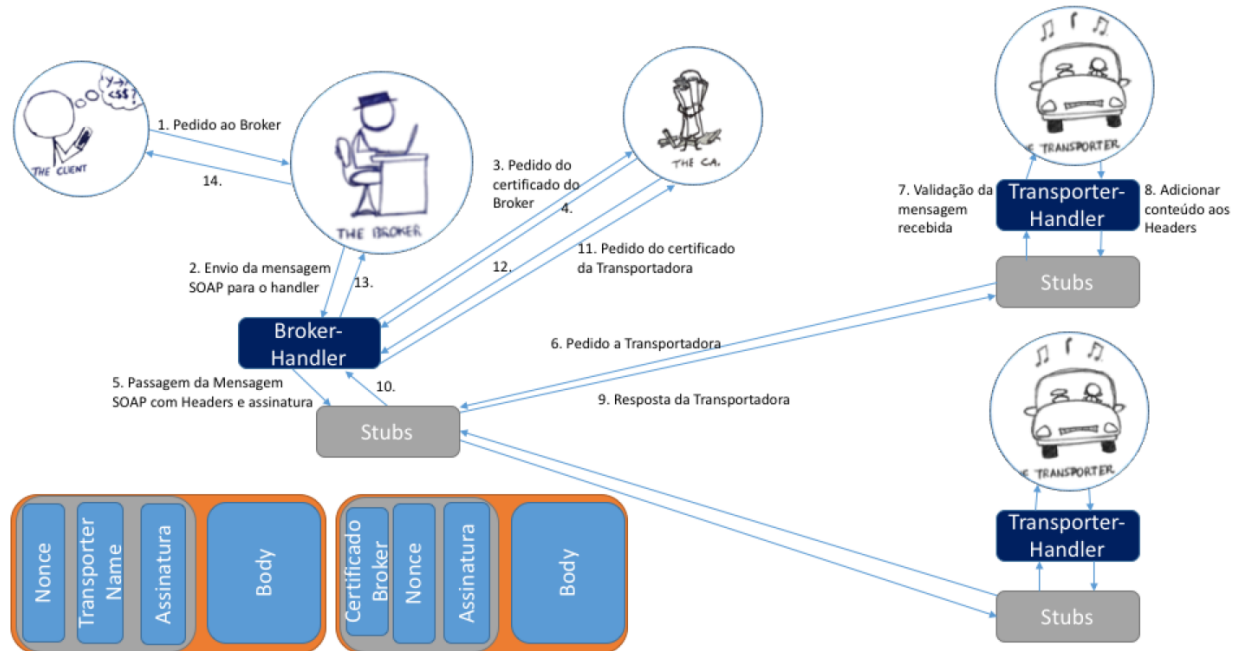
José Semedo

78294



# 1 Segurança

## 1.1 Esquema



## 1.2 Descrição do Esquema

O cliente do broker começa por fazer um pedido, o broker de seguida envia pedidos para as transportadoras. As mensagens antes de serem passadas aos stubs vão passar pelo handler do broker que vai adicionar uma assinatura, um nonce (número random de 16 bytes) e o certificado do broker que é pedido à CA.

O handler da transportadora verifica se a mensagem foi enviada pelo broker, se é uma mensagem nova e se não foi adulterada. Quando a transportadora envia a sua resposta ao broker, o seu handler vai adicionar à mensagem SOAP o nome da transportadora, um nonce e a assinatura da mensagem.

