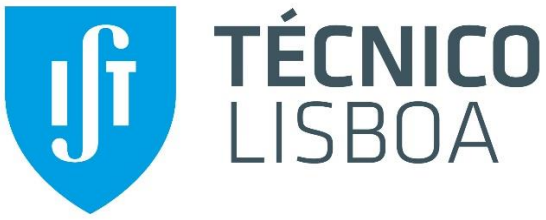
Sistemas Distribuídos



Relatório da 3ª Entrega do Projecto (P3)

Grupo A68



João Silveira
80789

Pedro Orvalho
81151

Rodrigo Mira
81271

https://github.com/tecnico-distsys/A68-Komparator

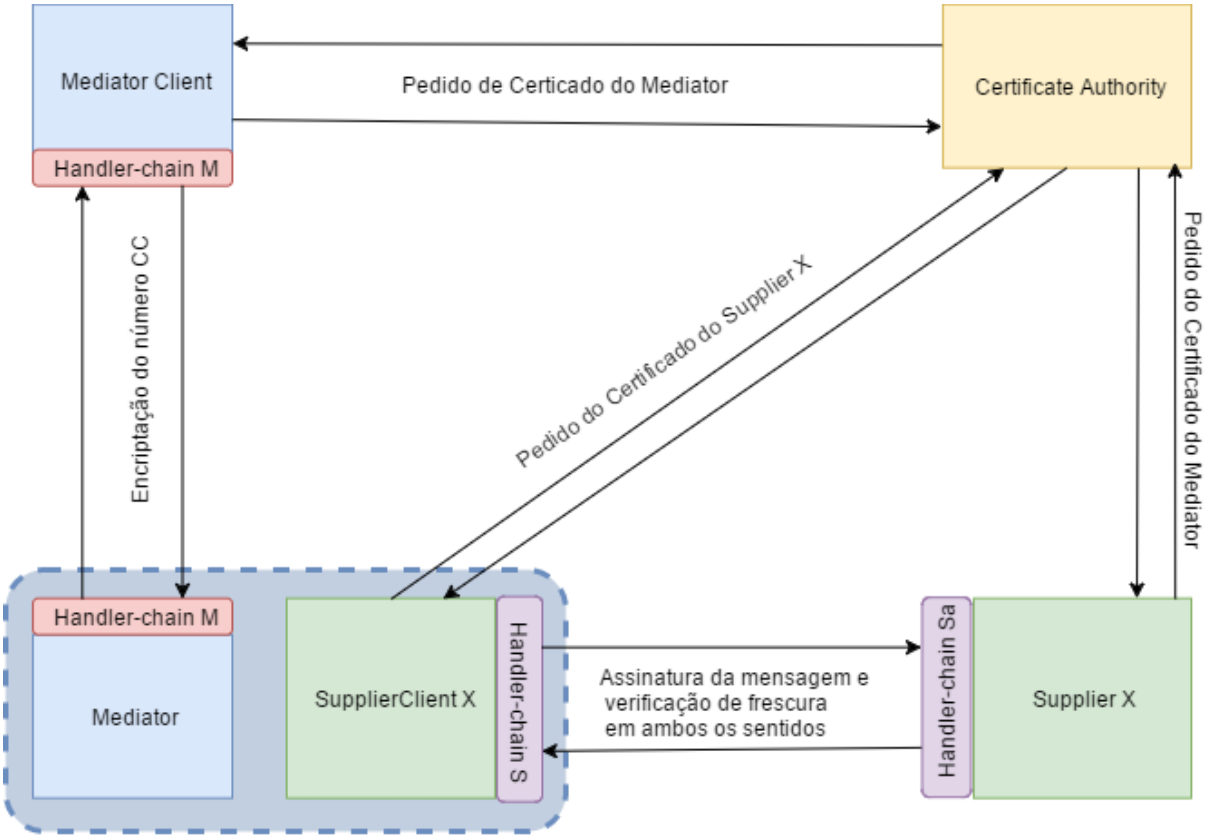


Figura 1 – Esquema da solução de segurança

Confidencialidade

A confidencialidade é necessária no envio do número de CC do MediatorClient para o Mediator. Esta é garantida através da encriptação e desencriptação do mesmo usando o protocolo "RSA/RCB/PKCS1Padding", implementadas no CryptoHandler presente na Handler-chain M.

```
<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>Cart1</cartId>
            <creditCardNr>AAnyh2qeGK/vPtXM5f2LilQh+/0e2anj0+6XO7
3R2xtURIMZV7R3N56Dbs9z0O5jWDpTGfeDoQJZuOdeALJYA9SV2d
Wly8qO4MtaTaNo+7S1Tuwsy8jbqAoAt6FIQCwXl5agIvRyciEpgC
cYgLh6HOXKgabSQV0J82LX4/Fk+lWV8aWi1Nk2MR5X5/p084+XHQ
h14ZcxlOGA4E7sBZoZXelWLkCnCxRiCY0+ikBwU7huSveRrFo1R5
ooaxPt+MMQGUhHPSYfVWfgzBxxpr0HFfheUVRicUFmI7RVJW1Uhp
efMTANdrq4RiW4kXRSewiraMs+Ap
fKqIwJCsGr76Xhjw==</creditCardNr>
        </ns2:buyCart>
    </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/>
    <S:Body>
        <ns2:buyCartResponse
            xmlns:ns2="http://ws.mediator.komparator.org/">
            <shopResult>
                <id>CartResult1</id>
                <result>COMPLETE</result>
                (...)
                <totalPrice>60</totalPrice>
            </shopResult>
        </ns2:buyCartResponse>
    </S:Body>
</S:Envelope>
```

Figura 2 – Mensagens SOAP entre MediatorClient e Mediator (operação buyCart: pedido e resposta)

Na mensagem de pedido é evidente a encriptação do campo creditCardNr do elemento buyCart do SoapBody (representada em base 64). De resto, o Soap Header e Body não são alterados pelos handlers.

Autenticidade, Integridade e Não-repúdio

Todas estes requerimentos são necessários na comunicação entre um SupplierClient X e um Supplier X. Estes são todos garantidos através da assinatura digital dos dados em ambos os lados, utilizando o algoritmo de assinatura "SHA256withRSA", implementada no AuthenticityHandler presente na Handler-chain S.

1. **Autenticidade:** As mensagens são enviadas em conjunto com uma assinatura de toda a respectiva mensagem, usando a chave privada do emissor. Assim, sendo que o emissor é o único que pode ter esta chave, temos garantia de que foi mesmo este que a enviou.
2. **Integridade:** Ao chegar ao emissor, a mensagem é verificada com a assinatura, que é em si um digest desta. Assim, podemos verificar se o conteúdo da mensagem que recebemos é o mesmo do que quando foi assinada do lado do emissor, garantindo que não foi alterado entretanto. **Este aspecto é testado através de um ataque ao campo price da operação getProduct, usando o AttackHandler presente na Handler-chain Sa.**

