TÉCNICO LISBOA

Licenciatura em Engenharia de Telecomunicações e Informática

Unidade Curricular de Sistemas Distribuídos

Ano lectivo 2015/2016

Grupo T38

Repositório Git Hub:
https://github.com/tecnico-softeng-distsys-2015/T_38-project.git

Duarte Clara, nº76832

Rúben Martins, nº79532

Segurança

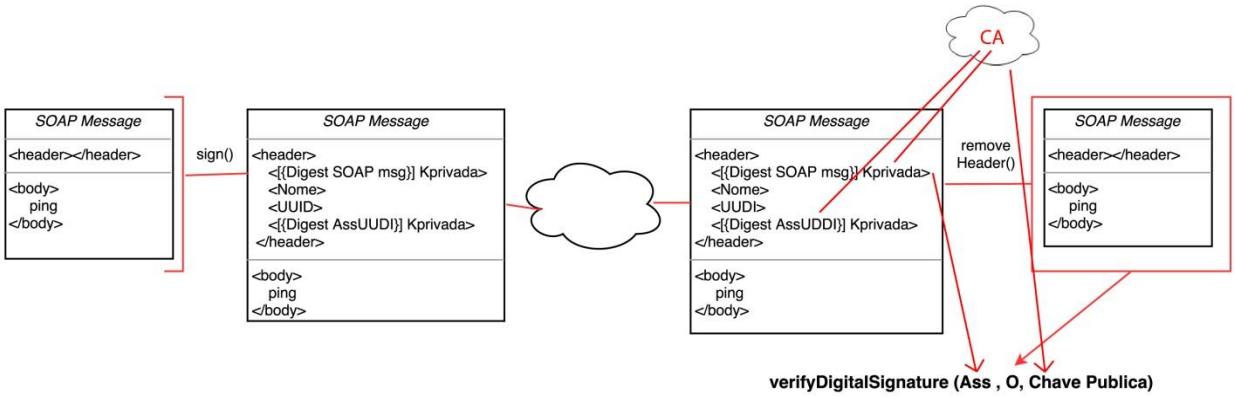

Figura 1 – Mensagens SOAP trocadas entre o Broker e as Transporters

Racional

Foi criado um servidor de CA (novo Web Service) onde é feita a distribuição de certificados com as chaves públicas do serviço ao qual se tenta saber a sua chave pública (usado para fazer a verificação da assinatura). É feita a verificação se o certificado retornado foi devidamente assinado pelo CA. Foram usados SOAP Handlers para interceptar as mensagens que eram enviadas. Para tal foi implementada um biblioteca de Handlers no Transporter Server e no Broker Server (Transporter-ws-cli) onde o Handler UpaHeaderHandler faz a intercepção das mensagens e implementa os requisitos de segurança pretendidos no contexto deste projcto: autenticidade, integridade, não repudio e, ainda, a frescura da mensagem.

Este UpaHeaderHandler funciona da seguinte forma:

- Para uma mensagem que vai ser enviada (Outbound) é adicionado ao Header da mensagem SOAP a assinatura da mensagem original com a chave privada do emissor $\{[D]\}_{kprivada}$, (sendo D o resumo da mensagem SOAP sem header, o nome do emissor, identificador único (UUID) e a assinatura desse mesmo identificador $\{[DUUID]\}_{kprivada,}$ sendo DUUID o resumo do identificador único e sendo $k_{privada}$ a chave privada obtida através da KeyStore do emissor);

- Para uma mensagem que vai ser recebida (Inbound) é lido no Header o nome do emissor (sendo que este é usado para pedir ao servidor CAS o certificado que contém a chave pública do emissor para posteriormente verificar a assinatura do emissor), a assinatura da mensagem original, o identificador único e a e a assinatura desse mesmo identificador;

Este identificador único (UUID) vai ser usado para garantir a frescura das mensagens. Para tal é usada uma FIFO (queue) que guarda os últimos 200 identificadores únicos recebidos onde ser verifica se a mensagem que recebida já está FIFO. Se estiver, significa que a mensagem é repetida e esta é ignorada.

