

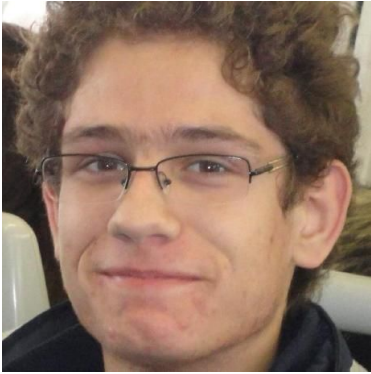


Sistemas Distribuídos 15/16

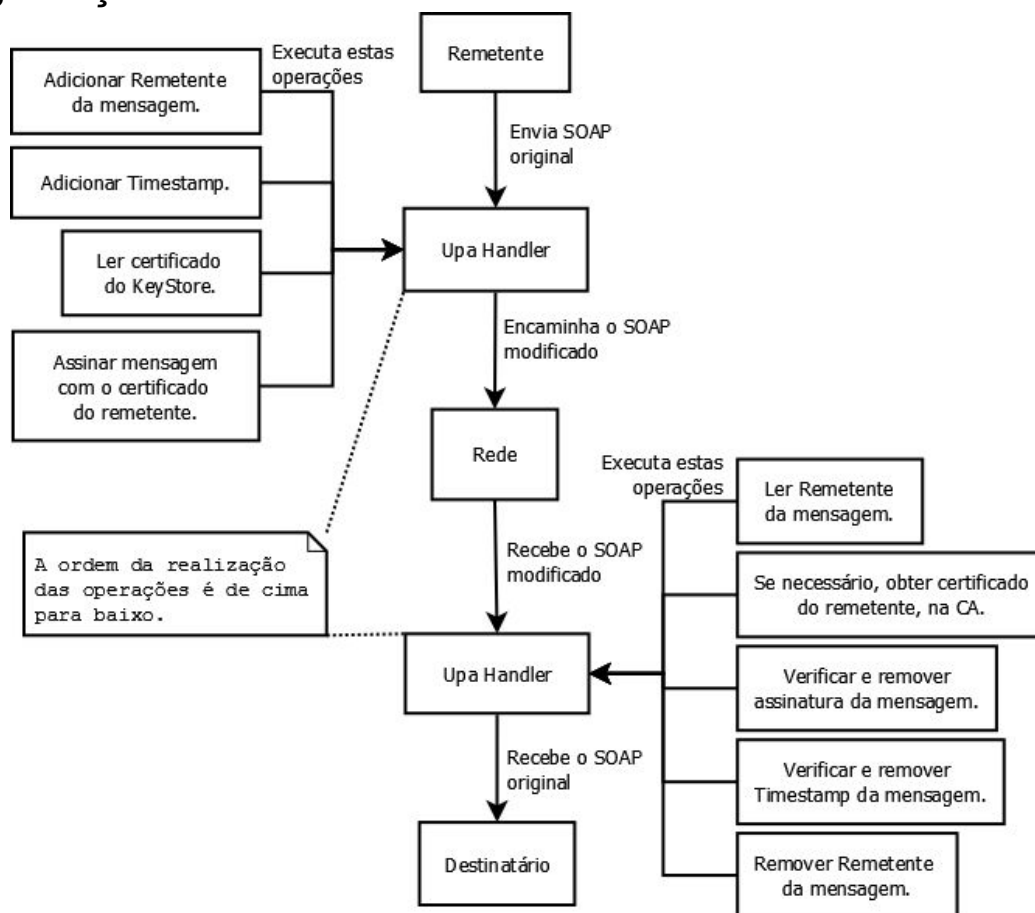
		
João Serras	Daniel Caramujo	Francisco Santos
79664	79714	79719

Grupo: A43

URL do Repositório:

https://github.com/tecnico-distsys/A_43-project

Segurança



O *UpaHandler* funciona em qualquer um dos sentidos da relação entre *Broker* e *Transporters*, por isso preferiu-se utilizar os nomes **Remetente** e **Destinatário**.

O funcionamento da solução é o seguinte:

1. O **Remetente** ao ser iniciado inicializa uma variável à qual o *handler* tem acesso que define o seu nome.
2. A classe que trata da parte funcional do *Web Service* envia para o *handler* a mensagem SOAP como se fosse para enviar para o outro serviço.
3. O *handler* do **Remetente** recebe a mensagem:¹
 - a. Adiciona o nome do remetente e o *Timestamp* ao *Header*;
 - b. Assina a mensagem usando a chave privada da sua *KeyStore*;
 - c. Verifica se a assinatura está correta e envia a nova mensagem SOAP modificada.
4. O *handler* do **Destinatário** recebe a mensagem:
 - a. Lê quem é o remetente e se necessário², pede à CA o certificado deste;
 - b. Verifica se a assinatura bate certo, utilizando o certificado e remove-a do *Header*;
 - c. Verifica se o *Timestamp* está dentro do tempo válido (1 minuto);
 - d. Retira o *Timestamp* e o remetente e envia a mensagem SOAP original ao **Destinatário**.

Em qualquer um dos passos de verificação, se houver alguma suspeita que a mensagem tenha sido proveniente de um ataque, é despoletada uma exceção.

¹ A descrição assegura a autenticidade, integridade, não repúdio e a frescura da mensagem.

² Certificado não presente, entrada não existente na tabela de contagens ou contagem de mensagens superiores ao definido.

Replicação

