Ambiente Virtual de Avaliações Utilizando Certificados Digitais

Fernando Gevard – Acadêmico
Paulo Fernando da Silva - Orientador

Roteiro

- Introdução
  - Objetivos do trabalho
- Fundamentação teórica
  - Avaliações à distância, aspectos de segurança da informação, certificado digital e os trabalhos correlatos
- Desenvolvimento do ambiente
  - Requisitos principais, especificação, implementação, operacionalidade e resultados e discussão
- Conclusão
  - Extensões

FURB

Introdução

- Ambiente Virtual de Avaliações Utilizando Certificados Digitais.
  - Desenvolvimento da funcionalidade de avaliações de um AVA.
  - Utilização de certificados digitais para autenticação do cliente.
  - Geração de diplomas virtuais assinados digitalmente.

FURB

Objetivos do Trabalho

- Disponibilizar um sistema web para um professor cadastrar questões e gerar avaliações para serem executadas por seus alunos;
- Garantir o controle de acesso de usuários com certificado digital;
- Garantir o controle de acesso às informações e a autenticação do usuário;
- Garantir a proteção das senhas de acesso dos usuários utilizando funções de *hash;*

FURB

Objetivos do Trabalho

- Garantir a trilha de auditoria para visualizar as ações dos usuários;
- Apresentar um relatório final com o resultado da avaliação executada pelo aluno;
- Garantir a geração de um diploma virtual do aluno, contendo informações sobre o aluno e a assinatura digital do diretor do sistema, utilizando um e-CPF;
- Garantir que qualquer usuário do sistema possa fazer a verificação da assinatura digital do diploma virtual do aluno.

FURB

Fundamentação teórica

* Assuntos principais *

Certificado Digital

- ICP-BRASIL
  - e-CPF

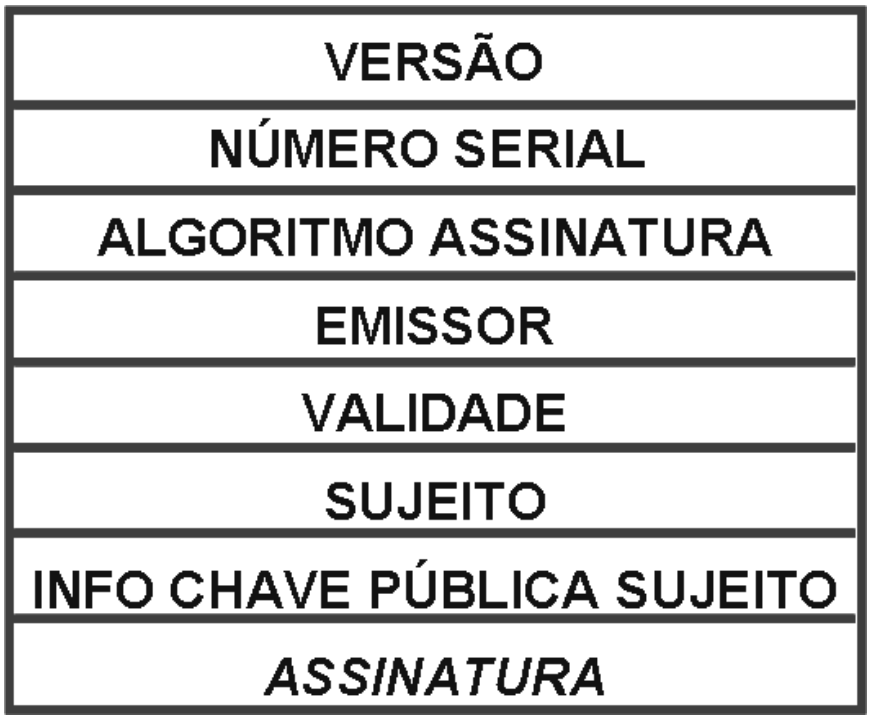
- Uma Autoridade Certificadora (AC) garante a autenticidade de um Certificado Digital.

- A AC assina a chave pública (certificado) de um cliente utilizando a sua chave privada.

FURB

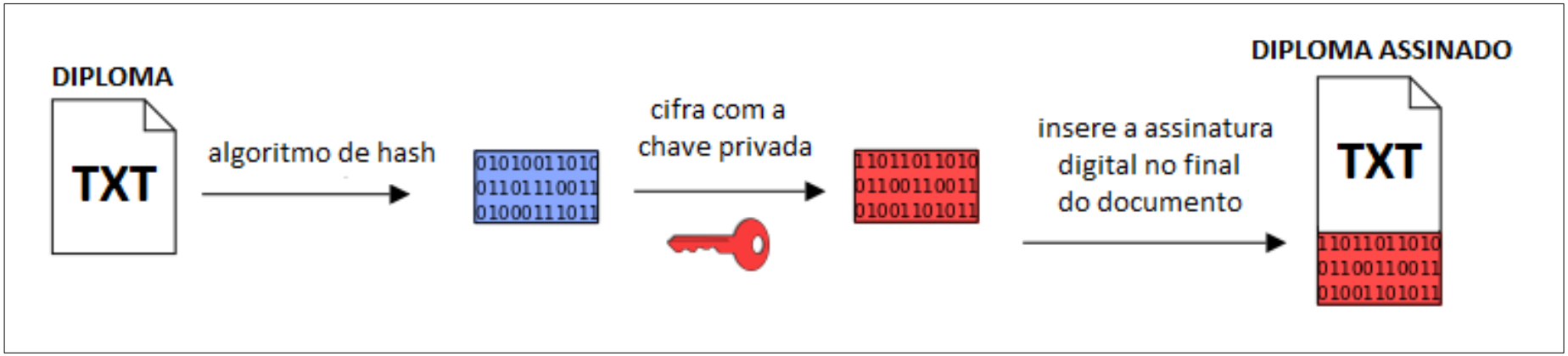
Certificado Digital

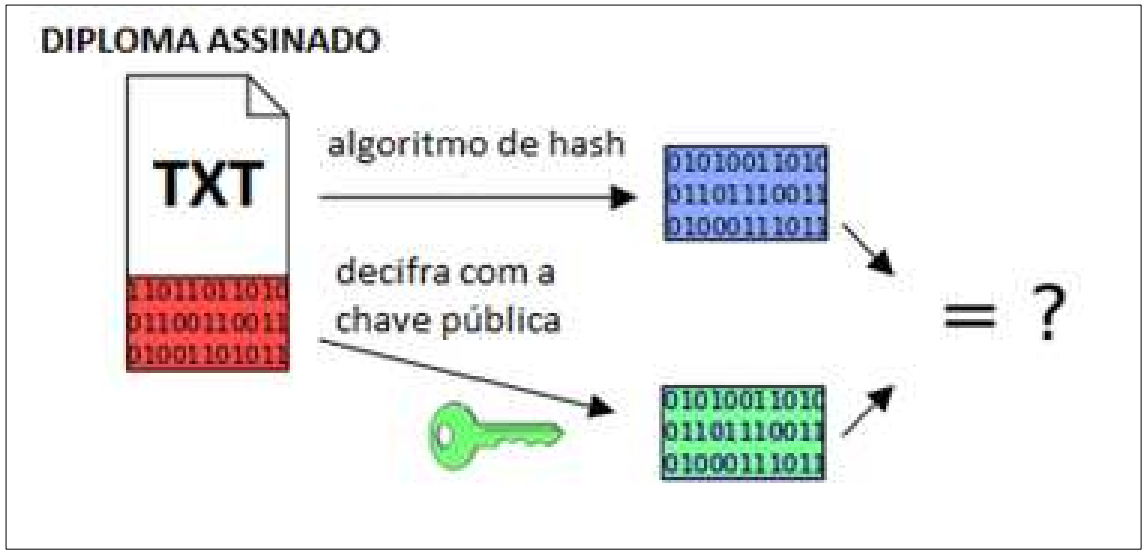
- Formato de um Certificado Digital:



FURB

Assinatura Digital





Trabalhos Correlatos

- Software de Apoio a Geração de Avaliações de Aprendizagem (DANEY, 2007);
- Ambiente Virtual de Aprendizagem da Universidade Regional de Blumenau (FURB, 2009);
- Protótipo de Software para Emissão de Certificados Digitais (MATHIAS, 2007).

FURB

Desenvolvimento do Ambiente

Desenvolvimento do Ambiente

Especificação

Requisitos principais

- Entrada de usuários com certificado digital válido;
- Autenticação do usuário;
- Auditoria de segurança para usuários administradores;
- Cadastrar de questões;
- Configurar uma avaliação com as questões cadastradas;
- Executar uma avaliação gerada pelo professor;
- Gerar um relatório das avaliações executadas;
- Gerar um diploma virtual em formato de texto e assinado digitalmente com a sua chave privada;
- Excluir qualquer diploma virtual gerado por ele anteriormente;
- Verificar e validar a assinatura digital do diretor contido no diploma virtual gerado.

FURB

Diagrama de casos de uso

- Diagrama de casos de uso executados pelo diretor.

