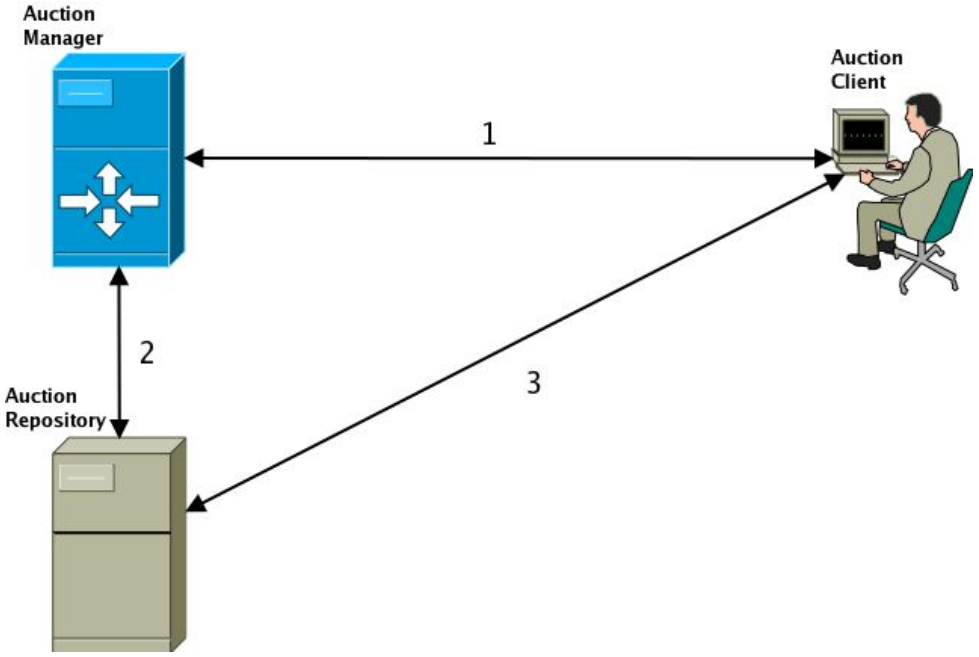
Milestone Segurança

Canais de Comunicação

Serão necessários três canais de comunicação:



1. **Canal Auction Client <-> Auction Manager**
    a. Criação e remoção de leilões ativos.

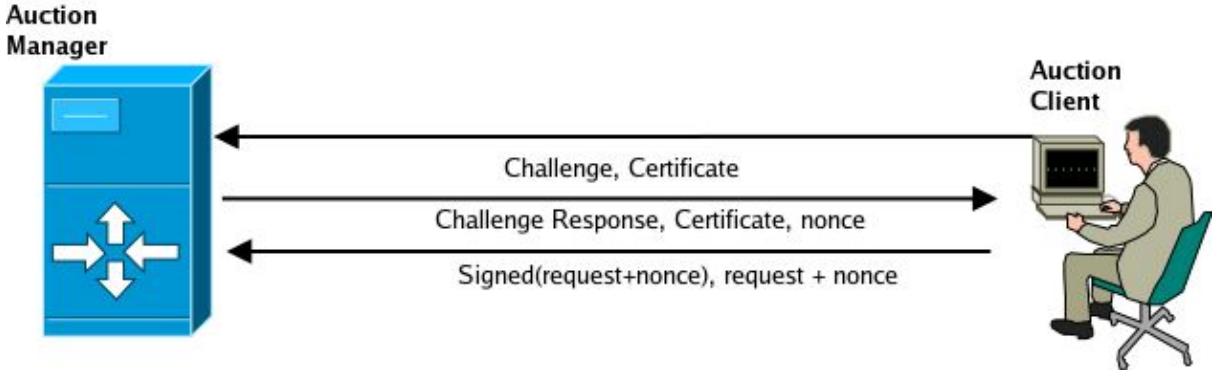
2. **Canal Auction Manager <-> Auction Repository**
    a. Criação e remoção de instâncias de leilões após pedido de utilizador.
    b. Validação dinâmica de ofertas.

3. **Canal Auction Repository <-> Auction Client**
    a. Leitura de leilões ativos.
    b. Criação de ofertas.

Autenticação / Geração de Session

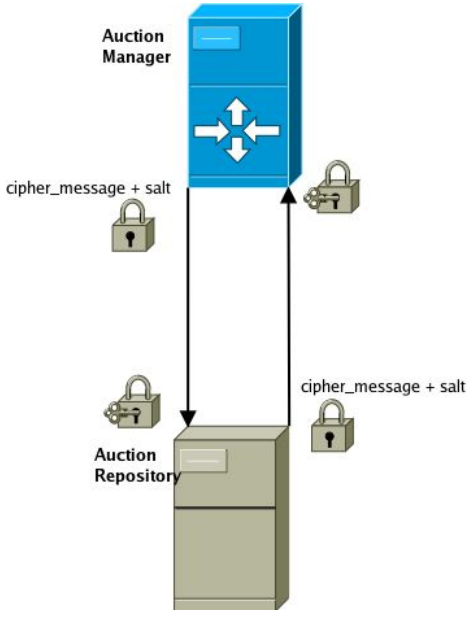
Canal Auction Client <-> Auction Manager

Este canal é apenas usado para criação e remoção de leilões. Isto significa que não existe a necessidade de uma sessão entre os dois. Contudo, é necessário certificar e identificar a origem das mensagens. Para existir comunicação neste canal é necessário que o Auction Manager e o Auction Client possuam pares de chaves em que a chave pública é certificada. No caso do Auction Client usamos, obviamente, o cartão de cidadão.



