PUC-Rio – Departamento de Informática
INF1416 – Segurança da Informação
Prof.: Anderson Oliveira da Silva

Trabalho 3
(apresentações: 17/10/2016 e 19/10/2016)

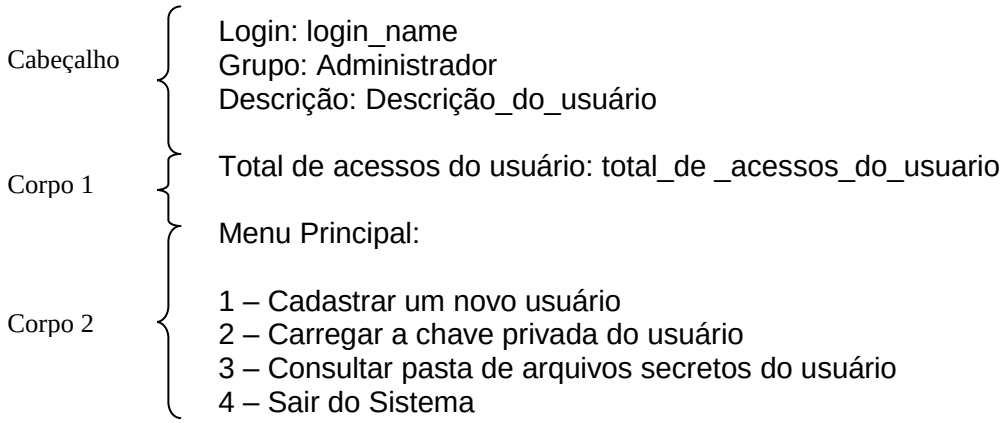
Construir um sistema em Java (plataforma JDK SE 1.8.0) que utiliza um banco de dados relacional (ex: MySQL) e um processo de autenticação forte bifator formado por três etapas, conforme especificado a seguir.

Na primeira etapa de autenticação, deve-se solicitar a identificação do usuário (*login name*) no sistema. Se a identificação for inválida, o usuário deve ser apropriadamente avisado e o processo deve permanecer na primeira etapa. Se a identificação for válida e o acesso do usuário estiver bloqueado, o mesmo deve ser apropriadamente avisado e o processo deve permanecer na primeira etapa. Caso contrário, o processo deve seguir para a segunda etapa.

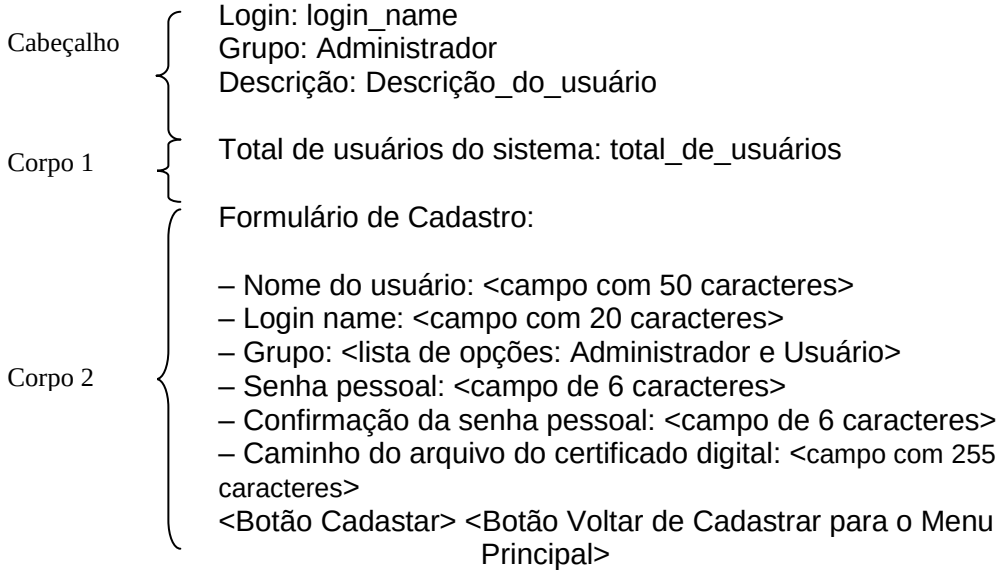
Na segunda etapa, deve-se verificar a senha pessoal do usuário (algo que ele conhece) que é fornecida através de um teclado virtual fonético com 5 botões, cada um com três fonemas (vide tabela de fonemas do anexo), que são selecionados aleatoriamente e sem repetição entre todos os botões. As senhas pessoais são sempre formadas por três fonemas. Não podem ser aceitas sequências de repetições de fonemas. Se a verificação for negativa, o usuário deve ser apropriadamente avisado e o processo deve contabilizar um erro de verificação de senha pessoal. Após três erros consecutivos sem que ocorra uma verificação positiva entre os erros, deve-se seguir para a primeira etapa e o acesso do usuário deve ser bloqueado por 2 minutos (outros usuários poderão tentar ter acesso). Se a verificação for positiva, o processo deve seguir para a terceira etapa.

