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

Trabalho 4 – Cofre Digital (Digital Vault)
(entrega: 14/5/2023, 23:59h – todos os grupos)
(apresentações: 15/5/2023, 17/5/2023, 19/5/2023)

Construir um sistema em Java (plataforma JDK SE 1.8.0) que utiliza um banco de dados relacional (ex: SQLLite, MySQL), um processo de autenticação forte bifator formado por três etapas e controle de integridade, autenticidade e sigilo para proteger a pasta de arquivos secretos chamada de Cofre Digital.

Quando o cofre digital for executado pela primeira vez (processo de partida do sistema), sem nenhum usuário cadastrado no sistema, a aplicação deve fazer o cadastro do usuário administrador da pasta segura, conforme descrito na opção de cadastro. A frase secreta da chave privada do administrador deverá ser mantida em memória para que o sistema tenha acesso essa chave privada durante a sua execução. Logo, após esse cadastro inicial, o sistema deverá iniciar o processo de autenticação de usuários. Tipicamente, o administrador do sistema deverá ser o primeiro a entrar no sistema para fazer o cadastro dos demais usuários do sistema. Se o sistema for encerrado, a chave secreta do usuário deverá ser apagada da memória.

Quando o cofre digital for executado da segunda vez em diante (novo processo de partida do sistema), a aplicação deverá solicitar a frase secreta da chave privada do administrador, que deve passar pelo processo de validação, da mesma forma como realizado no processo de cadastro. Se a validação da chave privada for negativa, o sistema deve notificar o usuário do ocorrido e deve encerrar a execução do sistema. Se a validação da chave privada for positiva, o sistema deverá manter a frase secreta em memória e iniciar o processo de autenticação de usuários.

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 sobrecarregado* com cinco botões, cada um com dois números, que são distribuídos aleatoriamente e sem repetição entre todos os botões. As senhas pessoais são sempre formadas por oito, nove ou 10 números. A cada pressionamento de um botão, os números são redistribuídos aleatoriamente entre os cinco botões. Se a verificação da senha 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 o *token do usuário* (algo que ele possui) fornecido para o sistema através do aplicativo iToken. Esse aplicativo gera o valor do token utilizando uma *semente secreta* de 16 bytes concatenada com o *carimbo de tempo atual* (ano, mês, dia, hora e minuto) representado em milissegundos passados desde Janeiro 1, 1970, 00:00:00 GMT (método *long getTime()* da classe *Date*). O iToken deve usar essa concatenação como semente do SHA1-PRNG e produzir um valor inteiro positivo de 6 dígitos, que é o token do momento, válido por 1 minuto. A cada novo minuto, o valor do token deve ser recalculado pelo

iToken. Esse valor deve ser fornecido pelo usuário na tela de autenticação do programa Cofre Digital, que, por sua vez, deve trabalhar com uma margem de erro de um minuto a menos e um minuto a mais. Para isso, deve calcular três valores de token: um com o minuto preciso do tempo, outro com um minuto a mais do tempo e outro com um minuto a mais do tempo. Qualquer um dos três valores calculados deve ser aceito como válido se for fornecido pelo usuário. Se a verificação for negativa para os três valores calculados, o usuário deve ser apropriadamente avisado e o processo deve contabilizar um erro de verificação de token, retornando para o início da terceira etapa. Após três erros consecutivos sem que ocorra uma verificação válida do token, 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.

A *semente secreta* do token deve ser armazenada de forma criptografada no aplicativo iToken e no programa Cofre Digital com o algoritmo simétrico DES/ECB/PKCS5Padding. A chave DES deve ter 56 bits e deve ser gerada a partir da *senha pessoal do usuário* cadastrada no programa Cofre Digital. O aplicativo iToken deve solicitar a senha pessoal do usuário na sua inicialização. Essa senha deve ser informada ao aplicativo usando um *teclado virtual numérico sobrecarregado* com cinco botões semelhante ao do programa Cofre Digital que, por sua vez, deve gerar um *arquivo de trabalho* no formato ASCII (token.txt) para o aplicativo iToken contendo duas linhas: uma com o hash bcrypt da senha pessoal do usuário; e outra como texto cifrado da semente secreta do token criptografada com o algoritmo simétrico DES/ECB/PKCS5Padding. A chave DES deve ter 56 bits e deve ser gerada a partir da *senha pessoal do usuário*. O texto cifrado deve estar no formato BASE64.