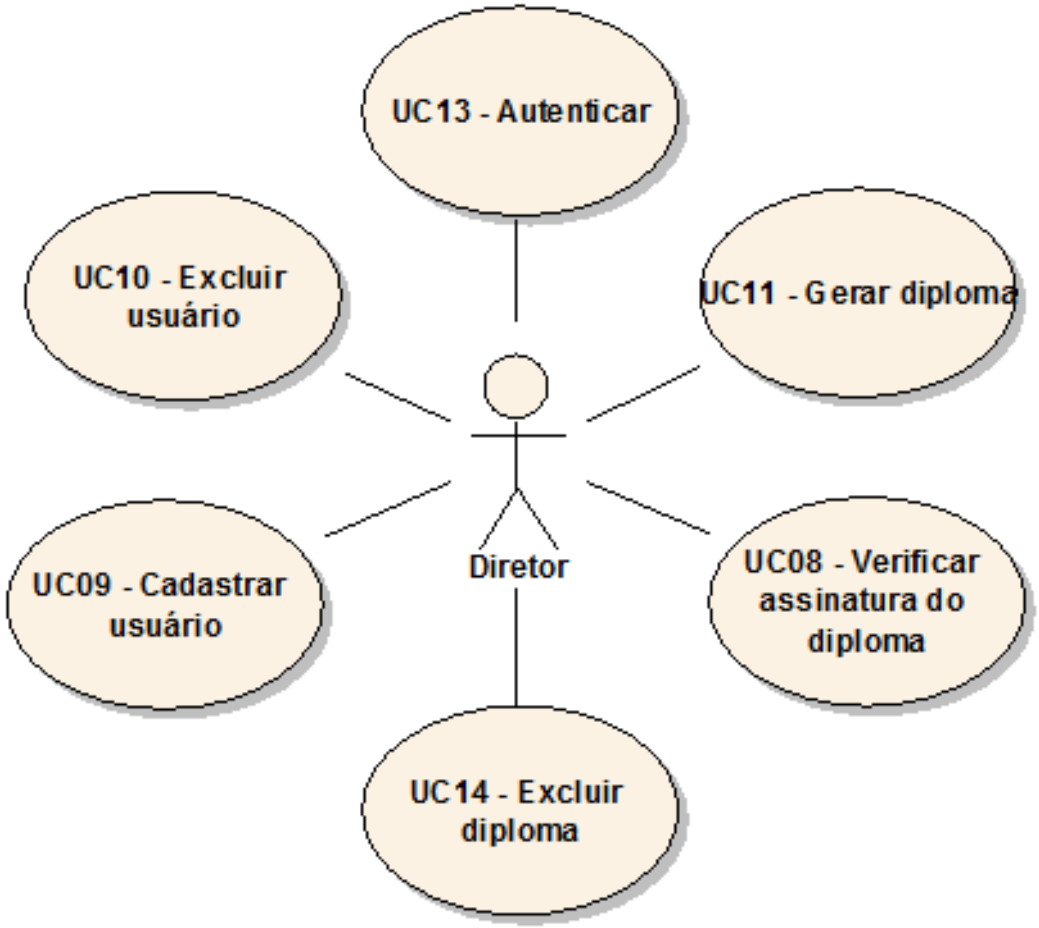


Diagrama de casos de uso

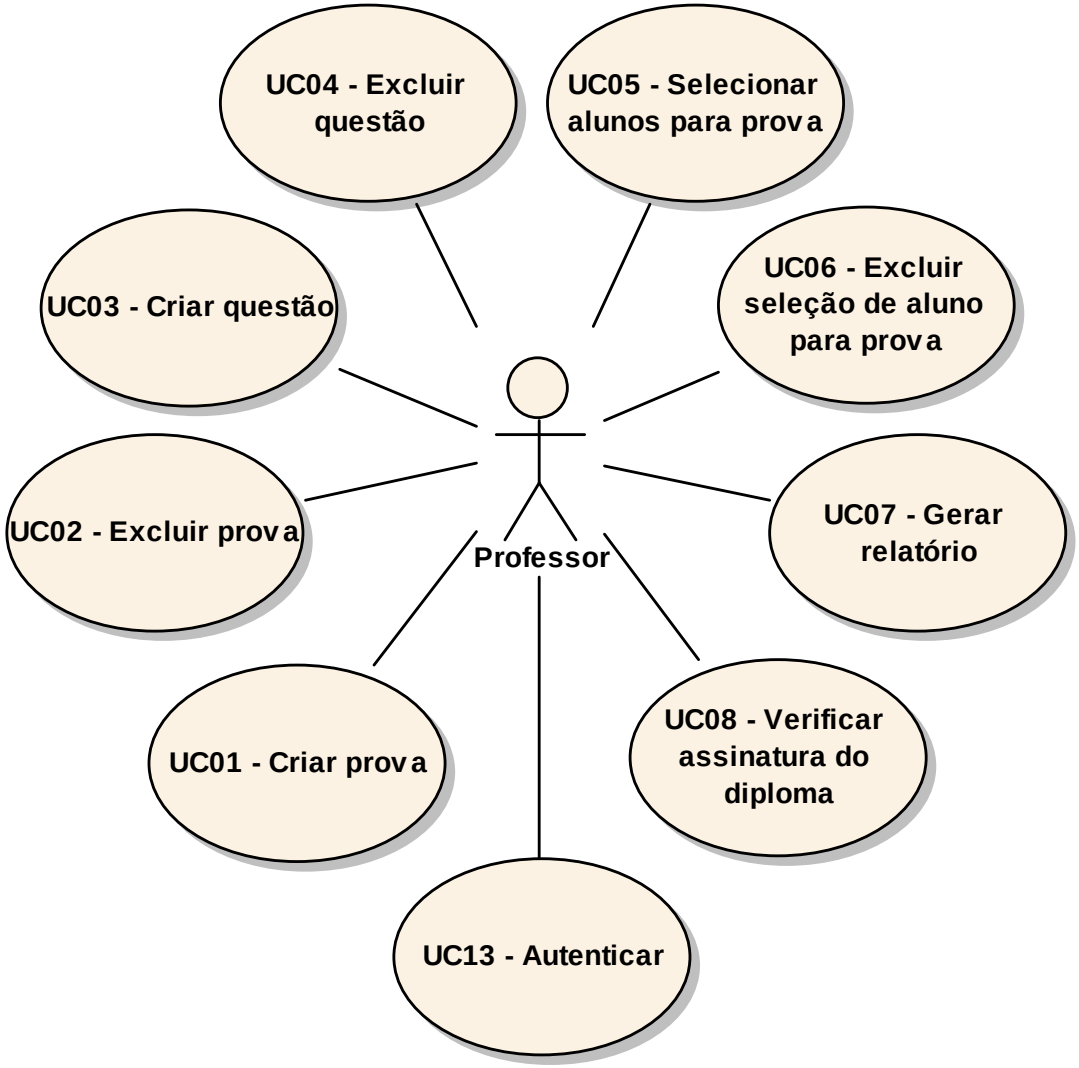


Diagrama de casos de uso

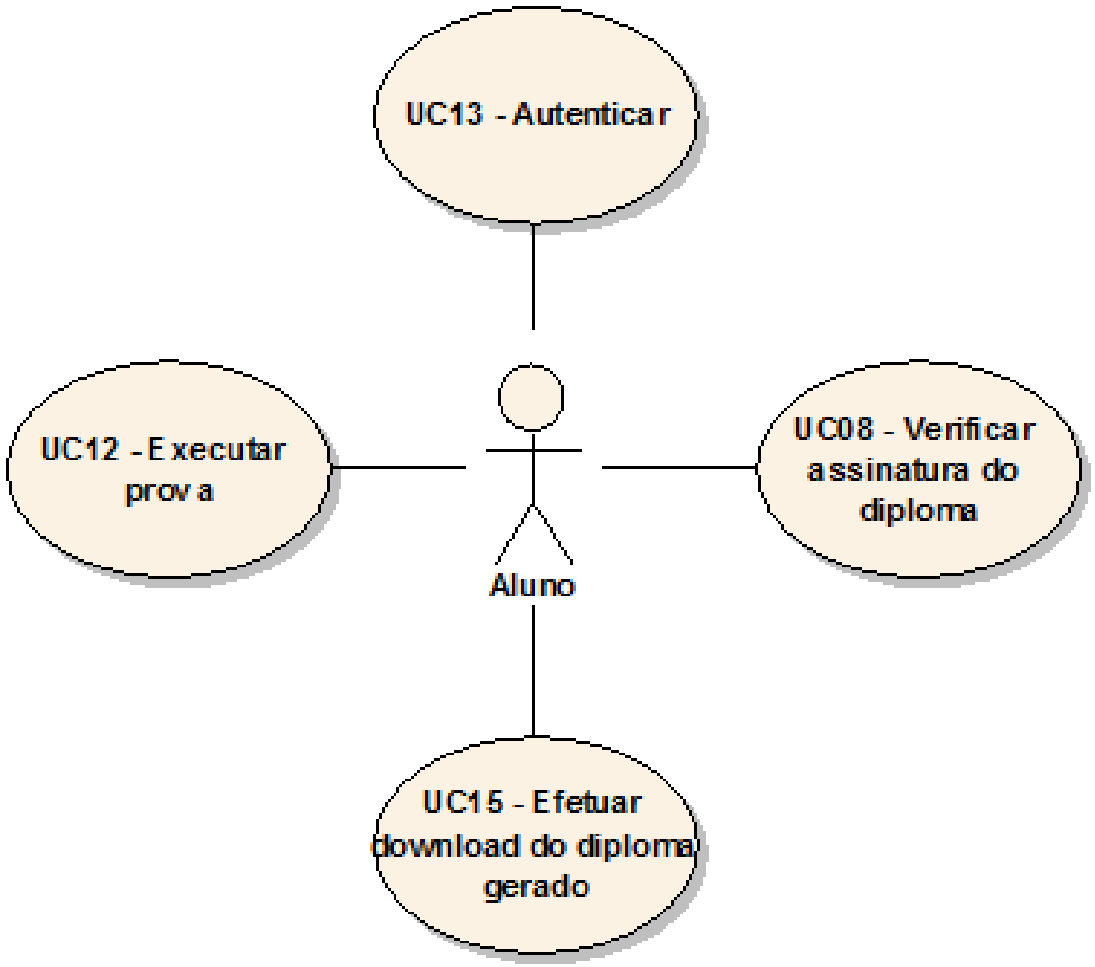


Diagrama de casos de uso

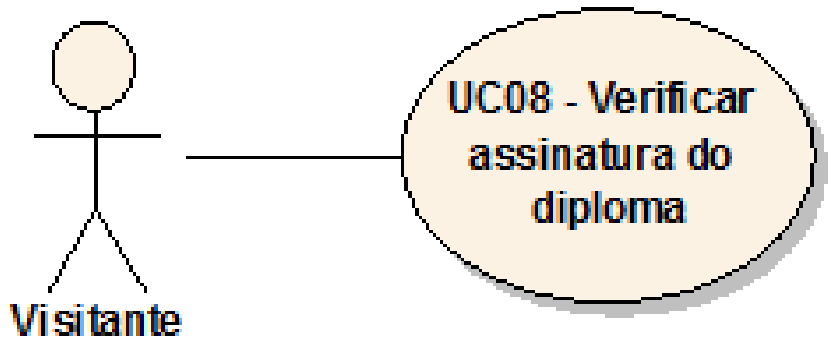
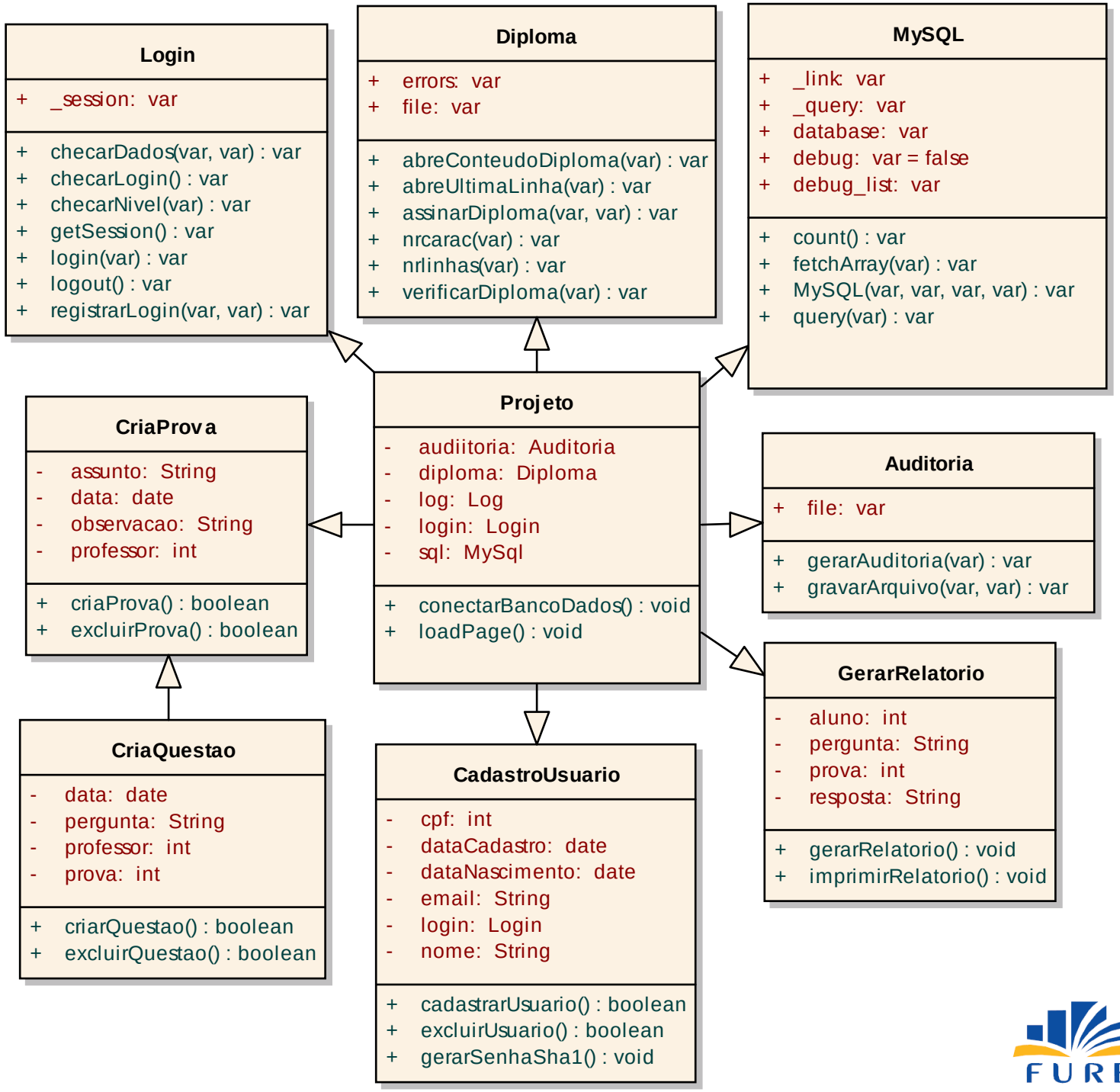
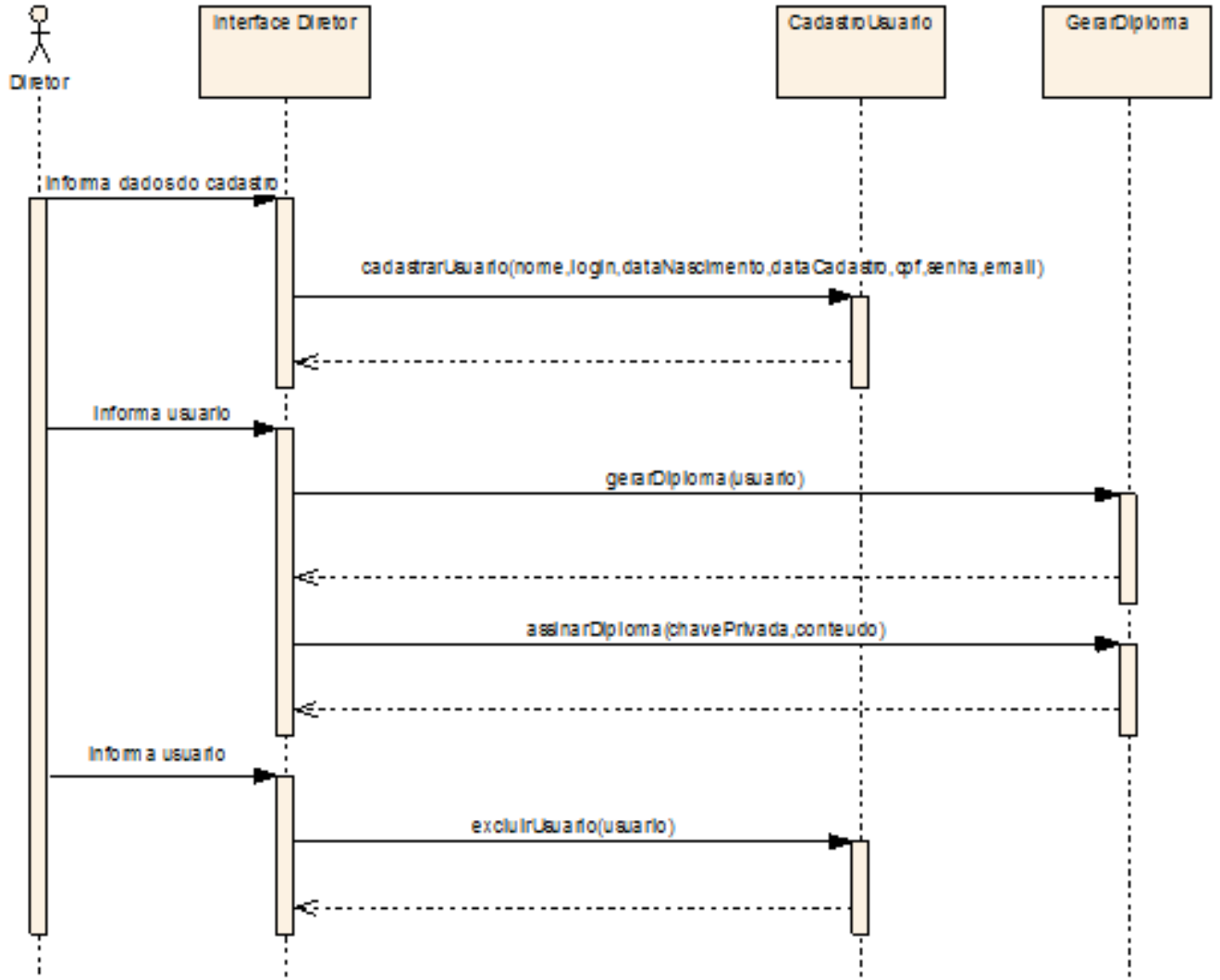


Diagrama de Classes



FURB

Diagrama de Seqüência