Na terceira e última etapa de autenticação, deve-se verificar se o usuário possui a Transaction Authetication Number List (TAN List) fornecida pelo sistema no momento do cadastro do usuário. Essa TAN List possui 10 senhas de única vez (one-time passwords) gravadas no arquivo texto ASCII <login_usuário-tan.txt>. No momento da autenticação do usuário, o sistema deve selecionar aleatoriamente um valor de 1 até 10 e solicitar que o usuário entre com a senha posicionada na linha correspondente do arquivo de senhas de única vez. Cada senha só pode ser utilizada uma única vez no processo de autenticação do usuário. Se a verificação for negativa, o usuário deve ser apropriadamente avisado e o processo deve contabilizar um erro de verificação senha de única vez, retornando para o início da terceira etapa. Após três erros consecutivos sem que ocorra uma verificação válida da senha de única vez, deve-se seguir para a primeira etapa e o acesso do usuário deve ser bloqueado por 2 minutos (outros usuários poderão tentar ter acesso). Se a verificação for positiva, o processo deve permitir acesso ao sistema.

Após um processo de autenticação positivo, o sistema deve apresentar uma tela com informações e menus distintos em função do grupo do usuário no sistema. Para organizar a apresentação, a tela é dividida em três partes: cabeçalho, corpo 1 e corpo 2. Para o grupo administrador, o sistema deve apresentar a Tela Principal com as informações do usuário no cabeçalho, o total de acessos do usuário no corpo 1, e o Menu Principal no corpo 2, conforme abaixo:



Quando a opção 1 for selecionada, a Tela de Cadastro deve ser apresentada com o mesmo cabeçalho da Tela Principal, com o total de usuários do sistema no corpo 1 e com o Formulário de Cadastro no corpo 2, conforme abaixo:



Os valores entrados nos campos devem ser criticados adequadamente. As senhas pessoais são sempre formadas por 6 fonemas selecionados pelo usuário com base na tabela de fonemas do anexo. Não podem ser aceitas senhas com fonemas repetidos.

Quando o Botão Cadastrar for pressionado, o sistema deve gerar a TAN List do usuário formada por 10 senhas de única vez (one-time passwords) geradas aleatoriamente e armazenadas em um arquivo texto ASCII, cada uma em uma linha, constituindo, assim, um arquivo com 10 linhas. O nome padrão do arquivo é <login_name>-tan.txt. Essas senhas possuem 4 caracteres e são formadas por dígitos de 0 a 9 e letras maiúsculas de A a Z selecionados aleatoriamente. Em seguida, o sistema deve apresentar uma tela de confirmação dos dados fornecidos, a TAN List do usuário e os seguintes campos do certificado digital: Versão, Série, Validade, Tipo de Assinatura, Emissor e Sujeito (Friendly Name). Se os dados forem confirmados, deve-se incluir o usuário no sistema apenas se o login name for único, notificando o usuário em caso de erro. A senha pessoal deve ser armazenada no banco de dados conforme o requisito para armazenamento de senhas. O certificado digital deve ser carregado e armazenado no banco de dados. Se o cadastro for efetivado, deve-se retornar à Tela de Cadastro com o formulário vazio. Caso contrário, deve-se retornar à Tela de Cadastro com o formulário preenchido com os dados fornecidos. Quando o Botão Voltar de Cadastrar para o Menu Principal for pressionado, deve-se retornar à Tela Principal.

