# Milestone

Departamento de Electrónica, Telecomunicações e Informática

UNIVERSIDADE DE AVEIRO

Sandra Moreira 76471, Ana Cruz 76351
simoreira@ua.pt, anapatriciacruz@ua.pt

4 de Novembro de 2017

# Capítulo 1

# Implementação

## 1.1 Segurança

### 1.1.1 Configuração da Session Key e Autenticação

Quando é estabelecida uma tentativa de conexão por parte de um utilizador, por cada sessão, é gerada uma Secret Key recorrendo ao algoritmo de Diffie Hellman.

Se ainda não existir informação acerca da chave pública do utilizador, é gerado o par de chaves a partir do algoritmo RSA. Dessa forma, a chave pública é passada para o servidor, sendo que a chave pública e privada do utilizador, assim como a chave pública do servidor, são também guardados do lado do cliente.

Posto isto, a conexão é cifrada recorrendo à Secret Key gerada inicialmente.

Finalmente, é feita a autenticação a partir da chave privada do utilizador.

### 1.1.2 Garantia de Respostas

A cada pedido do utilizador ao servidor, é necessário garantir que as respostas são enviadas corretamente face ao pedido que foi feito. Para isso, pensamos em ter um valor de verificação, sendo esse valor uma string com um tamanho fixo gerada aleatoriamente no pedido do cliente para o servidor e vice-versa. É também necessária a existência de uma Hash Table com valores de referência para cada tipo de mensagem. Assim, quando o utilizador faz um pedido ao servidor, o cliente envia no seu pedido, o valor de verificação. Do lado do servidor, é identificado o tipo da mensagem, obtendo-se o seu valor de referência a partir da Hash Table. É, depois, calculada a hash da concatenação do valor de verifiação com o valor de referência do tipo de mensagem recorrendo à hash function SHA-256. O valor de hash é depois enviado num campo da mensagem de resposta de volta para o cliente. Aí, o cliente faz o mesmo processo com o seu valor de verificação e valor de referência do tipo de mensagem, comparando, por fim, o valor recebido com o valor calculado.

### 1.1.3 Cartão de Cidadão

Inicialmente, pretendemos fazer toda a implementação sem o cartão de cidadão, mas mantendo-a modular o suficiente para depois a integração desse módulo não ser demasiado complicada.

Aquando a introdução do Cartão de Cidadão, a autenticação passará a ser feita com o par de chaves existentes no Cartão de Cidadão, substituíndo, assim, as chaves geradas a partir de RSA. Ou seja, a autenticação mantém-se igual mas as chaves passam a ser as do Cartão de Cidadão.

### 1.1.4 Comprovativos de receção

A cada mensagem enviada, o destinatário tem o poder de enviar um comprovativo de receção ao remetente. Para isto, e de forma a comprovar que de facto foi o destinatário que recebeu a mensagem e enviou o comprovativo, a mensagem RECEIPT será enviada com a mensagem recebida assinada pela chave privada do recetor. De forma a validar este comprovativo, o remetente, quando recebe o comprovativo, verifica a assinatura através da chave pública do destinatário.

No entanto, um utilizador só pode enviar um comprovativo de uma mensagem que efetivamente leu. Assim, é sempre necessário verificar se o ID da mensagem existe na receipt box do utilizador.

### 1.1.5 Cifragem das mensagens

De forma a garantir a segurança nas trocas de mensagens entre os utilizadores iremos usar dois tipos de cifras, algoritmo RSA e AES. AES para a geração de chaves de sessão entre os utilizadores e RSA para a geração de chaves que permitem a passagem de forma segura das chaves de sessão entre os utilizadores.

Inicialmente, os utilizadores quando se ligam ao servidor, trocam as suas chaves RSA públicas com o mesmo (e vice-versa) e estas vão ser usadas para cifrar as mensagens que vão passar as chaves de sessão entres os utilizadores. Os utilizadores trocam também entre si, as suas chaves públicas aos quais se vão ligar para que futuramente as mensagens possam ser cifradas com as chaves correspondentes dos mesmos.

A chave AES é criada por cada conexão com o servidor e serão geradas aleatoriamente para cada utilizador. Estas chaves serão usadas para cifrar as mensagens futuras que serão trocadas entre os vários clientes. Cada utilizador terá uma chave de sessão com o utilizador com o qual está ligado.

Assim, para que haja uma troca de mensagens de forma segura entre os utilizadores, existem duas camadas de cifragem, uma com a chave de sessão dos utilizadores e outra com a chave de sessão com o servidor. Desta forma, um userA quando pretende enviar uma mensagem para um userB, a mensagem será cifrada com a chave de sessão do userA-B, e posteriormente com a chave pública RSA do userB. Quando esta chega ao destinatário, é decifrada com a chave pública RSA do userB e depois com a chave de sessão userB-A.

Cada utilizador é responsável pela cifragem das suas mensagens guardadas na sua receipt box. Deste modo, as mensagens serão cifradas e decifradas por uma chave AES única.

Todas as mensagens são assinadas com a chave privada do remetente, garantindo a integridade, e validadas com a chave pública do destinatário.