FURB

Implementação

Tecnologias e ferramentas utilizadas

- Linguagem de programação PHP.
  - DreamWeaver CS5;
- Banco de dados:
  - MySQL.
- Servidor:
  - Apache 2.

FURB

Operacionalidade

Operacionalidade do Certificado Digital

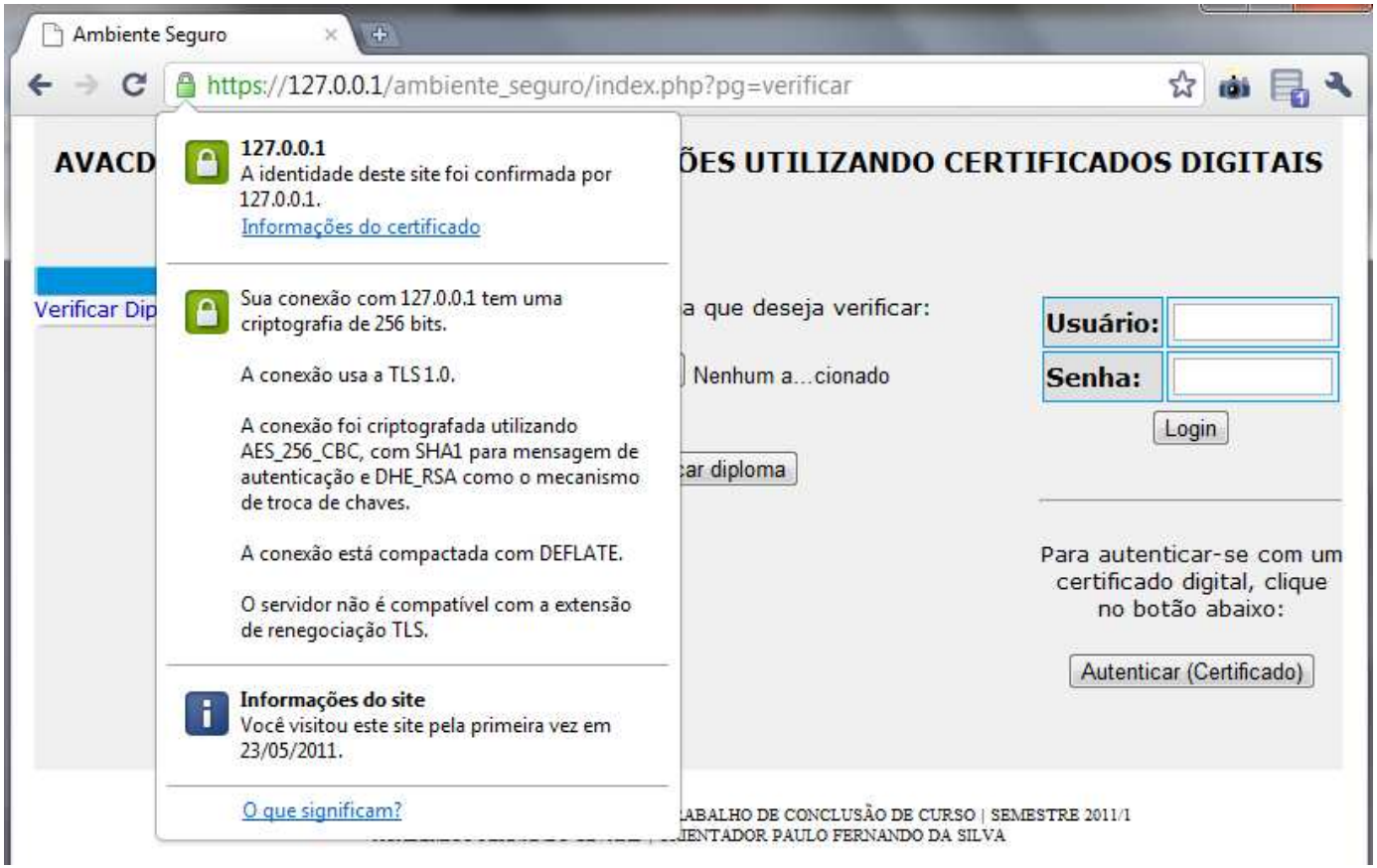
Operacionalidade do Certificado Digital

Certificado Digital do Servidor (auto assinado)

