



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

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.

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*;

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.



Fundamentação teórica

* Assuntos principais *

Certificado Digital

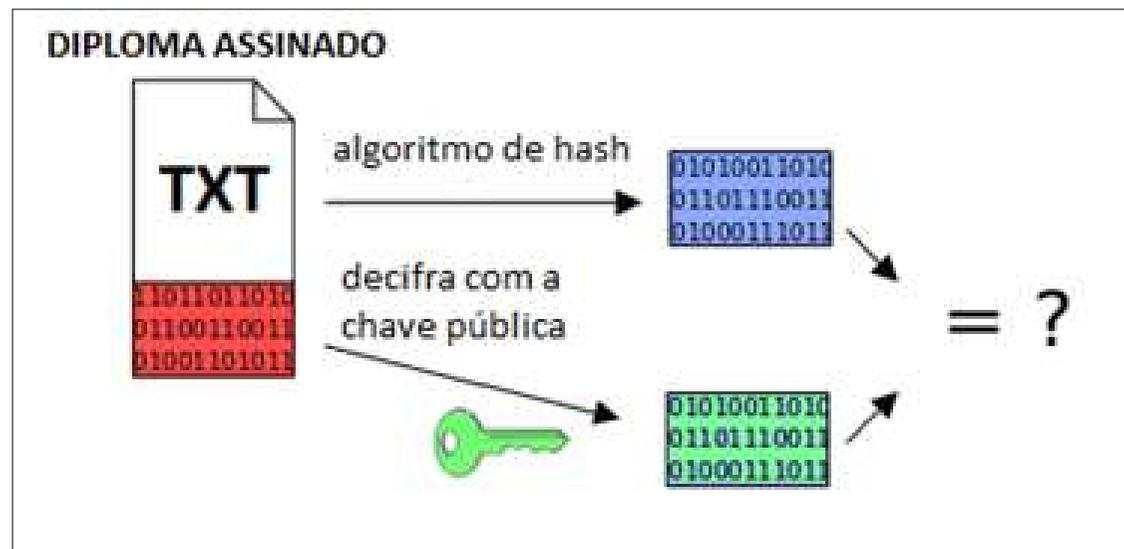
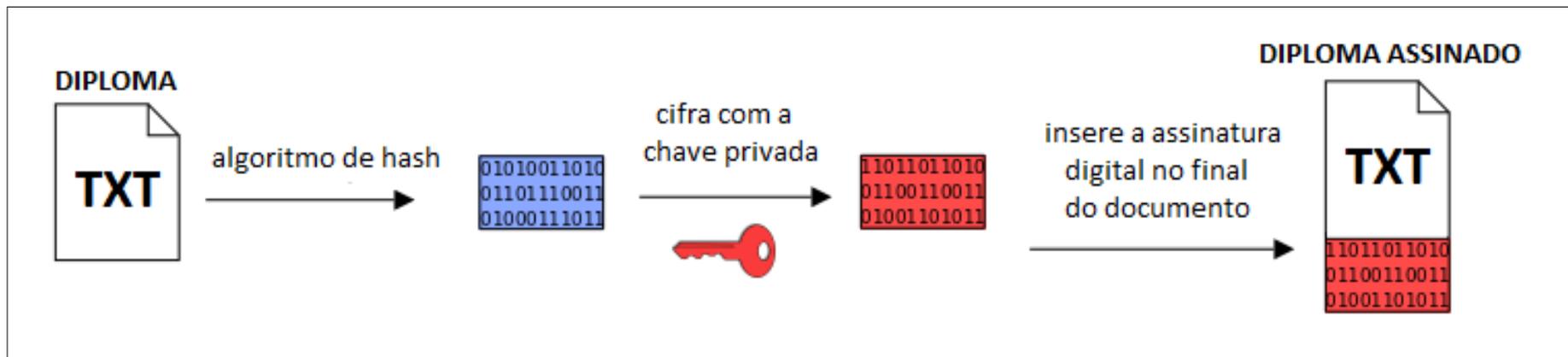
- ICP-BRASIL
 - e-CPF
- Uma Autoridade Certificadora (AC) garante a autenticidade de um Certificado Digital.
- A AC assina a chave pública (certificado) de um cliente utilizando a sua chave privada.