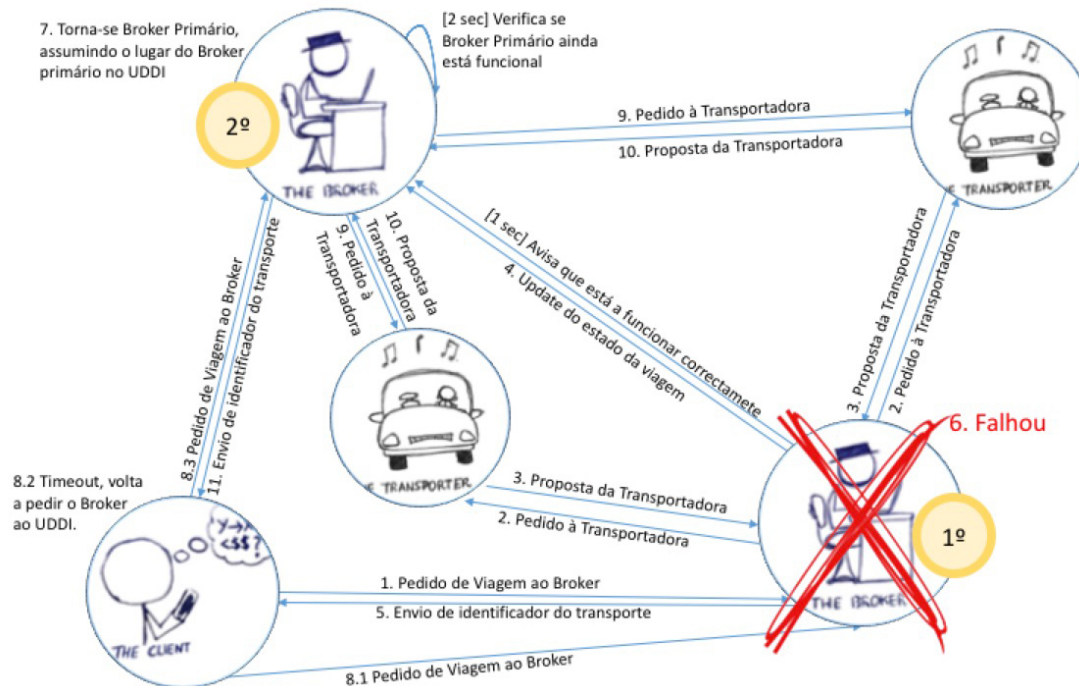
Por fim quando a mensagem chega ao handler do broker, este vai pedir o certificado da transportadora que enviou a mensagem à CA e vai verificar a assinatura e o nonce dessa mensagem. Se tudo estiver correcto a mensagem é passada ao broker, caso contrário é gerada uma exceção.

## 1.3 Racional

Para garantir as propriedades pedidas no projecto, o handler do broker faz o digest do body e de um nonce, cria a assinatura e adiciona-a e esse nonce ao header juntamente com o seu certificado que pede à CA (como no protocolo https). Nas transportadoras o handler vai fazer o digest do body de um nonce e do nome da transportadora, precisamos de adicionar o nome da transportadora para o broker saber de que transportadora é que deve pedir o certificado à CA, assim depois de calculado o digest faz a assinatura e adiciona-a ao header juntamente com o nonce e o nome da transportadora.

## 2 Replicação

### 2.1 Esquema



### 2.2 Descrição da Figura e Racional

### 2.3 Funcionamento do Broker Primário

Inicialmente o comportamento do broker encontra-se em funcionamento normal, já implementado na entrega anterior. No entanto, de 1 em 1 segundo este envia uma prova de vida ao broker secundário indicando que se encontra em funcionamento. Também é feito um update no final do método de pedido de transporte enviando ao broker secundário o transporte criado no final da execução do método. Foi também alterado o método de limpeza de transportes, para propagar a limpeza dos transportes para o broker secundário.

### 2.4 Funcionamento do Broker Secundário

O broker secundário é um "broker primário adormecido" sendo que se encontra a receber updates de transportes do broker primário que regista. Este possui um timer de dois segundos que é reiniciado sempre que recebe uma prova de vida do broker primário. Caso este timer chegue ao fim, o broker secundário assume o lugar do Broker primário no UDDI, passando agora a receber os pedidos do cliente, comportando-se como se fosse o primário.

### 2.5 Funcionamento do cliente do Broker

No cliente do broker implementamos um sistema de timeouts de 10 segundos de ligação e de espera de resposta da parte do broker. Caso o timeout ocorra, o cliente faz um novo pedido ao UDDI que já terá o endpointaddress do broker secundário. Assim, os novos pedidos já são feitos para o broker secundário.