FURB

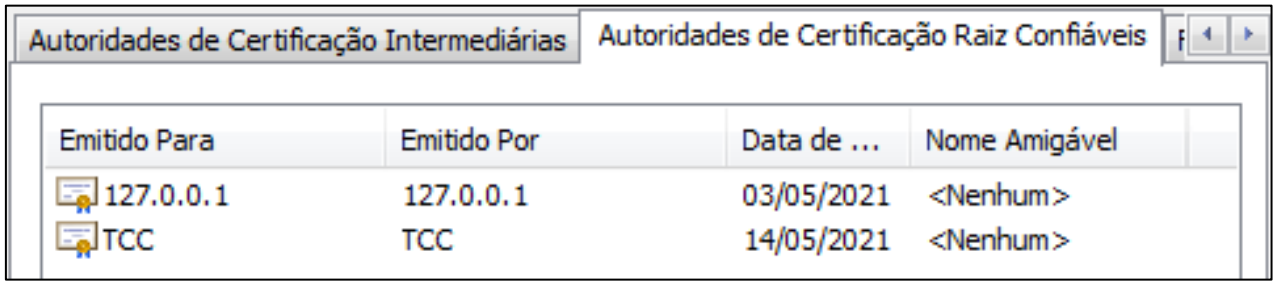
Operacionalidade do Certificado Digital

Detalhes do Certificado Digital do Servidor (auto assinado)

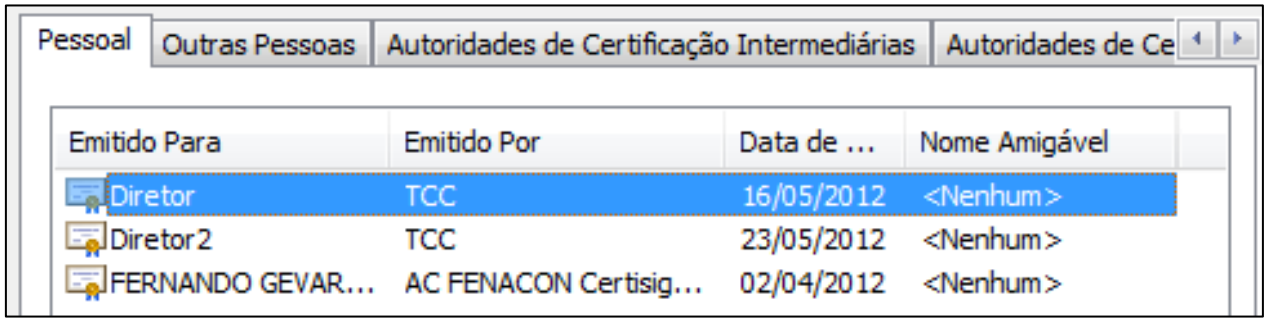


Operacionalidade do Certificado Digital

Repositório de autoridades de certificação raiz confiáveis



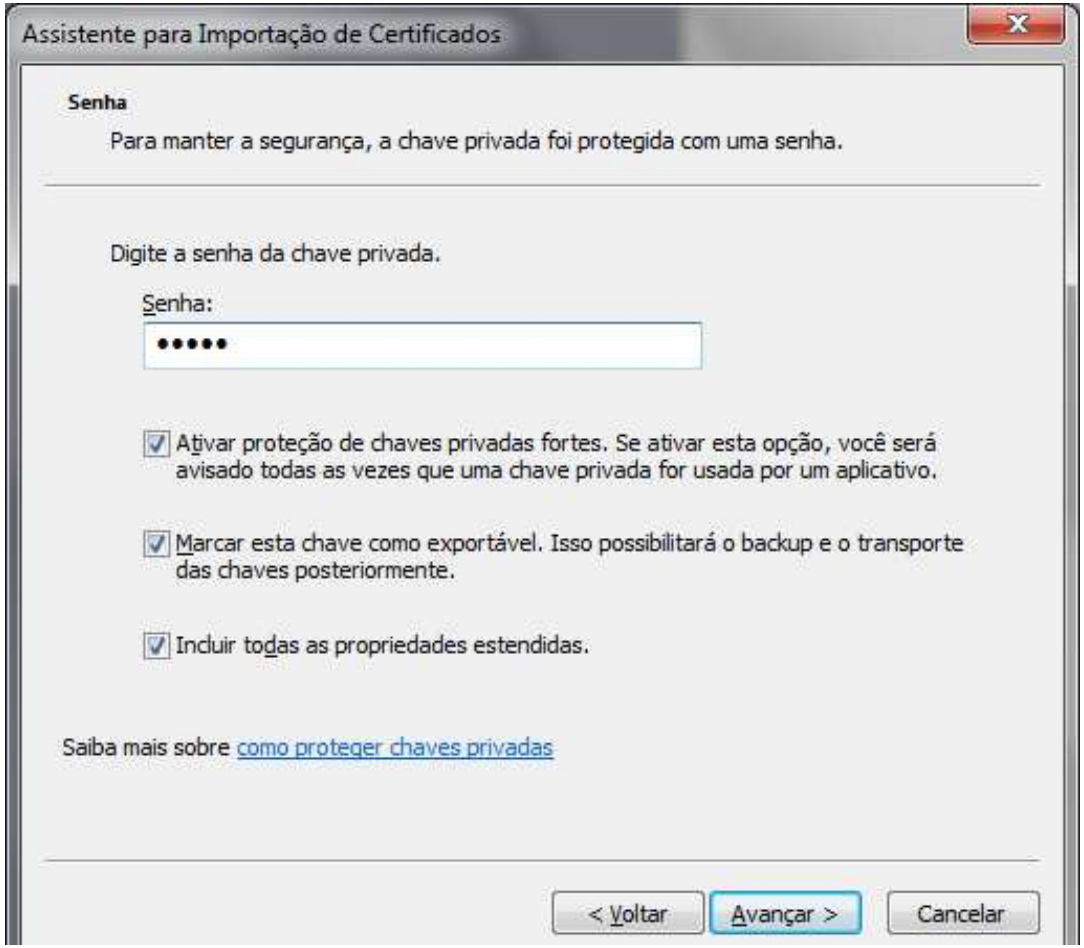
Repositório pessoal de certificados



FURB

Operacionalidade do Certificado Digital

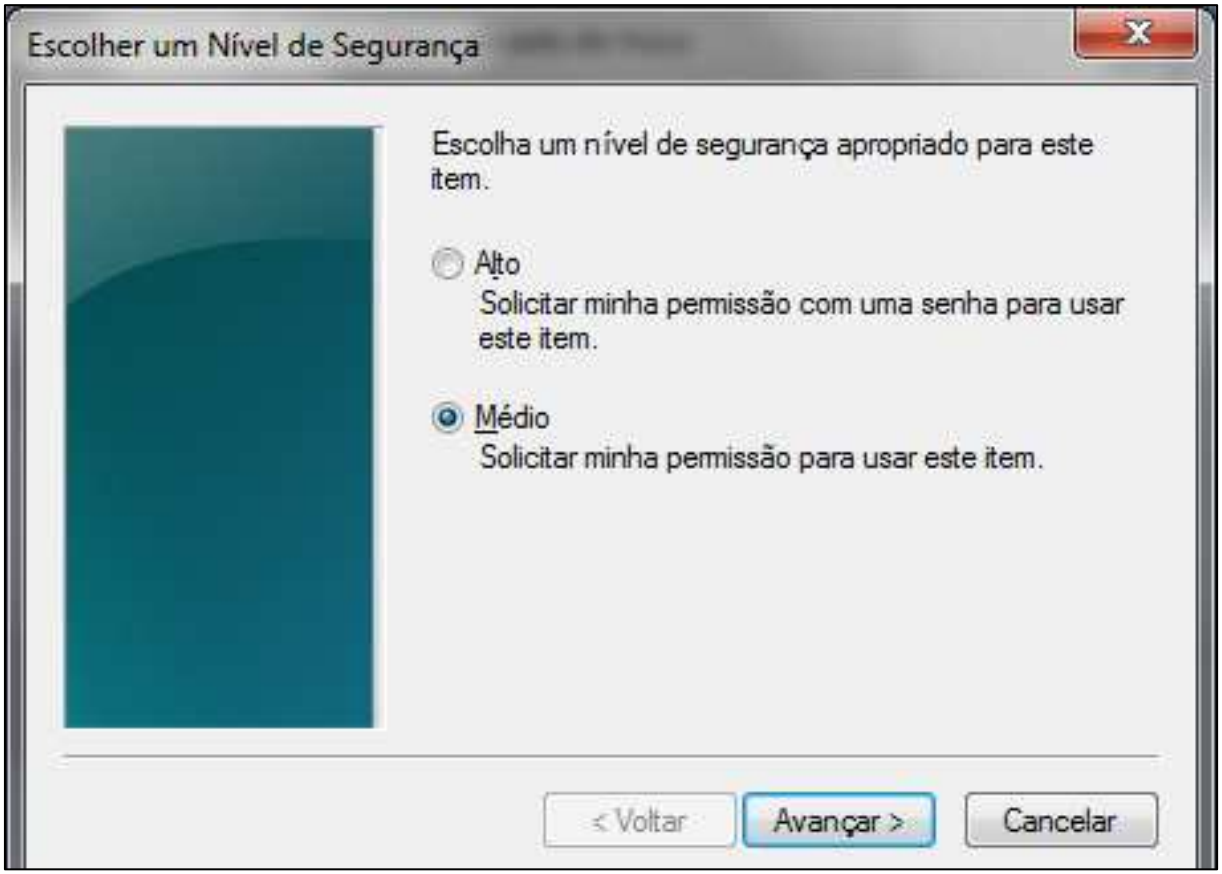
Opções de instalação do certificado do diretor



