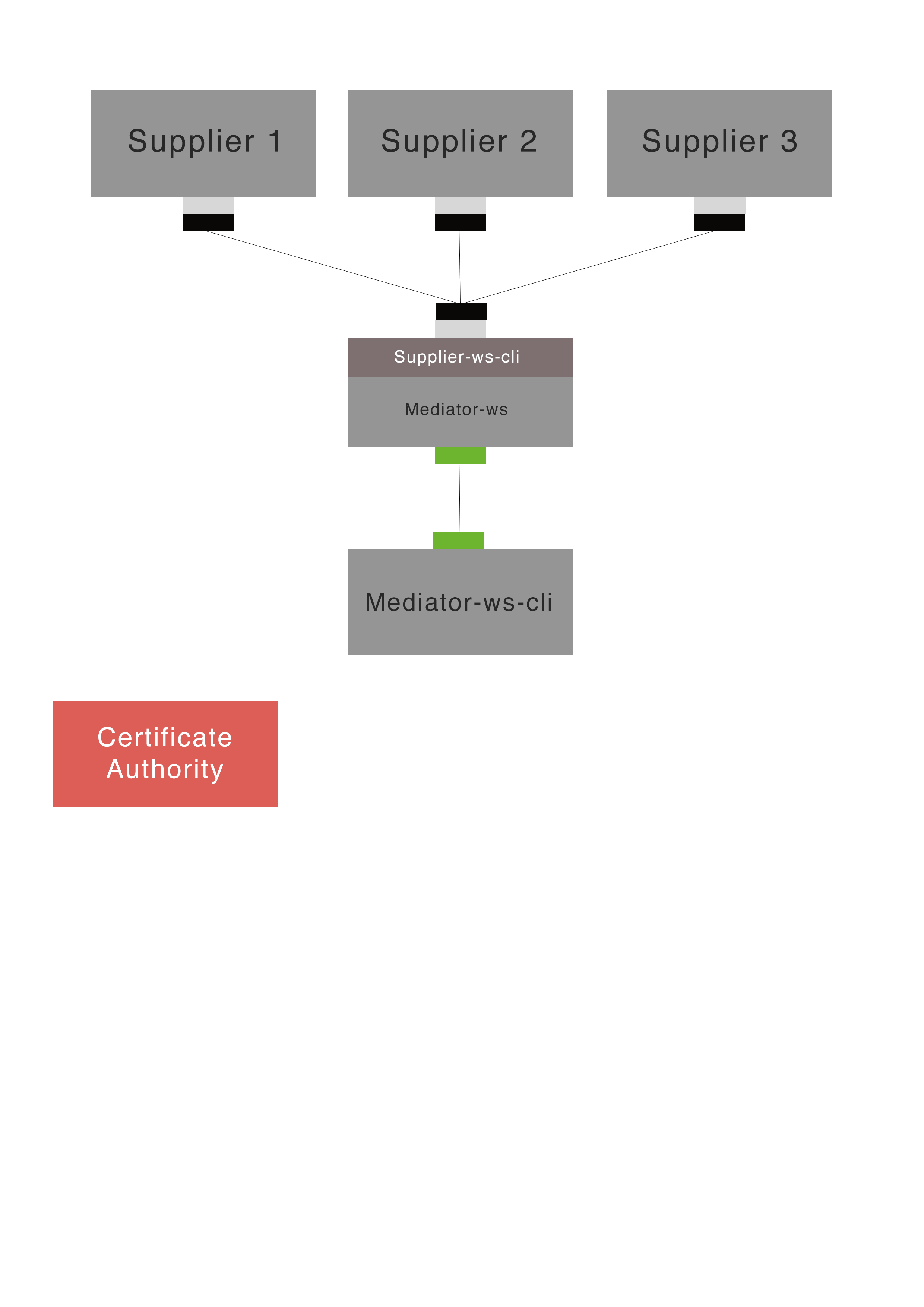


Sistemas Distribuídos

|  |  |  |
| --- | --- | --- |
| Grupo T04  Repositório GitHub: <https://github.com/tecnico-distsys/T04-Komparator> | | |
|  |  |  |
| 81900 – Nuno Anselmo | 81936 – Liliana Oliveira | 82047 – André Mendes |

**Pressupostos:**

TimestampHandler

SignatureHandler

CipherHandler

Módulos

**Legenda:**

* Certificate Authority tem ligação a todos os SignatureHandlers
* Foi ignorada a representação do LoggingHandler visto não pôr em risco a segurança

**Descrição:**

CreditCardCipherHandler – Encarregue de cifrar apenas o número de cartão de crédito quando o cliente envia numa operaçãoo buyCart. Cifra com a chave pública do Mediator e o Mediator descifra com a sua chave privada, o que segura o canal se alguém estiver no meio.

TimeStampHandler- Encarregue de marcar as mensagens com o tempo de envio e com um nonce, garantindo a inexistência de mensagens duplicadas em toda a longevidade da aplicação.

SignatureHandler – Encarregue de garantir a autenticidade e integridade através do uso de assinaturas sobre um checksum da mensagem, de modo a que se a mensagem for alterada, os checksums não coincidem ou porque alguém adulterou os dados (integridade) ou porque o receptor ao desencriptrar com a chave pública se obtém algo diferente do esperado (autenticidade).

Certificate Authority – Responsável por centralizar todos os certificados tornando-os disponíveis para quem precisar.

**SOAP messages**

Figura – Formato da mensagem entre Supplier e Mediator

**SOAP Message**

**SOAP Part**

**SOAP Envelope**

**SOAP Header**

**SOAP Body**

**Timestamp**

**Nonce**

**Signature**

**Message Data**

Figura - Formato de mensagem entre Mediator e Mediator-cli

**SOAP Message**

**SOAP Part**

**SOAP Envelope**

**SOAP Header**

**SOAP Body**

**Encrypted Timestamp**

**Encrypted Nonce**

**Encrypted Data**

Em qualquer um dos handlers os campos SOAP Message/Part/Envelope não são alterados.

Figura 1 – mensagem é **assinada**, é inserido um timestamp (número) e um nonce (base64), e é gerada a assinatura de toda a SOAPMessage, que é depois inserida no header.

Figura 2 - mensagem é **cifrada**, é inserido um timestamp (número) e um nonce (base64), e todos os campos são depois individualmente cifrados. A chave secreta para a cifra foi criada pelo Mediator Client, cifrada com a chave pública do Mediator, e transferida para o Mediator durante a primeira ligação. Todos os dados são sempre cifrados por esta chave secreta.