O requisito para armazenamento da senha fonética pessoal é o seguinte:

Valor_Armazenado(senha_texto_plano) = HEX(HASH_MD5(senha_texto_plano + SALT))

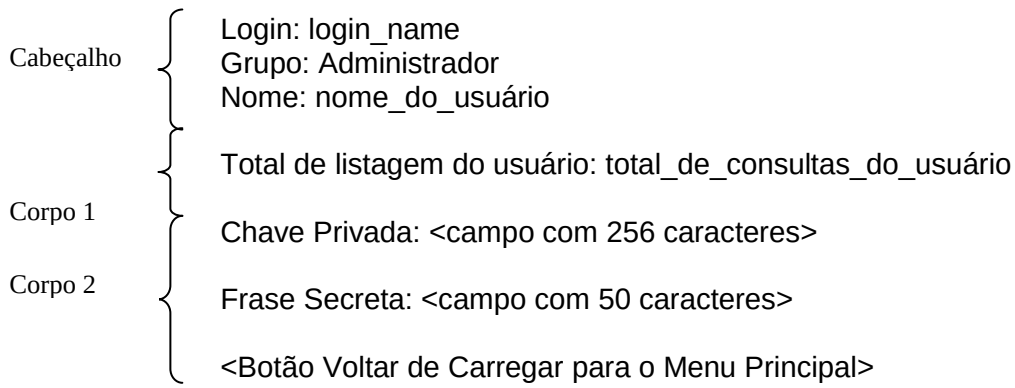
Onde,
HEX = representação hexadecimal.
HASH_MD5 = função hash MD5.
+ = concatenação de string.
senha_texto_plano = senha em texto plano (string).
SALT = valor aleatório entre 000000000 e 999999999 (string numérica).

O arquivo da chave privada é binário e deve ser armazenado em um token (por exemplo, pendrive). O arquivo do certificado digital é ASCII codificado em BASE64, no formato PEM (Privacy Enhanced Mail) e padrão X.509. Por questão de segurança, o arquivo da chave privada está criptografado com DES/ECB/PKCS5Padding. A chave DES deve ter 56 bits e deve ser gerada a partir de uma FRASE SECRETA do usuário dono da chave privada. O Java oferece classes prontas para gerar a chave simétrica com base em uma FRASE SECRETA (KeyGenerator e SecureRandom). O PRNG para geração da chave DES é o SHA1PRNG.

A chave privada decriptada usa o padrão PKCS8 e o certificado digital usa o padrão X.509, ambos codificados em BASE64. O Java oferece classes prontas para manipular com os dados codificados que estão armazenados nesses arquivos, respectivamente, as classes PKCS8EncodedKeySpec, X509Certificate e Base64. A partir da decodificação dos dados dos arquivos feita por essas classes, o Java também possibilita a restauração das chaves privadas e públicas com as classes KeyFactory, PrivateKey e PublicKey, e do certificado digital com a classe CertificateFactory.

Os dados fornecidos devem ser armazenados no banco de dados em quatro tabelas: Usuarios, Grupos, Mensagens e Registros. A tabela Usuários deve guardar as informações pessoais dos usuários, inclusive o valor armazenado para a senha pessoal fonética do usuário, conforme o requisito de armazenamento de senhas. O certificado digital do usuário também deve ser armazenado neste registro. A tabela Grupos deve armazenar os grupos do sistema (cada grupo possui um GID, número decimal único de identificação do grupo). A tabela Mensagens deve armazenar as mensagens da tabela de mensagens de registro. E, a tabela de Registros deve armazenar os registros relacionados ao uso do sistema, identificando a data e hora de um registro, relacionando com um usuário quando necessário.

Quando a opção 2 for selecionada, a Tela de Carregar a Chave Privada do Usuário deve ser apresentada com o mesmo cabeçalho e corpo 1 da Tela Principal, e com o total de consultas feitas pelo usuário corrente no corpo 2, conforme abaixo:



O campo Chave Privada deve ser utilizado para receber o caminho do arquivo da chave privada do usuário. O campo Frase Secreta deve ser utilizado para receber a Frase Secreta que

possibilita a decriptação da chave privada. O arquivo da chave privada é binário, resultado da criptografia da chave privada codificada em BASE64, no formato PEM (Privacy Enhanced Mail) e padrão PKCS8, com o algoritmo simétrico DES/ECB/PKCS5Padding e uma chave secreta. O sistema deve receber a frase secreta de decriptação da chave privada, que deve ser utilizada como semente do SHA1PRNG para recuperar a chave secreta. Depois de decriptar o arquivo binário, deve-se gerar uma assinatura digital no padrão RSA (MD5withRSA) para um array aleatório de 512 bytes e, em seguida, verificar a assinatura digital com a chave pública do usuário. A chave privada só deve ser aceita se a assinatura digital for verificada positivamente. O usuário deve ser notificado sobre o sucesso ou insucesso da verificação da chave privada. As mensagens apropriadas devem ser registradas com base na tabela de mensagens de registro. Quando o Botão Voltar de Carregar para o Menu Principal for pressionado, deve-se retornar à Tela Principal.