FURB

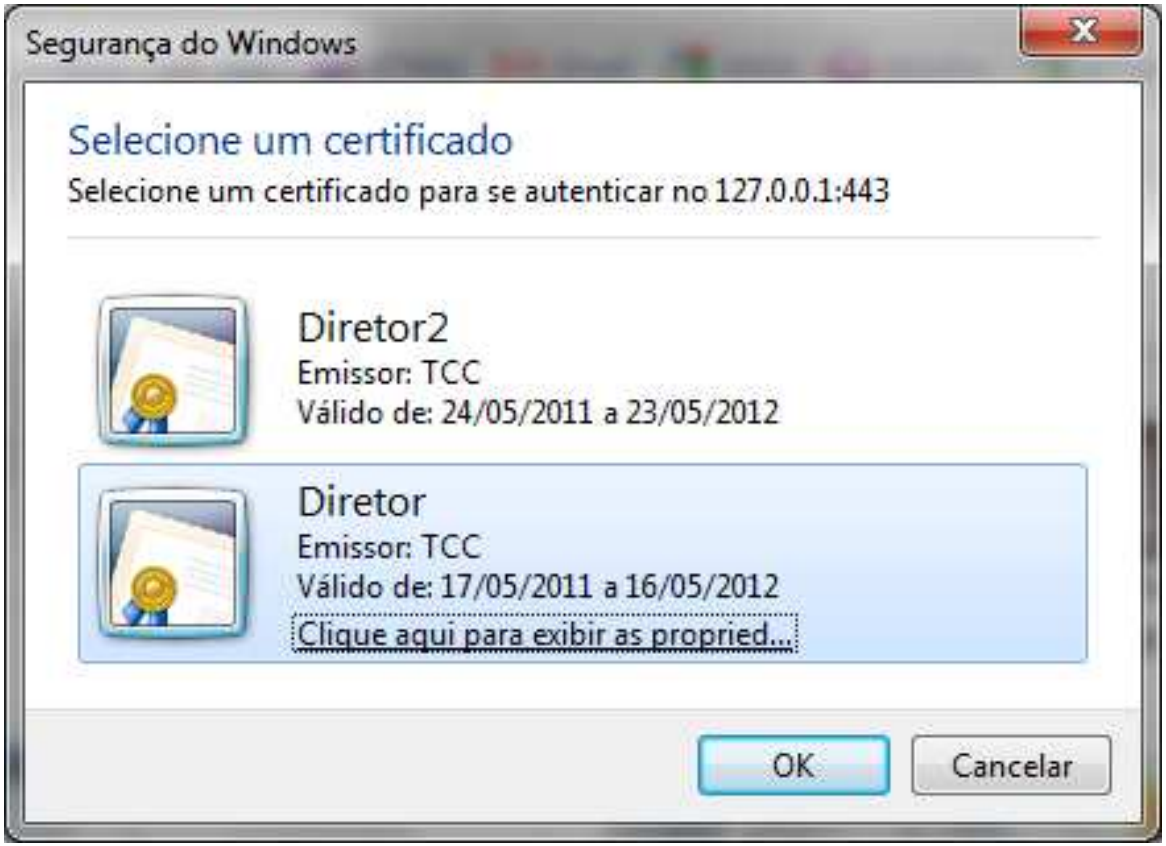
Operacionalidade do Certificado Digital

Nível de segurança da chave privada do diretor



Operacionalidade do Certificado Digital

Selecionando um certificado válido para autenticar o cliente



Operacionalidade das Funcionalidades Gerais

Operacionalidade das Funcionalidades Gerais

Utilização da função de *hash* para armazenar a senha do usuário

idusuario	login	senha	nome	cpf	dt_nascimento	dt_cadastro	nivel
4	proff	78be2913e9faa3c49fdf2ffc1f92d9eae3522497	PROF	4294967295	1222-12-12	2011-04-02	2
5	diretor	a381c49be4281e966501440a58ef30914abc4b37	DIRETOR	0	1988-1-1	2011-04-19	3
19	aluno1	f72eafc539768d2970925fd963a8f3b015a917c6	ALUNO1	198798	1999-1-1	2011-05-11	1
20	aluno2	b7ef9da90a2bd79099ebd48db885344a872bb155	ALUNO2	9879879	1999-1-1	2011-05-11	1

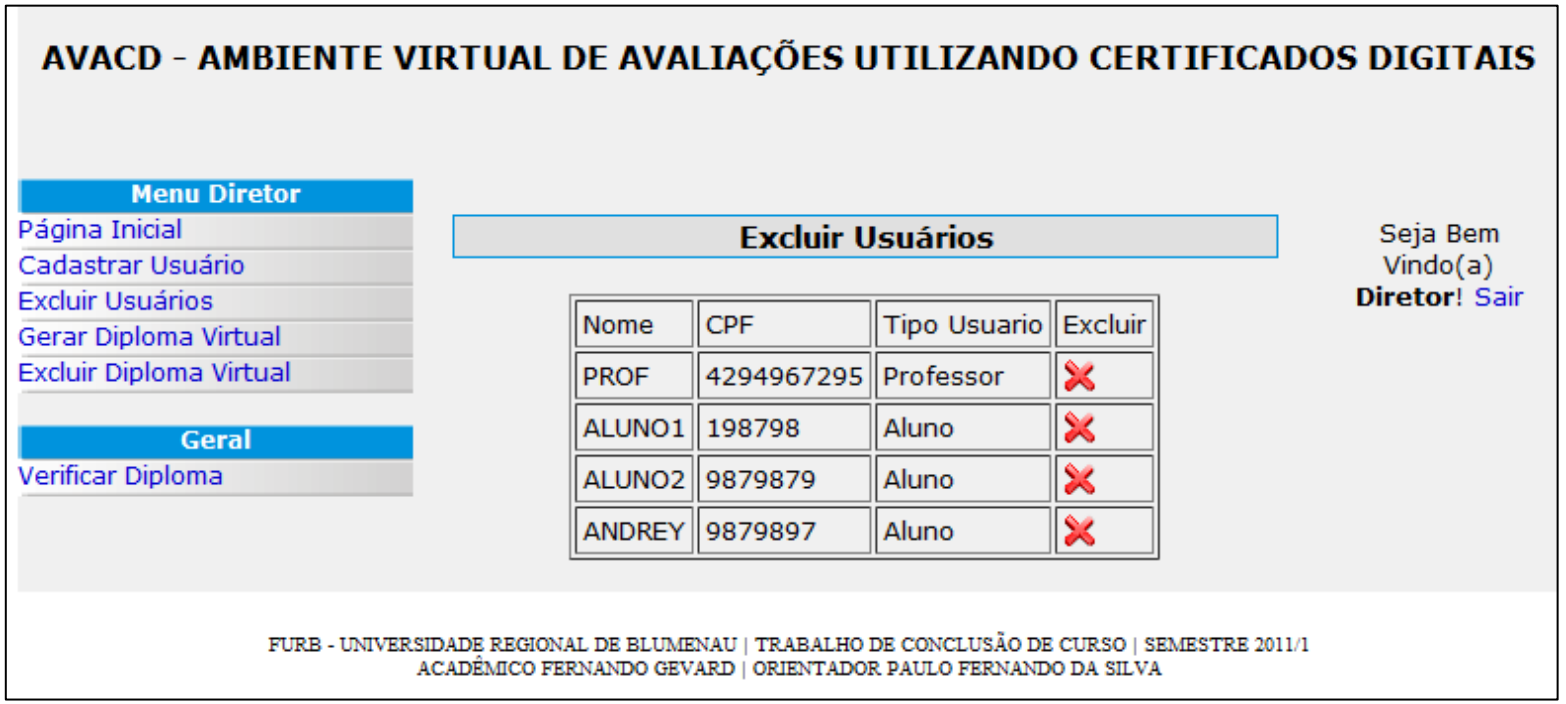
FURB

Operacionalidade das Funcionalidades Gerais

Cadastro de Usuários

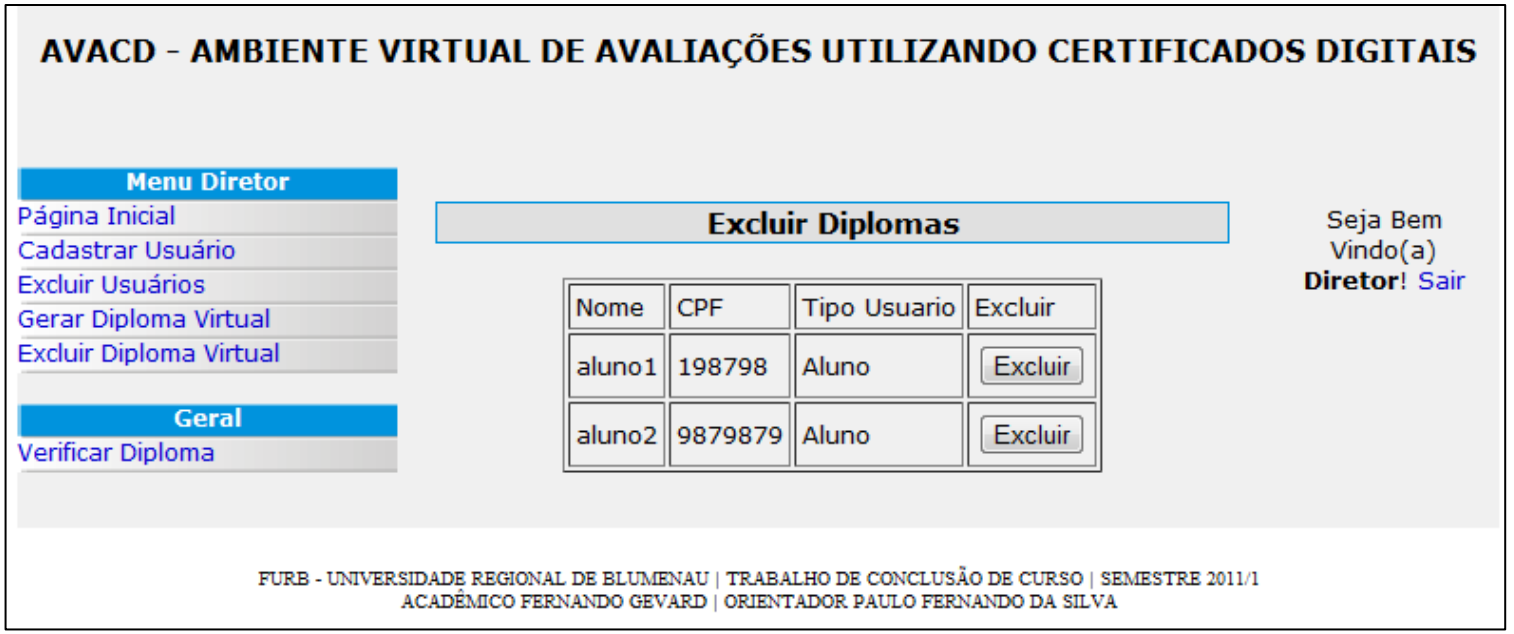
Operacionalidade das Funcionalidades Gerais

