Guião de demonstração

Instruções de instalação e configuração

1. Obtenção do código entregue através do git executando o comando “git clone -b SD_P3 https://github.com/tecnico-distsys/A52-Komparator/”
2. Compilar o projeto através do master pom.xml na diretoria base do projeto utilizando o comando “mvn install -DskipITs”
3. Abrir 1 terminal onde irá ser executado o servidor Mediator: entrar na pasta mediator-ws e utilizar o comando “mvn clean compile exec:java”
4. Abrir 3 terminais para os servidores Supplier: entrar na pasta supplier-ws e utilizar o comando “mvn clean compile exec:java -Dws.i={NumeroS}” sendo os valores de NumeroS 1,2 e 3.

Caso 1: funcionamento normal

Descrição	Executar uma operação buyCart para observar que o número de cartão de crédito enviado para o servidor Mediator está encriptado e que as mensagens transmitidas entre o servidor Supplier e o cliente Supplier têm timestamp, assinatura e nome do serviço do emissor no header.
Estado inicial	Os 3 terminais de servidores Supplier e o do servidor Mediator estão em execução.
Instruções de execução	1. Abrir 1 terminal na pasta mediator-ws-cli (MediatorClient) 2. Executar um caso de teste de sucesso básico através do comando: “mvn verify -Dit.test=BuyCartIT#completeBuyOneItemOneCartTest” 3. Analisar mensagens impressas nos terminais de cada servidor
Resultados esperados	A mensagem SOAP enviada pelo MediatorClient para o servidor Mediator tem o número de cartão de crédito cifrado na tag <creditCardNr> do Body. As mensagens enviadas entre os servidores Suppliers e o cliente Supplier associado ao servidor Mediator contém os 3 elementos no header: o timestamp, a assinatura e o nome do serviço que enviou a mensagem.

Caso 2: resistência a um ataque

Descrição	Executar uma operação getProduct com um argumento de id especifico (“HARAMBE”) para ativar o handler de simulação de ataque (AttackingHandler). O handler irá alterar o preço existente na mensagem de resposta enviada do servidor Supplier para o cliente de 10 para 666.
Estado inicial	Os 3 terminais de servidores Supplier e o do servidor Mediator estão em execução.
Instruções de execução	1. Abrir 1 terminal na pasta supplier-ws-cli (SupplierClient) 2. Executar o caso de teste de simulação de ataque através do comando: “mvn verify -Dit.test=GetProductIT#attackHarambeTest” 3. Analisar mensagens impressas nos terminais de cada servidor
Resultados esperados	O teste tem sucesso porque recebe uma RuntimeException, ou seja, o cliente recusou a mensagem alterada pelo atacante.