Sistemas Distribuídos 2015-2016

Grupo A33

URL do repositorio:
https://github.com/tecnico-distsys/A_33-project

Membros:
Henrique Caldeira, 75838
Miguel Fonseca, 67040

Segurança:

Distribuiçao de chaves:

Começá-mos por criar um novo webservice, authentication-server-ws, responsável por distribuir chaves públicas e certificados de chave pública pelos intervenientes.
Cada um dos intervenintes(broker e transporters) tem as suas chaves privada e pública a partida, em que a chave privada é apenas conhecida por ele e pelo authentication-server.
Sendo assim:

1. O serviço Broker tem uma keystore que contém um par de chaves pública-privada.
2. Os serviço Trasporter tem uma keystore que contém dois para de chaves, uma para cada um dos Transporters esperados, 1 e 2.
3. O Authentication-Server acesso a estas duas keystores, assim como a sua própria keystore, que contém o seu par de chaves.

Estas keystores e chaves foram geradas usando o comando “keytool” do linux, e guardadas em ficheiros.

Foram também gerados 3 certificados de chave pública, um para cada interveniente (Broker, Transporters) e um outro para o Authentication-Server. Inicialmente, apenas o Authentication-Server detém estes certificados, guardados em ficheiros, que os intervenientes podem lhe podem pedir.
Os certificados foram gerados recorrendo novamente á ferramenta “keytool”, usando as chaves publicas anteriormente geradas.

Comunicaçao:

De modo a cumprir o requisitos, decidimos adicionar as mensagens SOAP:

1. Um digest(resumo) da mensagem a enviar, encriptada como a chave privada do emissor (garante nao-repudio da mensagem por parte do emissor).
2. Um certificado de chave publica do emissor (garante autenticaçao).
3. Um nonce, gerado através de numeros aleatorios e da data actual, de modo a contrariar ataques que repetiçao de mensagem.

Um receptor vai, ao receber a mensagem, por esta ordem:

1. Decifrar o resumo recebido, usando a chave publica do emissor.
2. Gerar o resumo da mensagem e comparar com o resumo recebido. Se forem diferentes, rejeita a mensagem.
3. Retirar o nounce, e verificar se este ainda nao se encontra na lista da nonces recebidos. Se nao se encontrar, adiciona-o a lista e aceita a mensagem. Se ja tiver o nonce, rejeita a mensagem.

4. Guarda a mensagem com o certificado, de modo a o emissor nao poder repudiar o envio da mensagem mais tarde.