Excluir de Usuários



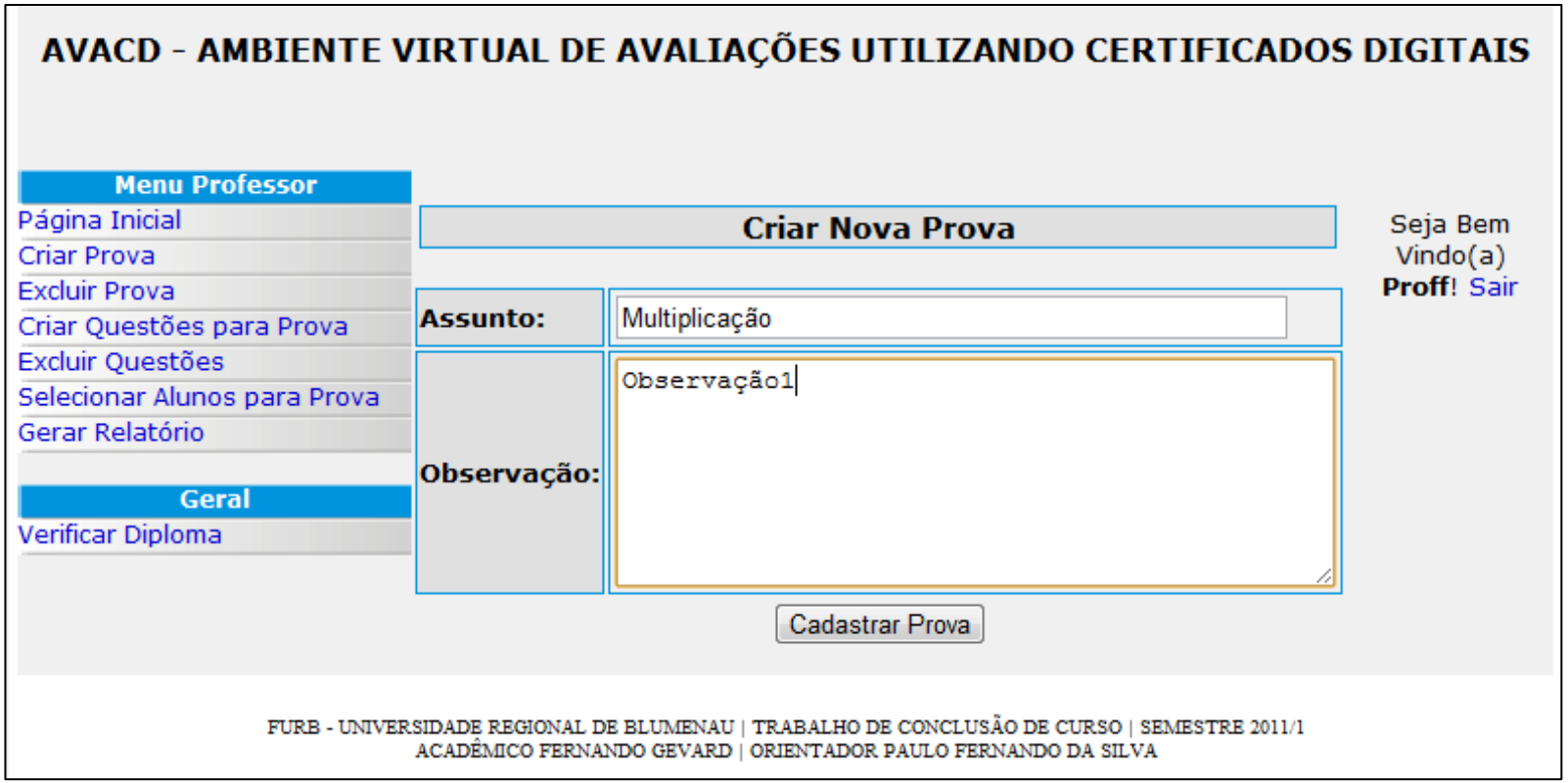
Operacionalidade das Funcionalidades Gerais

Excluir de Diplomas



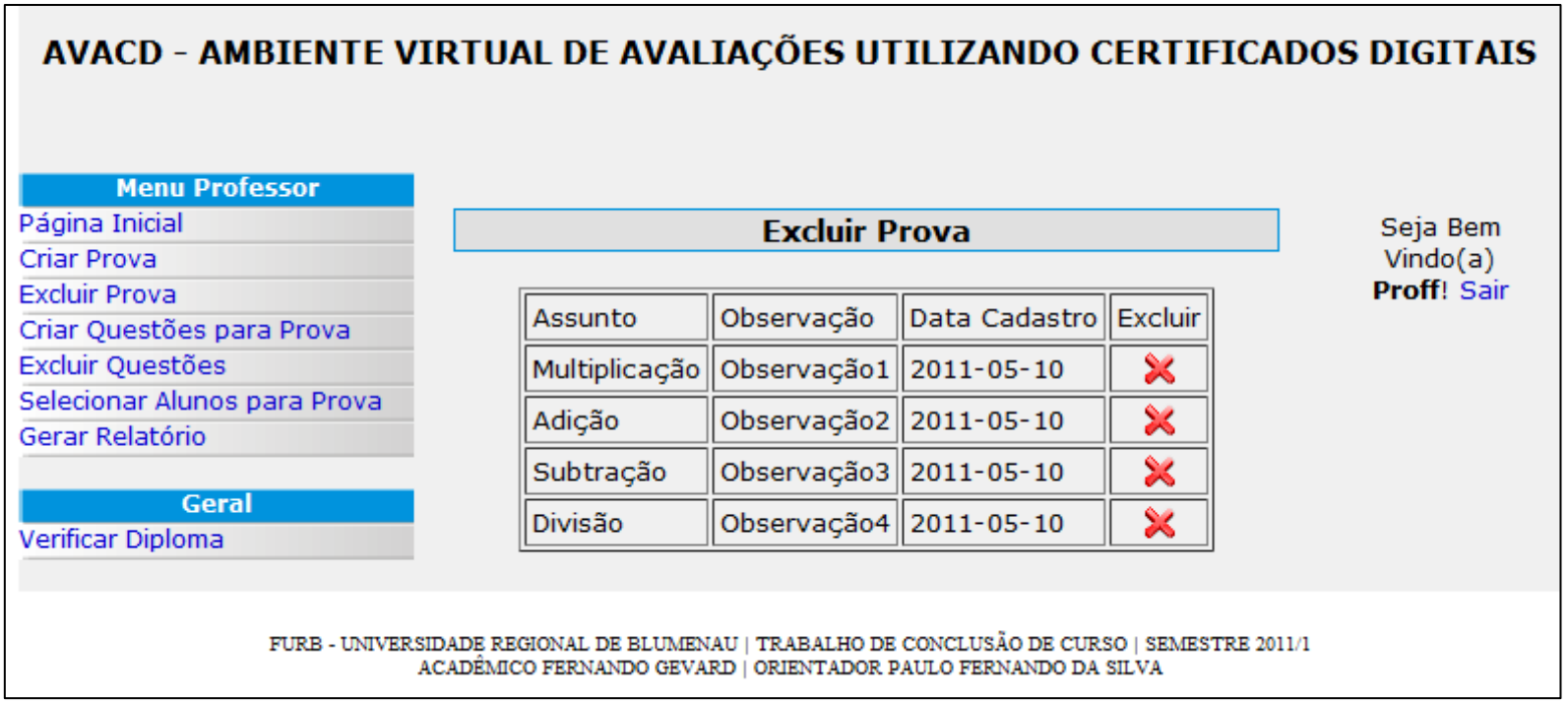
Operacionalidade das Funcionalidades Gerais