Frescura

A frescura é necessária na comunicação entre um SupplierClient X e um Supplier X. Esta é garantida através do DateHandler presente na Header-chain S, que regista a data de envio no Header das mensagens SOAP. Se a diferença entre esta data e a data actual for acima de 3 segundos, a mensagem é descartada.

No entanto o intervalo de 3 segundos pode permitir ataques de repetição neste intervalo de tempo. Esta situação poderia tentar-se evitar com a introdução de um campo aleatório que seria guardado do lado do recetor. À chegada de uma nova mensagem confirmar-se-ia se esse campo já foi utilizado anteriormente.

```
<S:Envelope
    xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <l:date xmlns:l="http://lmao">Fri May 05 16:20:49 WEST 2017
        </l:date>
        <l:wsName xmlns:l="http://lmao">A68_Mediator</l:wsName>
        <l:signature
            xmlns:l="http://lmao">b/0Trbh0H8orwZ+mtpJ0kgscQDz6V
            (...)
            oIJM+Qg==
        </l:signature>
    </SOAP-ENV:Header>
    <S:Body>
        <ns2:ping xmlns:ns2="http://ws.supplier.komparator.org/">
            <arg0>client</arg0>
        </ns2:ping>
    </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>
        <l:date xmlns:l="http://lmao">Fri May 05 16:20:50 WEST 2017
        </l:date>
        <l:wsName xmlns:l="http://lmao">A68_Supplier1</l:wsName>
        <l:signature
            xmlns:l="http://lmao">c/upTrM/gXpELDoiLWwmBN1Ysao9C
            (...)
            bdL5Edg==
        </l:signature>
    </SOAP-ENV:Header>
    <S:Body>
        <ns2:pingResponse xmlns:ns2="http://ws.supplier.komparator.org/">
            <return>Hello client from Supplier</return>
        </ns2:pingResponse>
    </S:Body>
</S:Envelope>
```

Figura 3 – Mensagens SOAP entre Supplier e SupplierClient (operação ping: pedido e resposta)

Nestas mensagens vemos duas adições ao SoapHeader original. Em primeiro lugar, temos o elemento "date", adicionado pelo DateHandler. Em segundo lugar, temos o elemento "signature" adicionado pelo AuthenticityHandler, que contém a assinatura de toda a mensagem (representada em base 64) incluindo a data. De resto, as mensagens SOAP não sofrem alterações.

Nota: As KeyStores (*.jks) foram colocadas na pasta resources do módulo security. O ideal seria coloca-las nos seus respetivos módulos, no entanto, como foi discutido com o nosso Professor dos Laboratórios, tal não foi possível em tempo útil.