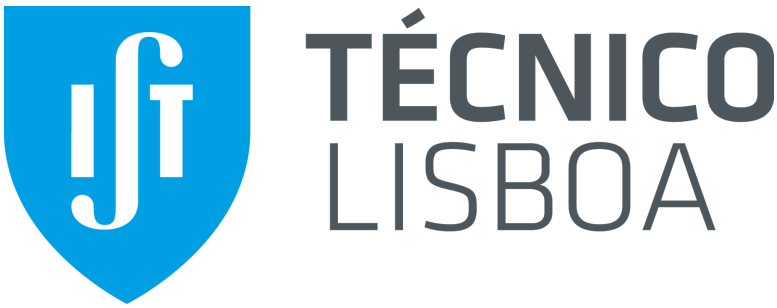
Grupo Nº 24



Sistemas Distribuídos

2º Semestre 2015/2016

Grupo A24

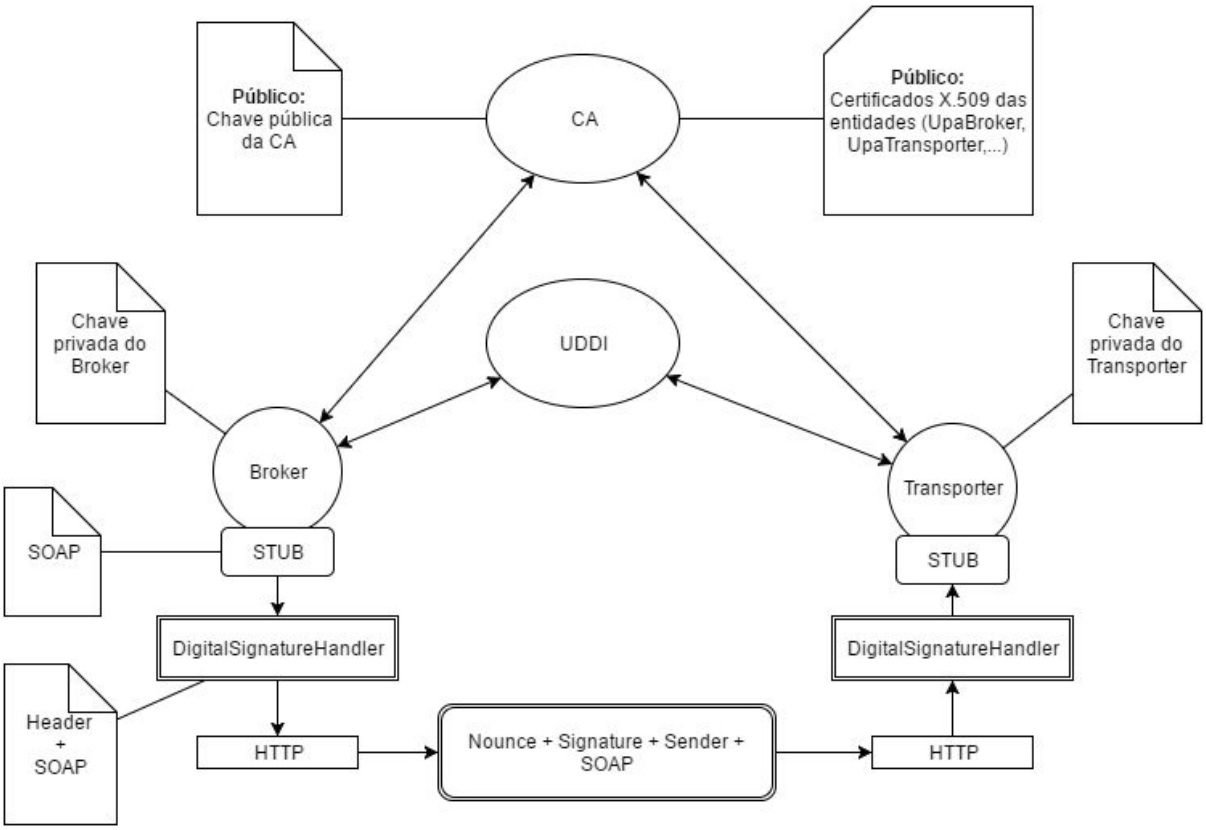
Upa Transportes

Relatório de Projecto

https://github.com/tecnico-distsys/A_24-project

Pedro Duarte	78328	
Gonçalo Ferreira	78596	
Gonçalo Fialho	79112	

Segurança



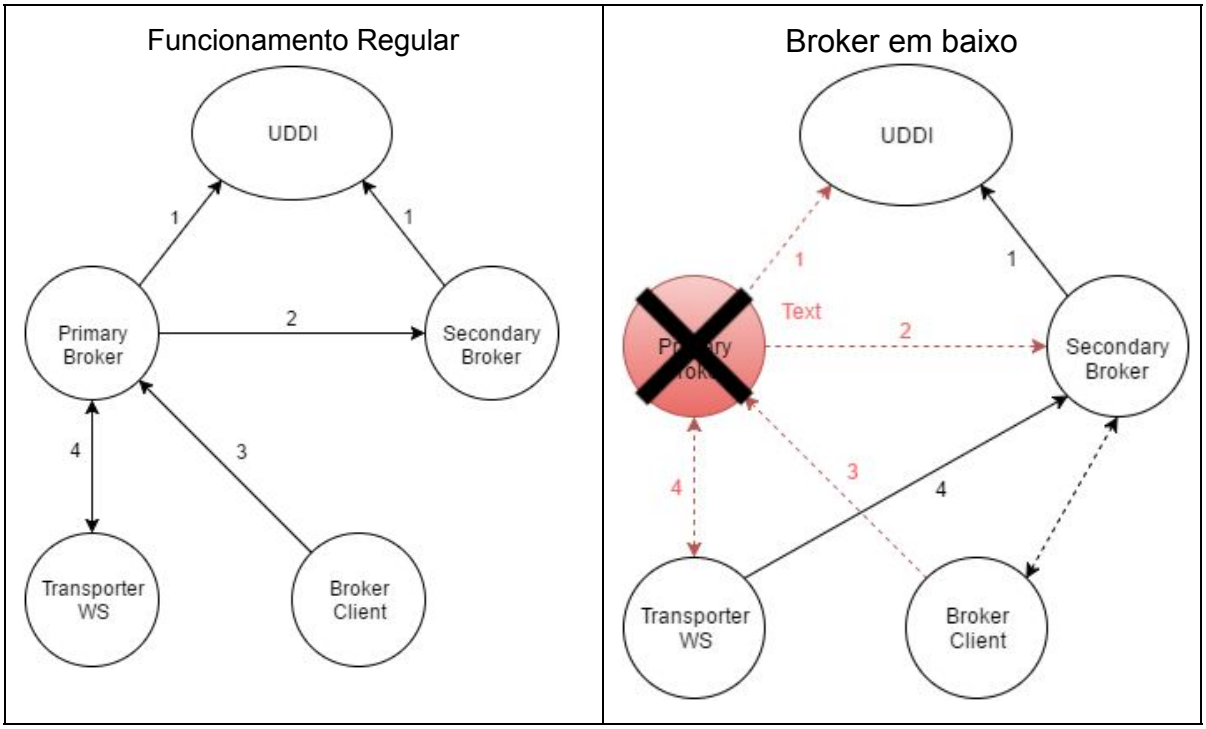
- A **CA tem os certificados de todas as entidades existentes** (parte-se do princípio que estes já foram emitidos e as entidades "registadas"): UpaBroker1 (Broker principal), UpaBroker2 (Broker secundário), UpaTransporter1, etc.;
- As entidades já geraram as suas próprias **chaves privadas**;
- O DigitalSignatureHandler computa o resumo, o nounce e envia junto com a mensagem SOAP;
- Assim a mensagem SOAP enviada é:

  Nounce + Assinatura + Remetente + Mensagem SOAP

- A assinatura é de **chave assimétrica** para garantir o **não repúdio** das mensagens, além da **autenticação** e **integridade**;
- O nonce serve para garantir a **frescura** das mensagens;
-

Parte-se do princípio que o Broker já obteve o certificado de todas as Transportadoras registadas no UDDI. Assim, quando faz um pedido genérico a uma Transportadora, o Broker coloca no contexto de mensagem o seu identificador; o Handler (lado do Broker) adiciona o identificador, o nonce e a assinatura ao header da mensagem SOAP; de seguida, quando a mensagem chega à Transportadora, o Handler (lado da Transportadora) obtém o identificador do remetente, o nonce (e guarda-o para posterior verificacao) e a assinatura, calcula o resumo da mensagem recebida e compara-o com o resumo da assinatura para autenticação do remetente. Na resposta da Transportadora ao Broker, o processo é análogo.

Replicação



1) Registo dos Broker's no UDDI
2) Servidor Primário envia imAlive a cada 0.5 segundos e faz update da informação recebida das funções *requestTransport*, *listTransports*, *clearTransports*, *viewTransport*.
3) O Cliente evoca as funções de *requestTransport*, *listTransports*, *clearTransports* e *viewTransports*.
4) O Broker realiza os pedidos às transportadoras e calcula a oferta mais baixa, enviando de seguida a informação ao cliente e ao Secondary Broker (ponto 2).

Após a "morte" do Primary Broker o Secondary Broker regista-se no UDDI como sendo o "UpaBroker" principal, esta acção faz com que as transportadoras e clientes que estão em contacto com o Primary Broker não se apercebam do que aconteceu, pois o Secondary Broker trata de se auto-denominar como sendo o Primary Broker.

Após esta alteração é tido em conta de que o Primary Broker não recupera, ou seja, não volta a ser ligado, dando completa responsabilidade ao Secondary Broker para manter a conexão e comunicar com os restantes servidores.

O Broker Client utiliza ***timeouts*** para estabelecer quanto tempo o cliente deve esperar até se estabelecer uma ligação com o servidor, assim como o tempo que o cliente deve esperar para receber uma resposta a uma chamada de função do servidor.