Criar Nova Prova



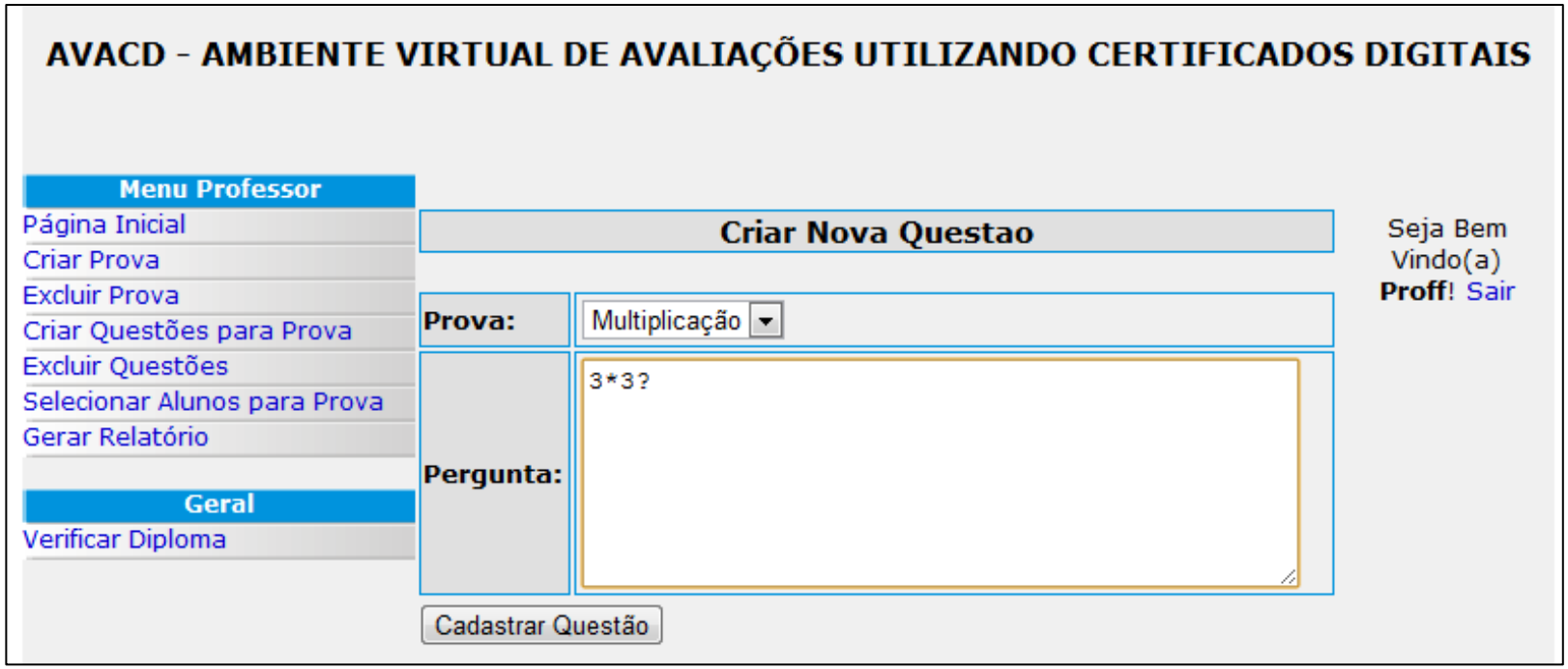
Operacionalidade das Funcionalidades Gerais

Excluir Prova



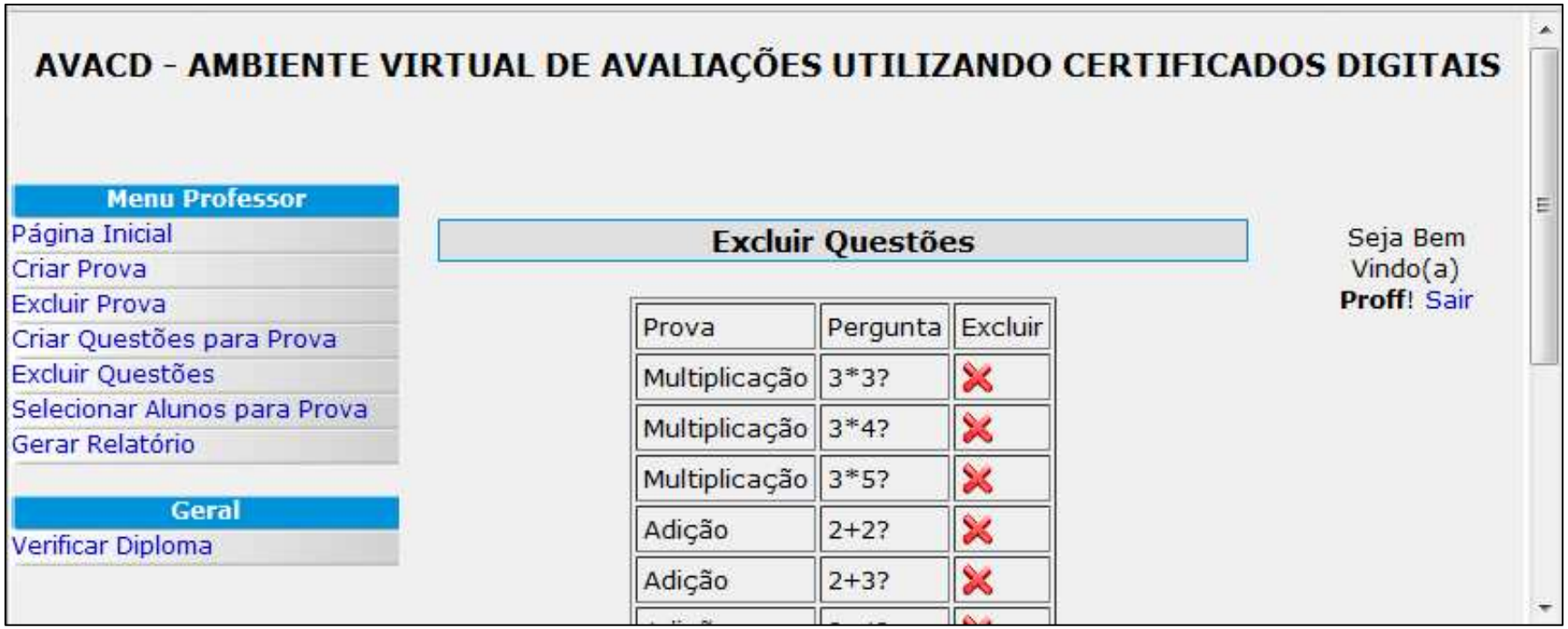
Operacionalidade das Funcionalidades Gerais

Criar Nova Questão



Operacionalidade das Funcionalidades Gerais

Excluir Questões



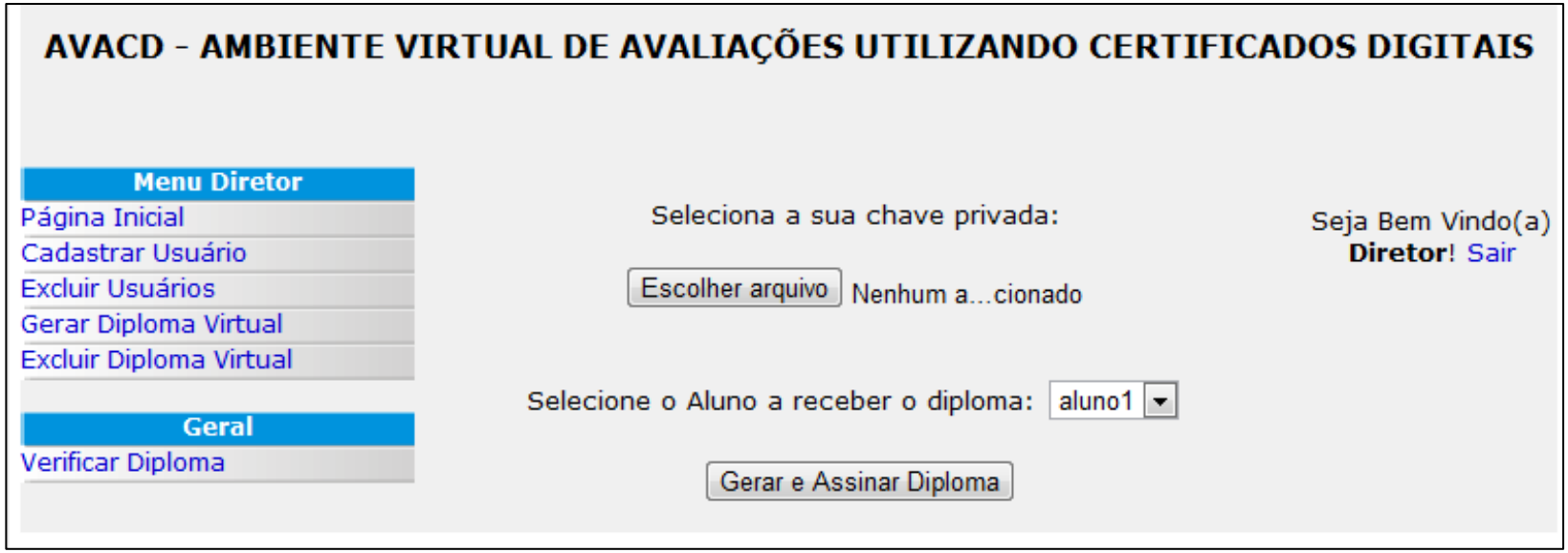
Operacionalidade das Funcionalidades Gerais

Selecionar Alunos para Prova

Operacionalidade da Assinatura Digital e Verificação

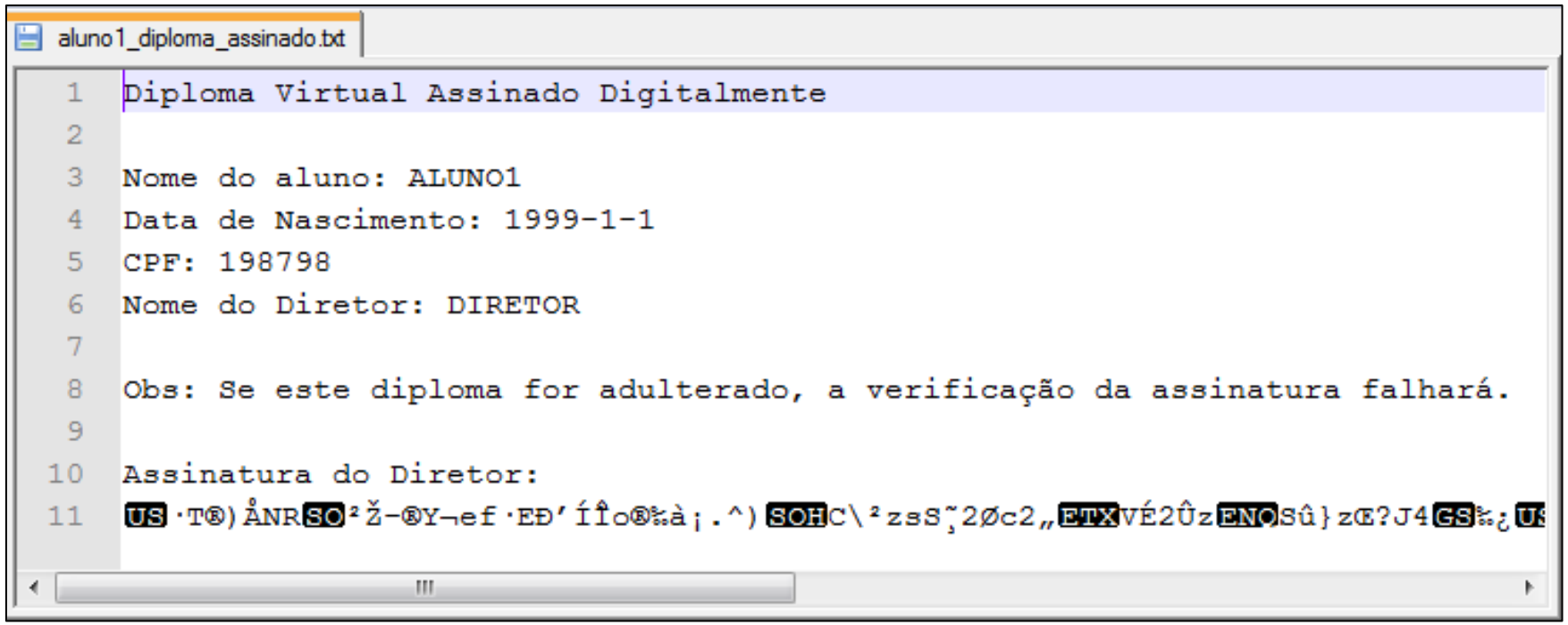
Operacionalidade da Assinatura Digital e Verificação