A comunicação é iniciada com o envio de um challenge e o certificado do utilizador para o servidor. O servidor responde ao challenge usando a sua chave pública e enviando o seu certificado para que o utilizador o possa validar. Na mesma mensagem o servidor envia também um nonce ao utilizador de maneira a tornar o request único. O utilizador termina por enviar o pedido a realizar (criação / remoção de leilão) assinado junto com o nonce. Mais detalhes sobre a criação / remoção do leilão encontra-se na página 4.

Canal Auction Manager <-> Auction Repository



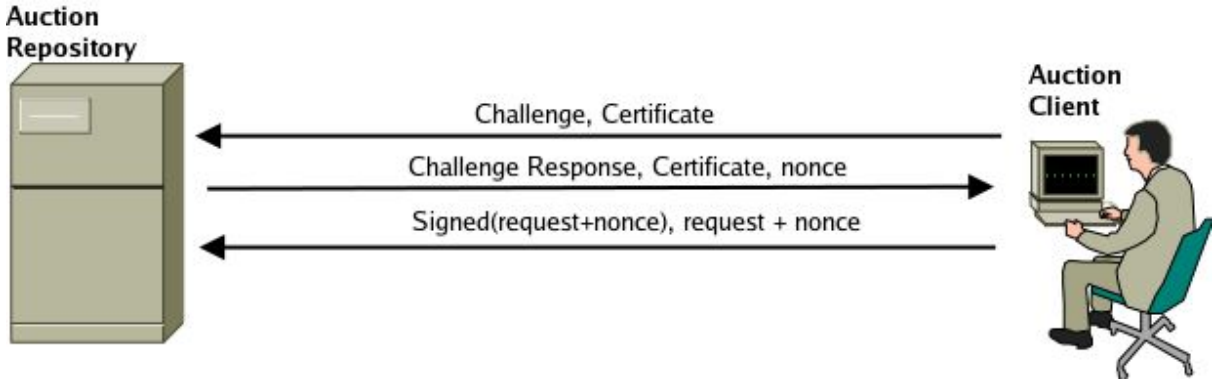
De maneira a garantir a confidencialidade na comunicação entre os servidores, as mensagens serão cifradas com uma chave simétrica previamente instaladas fisicamente nos servidores. É adicionado salt na cifragem de maneira a prevenir a duplicação de textos cifrados.

Canal Auction Repository <-> Auction Client

A comunicação neste canal tem a necessidade de ser confidencial de maneira a impedir fraudes nas ofertas de leilão.

Este canal é usado quando o cliente quer fazer uma oferta para um leilão, tal como se explica mais detalhadamente na descrição de criação de uma oferta na secção de Comunicação.

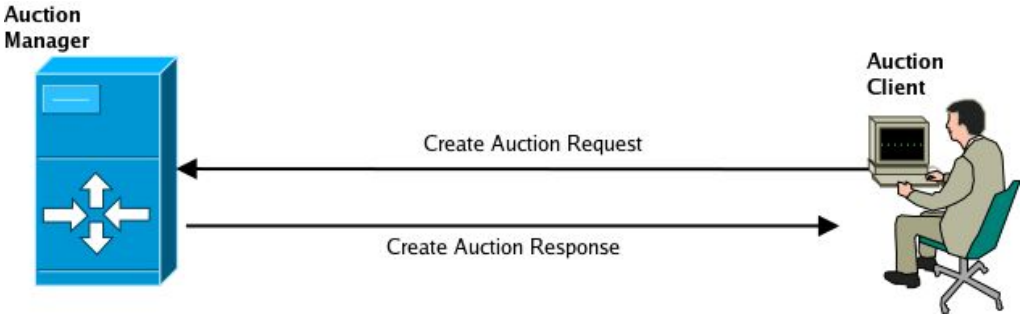
Neste caso, temos uma situação bastante semelhante ao que se passa entre o Auction Manager e o Auction Cliente.



Comunicação

Canal Auction Client <-> Auction Manager

Criação e remoção de leilões ativos.

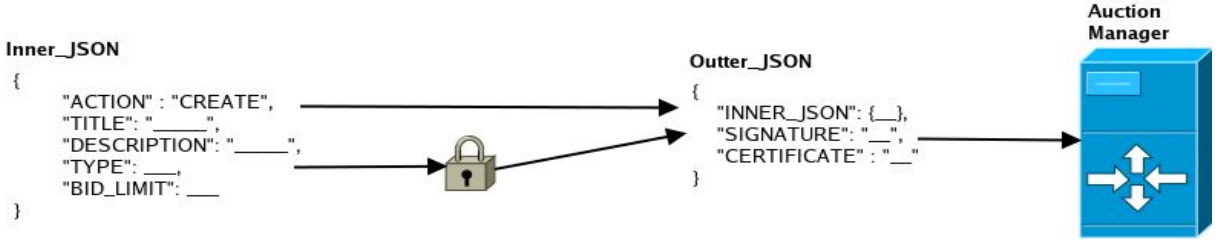


O pedido de criação de um leilão será realizado por o Auction Client após pedido dos parâmetros necessários ao utilizador.