Certificado Digital

- Formato de um Certificado Digital:

VERSÃO
NÚMERO SERIAL
ALGORITMO ASSINATURA
EMISSOR
VALIDADE
SUJEITO
INFO CHAVE PÚBLICA SUJEITO
<i>ASSINATURA</i>

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).



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.

Diagrama de casos de uso

- Diagrama de casos de uso executados pelo diretor.

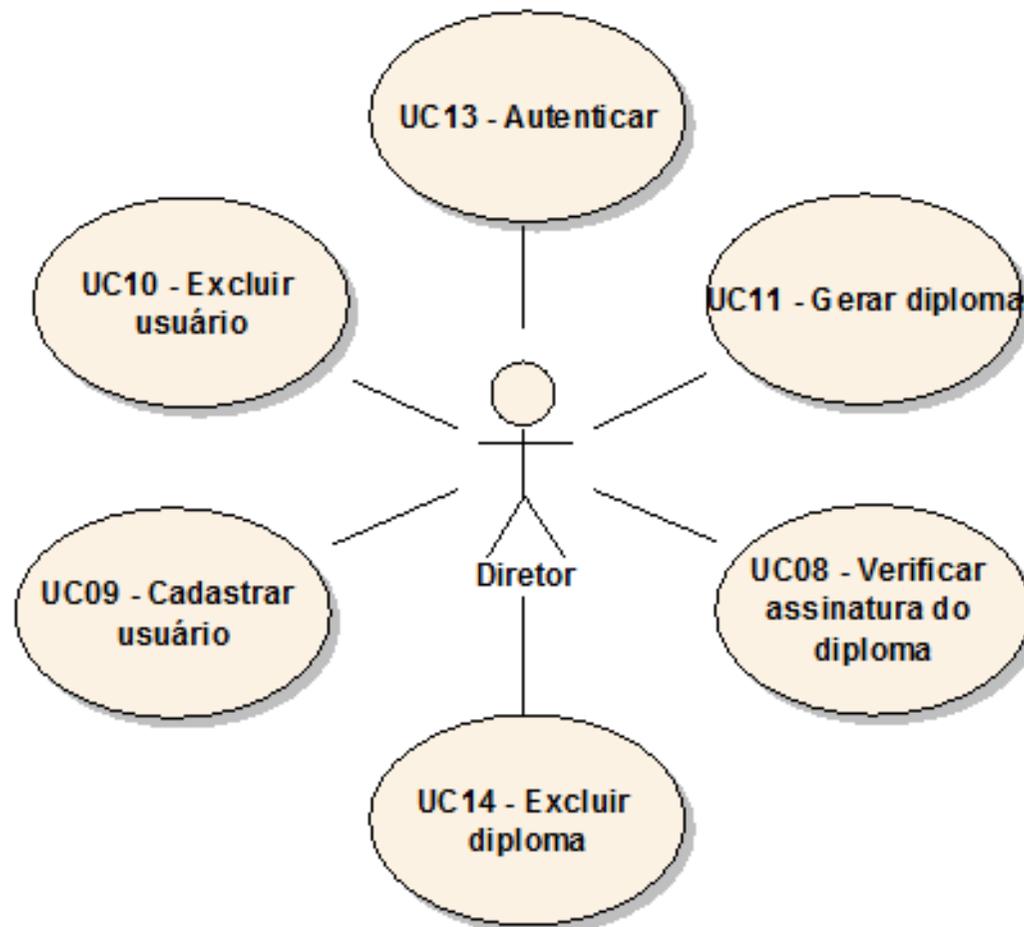


Diagrama de casos de uso

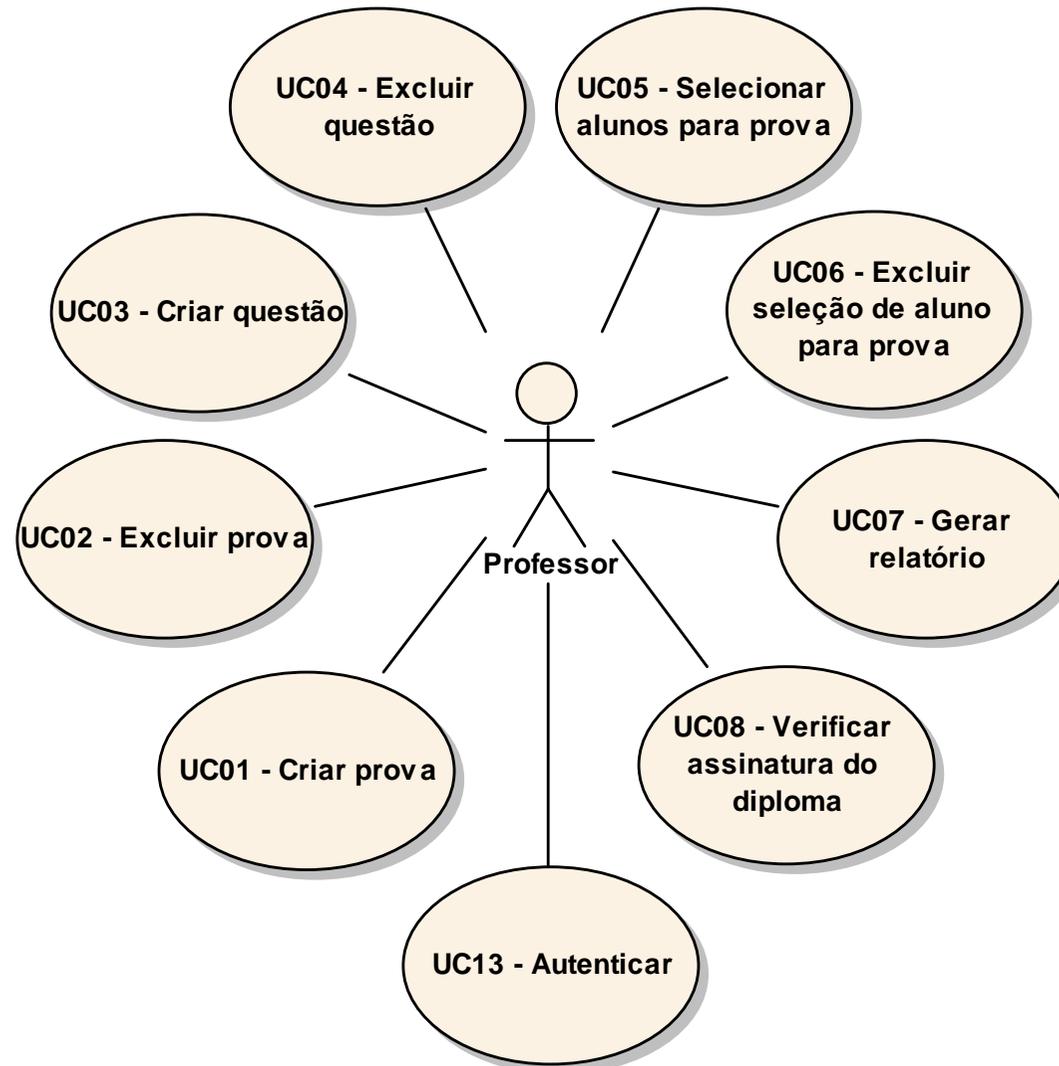


Diagrama de casos de uso

