Secure Messaging Repository System

Verónica Rocha (68809), Miguel Ferreira (72583), P01G01

Aveiro, 4 de Fevereiro de 2018

MIECT

Índice

1. Melhorias no Trabalho 1
2. Troca de Mensagens entre Cliente e Servidor 1
    2.1. Estabelecimento de Sessão 1
    2.2. Troca de Mensagens 3
    2.3. Autenticação do Servidor 4
3. Comunicação entre Clientes 5
    3.1. Dados de segurança do utilizador 5
    3.2. Mensagens Cliente-Cliente 5
4. Executar o programa 6

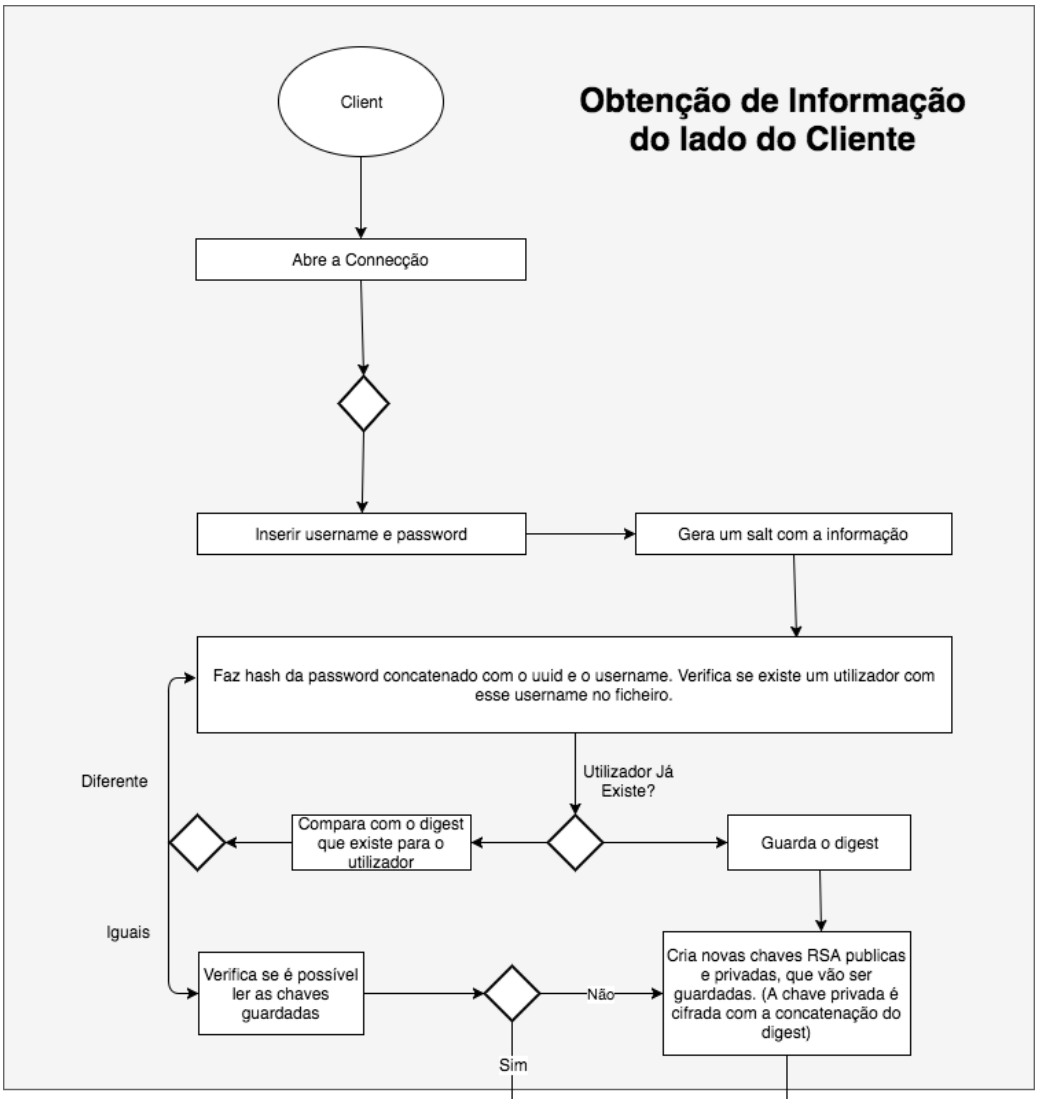
1. Melhorias no trabalho

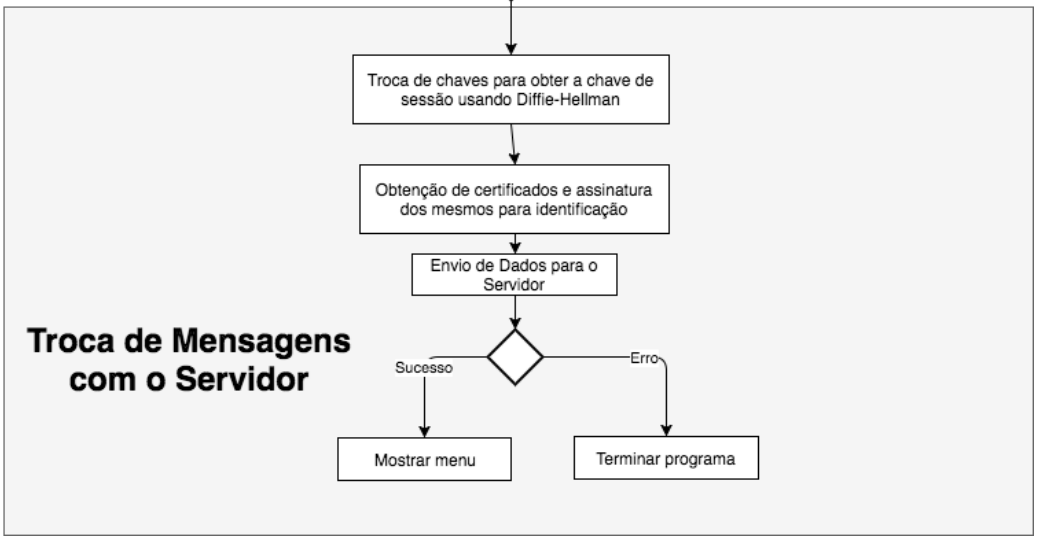
- Autenticação de utilizadores usando password
- Usar a password inserida pelo utilizador de modo a cifrar a chave privada
- O utilizador é identificado pelo seu uid e pelos dados do cartão de cidadão: Nome completo e número do cartão.
- Validação da Cadeia de certificados
- Autenticação do servidor
- Permitir comunicação segura entre clientes
- Todas as mensagens entre o cliente e servidor (excepto as mensagens de setup de sessão e troca de chaves DH) são cifradas e assinadas
- Mensagens guardadas no Receipt Box são cifradas com a chave pública pessoal do utilizador
- Contador de mensagens para garantir que o cliente e servidor estão sincronizados e que não há duplicação de mensagens

