Aplicação de requisitos de segurança no projeto de rastreabilidade bovina conforme a iso 15.408

Andrey Carmisini – Acadêmico
Paulo Fernando da Silva - Orientador

Roteiro

- Introdução
  - Objetivos do trabalho
- Fundamentação teórica
  - Aspectos de segurança da informação, norma ISO/IEC 15.408 e os trabalhos correlatos
- Desenvolvimento do framework
  - Requisitos principais, especificação, implementação, operacionalidade e resultados e discussão
- Conclusão
  - Extensões

Introdução

- Laboratório de Desenvolvimento e Transferência de Tecnologia - LDTT.
  - Projeto de Rastreabilidade Bovina.
- Desenvolvimento do Framework de segurança.
  - Conforme a ISO/IEC 15.408.

Objetivos do trabalho

- Identificar os principais requisitos funcionais da norma ISO/IEC 15.408 aplicáveis ao Projeto de Rastreabilidade Bovina;
- Garantir a auditoria de segurança;
- Garantir a proteção dos dados do usuário;
- Realizar cópia de segurança e restauração;
- Criar um atualizador de versão;

Fundamentação teórica

Aspectos de segurança da informação

- Confidencialidade;
- Integridade dos dados;
- Disponibilidade;
- Autenticação;

Aspectos de segurança da informação

- Não repúdio;
- Legalidade;
- Privacidade;
- Auditoria.

Norma ISO/IEC 15.408

- Objetivo da norma
  - fornecer um conjunto de critérios fixos que permitem especificar a segurança de uma aplicação (ALBUQUERQUE; RIBEIRO, 2002, p. 7).

Norma ISO/IEC 15.408

Nome da classe	Sigla
Auditoria	FAU
Proteção de dados do usuário	FDP
Criptografia	FCS
Autoproteção	FPT
Canais seguros	FTP
Autenticação	FIA
Acesso ao sistema	FTA
Gerenciamento de segurança	FMT
Utilização de recursos	FRU
Privacidade	FPR

Trabalhos correlatos

- Segurança no Desenvolvimento de Aplicações Web (GOMES; SANTOS, 2006);
- PASS - Processo de Apoio à Segurança de Software (NUNES, 2007).

Desenvolvimento do Framework

Especificação

Requisitos principais

- Permitir ao PRB gerar nova versão do sistema;
- Permitir ao PRB gerar trilha de auditoria;
- Permitir ao PRB gerar criptografia dos dados;
- Permitir ao PRB gerar hash dos dados;
- Permitir ao usuário realizar cópias de segurança;
- Permitir ao usuário realizar a restauração da base de dados.

Diagrama de casos de uso

- Diagrama de casos de uso executados pelo PRB.