Quando a opção 3 for selecionada, a Tela de Consultar Pasta de Arquivos Secretos do Usuário deve ser apresentada com o mesmo cabeçalho e corpo 1 da Tela Principal, e com o total de consultas feitas pelo usuário corrente no corpo 2, conforme abaixo:

Cabeçalho	Login: login_name Grupo: Administrador Nome: nome_do_usuário
Corpo 1	Total de consultas do usuário: total_de_consultas_do_usuário Caminho da pasta: <campo com 255 caracteres> <Botão Listar>
Corpo 2	Tabela com nomes dos arquivos secretos do usuário e respectivos HEXADECIMAL_ASSINATURA _DIGITAL e HEXADECINAL_ENVELOPE_DIGITAL <Botão Voltar de Consultar para o Menu Principal>

O caminho da pasta de arquivos secretos do usuário será fornecido no campo destinado a essa informação. Quando o Botão Listar for pressionado, deve-se decriptar o arquivo de índice da pasta (cifra DES, modo ECB e enchimento PKCS5) chamado index.enc, verificar sua integridade e autenticidade, listar seu conteúdo apresentando o nome código dos arquivos, o nome secreto dos arquivos, os respectivos donos e grupos de cada arquivo, e o status de integridade e autenticidade dos arquivos (OK ou NOT OK). O envelope digital do arquivo de índice é armazenado no arquivo index.env (protege a semente SHA1PRNG que gera a chave secreta DES) e a assinatura digital do arquivo de índice é armazenado no arquivo index.asd (protege o digest no formato hexadecimal). O envelope digital e a assinatura digital são gerados com as respectivas chaves assimétricas do usuário e a classe Signature. O arquivo de índice decriptado possui zero ou mais linhas formatadas da seguinte forma:

NOME_CODIGO_DO_ARQUIVO<SP>NOME_SECRETO_DO_ARQUIVO<SP>DONO_ARQUIVO <SP><GRUPO_ARQUIVO><EOL>

Onde:

NOME_CODIGO_DO_ARQUIVO: caracteres alfanuméricos.
NOME_SECRETO_DO_ARQUIVO: caracteres alfanuméricos.
DONO_ARQUIVO: caracteres alfanuméricos.
GRUPO_ARQUIVO: caracteres alfanuméricos.
<SP> = caractere espaço em branco.
<EOL> = caractere nova linha (\n).

Quando um clique de mouse for efetuado sobre o nome secreto de um arquivo da lista apresentada, o sistema deve decriptar o arquivo secreto (cifra DES, modo ECB e enchimento PKCS5), localizado na pasta corrente, verificar sua autenticidade e integridade, e gravar os dados decriptados em um novo arquivo. O nome do arquivo criptografado termina com a extensão *.enc*. A assinatura digital, gerada com a classe Signature e a chave assimétrica do usuário, é mantida em um arquivo com mesmo nome, com a extensão *.asd* (protege o digest do conteúdo do arquivo). O envelope digital do arquivo é mantido em um arquivo com mesmo nome, com a extensão *.env* (protege a semente SHA1PRNG que gera a chave secreta DES). Quando o Botão Voltar de Consultar para o Menu Principal for pressionado, deve-se retornar à Tela Principal.

Quando a opção 3 for selecionada, a Tela de Saída deve ser apresentada com o mesmo cabeçalho e corpo 1 da Tela Principal, e uma mensagem de saída no corpo 2, conforme abaixo:

Cabeçalho	Login: login_name Grupo: Administrador Nome: nome_do_usuário
Corpo 1	Total de acessos do usuário: total_de_acessos_do_usuário
Corpo 2	Saída do sistema: Mensagem de saída. <Botão Sair> <Botão Voltar de Sair para o Menu Principal>

O sistema deve apresentar a mensagem de saída “Pressione o botão Sair para confirmar.” e os dois botões. Quando o Botão Sair for pressionado, deve-se encerrar o sistema. Se o botão <Voltar de Sair para o Menu Principal> for pressionado, deve-se retornar à Tela Principal.

