TÉCNICO LISBOA

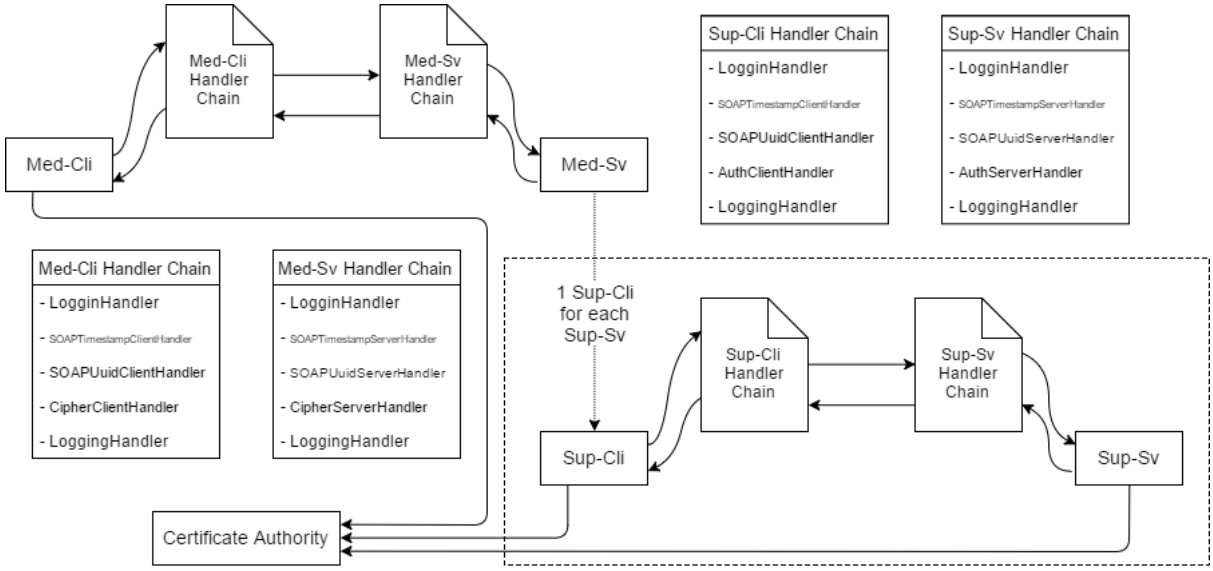
T63 - Komparator

https://github.com/tecnico-distsys/T63-Komparator

João Pedro Carvalho - LETI - 76416
https://github.com/JoaoPedroCarvalho

Oeiras, 05 de Maio de 2017

Diagrama dos serviços



Tendo como metas de projecto assegurar a frescura, unicidade, integridade e confidencialidade, a solução tomada baseou-se individualidade em cada um de um dos objetivos juntando-os pelas capacidades dos *SOAP handlers.* Tal é visível no diagrama a cima disposto que representa o sentido das mensagens e os principais elementos por elas envolvidos. É também apresentada a ordem dos *handlers* que cada cadeia de serviço individual executa.

Para se partir de uma base considerada como segura foi preciso tomar certos pressupostos, sendo eles a existência, desde o *startup*, do certificado da Entidade Certificadora (*Certificate Authority*), que permite verificar todo e qualquer certificado por esta emitida, bem como a robustez entre o serviço *Med-Sv* e *Sup-Cli*. Outro caso é o da ligação entre qualquer serviço e a *CA* ou entre *Med-Sv* e a entidade de validação de cartões de crédito.

As cadeias de *handlers* usadas trabalham em pares e de forma inversa, de forma a que a última chamada no *handler* do emissor será a primeira a ser chamada pelo receptor e vice-versa. As cadeias

A frescura foi assegurada pela adição de um *header* (cabeçalho) ao *SOAPEnvelope* [1] com a respectiva data e hora de quando foi gerado e uma verificação no receptor de um *timeout* de 3 segundos. A unicidade por sua vez é garantida pela adição de um segundo *header* com um *UUID*[2] gerado no momento. À chegada é averiguado se o *UUID* já foi anteriormente recebido, analisando uma lista que contém as mensagens previamente analisadas e rejeitando caso já tenha sido registada.

A propriedade de integridade é garantida em conjunto com a autenticidade do emissor com uso na ferramenta de assinatura digital, fazendo o digest do *SOAPMessage* e cifrando-o com a chave privada do emissor sendo posteriormente decifrada com a chave pública, vinda num certificado fornecido pela *CA*.

No caso da confidencialidade é feita a cifra do número do cartão de crédito quando este é emitido pelo Med-Cli usando a chave pública do serviço Med-Sv, novamente fornecida na forma de certificado enviado pela *CA*. Em qualquer um dos casos na eventualidade de a mensagem ser rejeitada é enviada uma excepção para o emissor que faz parar a execução.

[1] http://docs.oracle.com/javaee/5/api/javax/xml/soap/SOAPEnvelope.html
[2] https://docs.oracle.com/javase/7/docs/api/java/util/UUID.html