Grupo *42* **Turno** *3ªF 11h00*

Bruno **Almeida**
69827

Dharita Queshil
75669

Pedro **Fialho**
75713

Introdução

A entrega final do projecto de Sistemas Distribuídos e Engenharia de Software consistiu na implementação de aspectos não funcionais, nomeadamente segurança e tolerância a faltas, de forma a garantir uma melhor qualidade de serviço.

Sendo a nossa parte do SD-ID.A que corresponde à parte de segurança, e ainda o SD-Store.B que corresponde à replicação activa, baseada em quóruns.

Ao longo deste relatório serão especificados aspectos relacionados com o desenvolvimento do projecto final, bem como a resolução de problemas.

SD-ID.A - Protocolo Kerberos

Tal como apresentado na imagem abaixo, o protocolo Kerberos no primeiro *round-trip* envia do cliente, sendo este o BubbleDocs, duas strings, uma delas composta pelo identificador do cliente (username), e a outra com a password desse mesmo cliente, o identificador do servidor ao qual se quer comunicar (sd-store) e ainda um número aleatório, designado como nonce, que serve para garantir a integridade da ligação entre o cliente e o servidor de autenticação (request_authentication), pois este valor irá ser retornado com uma modificação prevista pelo cliente.

O servidor de autenticação do Kerberos (sd-id) processa então esta informação, gerando um ticket (composto pelo username, pelo nome do servidor ao qual se quer ligar, os timestamps do ticket (ou seja, data de criação e de experição deste) e ainda uma chave partilhada que apenas o servidor e o cliente conhecem(Kcs)). Este ticket é ainda encriptado por uma chave gerada que somente os servidores, sd-id e sd-store, conhecem.

Depois de gerar o ticket, o servidor de autenticação envia este ticket e a Kcs com um nonce, encriptados com a hash da password.

No segundo round trip, o cliente envia, no cabeçalho dos soap handlers, o ticket, um tocken de autenticação encriptado com chave partilhada que contém o username e o tempo de pedido. Este envia também um MAC de toda essa mensagem.

O servidor, após receber os dados enviados pelo cliente, começa por fazer a verificação do MAC. Se este estiver correcto, o servidor desencripta o resto da mensagem e verifica se o pedido é válido de acordo com o token recebido.

Caso o pedido seja válido, o servidor encripta o MAC recebido e volta a enviá-lo ao cliente que, por sua vez, o desencripta e verifica a sua integridade.

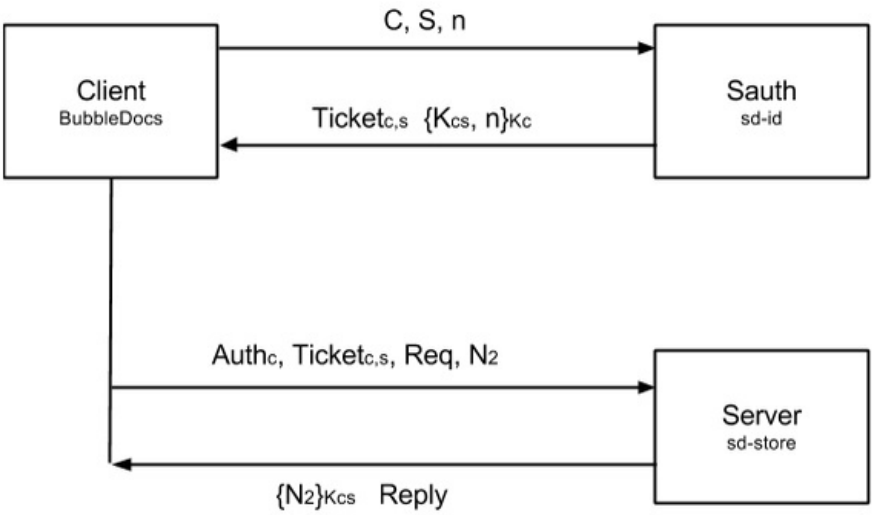

Imagem 1 - Protocolo Kerberos

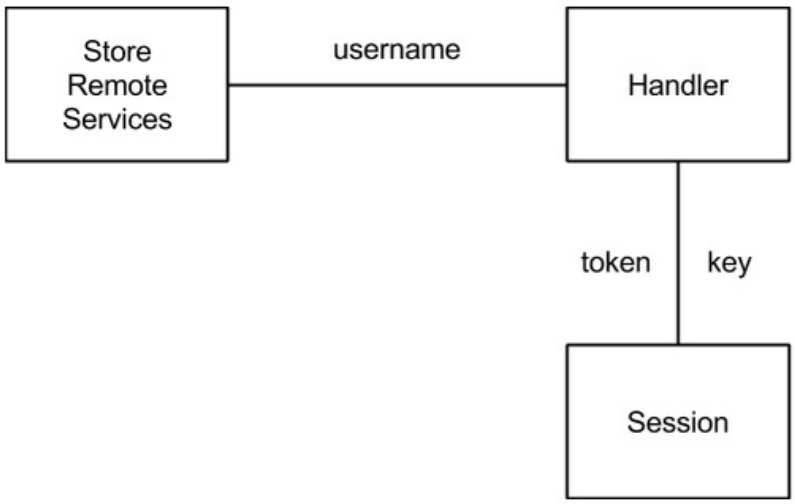

Imagem 2 - Funcionamento do handler

Requisitos não implementados:

- Na segunda round trip do servidor de autenticação do Kerberos, apenas encriptamos o ticket, passando os restantes objectos desencriptados, devido a um erro de bad padding.

- SD-Store.B.

- Testes locais de SD, devido a um erro de Client Transport (the server sent http status code 404 not found).