Gerando um Diploma



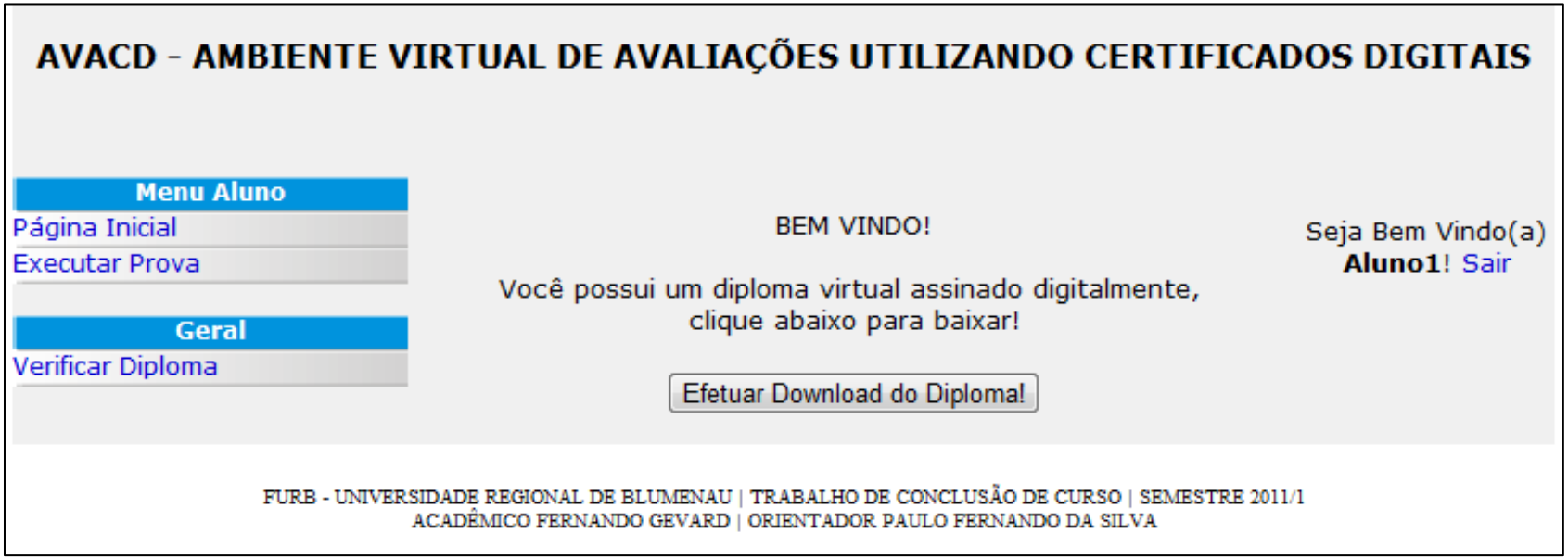
Operacionalidade da Assinatura Digital e Verificação

Diploma Gerado



Operacionalidade da Assinatura Digital e Verificação

Download do Diploma (pelo Aluno)



Operacionalidade da Assinatura Digital e Verificação

Verificação do Diploma (Autenticidade e Integridade)

Operacionalidade da Auditoria

Operacionalidade da Auditoria

Ações dos usuários geradas pelo processo de auditoria:

- Fazer autenticação
- Cadastrar usuários
- Excluir usuários
- Gerar e assinar diploma
- Excluir diploma
- Verificar diploma
- Criar prova
- Excluir prova
- Criar questões para prova
- Excluir questões
- Selecionar aluno para prova
- Excluir seleção de aluno para prova
- Gerar relatório
- Executar prova
- Efetuar o download do diploma
- Sair do sistema

FURB

Operacionalidade da Auditoria

Arquivo responsável por armazenar as trilhas de auditoria:

log.txt

```
[26/05/2011 11:07:49] - Usuario: diretor -  logado com sucesso!
[26/05/2011 11:09:03] - Usuario: diretor - cadastrou o usuário fernando com sucesso.
[26/05/2011 11:09:13] - Usuario: diretor - excluiu o usuario FERNANDO com sucesso!
[26/05/2011 11:10:26] - Usuario: diretor - gerou o diploma do aluno (aluno2) com sucesso!
[26/05/2011 11:10:29] - Usuario: diretor - excluiu o diploma do aluno aluno1 com sucesso!
[26/05/2011 11:11:02] - Usuario: diretor -  efetuou logout com sucesso!
[26/05/2011 11:11:20] - Usuario: diretor - verificou um diploma (válido) com sucesso!
[26/05/2011 11:12:06] - Usuario: proff -  logado com sucesso!
[26/05/2011 11:12:22] - Usuario: proff - criou a prova (assunto: Matemática) com sucesso!
[26/05/2011 11:12:36] - Usuario: proff - excluiu a prova (assunto: Divisão) com sucesso!
[26/05/2011 11:12:44] - Usuario: proff - criou a questão (1+1?) com sucesso!
[26/05/2011 11:12:55] - Usuario: proff - criou a questão (1+2?) com sucesso!
[26/05/2011 11:13:03] - Usuario: proff - excluiu a questao (1+2?) com sucesso!
[26/05/2011 11:13:11] - Usuario: proff - selecionou o aluno (aluno1) para realizar a prova (assunto: Matemática)
[26/05/2011 11:13:13] - Usuario: proff - selecionou o aluno (aluno2) para realizar a prova (assunto: Matemática)
[26/05/2011 11:13:17] - Usuario: proff - excluiu o aluno (aluno2) de executar a prova (assunto: Matemática)
[26/05/2011 11:13:27] - Usuario: proff -  efetuou logout com sucesso!
[26/05/2011 11:13:34] - Usuario: aluno1 -  logado com sucesso!
[26/05/2011 11:13:44] - Usuario: aluno1 - executou a prova (assunto: Matemática) com sucesso!
[26/05/2011 11:13:48] - Usuario: aluno1 -  efetuou logout com sucesso!
[26/05/2011 11:14:35] - Usuario: aluno2 -  logado com sucesso!
[26/05/2011 11:14:38] - Usuario: aluno2 - efetuou download do seu diploma virtual assinado!
[26/05/2011 11:14:40] - Usuario: aluno2 -  efetuou logout com sucesso!
[26/05/2011 11:14:49] - Usuario: proff -  logado com sucesso!
[26/05/2011 11:14:56] - Usuario: proff - gerou relatório da prova (assunto: Matemática) com sucesso!
[26/05/2011 11:15:00] - Usuario: proff -  efetuou logout com sucesso!
[26/05/2011 11:15:05] - Usuario:  - verificou um diploma (válido) com sucesso!
[26/05/2011 11:15:25] - Usuario:  - verificou um diploma (inválido) com sucesso!
```

Resultados e Discussão

Resultados e Discussão

Importantes itens para o desenvolvimento deste trabalho:

e-CPF

→ Assinar diploma

OpenSSL

→ Exportar chaves (e-CPF)

→ Gerar o certificado do servidor

→ Gerar o certificado da AC TCC

→ Gerar o certificado do Diretor

→ Converter os certificados para diversos formatos

Servidor

→ Utilizado o servidor Apache 2

FURB

Resultados e Discussão

Comparativo com os trabalhos correlatos:

Características	Possui a respectiva característica implementada?			
	Este Ambiente	**Trabalho Daney**	**Trabalho Mathias**	**AVA - FURB**
Cadastro de Usuários	Sim	Sim	Não	Sim
Níveis de permissão de acesso para cada usuário	Sim	Sim	Não	Sim
Cadastrar Provas	Sim	Sim	Não	Sim
Cadastrar Questões	Sim	Sim	Não	Sim
Gerar Relatório (Provas)	Sim	Sim	Não	Sim
Executar Provas	Sim	Não	Não	Sim
Autenticação	Sim	Sim	Não	Sim
Auditoria	Sim	Não	Não	Não
Proteção de dados do usuário (*hash*)	Sim	Não	Sim	Sim
Criptografia	Sim	Não	Sim	Não
Certificado Digital	Sim	Não	Sim	Não
Assinatura Digital	Sim	Não	Não	Não
Canais seguros (HTTPS)	Sim	Não	Não	Não

FURB

Conclusão

- Todos os objetivos foram atingidos;
- Foi implementado um ambiente virtual de avaliações utilizando certificado digital para autenticação;
- Linguagem PHP e banco de dados MySQL.

FURB

Extensões

Como extensão para o presente trabalho propõe-se:

- gerenciar várias chaves públicas de vários usuários do tipo diretor, para que mais diretores possam gerar e assinar um diploma virtual;
- permitir ao professor gerar de provas com questões já cadastradas e selecionadas de maneira aleatória pelo sistema;
- permitir ao professor informar o nível de dificuldade de cada questão cadastrada, para que seja possível gerar uma prova de acordo com o nível de dificuldade desejado;
- implementar mais tipos de questões além da questão do tipo dissertativa já existente;
- implementar um sistema de auto-correção de provas;
- implementar um quadro de notas para todos os alunos e gerar automaticamente diplomas virtuais assinados a partir da média final do aluno;
- permitir ao aluno a visualização de suas notas e médias.

FURB

Obrigado!