TÉCNICO LISBOA

Relatório
Sistemas Distribuídos 2015/16

https://github.com/tecnico-distsys/A_02-project

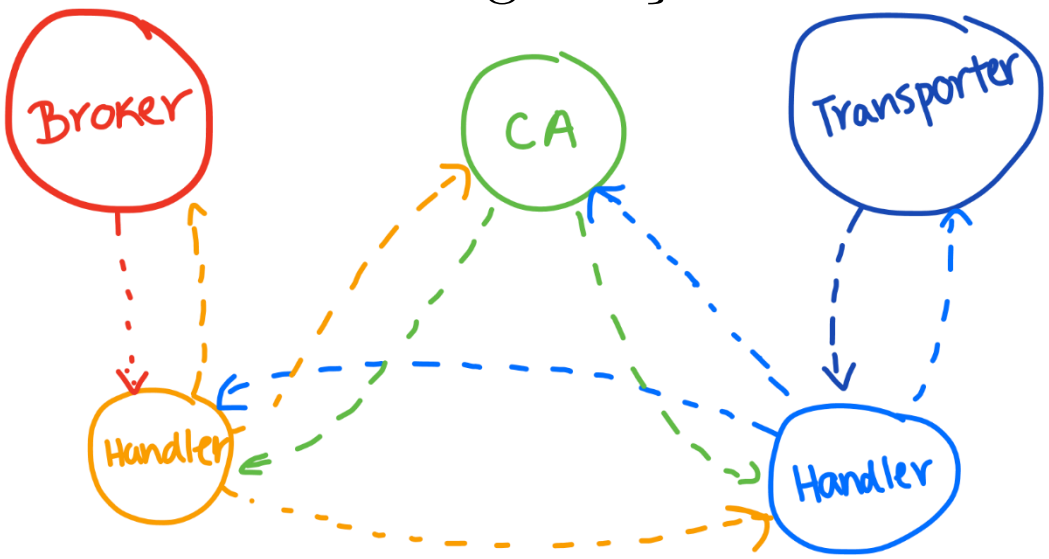
Grupo A02:

78606
Mariana Ribeiro

78778
Bernardo Cordeiro

78942
Rodrigo Bernardo

Segurança



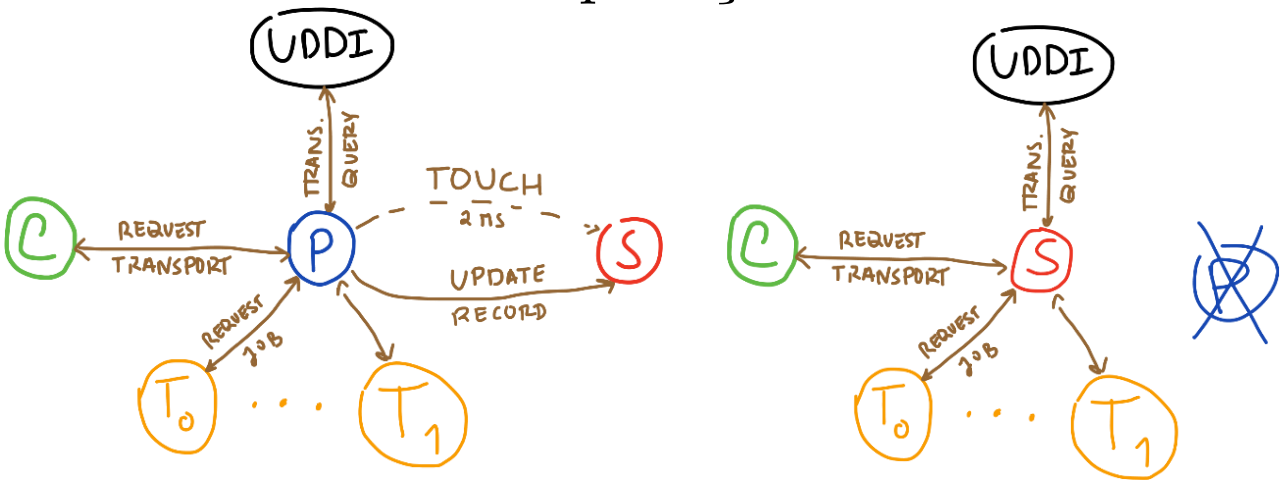
A nossa comunicação entre o Broker (vermelho) e o Transporter (azul escuro) é feita através de suporte a Handlers (laranja e azul claro respetivamente) que garantem a segurança da ligação Broker-Transporter recorrendo a um modelo de certificação que é garantido através da existência da entidade CA (verde).

O CA gerou, assinou e distribuiu os certificados necessários previamente para cada uma destas entidades. Esta entidade conhece todos os certificados que gerou (caso não os tenha revogado), é capaz de reconhecer um certificado válido e responder a pedidos de envio de certificados duma entidade, que são feitos pelos Handlers cada vez que fazem comunicação um com o outro.

Cada vez que uma mensagem chega duma entidade que está ligada ao Handler (Broker ou Transporter), este vai assinar a mensagem com a sua chave privada, coloca no header o resumo da mensagem e depois entrega a mensagem através da rede ao outro Handler que vai verificar a autenticidade e integridade da mensagem, pedido ao CA o certificado da entidade que enviou a mensagem.

A frescura da comunicação é garantida através da existência de um Nounce único gerado e enviado pelos Handlers em cada mensagem. O Nounce não pode ser alterado, pois verifica-se a integridade da mensagem.

Replicação



Descrição

Na imagem, "C" representa um cliente do broker, "P" representa o broker primário, "S" o servidor broker secundário (ou de backup), "UDDI" o servidor UDDI e os "Tx" representam as várias transportadoras.

O broker primário interatua com o cliente, o UDDI e as transportadoras de forma semelhante à da primeira entrega, com a diferença de que o cliente agora tem um timeout para receber a resposta por parte do servidor.

Para esta entrega foi criado um servidor de backup para satisfazer os requisitos da replicação. O servidor primário envia provas de vida de dois em dois milissegundos ao servidor secundário. Caso o secundário falhe em receber provas de vida, este toma o lugar do primário.

O servidor primário mantém sincronizado o estado do secundário com o seu.

Racional

A implementação baseou-se no padrão de desenho "estado". O BrokerPort passou a ter um atributo que representa o modo de execução ao qual são delegadas responsabilidades. PrimaryMode representa um servidor a actuar em modo primário e BackupMode representa um servidor a actuar como secundário. Quando o servidor secundário deixa de receber provas de vida por parte do primário, mudar o comportamento do BrokerPort é apenas uma questão de alterar o seu atributo de modo de BackupMode para PrimaryMode e fazer a republicação no UDDI.As duas novas operações, “touch” e “updateRecord” são ambas "oneway". A primeira serve para enviar uma prova de vida do servidor primário para o secundário. A segunda, actualiza o estado no servidor secundário. O estado é sincronizado sempre que são as seguintes operações no servidor primário: "requestTransport", "viewTransport", "listTransport" e "clearTransport".