2. Troca de Mensagens entre Cliente e Servidor

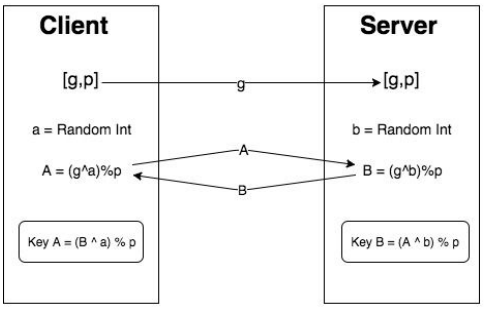
2.1. Estabelecimento de sessão

Quando um cliente se conecta, é necessário introduzir um username e password. O seu comportamento está descrito no esquema apresentado na figura abaixo.


Client
Obtenção de Informação do lado do Cliente
Abre a Connecção
Inserir username e password
Gera um salt com a informação
Faz hash da password concatenado com o uuid e o username. Verifica se existe um utilizador com esse username no ficheiro.
Utilizador Já Existe?
Diferente
Compara com o digest que existe para o utilizador
Guarda o digest
Iguais
Verifica se é possível ler as chaves guardadas
Não
Cria novas chaves RSA publicas e privadas, que vão ser guardadas. (A chave privada é cifrada com a concatenação do digest)
Sim


Troca de chaves para obter a chave de sessão usando Diffie-Hellman
Obtenção de certificados e assinatura dos mesmos para identificação
Envio de Dados para o Servidor
Troca de Mensagens com o Servidor
Sucesso
Erro
Mostrar menu
Terminar programa

Assumindo que o utilizador introduz os seus dados e que estes estão correctos, o cliente irá trocar mensagens do tipo “create” com o servidor de modo a estabelecer uma chave de sessão utilizado o algoritmo de Diffie-Hellman.