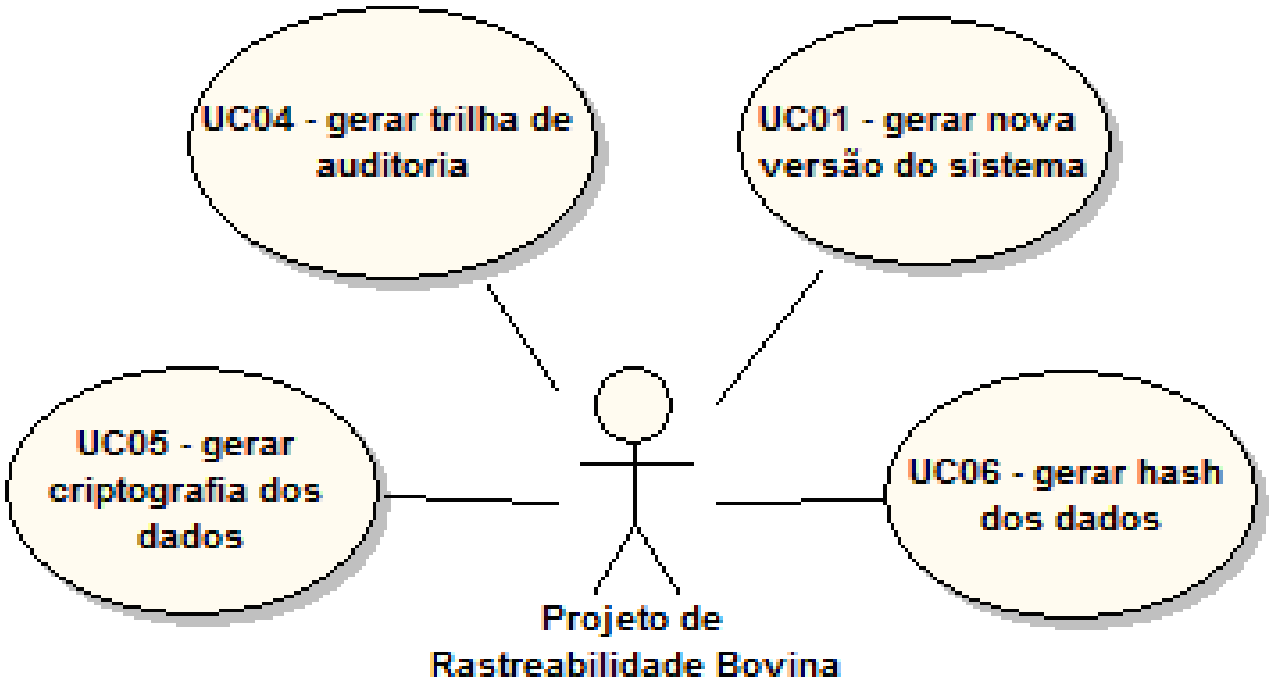
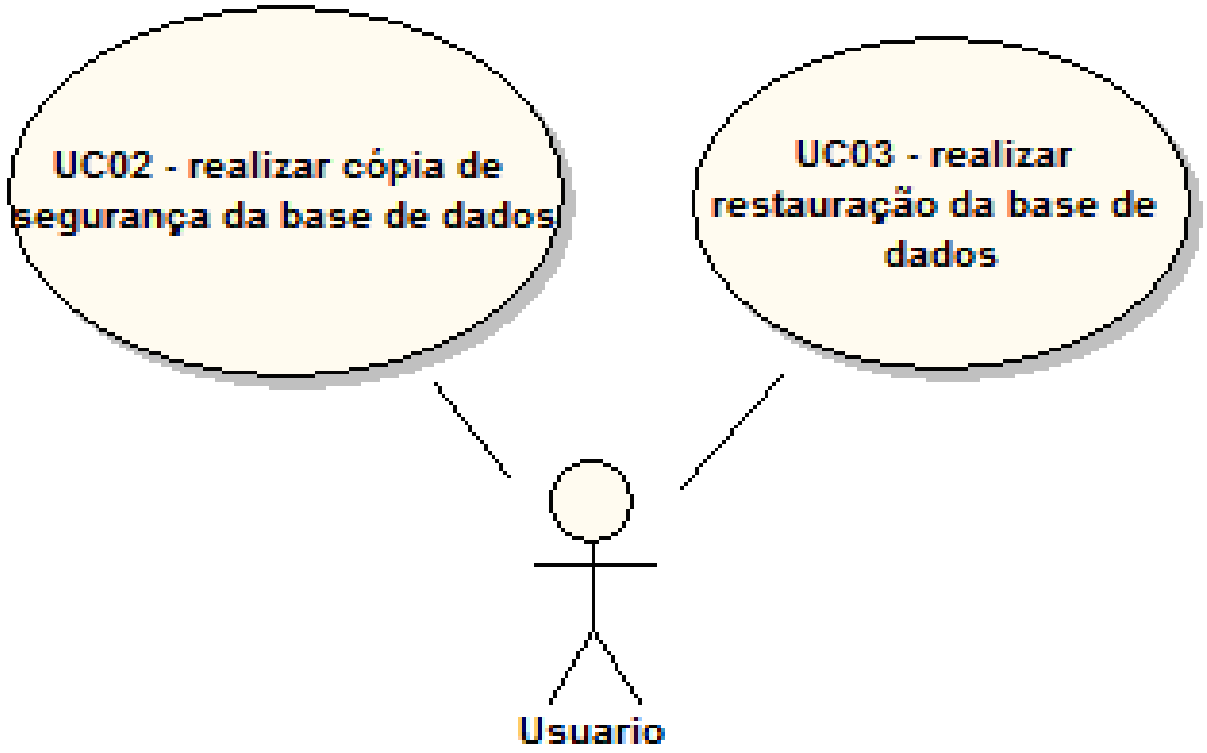
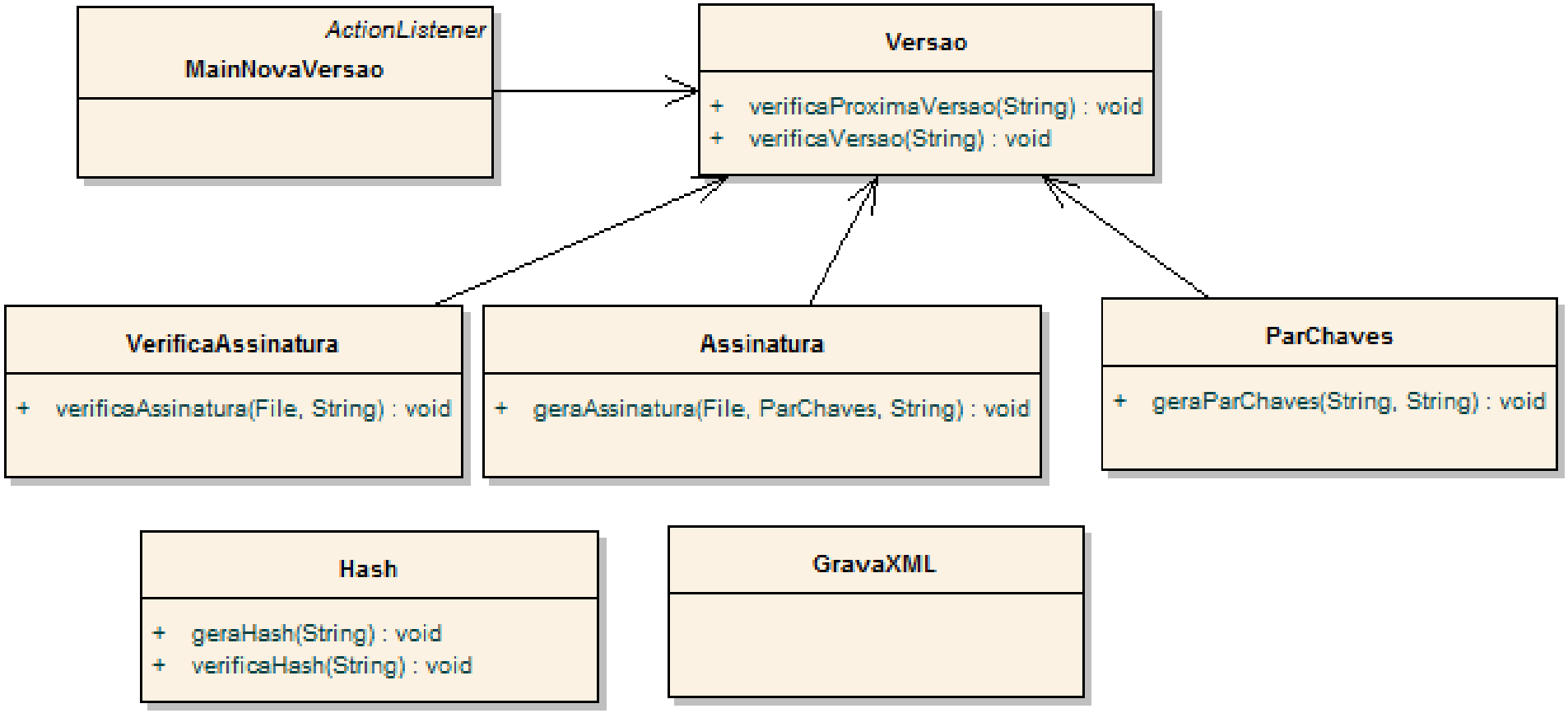


