Relatório Sistemas Distribuídos - Grupo 10 SD-ID.A / SD-STORE.B

Michael Santos
72471

Diogo Nicolau
72935

André Policarpo
73296

- **SD-ID.A**

Geração de chaves : as chaves geradas foram com o algoritmo DES, com o modo de cifra ECB e padding PKCS5. Embora o algoritmo DES seja um algoritmo de cifra fraco decidimos mantê-lo pois é suficiente para este caso em particular e não dispendíamos de tempo de sobra. Caso tivéssemos usado outro algoritmo teríamos escolhido o algoritmo Rijndael (AES) devido à sua elevada segurança. Para fazer o hash das password dos utilizadores utilizamos o algoritmo MD5 embora o algoritmo SHA-2 tivesse sido uma melhor escolha caso optássemos por uma maior segurança, mas não achámos necessário.

Ticket Kerberos : para o ticket usamos o formato “userID ; serviceName ; tBegin ; tPeriod ; Kcs” como String onde userID identifica o utilizador que usa o serviço, serviceName identifica o serviço a utilizar, tBegin indica as horas e os minutos (no formato hh:mm) que foi pedida a autenticação, tPeriod indica o tempo que o utilizador quer utilizar o serviço em horas e Kcs trata-se da chave criada com o hash da password do utilizador e a chave do serviço pedido. O mais indicado para o formato do ticket seria XML, pois assim não era necessário fazer parse de informação. Tal não foi implementado devido a insuficiência de tempo. Para armazenar os tickets utilizamos um singleton onde cada utilizador tem um ticket único.

Primeiro round-trip : no primeiro round-trip do protocolo Kerberos não utilizamos SOAP handlers pois utilizámos os argumentos das próprias funções remotas. Uma implementação mais correcta deste round trip envolveria handlers para passar a informação entre cliente e servidor.

Segundo round-trip : no segundo round-trip implementamos SOAP handlers para que enviam informação encriptada através de headers.

- **SD-STORE.B**

listDocs e createDocs : estes métodos foram implementados com base no protocolo Quorum Consensus com chamadas assíncronas.