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

Trabalho 3
(apresentações: 08/05/2017 e 10/05/2017)

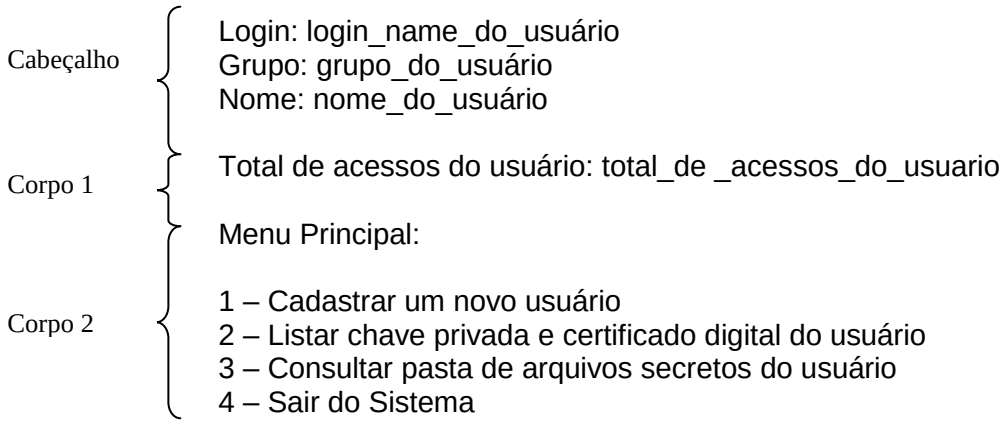
Construir um sistema em Java (plataforma JDK SE 1.8.0) que utiliza um banco de dados relacional (ex: MySQL) e um processo de autenticação forte bifator formado por três etapas, conforme especificado a seguir.

Na primeira etapa de autenticação, deve-se solicitar a identificação do usuário (*login name*) no sistema, que deve ser um e-mail válido. O e-mail do usuário deve ser coletado do seu respectivo certificado digital no momento do seu cadastramento 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.

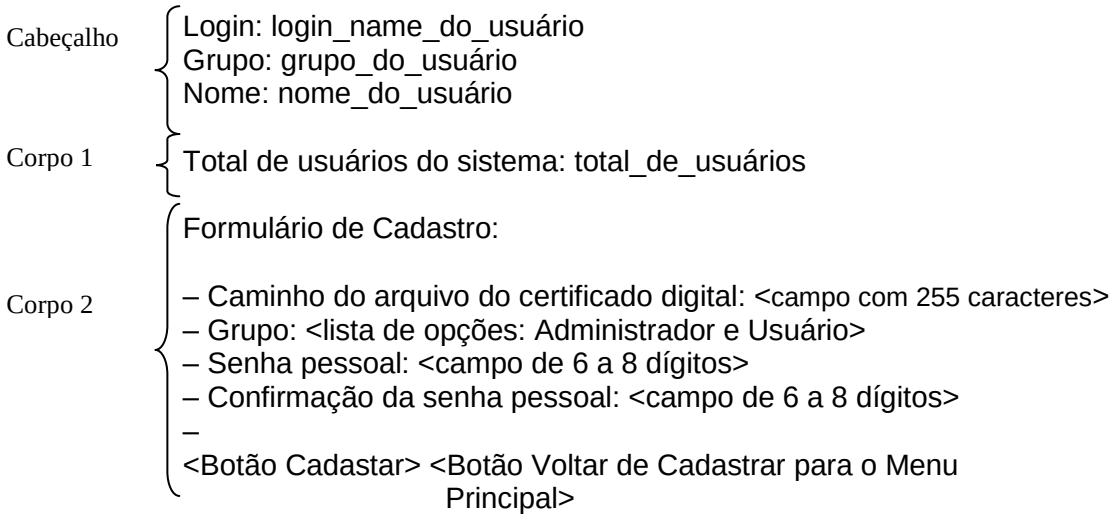
Na segunda etapa, deve-se verificar a senha pessoal do usuário (algo que ele conhece) que é fornecida através de um teclado virtual numérico com cinco botões, cada um com um com dois números, que são selecionados aleatoriamente e sem repetição entre todos os botões. As senhas pessoais são sempre formadas por seis ou oito números com valores de (0 a 9). Não podem ser aceitas sequências crescentes ou decrescentes de números ou repetições de números consecutivos. A cada pressionamento de botão, os números são redistribuídos aleatoriamente entre os cinco botões. 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 a chave privada do usuário (algo que ele possui) fornecida através de um arquivo 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 1024 bytes e, em seguida, verificar a assinatura digital com a chave pública do usuário. Se a verificação for negativa, o usuário deve ser apropriadamente avisado e o processo deve contabilizar um erro de verificação da chave privada, retornando para o início da terceira etapa. Após três erros consecutivos sem que ocorra uma verificação válida da chave privada, 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, no mínimo, 6 dígitos e, no máximo, 8 dígitos. Não podem ser aceitas sequências de repetições de dígitos ou sequências em ordem crescente ou decrescente. Quando o Botão Cadastrar for pressionado, o sistema deve apresentar uma tela de confirmação dos dados fornecidos e os seguintes campos do certificado digital: Versão, Série, Validade, Tipo de Assinatura, Emissor, Sujeito (Friendly Name) e E-mail. 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. O nome do usuário e o login name devem ser extraídos do campo de Sujeito do certificado. 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 no formato PEM. 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 pessoal é o seguinte:

Valor_Armazenado = HEX(HASH_SHA1(senha_texto_plano + SALT))

Onde,
HEX = representação hexadecimal.
HASH_SHA1 = função hash SHA-1.
+ = concatenação de string.

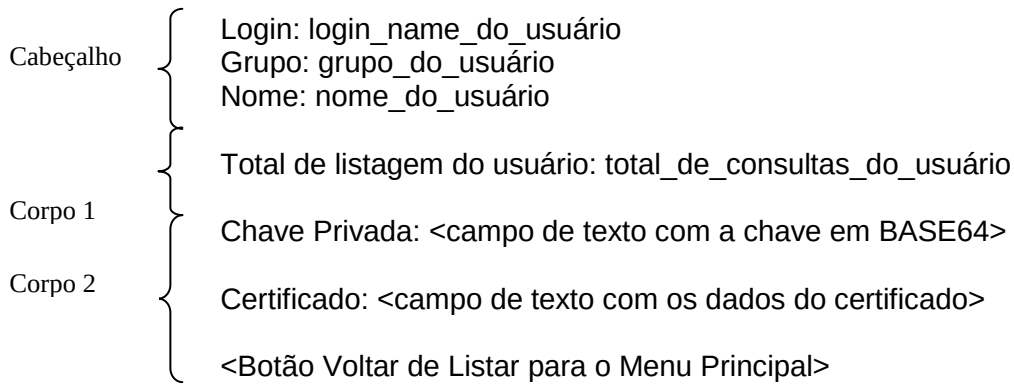
senha_texto_plano = senha em texto plano (string).
SALT = valor aleatório composto de 10 caracteres do conjunto [A-Z][a-z][0-9] (string).

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.

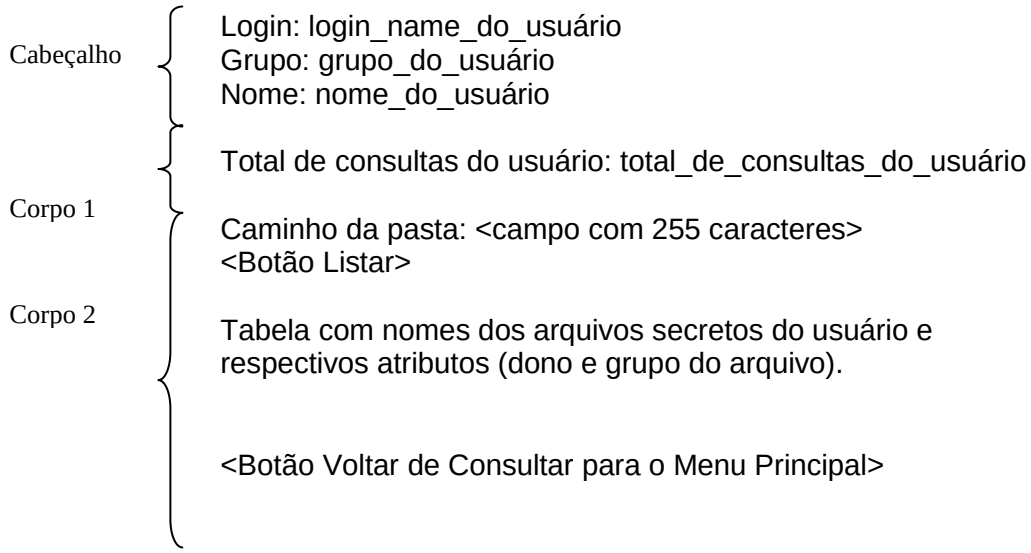
Os dados fornecidos devem ser armazenados no banco de dados em quatro tabelas: Usuarios, Grupos, Mensagens e Registros. A tabela Usuários deve guardar as informações pessoais dos usuários, inclusive o valor armazenado para a senha pessoal fonética do usuário, conforme o requisito de armazenamento de 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 Listar Chave Privada e Certificado Digital 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 de texto da chave privada deve apresentar a codificação BASE64 da chave privada do usuário. O campo de texto do certificado deve apresentar os campos Versão, Série, Validade, Tipo de Assinatura, Emissor e Sujeito (Friendly Name) do certificado do usuário. Quando o Botão Voltar de Listar 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:



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 e os respectivos donos e grupos de cada arquivo. 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:

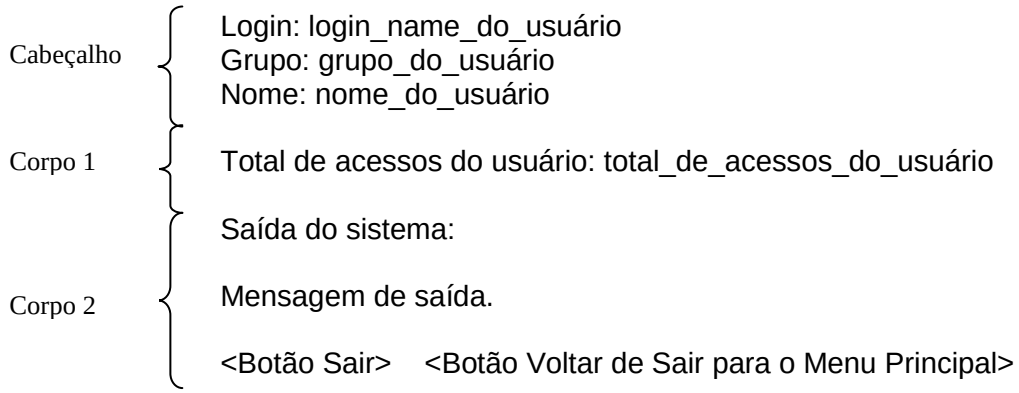
NOME_CODIGO_DO_ARQUIVO<SP>NOME_SECRETO_DO_ARQUIVO<SP>DONO_ARQUIVO<SP><GRUPO_ARQUIVO><EOL>

Onde:

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

Quando o nome secreto de um arquivo da lista apresentada for selecionado, o sistema deve verificar se o usuário pode ou não acessar o arquivo. A política de controle de acesso é simples: o usuário só pode acessar um arquivo se for o dono do mesmo ou se pertencer ao grupo do arquivo. Em caso afirmativo, o sistema deve (i) decriptar o arquivo secreto (cifra DES, modo ECB e enchimento PKCS5) selecionado, notificando o usuário sobre eventuais erros de integridade, autenticidade e sigilo; e (ii) gravar os dados decriptados em um novo arquivo. Caso contrário, o sistema deve notificar o usuário que ele não tem permissão de acesso. O nome do arquivo criptografado usa o nome código do arquivo e 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 4 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:



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 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	Chave privada verificada positivamente para <login_name>.
3004	Chave privada verificada negativamente para <login_name> (caminho inválido).
3005	Chave privada verificada negativamente para <login_name> (frase secreta inválida).
3006	Chave privada verificada negativamente para <login_name> (assinatura digital inválida).
3007	Primeiro erro da senha pessoal contabilizado para <login_name>.
3008	Segundo erro da senha pessoal contabilizado para <login_name>.
3009	Terceiro erro da senha pessoal contabilizado para <login_name>.
3010	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	Senha pessoal inválida fornecida por <login_name>.
6004	Caminho do certificado digital inválido fornecido por <login_name>.
6005	Confirmação de dados aceita por <login_name>.
6006	Confirmação de dados rejeitada por <login_name>.
6007	Botão voltar de cadastro para o menu principal pressionado por <login_name>.
7001	Tela de consulta da chave privada e certificado apresentada para <login_name>.
7002	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	Acesso permitido ao arquivo <arq_name> para <login_name>.
8010	Acesso negado ao arquivo <arq_name> para <login_name>.
8011	Arquivo <arq_name> decriptado com sucesso para <login_name>.
8012	Arquivo <arq_name> verificado (integridade e autenticidade) com sucesso para <login_name>.
8013	Falha na decriptação do arquivo <arq_name> para <login_name>.
8014	Falha na verificação (integridade e autenticidade) 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>.