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:

Cabeçalho	Login: login_name_do_usuário Grupo: grupo_do_usuário Nome: nome_do_usuário
Corpo 1	Total de acessos do usuário: total_de _acessos_do_usuario
Corpo 2	Menu Principal: 1 – Cadastrar um novo usuário 2 – Consultar pasta de arquivos secretos do usuário 3 – Sair do Sistema

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:

Cabeçalho
Login: login_name_do_usuário
Grupo: grupo_do_usuário
Nome: nome_do_usuário

Corpo 1
Total de usuários do sistema: total_de_usuários

Corpo 2
Formulário de Cadastro:

– Caminho do arquivo do certificado digital: <campo com 255 caracteres>
– Caminho do arquivo da chave privada: <campo com 255 caracteres>
– Frase secreta: <campo de 255 caracteres>
– Grupo: <lista de opções: Administrador e Usuário>
– Senha pessoal: <campo com 10 caracteres>
– Confirmação senha pessoal: <campo com 10 caracteres>

<Botão Cadastar> <Botão Voltar de Cadastrar para o Menu Principal>

Os valores entrados nos campos devem ser criticados adequadamente. As senhas pessoais são sempre formadas por oito, nove ou dez números formados por dígitos de 0 a 9. Não podem ser aceitas sequências de números repetidos. Quando o Botão Cadastrar for pressionado, o sistema deve conferir se as senhas digitadas são as mesmas e apresentar uma tela de confirmação com 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 (e-mail do usuário) 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 *frase secreta* da chave privada deve ser testada e a chave privada deve ser verificada com a validação da assinatura digital de um array aleatório de 4096 bytes com a chave pública que consta no certificado digital fornecido.
Se a verificação for negativa, o usuário deve ser apropriadamente avisado e o cadastrado do usuário não deve ser realizado. Se a assinatura digital for verificada com sucesso, então o sistema deve armazenar a chave privada no seu formato criptografado (binário) e a chave pública no seu formato PEM (Privacy-Enhanced Mail) na base de dados de forma associada ao UID do usuário na tabela Chaveiro. O registro do par chave privada e certificado digital deve receber uma identificação única de KID. O KID deve também ser armazenado no registro do usuário, na tabela Usuarios.

A senha pessoal deve ser armazenada no registro do usuário, na tabela Usuarios do banco de dados, conforme o requisito para armazenamento de senhas.

O requisito para armazenamento da senha pessoal é o armazenamento padrão do hash calculado pela função bcrypt, que armazena a *versão* do algoritmo usado pelo bcrypt (no caso do trabalho, versão 2y), o *custo* das iterações do bcrypt (no caso do trabalho, valor 12), o *SALT* codificado em BASE64 e o *HASH* codificado em BASE64, totalizando 60 caracteres, conforme mostrado a seguir:

Valor_Armazenado = $version$cost$BASE64(salt)BASE64(hash)

Exemplo de armazenamento da senha “13572468”:

$2y$12$TRQ1SYrgQdQyQtMsQov2UuhGUNCmH24rNaiiJxoANlfObGf.VAQz2

Onde,
2y = versão do algoritmo usado na função bcrypt.
12 = custo do bcrypt (2^12 iterações).

TRQ1SYrgQdQyQtMsQov2Uu = salto codificado em BASE64.
hGUNCmH24rNaiiJxoANlfObGf.VAQz2 = hash codificado em BASE64.

O provider BouncyCastle fornece a classe OpenBSDBCrypt. Essa classe possui o método *generate*, que gera o hash brcrypt versão 2y, e o método *checkPassword*, que compara um hash bcrypt com uma senha em texto plano.

A *semente secreta do token* deve ser gerada com 16 bytes e criptografada com o algoritmo simétrico DES/ECB/PKCS5Padding. A chave DES deve ter 56 bits e deve ser gerada a partir da *senha pessoal do usuário*. O texto cifrado deve estar no formato BASE64 e deve ser armazenado no registro do usuário na tabela Usuários do banco de dados.

Também deve ser gerado um *arquivo de trabalho* no formato ASCII (token.txt) para o aplicativo iToken contendo duas linhas: uma com o hash bcrypt da senha pessoal do usuário; e outra com o texto cifrado da semente secreta do token criptografada com o algoritmo simétrico DES/ECB/PKCS5Padding. A chave DES deve ter 56 bits e deve ser gerada a partir da *senha pessoal do usuário*. O texto cifrado deve estar no formato BASE64.