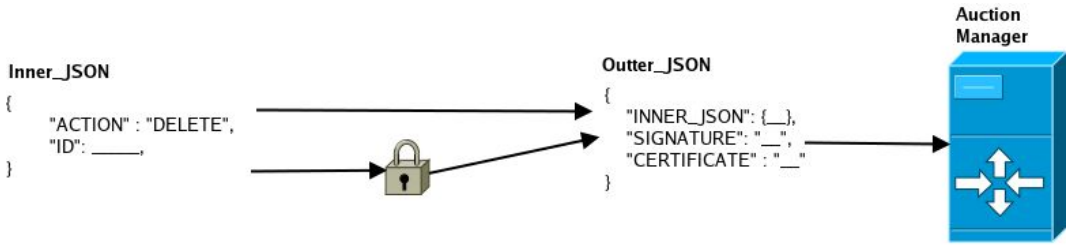
Um leilão é definido por:

(Required) Nome
(Required) Descrição
(Required) Tipo de Leilão
(Required) Tempo limite para novas ofertas
(Optional) Função para validação de ofertas.

Aspectos de segurança: Tendo em conta que a criação de um leilão não apresenta nenhum dado sensível, não existe a necessidade cifragem de dados. Contudo, é necessária a autenticação do utilizador. Isto será realizado com a assinatura digital do cartão de cidadão do utilizador.

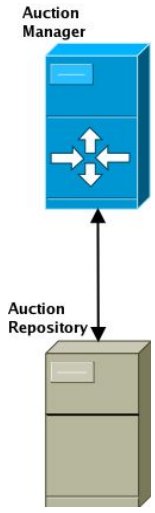


A remoção de um leilão será feita da mesma forma mas com diferenças ao nível do conteúdo do JSON.



Canal Auction Manager <-> Auction Repository

A comunicação entre estes dois servidores irá realizar-se sobre UDP/IP requests/responses.



Criação e remoção de instâncias de leilões após pedido de utilizador.

Após o pedido de criação do leilão por parte do utilizador, o Auction Manager irá verificar se os parâmetros são válidos. E, se for o caso, requisitará ao Auction Repository a criação deste leilão e do blockchain associado.

Validação dinâmica de ofertas.

Quando o utilizador apresenta uma oferta ao Auction Repository, este verificará a sua validação a partir da função dinâmica armazenada no Auction Manager.

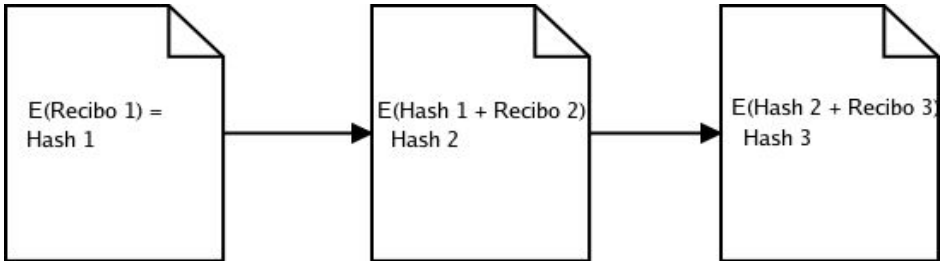
Canal Auction Repository <-> Auction Client

Leitura de leilões ativos e ofertas realizadas.

Chamada realizada do Auction Client para o Auction Repository. Devolve informação não sensível e totalmente pública pelo que não apresenta nenhum aspecto de segurança a discutir.

Criação de ofertas.

Por cada oferta adicionada ao leilão vai ser enviado um recibo ao cliente e armazenado numa memória não volátil. Isto é fundamental para que não haja problemas com troca de ofertas (inverter a ordem das ofertas). De maneira a evitar tentativas de trocas de ofertas de ambos os lados, é também adicionada a oferta a um blockchain. Neste caso, o blockchain tem um funcionamento semelhante a uma lista ligada ordenada, visto que pretende-se manter a ordem.



Será implementado um mecanismo denominado cryptopuzzle em que o envio das ofertas pode ser controlado prevenindo a ocorrência de spam, isto é controla a taxa de transferência com que as ofertas são enviadas.

Para o cliente fazer uma oferta:

1. Primeiro tem que pedir um cryptopuzzle;
2. Depois pode enviar a oferta para o Auction Repository;
3. A oferta é adicionada ao blockchain (depois de validada pelo Auction Manager);
4. É enviado um recibo para o cliente comprovando que a oferta foi adicionada ao leilão.

Catarina Silva, 76399
António Sérgio Silva, 76678