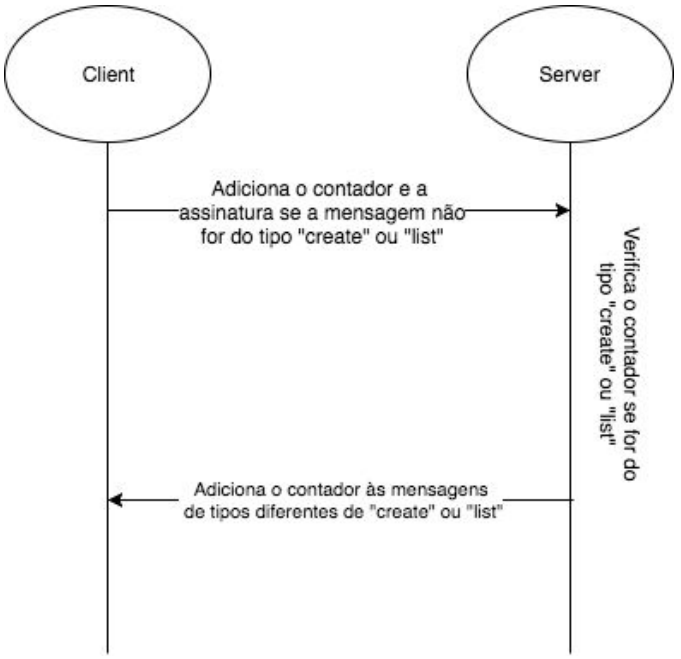
Depois de estabelecer a chave de sessão, o cliente irá enviar, numa mensagem devidamente cifrada com AES, a sua chave pública pessoal, o certificado do cartão de cidadão e a assinatura da chave sua chave pública.

Do lado do servidor, quando recebe esta mensagem, irá ocorrer uma verificação da assinatura da chave pública de modo a garantir a identidade do cliente.

O servidor irá verificar se o utilizador já existe no sistema ou não. No caso de não existir, os dados do cliente, bem como os campos de segurança como a chave pública pessoal e o certificado, serão guardados, caso contrário, o certificado obtido do cartão de utilizador que o cliente está a utilizar no momento em que executa o programa vai ser comparado com o que foi guardado em sessões prévias. Caso esta comparação não se verifique, é emitida uma mensagem de erro.

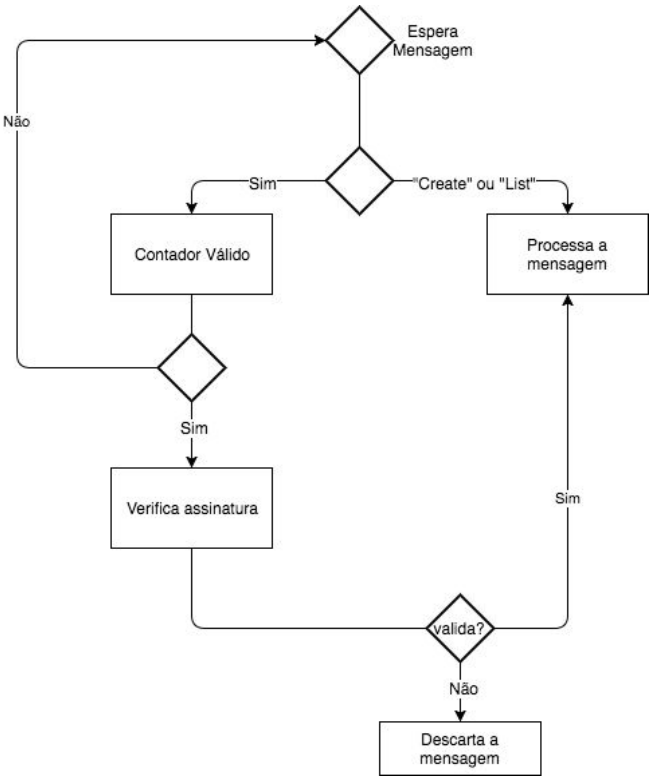
2.2. Troca de Mensagens

Para assegurar que as mensagens não são duplicadas por uma outra entidade e garantir a sua genuidade, existe um contador de mensagens, tanto do lado do cliente como do servidor, que faz a contagem das mensagens e compara com os resultados obtidos na troca de mensagens. Para este efeito, foi adicionado um campo “counter” às mensagens trocadas entre o servidor e o cliente em todas as mensagens, excepto nas do tipo “create” ou “list”, uma vez que as primeiras servem para o estabelecimento de sessão e as últimas são um pedido geral.



2.3. Autenticação do Servidor

A autenticação do servidor é feita através de chaves RSA assimétricas. O servidor gera um par de chaves sempre que é iniciado e manda a sua chave pública ao cliente. A partir daqui, todas as mensagens, excepto mensagens do tipo “create” e “list”, são assinadas usando este par de chaves.