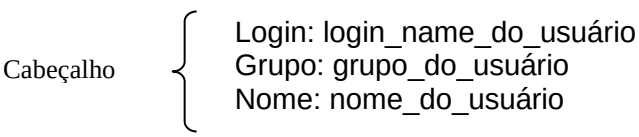
Se o cadastro for efetivado, deve-se retornar à Tela de Cadastro com o formulário vazio. Caso contrário, deve-se retornar à Tela de Cadastro com o formulário preenchido com os dados fornecidos. Quando o Botão Voltar de Cadastrar para o Menu Principal for pressionado, deve-se retornar à Tela Principal.

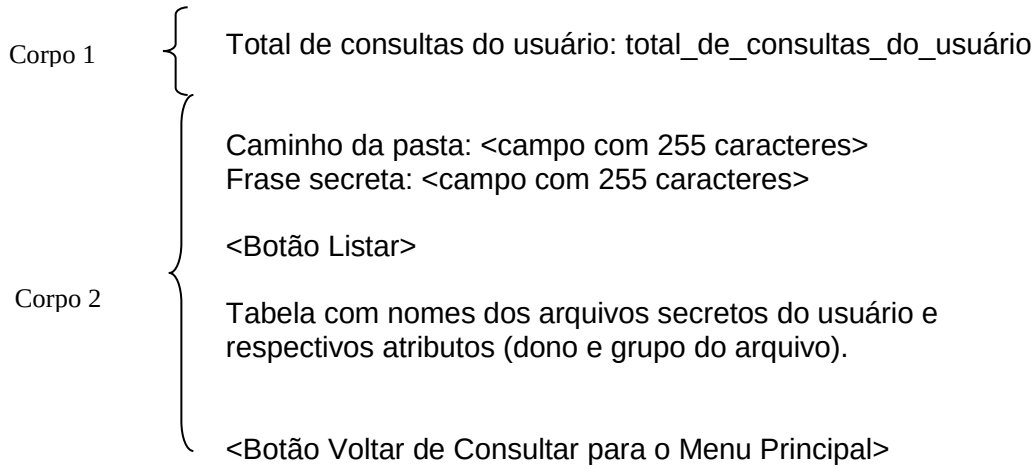
O arquivo da chave privada é binário e será fornecido em um token (por exemplo, pendrive). O arquivo do certificado digital é ASCII codificado em BASE64, no formato PEM (Privacy-Enhanced Mail) e padrão X.509. Por questão de segurança, o arquivo da chave privada está criptografado com DES/ECB/PKCS5Padding. 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*.

O banco de dados é organizado em cinco tabelas: Usuarios, Chaveiro, Grupos, Mensagens e Registros. A tabela Usuários deve guardar as informações pessoais dos usuários, inclusive o valor armazenado da senha pessoal do usuário, conforme o requisito de armazenamento de senhas (cada usuário deve ter um UID único). O certificado digital e a chave privada do usuário devem ser armazenados na tabela Chaveiro (cada par certificado digital e chave privada possui um KID único e estar associado a um único UID). 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 (cada mensagem deve ter um MID único). 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 (cada registro deve ter um RID único e um MID).

Quando a opção 2 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:





Quando o Botão Listar for pressionado, a frase secreta deve ser validade da mesma forma que foi previamente realizada durante o cadastro do usuário. Em caso de validação negativa, o usuário deve ser notificado de forma apropriada em função do erro. Se a validação for positiva, deve-se decriptar o arquivo de índice da pasta fornecida (cifra DES, modo ECB e enchimento PKCS5), chamado index.enc; verificar a integridade e autenticidade do arquivo de índice; e listar o conteúdo do arquivo de índice apresentando APENAS os atributos dos arquivos (nome código, nome, dono e grupo) do usuário ou do grupo do usuário. 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 armazenada no arquivo index.asd (representação binária da assinatura digital). O envelope digital e a assinatura digital são gerados com as respectivas chaves assimétricas do usuário administrador e as classes Cipher e 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 código do arquivo).
NOME_SECRETO_DO_ARQUIVO: caracteres alfanuméricos (nome original do arquivo).
DONO_ARQUIVO: caracteres alfanuméricos (atributo do arquivo).
GRUPO_ARQUIVO: caracteres alfanuméricos (atributo do arquivo).
<SP> = caractere espaço em branco.
<EOL> = caractere nova linha (\n).

Observação: O arquivo de índice da pasta pertence ao administrador do sistema.