Diagrama de casos de uso

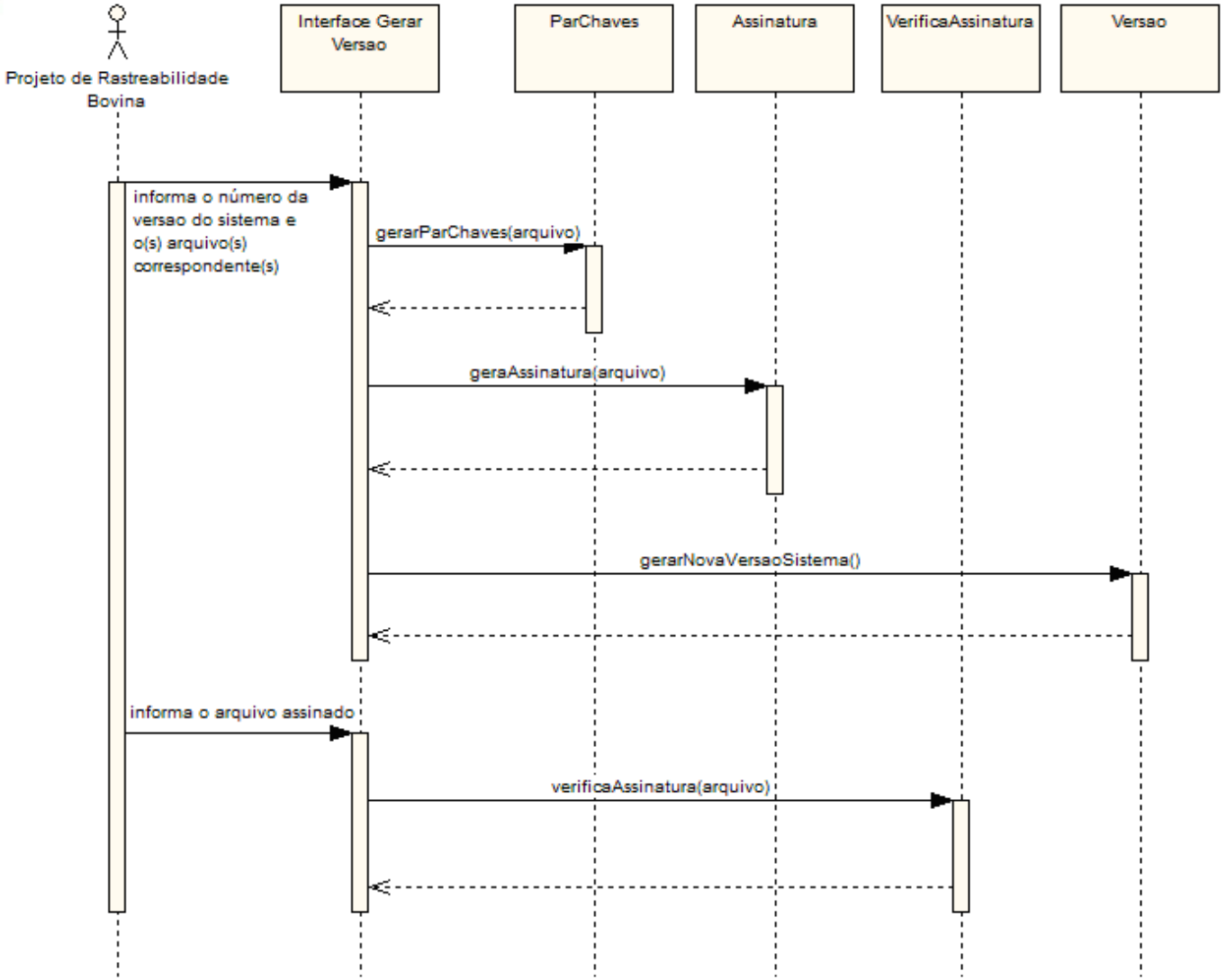
• Diagrama de casos de uso executados pelo usuário.



