Relatório Sistemas Distribuídos – Grupo 08

Pedro Miguel Caeiro – 69775 João Afonso Baptista – 69364 Maria Costa e Silva – 69682



Requisito SD-IA.A:

Foi implementada a versão 5, simplificada, do protocolo *Kerberos*, tendo como cliente a aplicação BubbleDocs, servidor de autenticação o SD-ID e servidor para o qual podemos fazer pedidos o SD-STORE.

Para toda a criptografia de chave simétrica usada foi escolhida a especificação AES com blocos de 128 bits, uma vez que garante muito mais segurança contra ataques do que a já desatualizada DES, ou suas variantes. Na chave de cliente, gerada a partir da *password*, foi usada uma mistura de PBE e AES.

Foram criadas diversas classes auxiliares para comunicação entre cliente e servidores que guardam como variáveis as diversas informações transmitidas durante a execução do protocolo *Kerberos*, desde o *ticket* ao autenticador, e que têm a capacidade de se transformar num *array* de *bytes*, correspondente à sua representação XML em *String,* e de se reconstruir através desse mesmo *array* de *bytes*, tornando muito mais fácil a sua transmissão e criptografia e seguindo a boa politica de factorização de código.

Foi, ainda, criada uma classe para gestão de credenciais de utilizadores, recorrendo ao padrão *Singleton*, de forma a podermos passar a chave de sessão, o *ticket* encriptado e a chave de encriptação de dados de cada utilizador entre o serviço ID, que o autentica, e os outros serviços a que pode recorrer, neste caso apenas o serviço de STORE.

Também recorremos a uma solução de *Message Authentication Codes* de forma a garantir a integridade do conteúdo das mensagens trocadas entre o cliente e o serviço SD-STORE, através da chave de sessão, usando uma solução HMAC com função de *hash* SHA256, pois apresenta uma qualidade criptografia substancialmente superior a uma solução com outras funções de *hash*, como, por exemplo, MD5.

Requisito SD-STORE.B:

O requisito B do projeto não foi implementado por mau *project management*, uma vez que, não só o requisito A ocupou muito mais tempo do que o previsto inicialmente, como o início do trabalho nesta parte do projeto não foi atempado.