Sistemas Distribuídos

2.º Semestre 2016/2017

SD-Komparator

https://github.com/tecnico-distsys/T36-Komparator.git

Relatório de Segurança

77941 – Adrian Quaresma

77941 – Tiago Taveira

78045 – André Monteiro

Authentication Handler

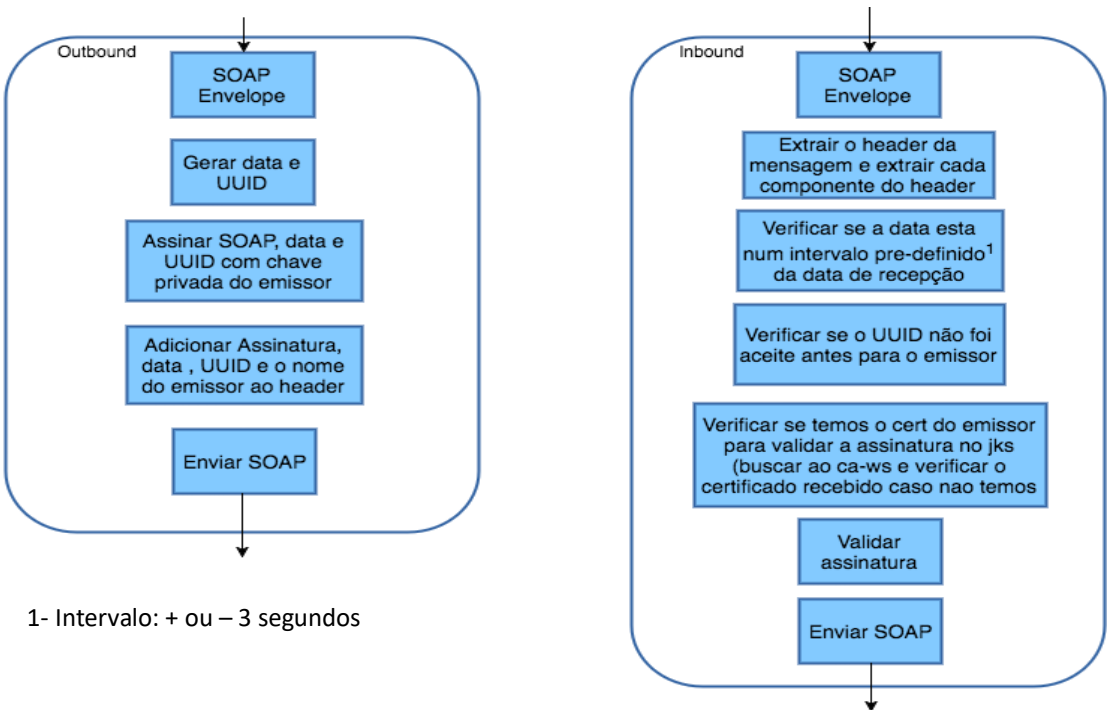
Raciocínio:

Os objetivos de garantir o não repúdio, autenticidade e a "frescura" das mensagens foram pensados para serem atingidos da seguinte forma:

1. **Não Repúdio e Autenticidade:** no cabeçalho das mensagens SOAP mandamos um digest assinado que contem o corpo da mensagem SOAP, a data em que foi criada a mensagem e do UUID da mensagem. Incluímos também no cabeçalho da mensagem o nome do emissor, e.g. "T36_Mediator", "T36_Supplier1".
   Quando o recetor recebe a mensagem compara a assinatura da mensagem com os elementos correspondentes da mensagem.