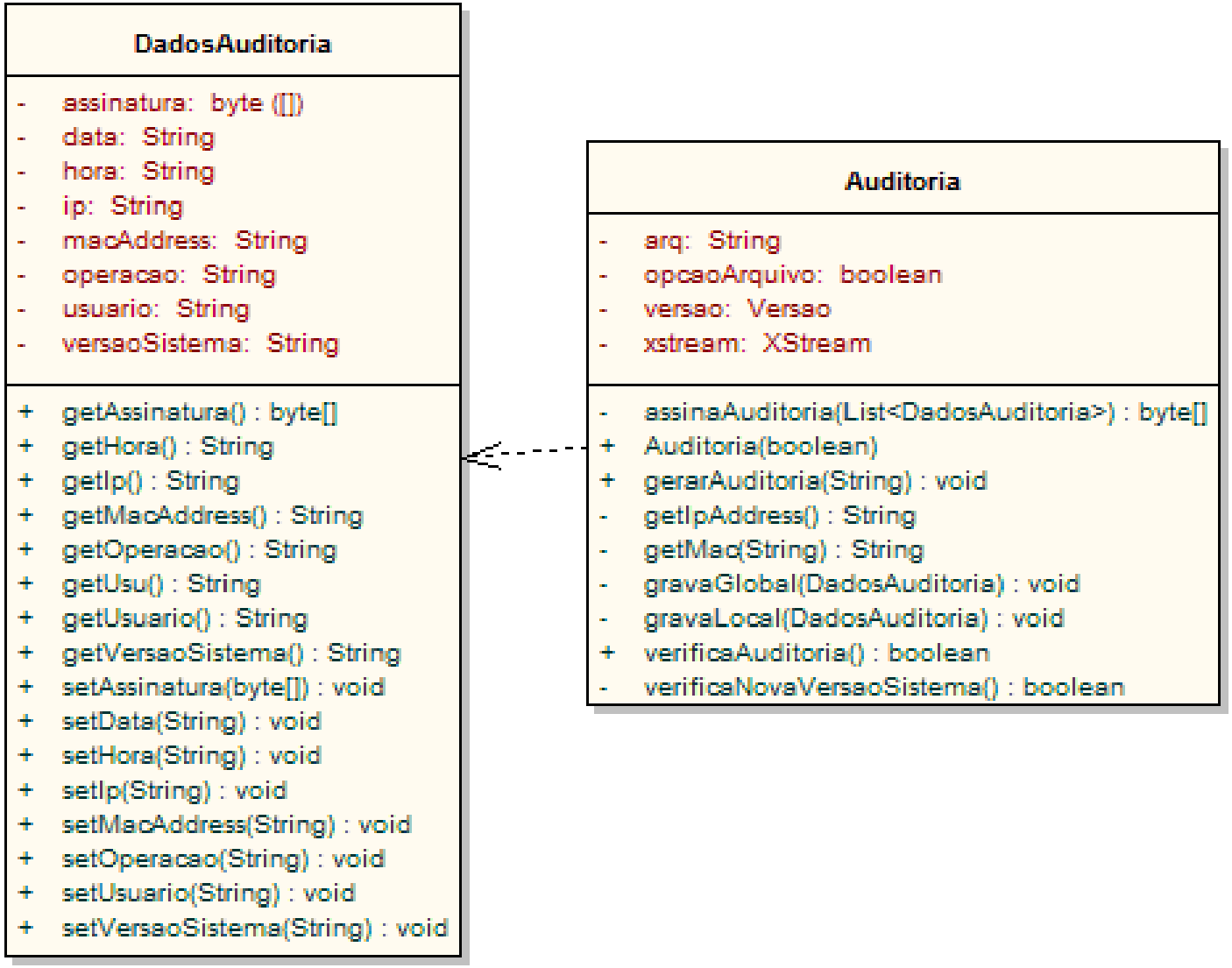
Especificação da classe FDP



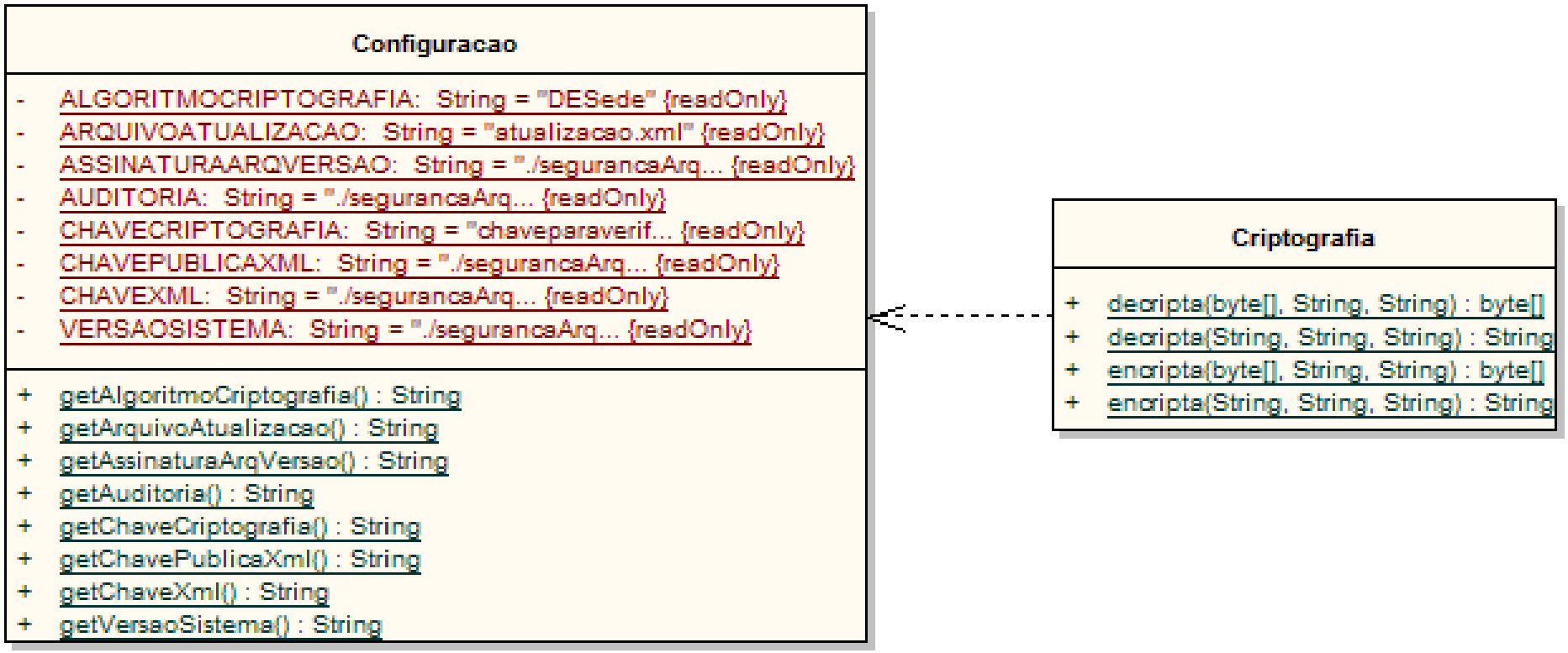
Especificação da classe FDP



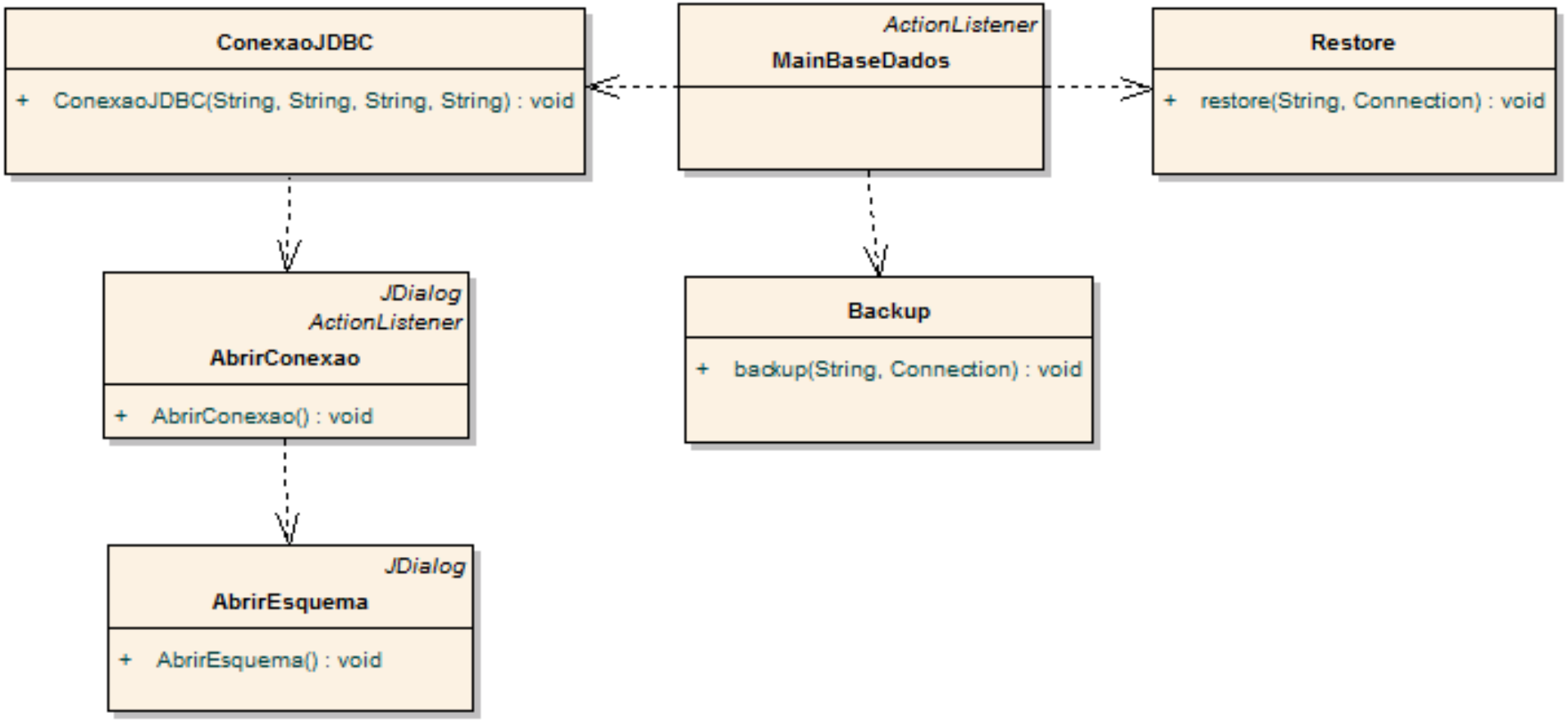
Especificação da classe FAU



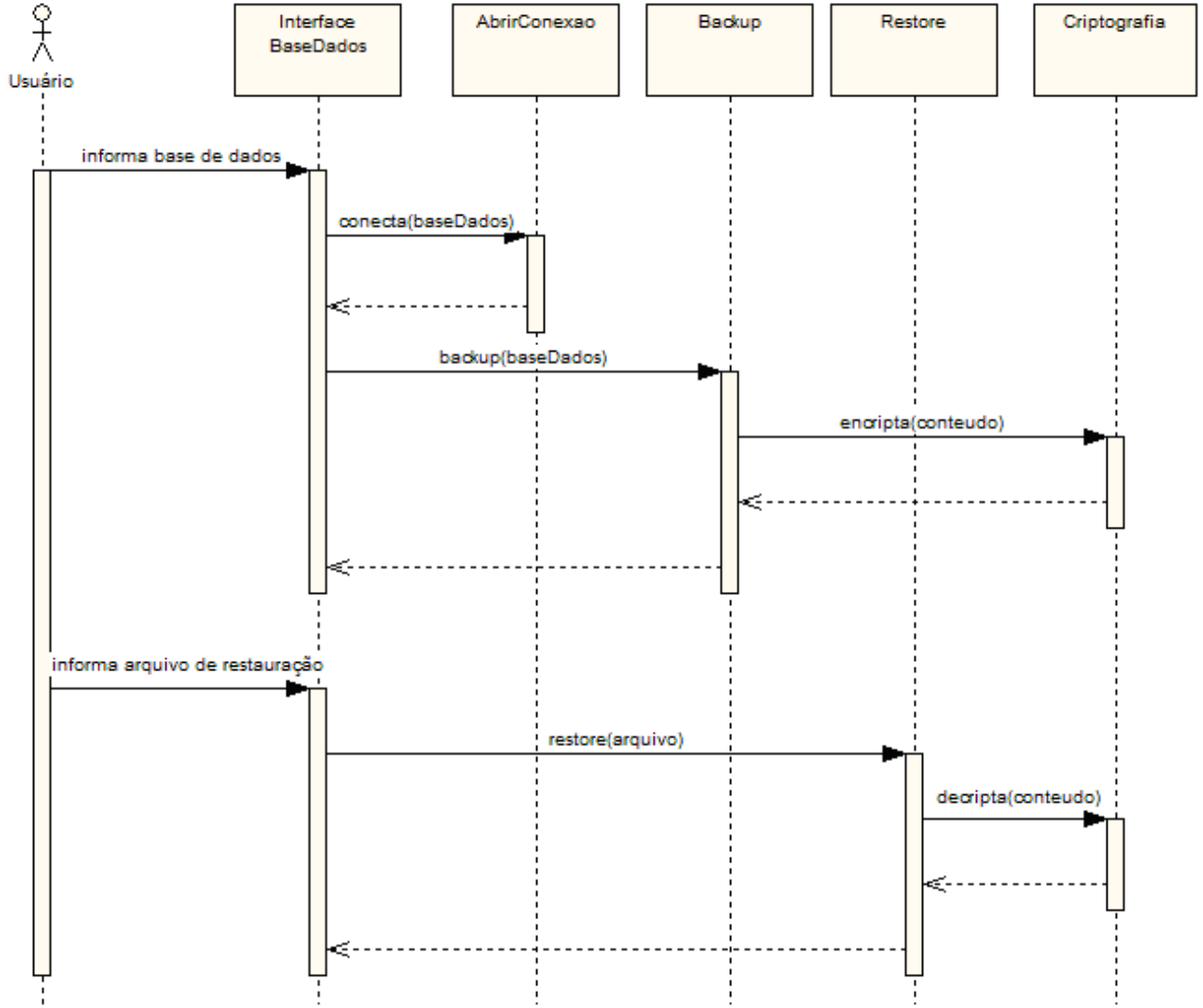
Especificação da classe FCS



Especificação da classe FPT



Especificação da classe FPT



Implementação

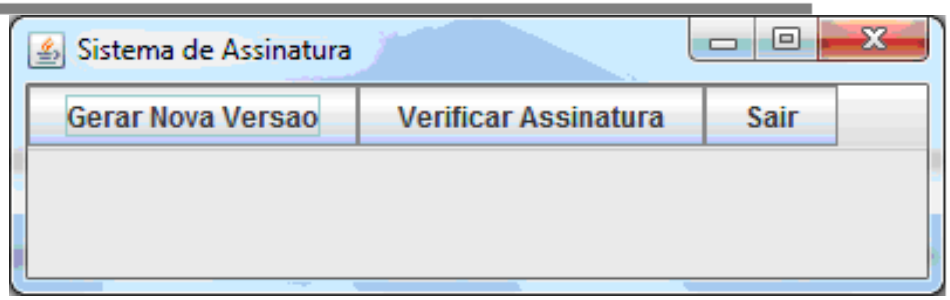
Tecnologias e ferramentas utilizadas

- Linguagem de programação Java.
  - Eclipse 3.4;
  - API JDBC.
- Bibliotecas:
  - XStream;
  - OpenSSL.