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. 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 com o nome secreto. 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 a extensão *.enc*. A assinatura digital, gerada com a classe *Signature* e a chave assimétrica do usuário, é mantida em um arquivo com o nome código e a extensão *.asd* (representação binária da assinatura digital). O envelope digital do arquivo é mantido em um arquivo com o nome código e 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 da Tela Principal. O corpo 1 deve apresentar o total de acessos do usuário corrente e o corpo 2 deve ser apresentado conforme abaixo:

Cabeçalho	Login: login_name_do_usuário Grupo: grupo_do_usuário Nome: nome_do_usuário
Corpo 1	Total de acessos do usuário: total_de _acessos_do_usuario
Corpo 2	Saída do sistema: Mensagem de saída. <Botão Encerrar Sessão> <Botão Encerrar Sistema> <Botão Voltar de Sair para o Menu Principal>

O sistema deve apresentar a mensagem de saída “Pressione o botão Encerrar Sessão ou o botão Encerrar Sistema para confirmar.” e os três botões. Quando o Botão Encerrar Sessão for pressionado, deve-se encerrar a sessão do usuário e iniciar o processo de autenticação de usuário. Quando o Botão Encerrar Sistema for pressionado, deve-se encerrar a execução do 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, o código da mensagem, quando possível, a identificação do usuário corrente e do arquivo selecionado para decriptação. Não é permitido armazenar o texto das mensagens dos registros nessa tabela. As mensagens e seus respectivos códigos devem ser armazenadas na tabela Mensagens do banco de dados. **Os registros devem ser visualizados em ordem cronológica apenas por um programa de apoio (logView) que deve também ser implementado.**

As mensagens de registro e os respectivos códigos estão listados na Tabela de Mensagens de Registro em anexo.

O **prazo de submissão do projeto** deste trabalho, com todos os fontes em Java, no sistema de EAD da PUC-Rio, é dia **14/5/2023, 23:59h**. O prazo máximo para submissão é dia **15/5/2023, 11:59h**. Cada integrante do grupo deve fazer uma submissão.

Tabela de Mensagens de Registro	
1001	Sistema iniciado.
1002	Sistema encerrado.
1003	Sessão iniciada para <login_name>.
1004	Sessão encerrada para <login_name>.
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	Primeiro erro da senha pessoal contabilizado para <login_name>.
3005	Segundo erro da senha pessoal contabilizado para <login_name>.
3006	Terceiro erro da senha pessoal contabilizado para <login_name>.
3007	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	Token verificado positivamente para <login_name>.
4004	Primeiro erro de token contabilizado para <login_name>.
4005	Segundo erro de token contabilizado para <login_name>.
4006	Terceiro erro de token contabilizado para <login_name>.
4007	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>.
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	Chave privada verificada negativamente para <login_name> (caminho inválido).
6006	Chave privada verificada negativamente para <login_name> (frase secreta inválida).
6007	Chave privada verificada negativamente para <login_name> (assinatura digital inválida).
6008	Confirmação de dados aceita por <login_name>.
6009	Confirmação de dados rejeitada por <login_name>.
6010	Botão voltar de cadastro para o menu principal pressionado por <login_name>.
7001	Tela de consulta de arquivos secretos apresentada para <login_name>.
7002	Botão voltar de consulta para o menu principal pressionado por <login_name>.
7003	Botão Listar de consulta pressionado por <login_name>.
7004	Caminho de pasta inválido fornecido por <login_name>.
7005	Arquivo de índice decriptado com sucesso para <login_name>.
7006	Arquivo de índice verificado (integridade e autenticidade) com sucesso para <login_name>.
7007	Falha na decriptação do arquivo de índice para <login_name>.
7008	Falha na verificação (integridade e autenticidade) do arquivo de índice para <login_name>.
7009	Lista de arquivos presentes no índice apresentada para <login_name>.
7010	Arquivo <arq_name> selecionado por <login_name> para decriptação.
7011	Acesso permitido ao arquivo <arq_name> para <login_name>.
7012	Acesso negado ao arquivo <arq_name> para <login_name>.
7013	Arquivo <arq_name> decriptado com sucesso para <login_name>.
7014	Arquivo <arq_name> verificado (integridade e autenticidade) com sucesso para <login_name>.
7015	Falha na decriptação do arquivo <arq_name> para <login_name>.
7016	Falha na verificação (integridade e autenticidade) do arquivo <arq_name> para <login_name>.
8001	Tela de saída apresentada para <login_name>.
8002	Botão encerrar sessão pressionado por <login_name>.
8003	Botão encerrar sistema pressionado por <login_name>.
8004	Botão voltar de sair para o menu principal pressionado por <login_name>.