TÉCNICO LISBOA

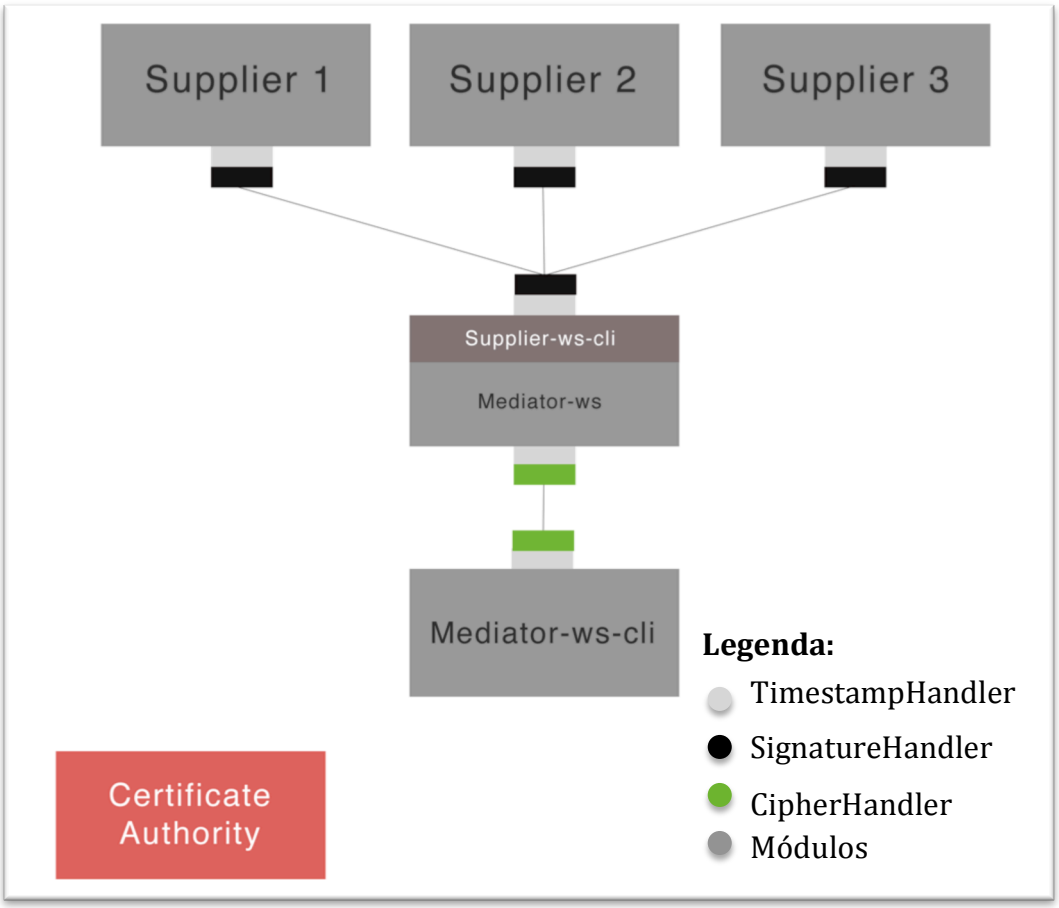
Sistemas Distribuídos

Grupo T04
Repositório GitHub: https://github.com/tecnico-distsys/T04-Komparator


81900 – Nuno Anselmo


81936 – Liliana Oliveira


82047 – André Mendes



Pressupostos:

- Certificate Authority tem ligação a todos os módulos.
- Foi ignorada a representação do LoggingHandler visto não tem qualquer impacto no funcionamento dos handlers.

Descrição:

CipherHandler – Encarregue de cifrar todas as mensagens trocadas entre Mediator-ws-cli e Mediator-ws. Cliente gera uma chave secreta AES na primeira ligação, cifra com a chave pública do mediator, e envia. Todos os campos de todas as mensagens são cifrados com a chave secreta.

TimeStampHandler- Encarregue de marcar as mensagens com o tempo de envio e com um nonce, garantindo a inexistência de mensagens duplicadas em toda a longevidade da aplicação.

SignatureHandler – Encarregue de garantir a autenticidade e integridade através do uso de assinaturas sobre um checksum da mensagem, de modo a que se a mensagem for alterada, os checksums não coincidem ou porque alguém adulterou os dados (integridade) ou porque a chave utilizada para assinar não pertence ao supplier que diz estar a responder (autenticidade).

Certificate Authority – Responsável por centralizar todos os certificados tornando-os disponíveis para quem precisar.

SOAP messages

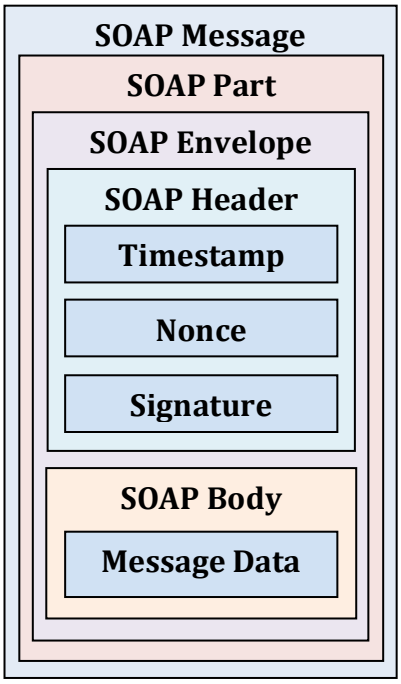


Figura 2 – Formato da mensagem entre Supplier e Mediator (Supplier-cli)

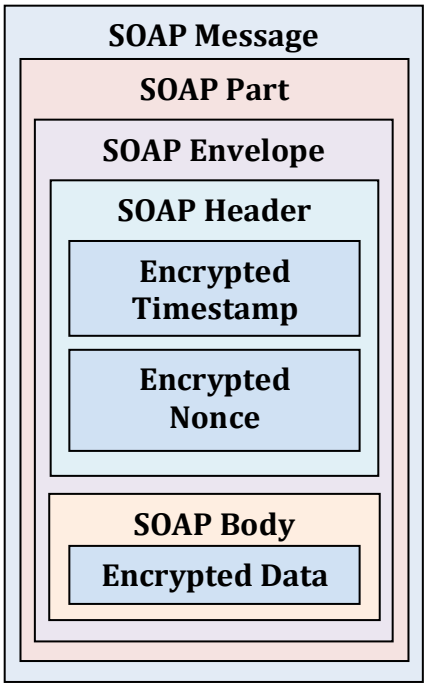


Figura 1 - Formato de mensagem entre Mediator e Mediator-cli

Figura 1 – mensagem é **assinada**: é inserido um timestamp (número) e um nonce (base64), e é gerada a assinatura de toda a SOAPMessage, que é depois inserida no header.

Figura 2 - mensagem é **cifrada**: é inserido um timestamp (número) e um nonce (base64), e todos os campos são depois individualmente cifrados.