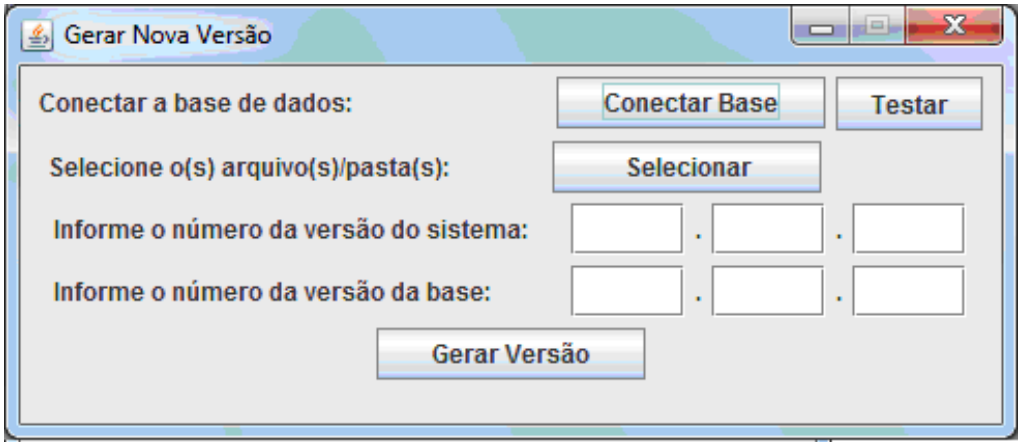
Operacionalidade

Operacionalidade da classe FDP

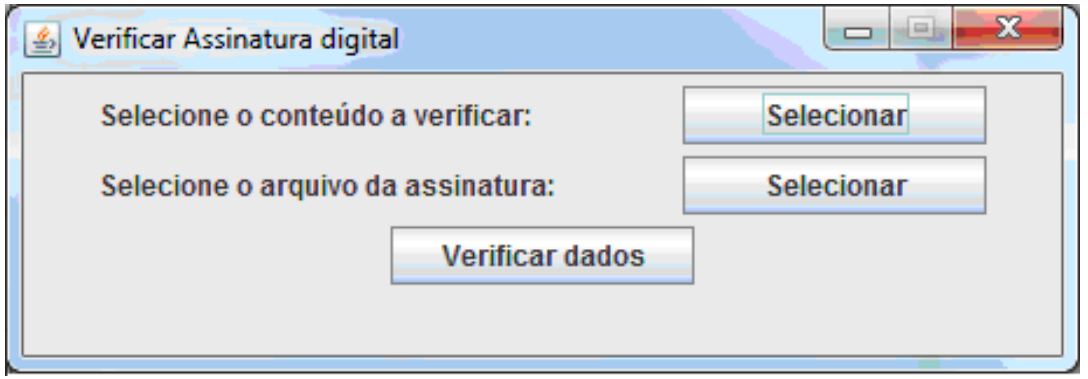
Interface inicial



Interface da geração da nova versão



Interface para a verificação da assinatura digital



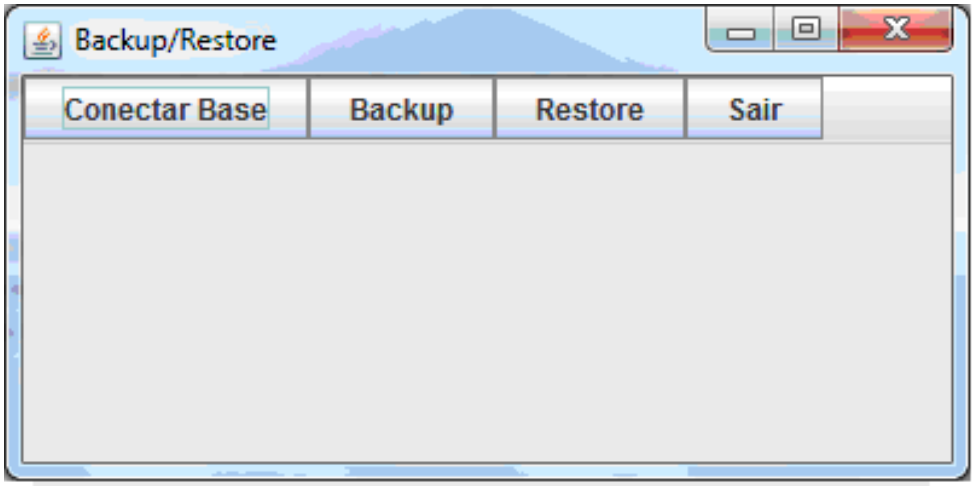
Operacionalidade da classe FDP

Arquivo – chaves.xml

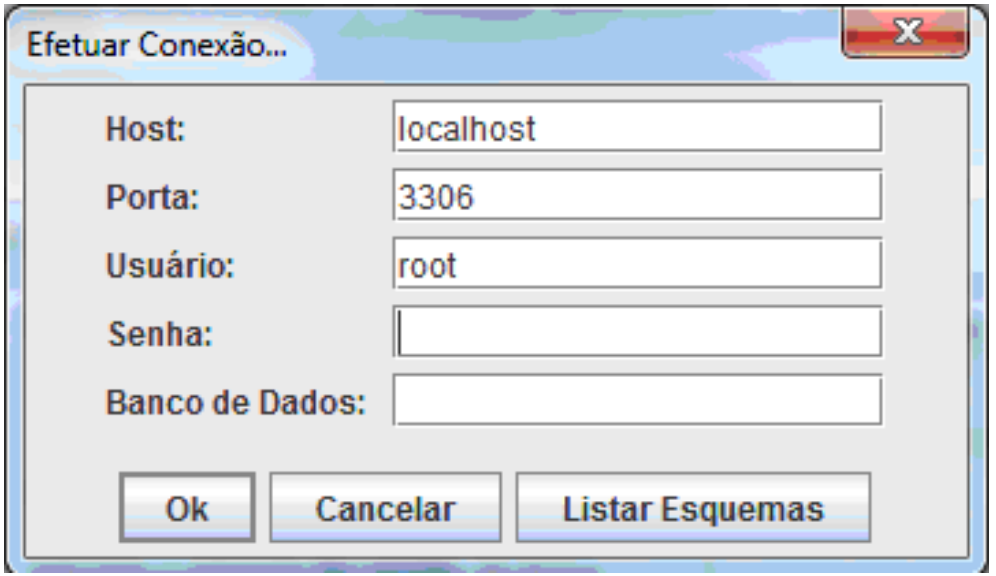
```
<list>
    <seguranca.assinatura.GravaXML>
        <versaoSistema>1.2.1</versaoSistema>
        <versaoBase>1.2.0</versaoBase>
        <chavePrivada>
            xtpraAPPnmdVe2qLUt8OmHraz/Uq+T615Er39oJnjS6XzdZOuagHte85aCTQuwtoCfCLxlF+TJCh
            8VI1o6kL8Uv7WvkuX19Cqbfpw5BDP2C3qHTB9D3A8N26IxUbRTSDBSlI1RoyqwWS41xr4hiFg/dz
            ITLhuFOhErOxrjiuPirGtjJaJ5bOtNbQk9EzUlsiecFVBaMzpq2DOF5HzMEOpDnW8lHiZr+AjgbZ
            mpvgQwAu/kA1cLFQslNw7Rgf8NVsTiNp73j8tDqSrgWsuM9gEG9oAoa1wXEJZv9kETK1PubCwlDj
            RGlU51zRGXIAW+aPKwfuhfVSp/veCkuGEgIRMZXyIzSVRHFOD4U51QSfYO2Z9XBuGLjw/tJCw97N
            keqVYYOFhC4AAyZQO6kr6F4lTIYHrLwkY5z3P42wVUDn1bJ9qCbezGoovBh7Z1isvuI+Zm4Ur9Ol
            iyHeVBVB6S/A73zQZOOSGWsvTrMSaD4ZKWgdAV78NVB8r95hDKJPKE/ubFYENBT1SBZvcLrU1T3I
            +xaGf/sqIbcrMFsTlpdi43Hu+vBx5do67sp3DvJSv1MeagVF6rX4fzQpHGITmz3SI5B7iHXKQxJf