Para a verificação das assinaturas (assinatura da SOAP message original e do identificador único) é guardada cada uma das assinaturas recebidas e é feita uma comparação destas assinaturas recebidas com uma nova assinatura pela chave publica do emissor. Se a verificação não falhar garante a autenticidade, a integridade da mensagem e o não repudio. Caso a verificação falhe a mensagem é considerada inválida e é ignorada.

Replicação

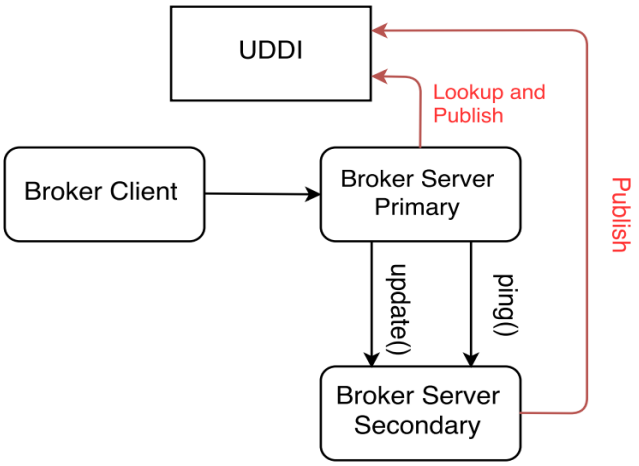

Figura 2 – Estado Inicial

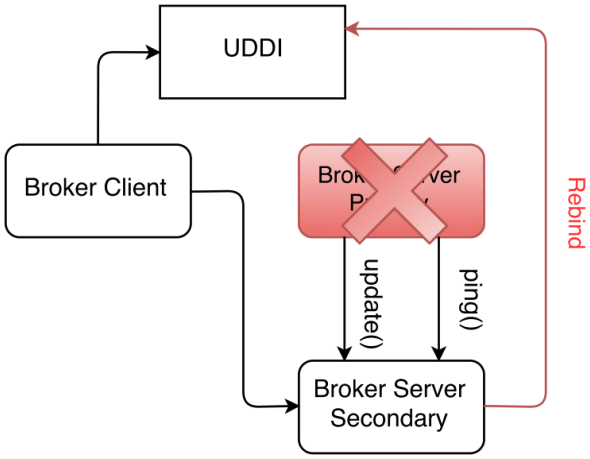

Figura 3 – Estado após falha do Broker Primário

Racional

A replicação no contexto deste projecto pretende tolerar falhas silenciosas no servidor corrector.

Como primeiro passo, é executada uma réplica do Broker (Broker Server Secondary). Este serviço regista-se no servidor de nomes e, caso o servidor primário não arranque dentro de um período de 10 segundos após esta publicação, este Broker Secondary assume-se como servidor primário. Caso arranque um servidor primário, o secundário fica a executar um ciclo em que verifica o estado do primário.

Em segundo lugar, inicia-se o servidor primário (Broker Server Primary). Este servidor, além de procurar pelas transportadoras activas, vai ainda procurar no servidor de nomes pelo secundário e guardar esse endereço (port), antes de publicar o serviço.

O servidor primário passa a comunicar unilateralmente com o secundário em dois instantes distintos:

- Periodicamente, enviando um ping para informar o secundário que se encontra a correr;

- Sempre que há um pedido de transporte, invocando a função update para actualizar a informação nas estruturas de dados do secundário;

No caso de falha no Broker primário, este deixa de enviar o ping ao secundário e este assume então o lugar de primário. Para isso, e tendo uma réplica dos dados do primário, basta ao secundário voltar a publicar o serviço com o nome do servidor primário para o substituir.

Depois disso, o cliente, ao tentar efectuar uma operação no broker, detecta que houve uma alteração e volta a contactar o servidor de nomes para que ele lhe passe o endereço do novo servidor.

Caso exista um pedido do cliente no período de transição entre servidores, esse pedido não é entregue e o cliente é convidado a realizar o pedido novamente.