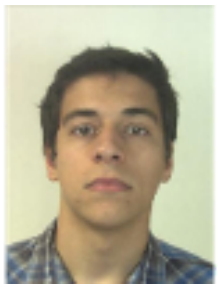
Projeto Komparator

Sistemas Distribuídos

2016/2017

GRUPO T50
https://github.com/tecnico-distsys/T50-Komparator

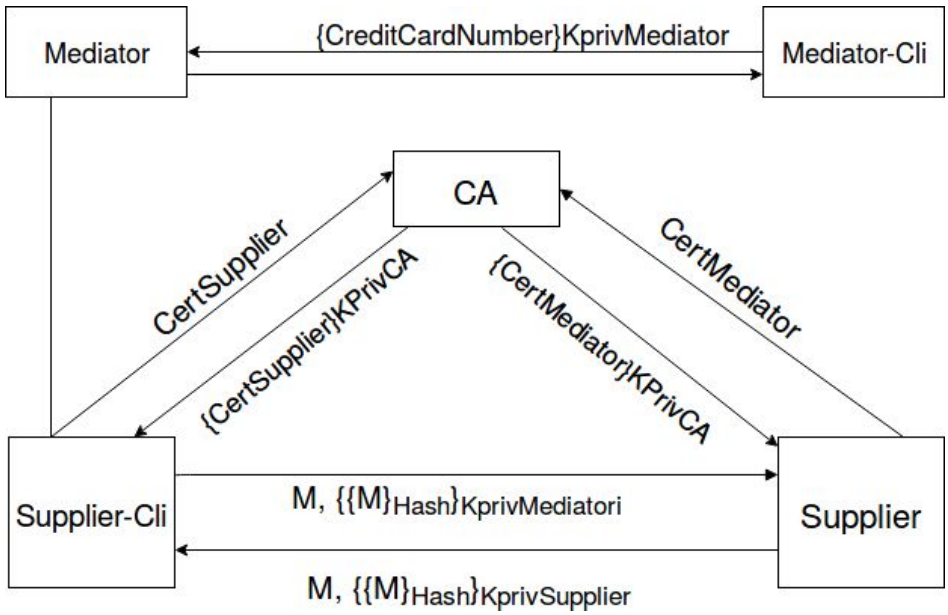


77917
Daniel Madruga
daniel.madruga@tecnico.ulisboa.pt

78013
Bruno Henriques
bruno.s.henriques@tecnico.ulisboa.pt

78042
Bruno Carola
bruno.carola@tecnico.ulisboa.pt

Esquema de Segurança



Segurança da comunicação entre Mediator-Cli e Mediator (CreditCardNr)

Quando o mediator-ws-cli faz a operação buyCart é necessário fornecer creditCardNr. Para garantir a confidencialidade este vai cifrado com a chave privada do mediator.
E é decifrada com a chave pública do mediator, isto no mediator-ws.

mediator-cli.xml Raw

```
<!-- LoggingHandler: Handling OUTbound message. (TOP-CHAIN) -->
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <S:Body>
    <ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/">
      <cartId>MyCart3</cartId>
      <creditCardNr>4556648855991861</creditCardNr>
    </ns2:buyCart>
  </S:Body>
</S:Envelope>

<!-- LoggingHandler: Handling OUTbound message. (BOTTOM-CHAIN)-->
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <S:Body>
    <ns2:buyCart xmlns:ns2="http://ws.mediator.komparator.org/">
      <cartId>MyCart3</cartId>
      <creditCardNr>
        o9u3SGmf0OU1/2lvew8iF0LGK4m4OC2NT6xBHHCBKFpFz+/UhUpjOUjHPTfT1La9Rb7UX2ToUEckqYNQ/F1/ZBC8pXcCPJiVkhIgv6PZK+BdYHLGVi/
        SHCAknEywgFkVyTdZ4vySER1X3lDO7Jrf82+sEbDrDGzntPvIYRhuvLpoypmbacLxCtfWJHvMgdyImulp1h/tFqlu9OnYwvU0/ptCZBY9xldZ3lOJtQ
        vaN6XPUFyJlf9RziNhczFojXVA2zYgLBpB5EUjdrNNTfzSBiBykCBn8PE98eYJXPr4LUZb7hYCk4r2uhqFspqnf1YbMCNHuGJVYvjOm9sNq0XWFA==
      </creditCardNr>
    </ns2:buyCart>
  </S:Body>
</S:Envelope>
```