            P1VOsi+K93ONtWoJO3nkwPnFWhiMUNxY2ZdeXIXM95avjknrOlABChq5J9fV55dxyoNU6TKc8zlZ
            M2dS4EtUzMzzCn5+sNTfZsWo3YZGz9OfF2aBcQfczZ5K1im/brgBBz7pnfMutCGOoLXMRxA/aP9a
            2AlkF3A/bOw6r8Cb2yleQRhMeVztBSurDnkGqXITryIJ113fewkjmA8VEKAROBwZHKCXuKl7vid5
            IaTtJj5zjEm4mKT1HQ==</chavePrivada>
        <chavePublica>
            MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpVoSghMqhqa1eY2SV4jZdG+dOgrMo7IVgssKd
            BsW1Muf+GYStRj9REU7dm2nn6O2hSOxrhFhxNWdDOxf6ylsMbfe3kPaOoulyndx9NX8LdOcvviix
            jPSryNHd5Crs6Y2AedlaJF+Z44x/TdToGiISOSaG9MlincCaUyIisoicqwIDAQAB
        </chavePublica>
    </seguranca.assinatura.GravaXML>
</list>
```

Operacionalidade das classes FPT e FCS

Interface inicial



Interface para efetuar conexão com a base de dados



Operacionalidade das classes FPT e FCS

Arquivo SQL original

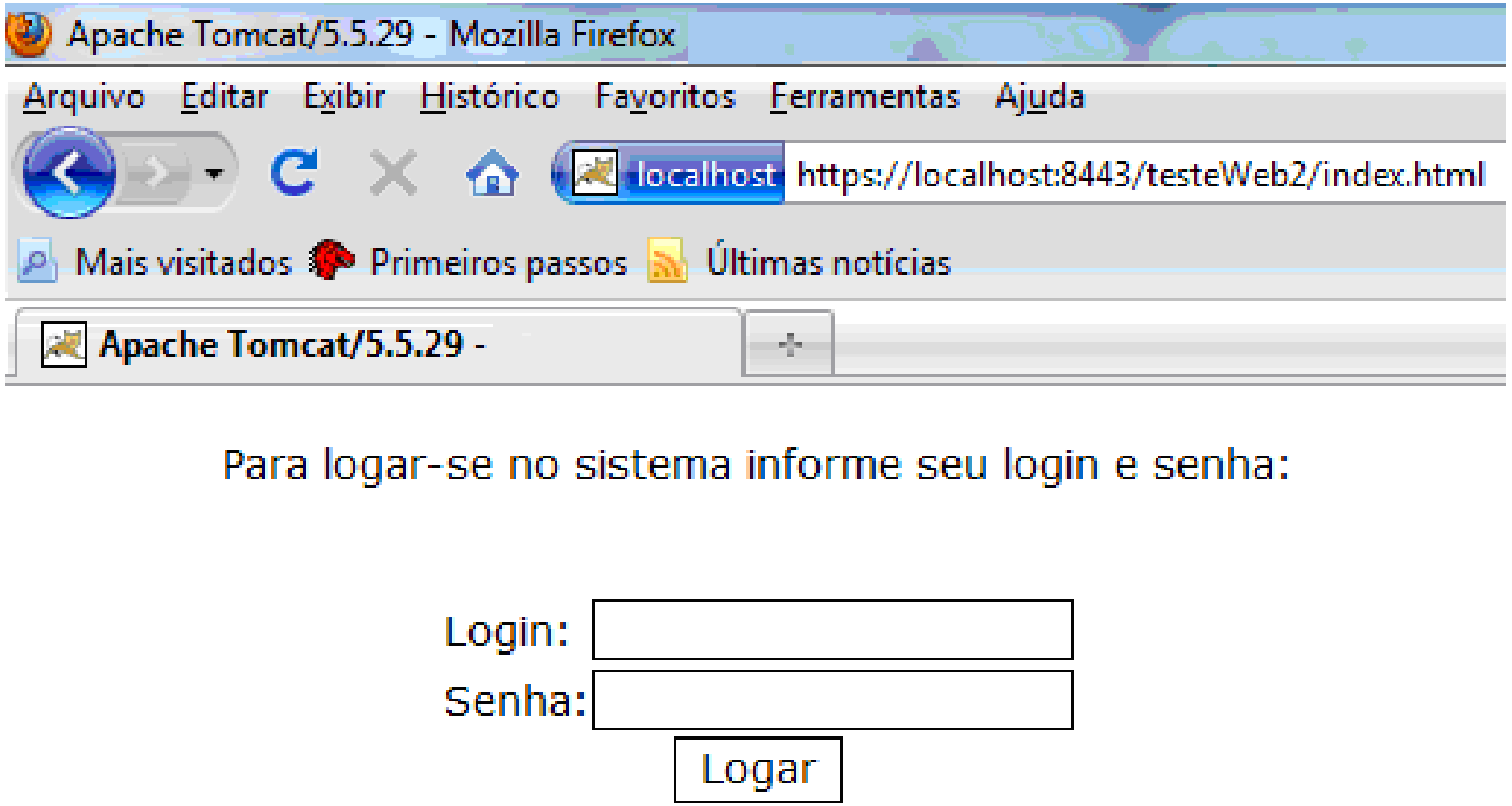
```
DROP SCHEMA IF EXISTS seguranca;
CREATE DATABASE IF NOT EXISTS seguranca;
USE seguranca;
DROP TABLE IF EXISTS `versaobase`;
CREATE TABLE `versaobase`(
  `nr_versao` VARCHAR(244) DEFAULT NULL,
  `data` date DEFAULT NULL,
  `idversao` int (11) unsigned DEFAULT NULL
   );
SET FOREIGN_KEY_CHECKS=0;
INSERT INTO `versaobase`
(`nr_versao`, `data`, `idversao`)
VALUES
("1.1.1","2010-06-24","1");
SET FOREIGN_KEY_CHECKS=1;
```

