Sistemas Distribuídos 2016-2017

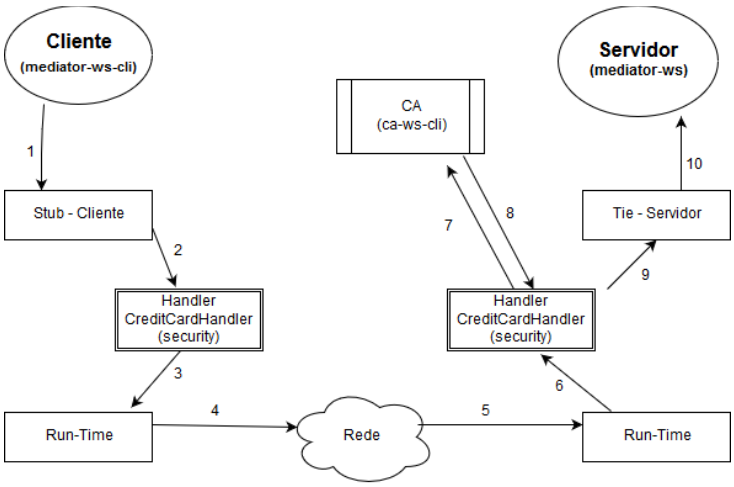
T06

Leonor Clemente, 78054

Ana Silva, 79304

GITHUB: https://github.com/tecnico-distsys/T06-Komparator

LEIC, Taguspark

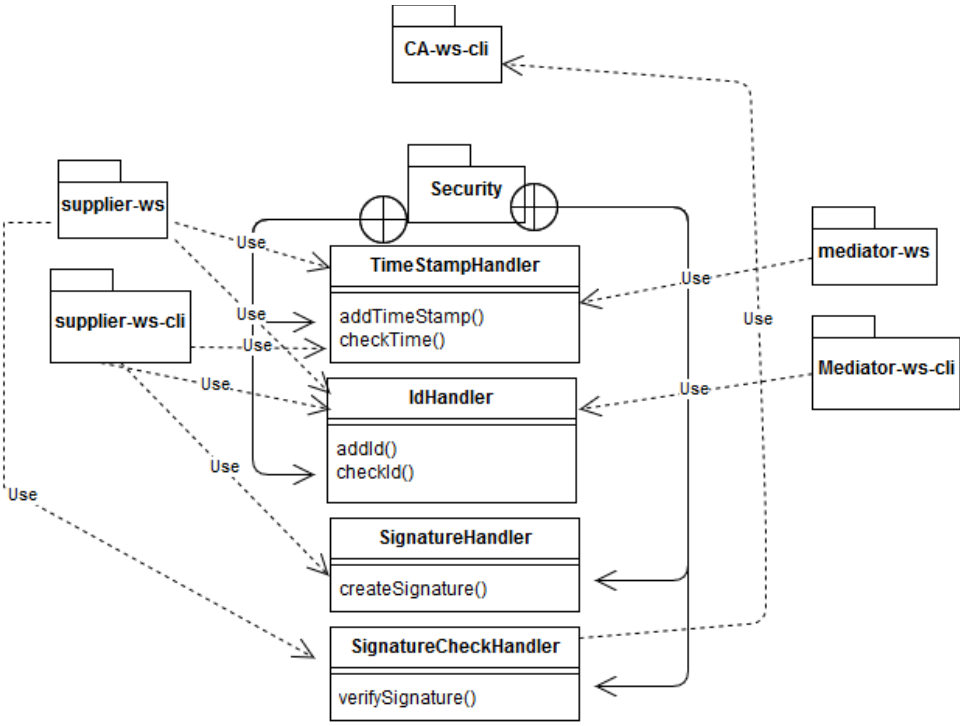


O diagrama acima demonstra os vários passos que acontecem quando é efectuado um pedido buyCart sendo condição necessária de segurança proteger o número de cartão de crédito no canal de comunicação entre o mediator e o mediator-ws-cli. Em seguida resume-se os diversos passos efectuados neste procedimento:

(1) Cliente (mediator-ws-cli) efectua um pedido buyCart onde passa o nome do carinho e o número de cartão de crédito
(2) O stub do Client envia esse pedido para o Handler (CreditCardHandler) que apanha a mensagem SOAP (Outbound). O handler retira do cabeçalho da mensagem SOAP o número de cartão de crédito e depois efectua a cifra desse número com a sua chave pública. Após cifrar, coloca o número já cifrado novamente no cabeçalho da mensagem SOAP.
(3) O handler envia a mensagem para RunTime.
(4) e (5) A mensagem passa na rede até chegar ao Servidor
(6) A mensagem SOAP é detectadapelo Handler (CreditCardHandler) mas desta vez do lado do Servidor (Inbound) . O handler procede então à extracção do cabeçalho da mensagem SOAP do número de cartão de crédito.
(7) O handler faz um pedido a CA de forma a obter o certificado do Mediator.
(8) A CA devolve o respectivo certificado. O Handler conseguem assim obter a chave privada e decifrar o número de cartão de crédito.
(9) Após obter o número decifrado o handler adiciona o número ao header da messagem SOAP e envia para o tie do servidor.
(10) É efectuado o pedido buyCart no servidor.
No final é devolvida a resposta do pedido efectuado ao cliente.

De forma a garantir a **Frescura** as mensagens antes de entrarem no handler responsável por cifrar o cartão de crédito (CreditCardHandler) passam pelo handler TimeStamp no lado do cliente (outbound) onde é adicionado uma marca temporal ao cabeçalho da mensagem SOAP e no mesmo handler mas no lado do servidor (Inbound), obtém-se essa marca temporal e verifica-se se a mensagem demorou mais de 3 segundos a chegar ao servidor. Se sim, essa mensagem é rejeitada.

De forma a garantir a **Unicidade** é adicionado no IdHandler do lado do cliente (outbound) um secure random number que ao chegar ao mesmo handler mas do servidor (inbound) verifica se esse número já existe numa lista global do programa. Caso exista significa que a mensagem é repetida e como tal ignora-a.



Para a assinatura digital além da utilização dos handlers mencionados anteriormente, que garantem a frescura e unicidade das mensagens, também é utilizado um handler que garante a **autenticidade e integridade** da mensagem que passa no canal de comunicação entre o supplier-ws e o supplier-ws-cli. Na assinatura digital o handler do lado cliente (outbound) cria, com a chave privada do emissor, a assinatura digital da mensagem SOAP a enviar e adiciona essa assinatura ao cabeçalho da mensagem assim como a identificação de quem está a enviar a mensagem. No handler do lado do Servidor (Inbound), tanto a assinatura como a identificação do emissor são removidos do cabeçalho da mensagem e é obitdo através da CA (ca-ws-cli) o certificado do respectivo emissor. É também obtido o certificado da CA (car.cer) e feita um verificação destes dois certificados de forma a garantir que o certificado do emissor foi assinado pela CA. Caso o passo anterior se confirme é então feita a verificação da assinatura utilizando a chave pública do emissor.

As mensagens SOAP terão o seguinte esquema:

Após adicionado o TimeStamp e Identificador único:
<S:Envelope ...><SOAP-ENV:Header><ts:TimeStamp xmlns:ts="http://org.komparator/security">2017-05-05T20:40:18</ts:TimeStamp><id:Identifier xmlns:id="http://org.komparator/security">79989BBBC375062456ECA4A46054738058660B29CAF-DAA2B8A74EFAFD54F8991</id:Identifier></SOAP-ENV:Header><S:Body><...></S:Body></S:Envelope>

Depois de cifrado o número de cartão de crédito (Inbound):
<S:Envelope ...><SOAP-ENV:Header><ts:TimeStamp xmlns:ts="http://org.komparator/security">2017-05-05T20:40:06</ts:TimeStamp><id:Identifier ...>0BE29924588E...</id:Identifier></SOAP-ENV:Header><S:Body><ns2:buyCart ...><cartId>Cart1</cartId><creditCardNr>LnaWRx9hojKNTOIBVP….</creditCardNr></ns2:buyCart></S:Body></S:Envelope>