TÉCNICO LISBOA

Sistemas Distribuídos

2016/2017

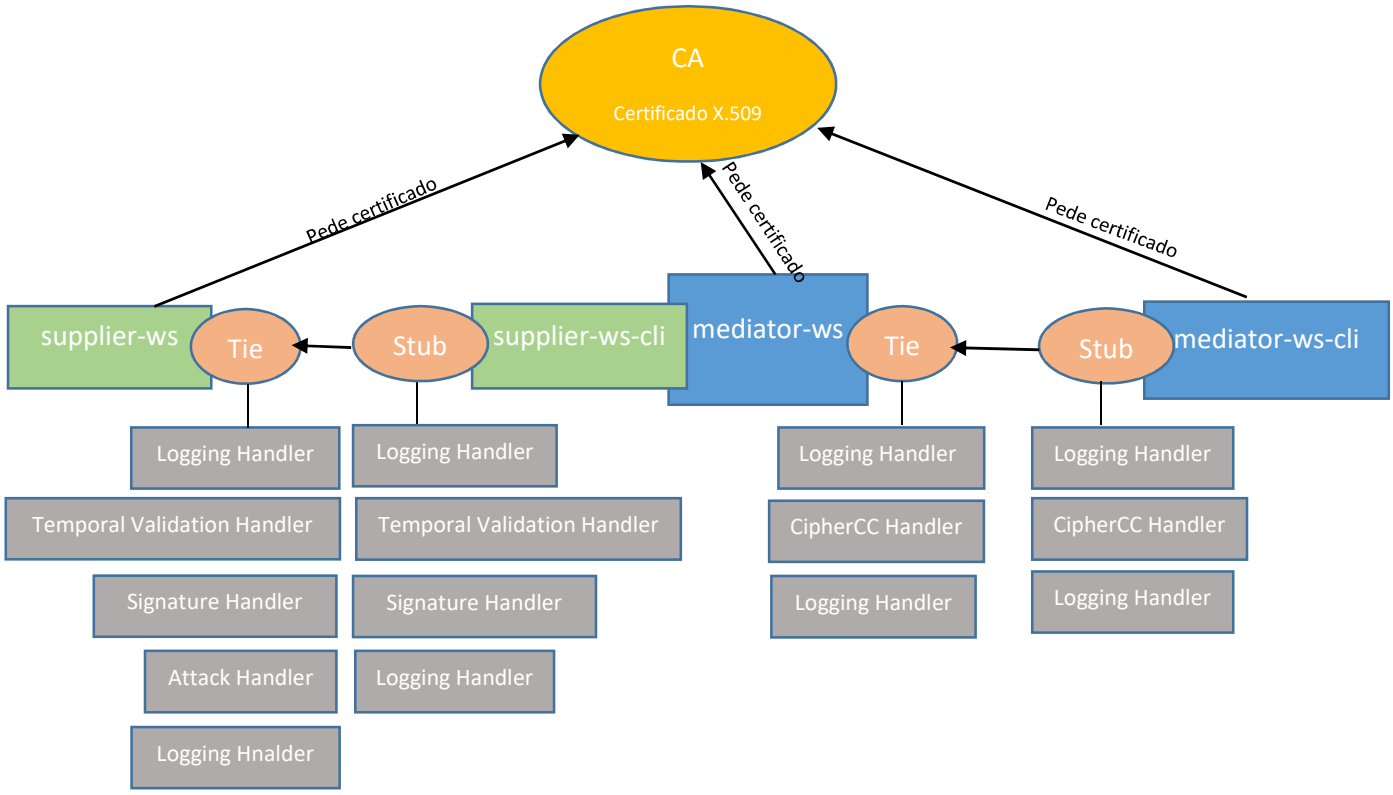
Grupo A63

GitHub - https://github.com/tecnico-distsys/A63-Komparator.git

João Moreira
80934

Rodrigo Lousada
81115

Carlos Antunes
81525



Proteção de dados (proteger privacidade e confidencialidade do cliente):

O mecanismo de encriptação utilizado é baseado na utilização de uma chave pública para cifrar os dados e uma chave privada para os decifrar. Desta forma o número do cartão de crédito é cifrado usando a chave pública do mediator-ws obtida através da leitura do certificado fornecido pela Certificate Authority . Para realizar a encriptação e feito um acesso ao body da SOAP message do qual é retirado o numero de cartão de crédito que é por sua vez encriptado usando uma chave assimétrica. A chave pública da CA é conhecida por todas as entidades participantes. Quando a mensagem é recebida o conteúdo encriptado é decifrado usando a chave privada do mediator-ws-cli. Esta chave privada é obtida de forma local através das keystores disponibilizadas (ficheiros.jks). Desta forma é assegurado que se a mensagem for intercetada o número do cartão de crédito estará inacessível.