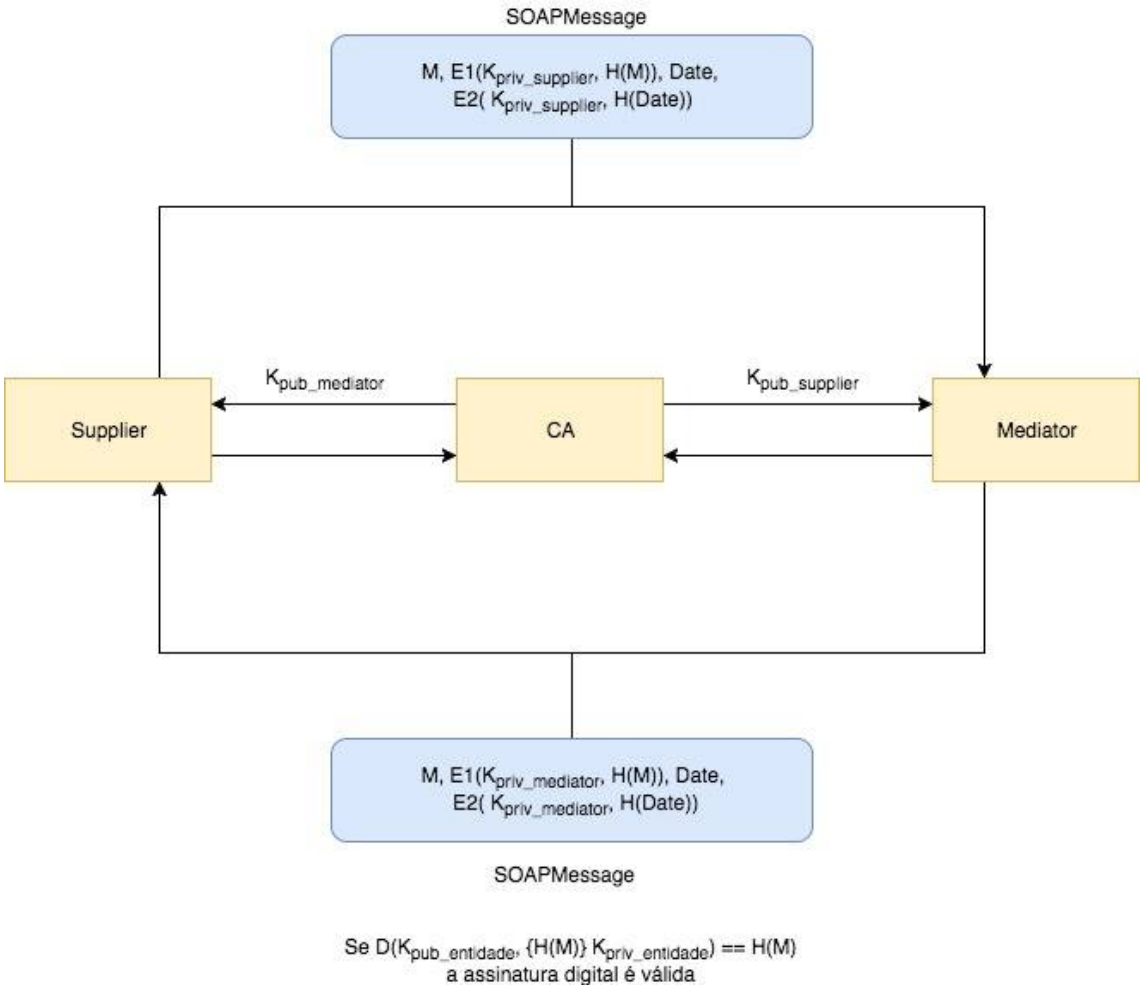
2. **Frescura:** a frescura é garantida pela data enviada na mensagem e pelo UUID, ou seja, quando uma mensagem está de saída adicionamos a data e o UUID e quando está de entrada verificamos se a data enviada com a mensagem esta dentro de um intervalo de +/- 3 segundos do tempo de receção da mensagem. Se não tiver é rejeitada. Também verificamos se o UUID para o emissor já foi tratado anteriormente ou não, se já foi tratado então a mensagem é rejeitada.

Figura Descritiva:



1- Intervalo: + ou – 3 segundos

Diagrama de Troca de Mensagens:



M – mensagem E1 - assinatura digital da mensagem E2 - assinatura digital do nonce
H - digest D - decifrar