Arquivo SQL criptografado

```
Tv1k34G/I/xMU1XLGqKRobrLhr14WvrK0gq8dZmdVQgG9zXyUifHeA==;
uRaLmeoHZOEa+uEXg1Vs8dG1XWVs3AD0usuGvXha+srSCrx1mZ1VCAb3NfJSJ8d4;
u5FnxoxnA6Pf2EMIJoqgJQ==;
so0aDTOabo4wqB/JYA1wlcqdua/0/FJPTAuB0jKb3hmiqWTLio9BCPpqu9GxxD2mLXT03UH/pDY/
T/wsCM2IVp9jph0TLercVwM4NOydo7w/Xe1q7iv2KiHpz5Q3wFHzrA6pLoLreBM5kOcsNHMWcC+b
+783oL7+BDcGqY5kh4vPU6G4RKaYhWuHXIDJGIdEd708UQyVdceB3CoNshHTs5Srh4wcHzHM3AMm
pjTRpd1dLhAP1wcHLQ==;
gTQ1w+rwO0mZLjL9AgbEtSJTjNnztgzNDkwT9zel4E4=;
BIZkBEw3utiRfetBdFb6Oexh86VhxRHzguoL7/iCaac4VrvYiy44M6qQjWh3H70bdRC/6t2HcGV9
3B9V6aauFWfhlwghM6RFcnDSVO0jCfFu4szRimc8IF1aTzeLuu7+;
gTO1w+rwO0mZLiL9AgbEtY9HiGl+a3VwDkwT9zel4E4=;
```

Operacionalidade das classes FAU e FTP

Tela de autenticação de usuários



Operacionalidade das classes FAU e FTP

Arquivo – auditoria.xml

```
<auditoria>
  <seguranca.auditoria.DadosAuditoria>
    <operacao>Login efetuado com sucesso!</operacao>
    <usuario>admin</usuario>
    <data>04/05/2010</data>
    <hora>09:57:06</hora>
    <versaoSistema>1.1.1</versaoSistema>
    <ip>201.54.196.81</ip>
    <macAddress>00-1E-68-20-3B-22</macAddress>
  </seguranca.auditoria.DadosAuditoria>
  <seguranca.auditoria.DadosAuditoria>
    <operacao>Logout efetuado com sucesso!</operacao>
    <usuario>admin</usuario>
    <data>04/05/2010</data>
    <hora>09:57:14</hora>
    <versaoSistema>1.1.1</versaoSistema>
    <ip>201.54.196.81</ip>
    <macAddress>00-1E-68-20-3B-22</macAddress>
    <assinatura>YocfdPd/DXjDECFSNUqr2qFs4bWj6dAW79IzTYn
    fJ3Ng6qpLXKh5SYkTcnYLOeFRH2698uuqVx20
lPiPzxHNQjqRG5d+15i7wQ9+KgK2OumzK2amQ9kCrFeMmVMDDFYUnL
Ni4dy1jOO67jPCmL8nhc86
00jWDRMmuh0WcMZqR/A=</assinatura>
  </seguranca.auditoria.DadosAuditoria>
</auditoria>
```

Resultados e discussão

Resultados e discussao

Nome da classe	Sigla	Itens atendidos
Proteção de dados do usuário	FDP	FDP_DAU.1 – autenticação básica dos dados
		FDP_DAU.2 – autenticação dos dados com identidade do gerador
		FDP_ETC.1 – exportação de dados com atributo de segurança
		FDP_IFC.1 – controle de fluxo de informação
		FDP_ITC.2 – importação de dados com segurança
Auditoria	FAU	FAU_GEN.1 – geração de dados para auditoria
		FAU_GEN.2 – associação do usuário ao evento de auditoria
		FAU_SAR.1 – revisão de auditoria
		FAU_SEL.1 – auditoria seletiva
		FAU_STG.1 – armazenamento protegido da trilha de auditoria
		FAU_STG.2 – garantia da disponibilidade dos dados para auditoria
Autoproteção	FPT	FPT_ITC.1 – confidencialidade dos dados exportados pela aplicação
		FPT_ITI.1 – detecção de modificações;
		FPT_ITT.1 – proteção básica de dados internos da aplicação
Criptografia	FCS	FCS_COP.1 – operação de criptografia
Canais seguros	FTP	FTP_ITC.1 – canal confiável entre funções de segurança
		FTP_TRP.1 – caminho confiável

Conclusão

- Todos os objetivos foram atingidos;
- Foram implementados os itens de segurança de suma importância ao PRB.
- Linguagem Java, biblioteca XStream e API JDBC;

Extensões

- Análise dos outros itens de segurança segundo a norma ISO/IEC 15.408;
- Implementação dos outros itens de segurança segundo a norma ISO/IEC 15.408.

Obrigado!