Para o grupo usuário, o sistema deve funcionar de forma equivalente. Porém, o cabeçalho das telas deve apresentar o grupo como Usuário e o Menu Principal não deve apresentar a opção Cadastrar um Novo Usuário. O corpo 2 deve continuar apresentando a mensagem “Total de acessos do usuário: total_de_acessos_do_usuário”.

Cada uma das operações executadas pelo sistema deve ser registrada em uma tabela de Registros no banco de dados, armazenando, pelo menos, a data e hora do registro, assim como o código do mesmo e, quando necessário, a identificação do usuário corrente e do arquivo selecionado para decriptação. Não é permitido armazenar as mensagens dos registros nessa tabela. Essas mensagens devem ser armazenadas na tabela Mensagens. **Os registros devem ser visualizados em ordem cronológica apenas por um programa de apoio (logView) que deve também ser implementado.** As mensagens de registro são apresentadas na tabela de mensagens, em anexo.

Tabela de fonemas válidos para uma senha pessoal do usuário		
BA	BE	BO
CA	CE	CO
DA	DE	DO
FA	FE	FO
GA	GE	GO

Tabela de Mensagens de Registro	
1001	Sistema iniciado.
1002	Sistema encerrado.
2001	Autenticação etapa 1 iniciada.
2002	Autenticação etapa 1 encerrada.
2003	Login name <login_name> identificado com acesso liberado.
2004	Login name <login_name> identificado com acesso bloqueado.
2005	Login name <login_name> não identificado.
3001	Autenticação etapa 2 iniciada para <login_name>.
3002	Autenticação etapa 2 encerrada para <login_name>.
3003	Senha pessoal verificada positivamente para <login_name>.
3004	Senha pessoal verificada negativamente para <login_name>.
3005	Primeiro erro da senha pessoal contabilizado para <login_name>.
3006	Segundo erro da senha pessoal contabilizado para <login_name>.
3007	Terceiro erro da senha pessoal contabilizado para <login_name>.
3008	Acesso do usuario <login_name> bloqueado pela autenticação etapa 2.
4001	Autenticação etapa 3 iniciada para <login_name>.
4002	Autenticação etapa 3 encerrada para <login_name>.
4003	Senha de única vez verificada positivamente para <login_name>.
4004	Primeiro erro da senha de única vez contabilizado para <login_name>.
4005	Segundo erro da senha de única vez contabilizado para <login_name>.
4006	Terceiro erro da senha de única vez contabilizado para <login_name>.
4009	Acesso do usuario <login_name> bloqueado pela autenticação etapa 3.
5001	Tela principal apresentada para <login_name>.
5002	Opção 1 do menu principal selecionada por <login_name>.
5003	Opção 2 do menu principal selecionada por <login_name>.
5004	Opção 3 do menu principal selecionada por <login_name>.
5005	Opção 4 do menu principal selecionada por <login_name>.
6001	Tela de cadastro apresentada para <login_name>.
6002	Botão cadastrar pressionado por <login_name>.
6003	Caminho do certificado digital inválido fornecido por <login_name>.
6004	Confirmação de dados aceita por <login_name>.
6005	Confirmação de dados rejeitada por <login_name>.
6006	Botão voltar de cadastro para o menu principal pressionado por <login_name>.
7001	Tela de carregamento da chave privada apresentada para <login_name>.
7002	Caminho da chave privada inválido fornecido por <login_name>.
7003	Frase secreta inválida fornecida por <login_name>.
7004	Erro de validação da chave privada com o certificado digital de <login_name>.
7005	Chave privada validada com sucesso para <login_name>.
7006	Botão voltar de carregamento para o menu principal pressionado por <login_name>.
8001	Tela de consulta de arquivos secretos apresentada para <login_name>.
8002	Botão voltar de consulta para o menu principal pressionado por <login_name>.
8003	Botão Listar de consulta pressionado por <login_name>.
8006	Caminho de pasta inválido fornecido por <login_name>.
8007	Lista de arquivos apresentada para <login_name>.
8008	Arquivo <arq_name> selecionado por <login_name> para decriptação.
8009	Arquivo <arq_name> decriptado com sucesso para <login_name>.
8010	Arquivo <arq_name> verificado (integridade e autenticidade) com sucesso para <login_name>.
8011	Falha na decriptação do arquivo <arq_name> para <login_name>.
8012	Falha na verificação do arquivo <arq_name> para <login_name>.
9001	Tela de saída apresentada para <login_name>.
9002	Botão sair pressionado por <login_name>.
9003	Botão voltar de sair para o menu principal pressionado por <login_name>.