Autenticação de mensagens trocadas entre mediator e os suppliers:

Para garantir a autenticação e integridade das mensagens usamos assinaturas digitais. Adicionamos uma *signature* ao body das mensagens SOAP enviadas, criada com uma chave pública obtida através de um pedido de certificado ao CA, e verificamos a validade da *signature* nas mensagens SOAP recebidas com a chave privada que é obtida de forma local através da keystore.

Garantir Frescura das mensagens:

Para garantir a validação temporal é criado um handler que acrescenta um cabeçalho a mensagem SOAP com a data e a hora atual (timestamp) à saída do cliente (outbound), que deve ser lido à chegada do servidor pelo handler (inbound message).Se a diferença temporal for superior a 3 segundos a mensagem é rejeitada. Isto permite que a mesma mensagem não seja enviada várias vezes num intervalo de tempo que neste caso é de 3 segundos.

Handlers:

TemporalValidationHandler: ao enviar uma mensagem, é responsável por inserir a data no header da mensagem SOAP. Ao receber uma mensagem, lança um a RuntimeException caso verifique que passaram mais de 3 segundos desde a data no header da mensagem. É desta forma responsável por assegurar a frescura das mensagens.

CypherCCHandler: procura o número do cartão de crédito em mensagens relativas à operação "BuyCart". Se for uma mensagem enviada, cifra-o com a chave pública obtida através do certificado que se encontra no módulo "ca-ws-cli"; se for uma mensagem recebida, decifra-o com a chave privada obtida através do certificado do nosso grupo que se encontra no módulo "security" (dado pelos professores da cadeira).

SigantureHandler: ao enviar uma mensagem, cria uma *signature* com a chave pública obtida através do certificado, acrescentando-a à mensagem. Ao receber uma mensagem, usa a chave privada obtida através do certificado do nosso grupo para verificar se a *signature* da mensagem é válida. Caso esta não seja, lança uma RuntimeException. É desta forma responsável por assegurar a autenticidade e integridade das mensagens.

AttackHandler: após feita a *signature* pelo SignatureHandler, procura o produto "XPTO" em mensagens relativas à operação "GetProduct" e altera o campo da mensagem correspondente ao ID do produto para "HACKED".

SOAP Messages

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <t:tempValidationHeader xmlns:t="http://org.komparator.A63">2017-05-05T21:06:03.745</t:tempValidationHeader><n:
        nameHeaderxmlns:n="http://org.komparator.A63">A63_Supplier2</n:nameHeader>
            <s:signatureHeader xmlns:s="http://org.komparator.A63">
            jH6/twCW5j38WHBozamcSAMsg0qTi1UFBgwpZWlmJnccbLLvUuBT5YWmJpgJVM1q958A0DfOuPnPF1znvO9hmqv33TxjS/X9Hp86ALpNaWbrVuhmorNeBfG2fv6
            c+STmKt2GYa9deEFUerjjFHZ9dbkxs4AgVE9YSopTSKe3sw3dltnXWIC428SZERgOk6NLceAKA4F1gDx8fZX73zmEApzxA/VJIGvWKkzwCeIZvts9fKgSFtpsQn
            chMnYwT/SjFXVsHFN7eX/smNYr7SSME9I4e3hAQvgkYSwyxtJClrd7oUNmvb+H1TIvCFMmI4CzWPahaBIUHvnQwFqaVHiTBQ==
            </s:signatureHeader>
    </SOAPENV:Header>
        <S:Body>
            <ns2:listProductsResponse xmlns:ns2="http://ws.supplier.komparator.org/"><products><id>X1</id><desc>Basketball</desc><
            quantity>10</quantity><price>10</price></products><products><id>Z3</id><desc>Soccer ball</desc><quantity>30</quantity><
            price>30</price></products></ns2:listProductsResponse>
        </S:Body>
</S:Envelope>
```

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <c:cipherCCHeader xmlns:c="http://org.komparator.A63"/>
    </SOAP-ENV:Header>
        <S:Body>
        <ns2:searchItems xmlns:ns2="http://ws.mediator.komparator.org/"><descText>CVS</descText></ns2:searchItems>
        </S:Body>
</S:Envelope>
```