3. Comunicação entre clientes

3.1. Dados de segurança do utilizador

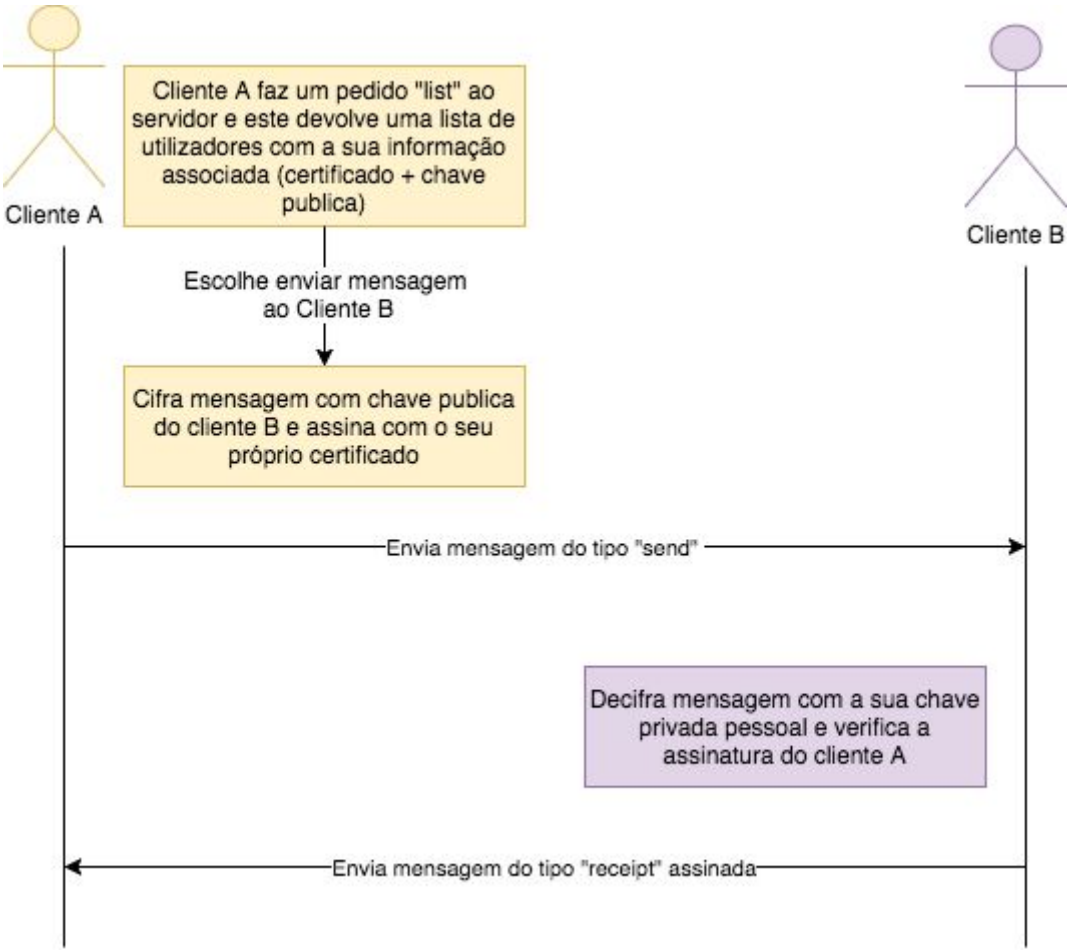
Para permitir uma comunicação segura entre clientes sem que o servidor “escute” a mensagem a ser enviada, foi necessário modificar os dados a ser enviados por cada utilizador. De modo a que o cliente que quer enviar uma mensagem consiga fazê-lo, irá necessitar de saber qual o utilizador através do seu campo uuid, da sua chave pública pessoal e do seu certificado.

```
user = { 'uuid' : uuid,
         'personal_public_key' : public_key,
         'certificate' : certificate }
```

Isto também implicou que as mensagens do tipo “list” devolvam não só a lista dos identificadores dos utilizadores, mas também os seus dados relativos à segurança, neste caso a chave pública e o certificado. O certificado, neste caso, também vai ser usado para retirar o nome e número do BI do dono do cartão.

3.2. Mensagens Cliente-Cliente

O processo de envio de uma mensagem entre dois clientes está descrito no esquema apresentado em baixo.



4. Executar o programa

Para executar o programa é necessário executar o servidor e em seguida os clientes.