Segurança da comunicação entre Supplier-Cli e Supplier

Garantir a Frescura

Para garantir a frescura das mensagens, cada mensagem envia um timestamp e um token. O timestamp é utilizado para descartar mensagens com mais de três segundos. Prevenindo que uma mensagem com mais do que três segundos possa ser processada. O handler que implementa esta lógica chama-se **TemporalHandler**.
O Token é guardado para caso um atacante volte a re-enviar a mensagem dentro dos três segundos essa mensagem não volte a ser processada. O handler que implementa esta lógica chama-se **FreshnessHandler**.
Assim é possível garantir a frescura da mensagem e segurança contra replay attacks.

Garantir a Integridade e Não Repúdio (**SignHandler**)

Mensagem Outbound

É adicionado um header (myRequestHeader) à mensagem SOAP com a seguinte estrutura:

timestamp # keyAlias # signedMessageText # messageToSign

- timestamp: Data de saída da mensagem
- keyAlias: Nome de quem vai assinar
- signedMessageText: Hash da mensagem seguido de assinatura de quem envia
- messageToSign: mensagem original

Mensagem Inbound

Pede à CA o certificado de quem envia a mensagem (através do keyAlias).
De cada vez que uma entidade recebe um certificado, verifica se este foi assinado pela CA.
Decifra a parte cifrada (signedMessageText) obtendo o hash (H) enviado.
Faz um hash (H') da mensagem enviada (messageToSign). Compara H com H'. Se forem iguais aceita a mensagem, caso contrário rejeita-a.

supplier-cli.xml

Raw

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
                <t:time xmlns:t="http://supplier.komparator.org/">2017-05-05T19:36:40.111</t:time>
                <id:token xmlns:id="http://supplier.komparator.org/">lYfL4OkYFUI555kUbAZzPA==</id:token>
                <e:myRequestHeader xmlns:e="urn:example">
      2017-05-05T19:36:40.111#T50_Supplier2#JWfS6h4iyK4ITpWnIqaGvDFJwxcaSvq1MPvEXAfHEhxZxEql/OiFpvX75IksHu4qZqal+MhaH+Wq
      Q48wChg8vTVzVmIyT8tZBeW/1Ac3APbca55hRlW2I/CuPGdxdtyFdlt6IDf9DeyP8pofMaFDx73zZQk9cfg6TBK5waLQqUI74qU8rcCOSjULvctcfq
      ZRvozQ5IOeb9kk3BrYMlFkiw1heCVrPwBbrAGW9Ug1lEFkZVCm66xAhbeR8+d/NxDtSUafkFILnm5pdxLEvW+/xz8ik0agq6gpm9Bqghj+i17/jiiR
      EvDP14kAOOuNxrqi+Ppo1XobB6Et309tXjDOGg==#&lt;S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:
      SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"&gt;&lt;SOAP-ENV:Header&gt;&lt;t:time xmlns:t="http://supplier
      .komparator.org/"&gt;2017-05-05T19:36:40.111&lt;/t:time&gt;&lt;id:token xmlns:id="http://supplier.komparator.org/"
      &gt;lYfL4OkYFUI555kUbAZzPA==&lt;/id:token&gt;&lt;/SOAP-ENV:Header&gt;&lt;S:Body&gt;&lt;ns2:createProductResponse x
      mlns:ns2="http://ws.supplier.komparator.org/"/&gt;&lt;/S:Body&gt;&lt;/S:Envelope&gt;
    </e:myRequestHeader>
      </SOAP-ENV:Header>
      <S:Body>
              <ns2:createProductResponse xmlns:ns2="http://ws.supplier.komparator.org/"/>
      </S:Body>
</S:Envelope>
```