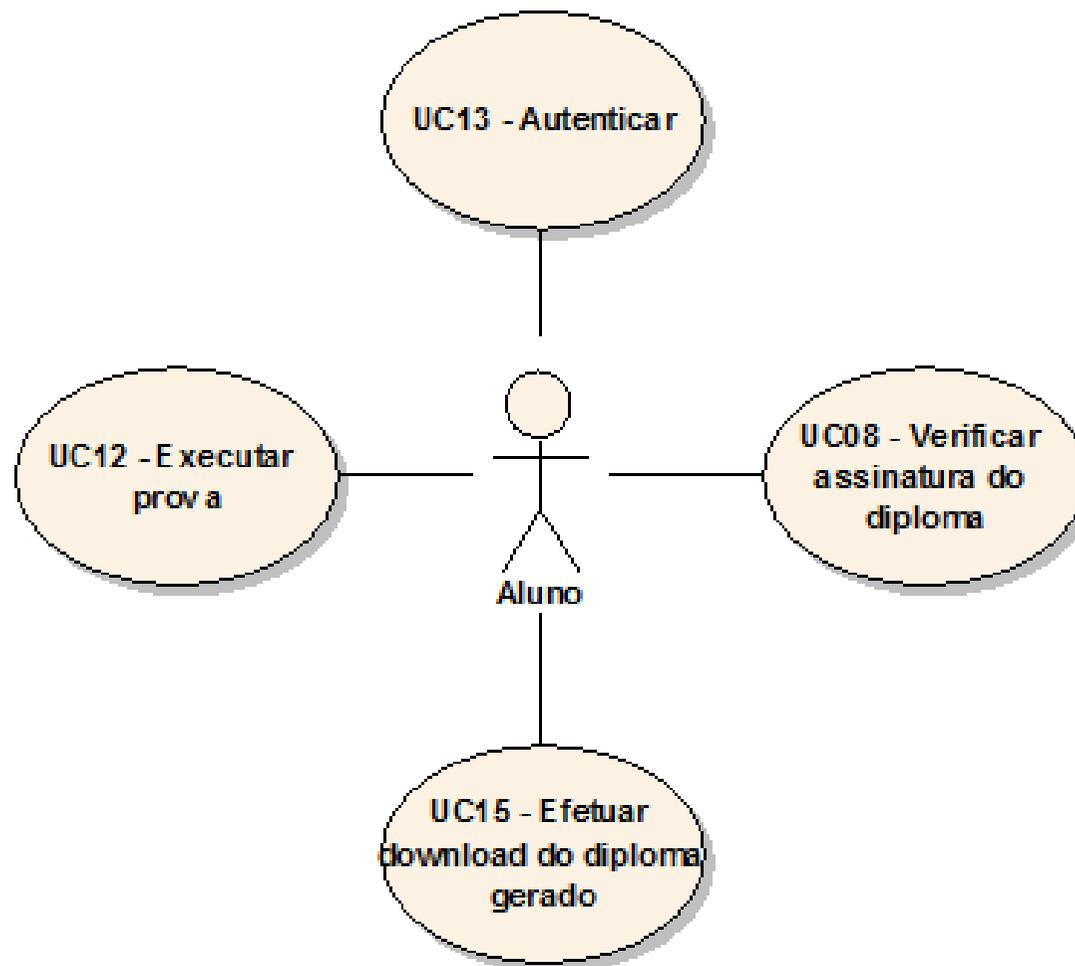


Diagrama de casos de uso

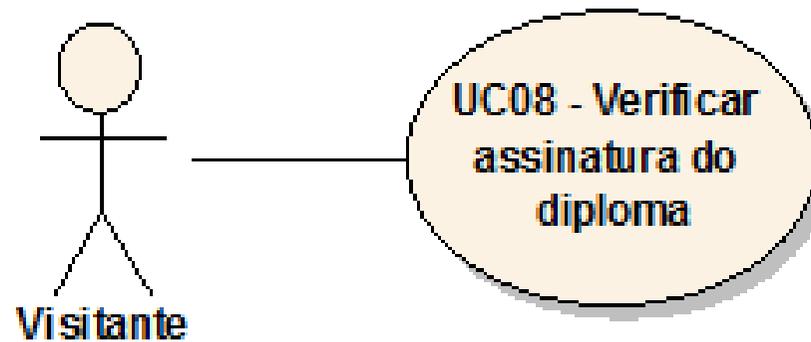


Diagrama de Classes

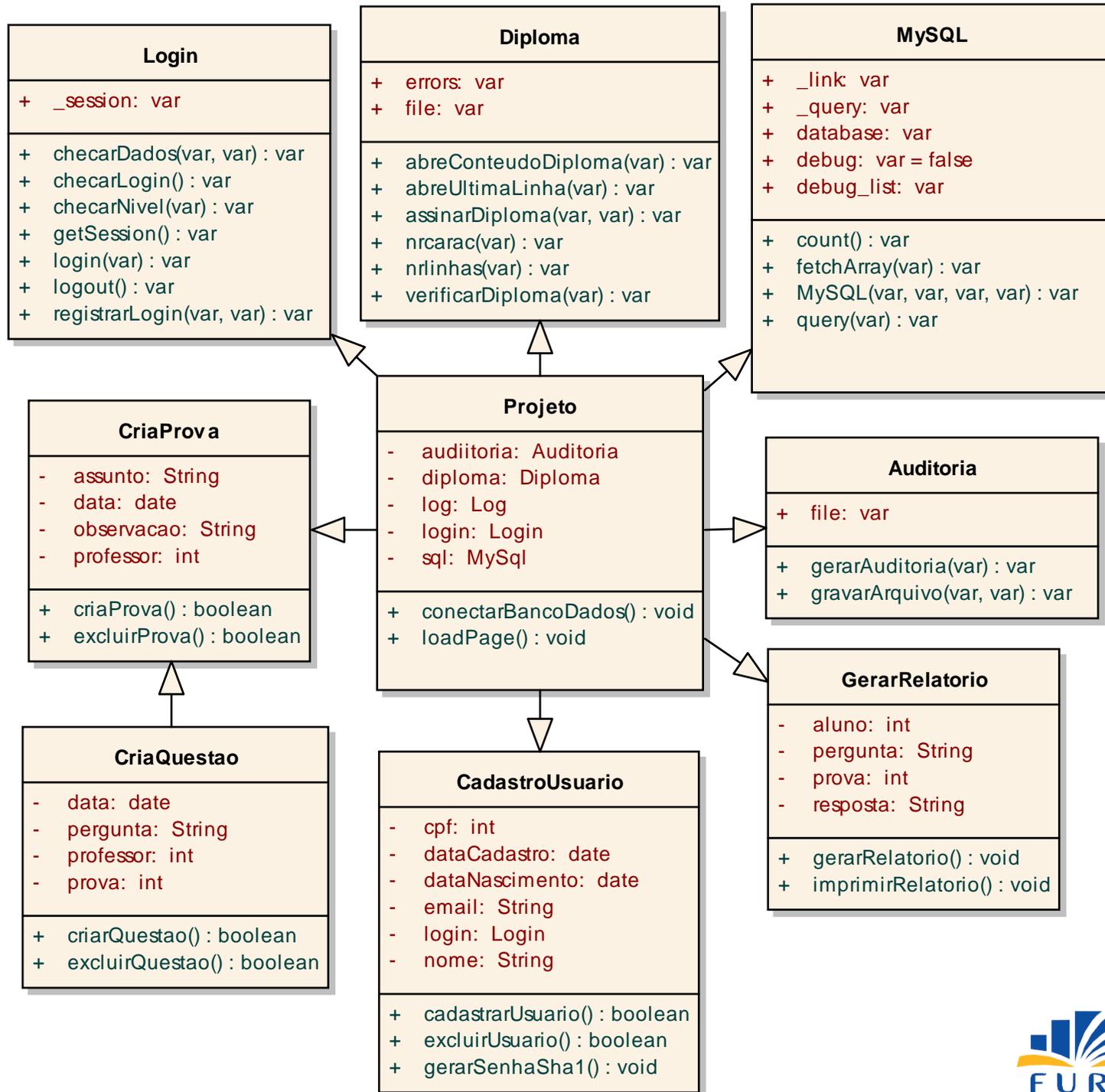
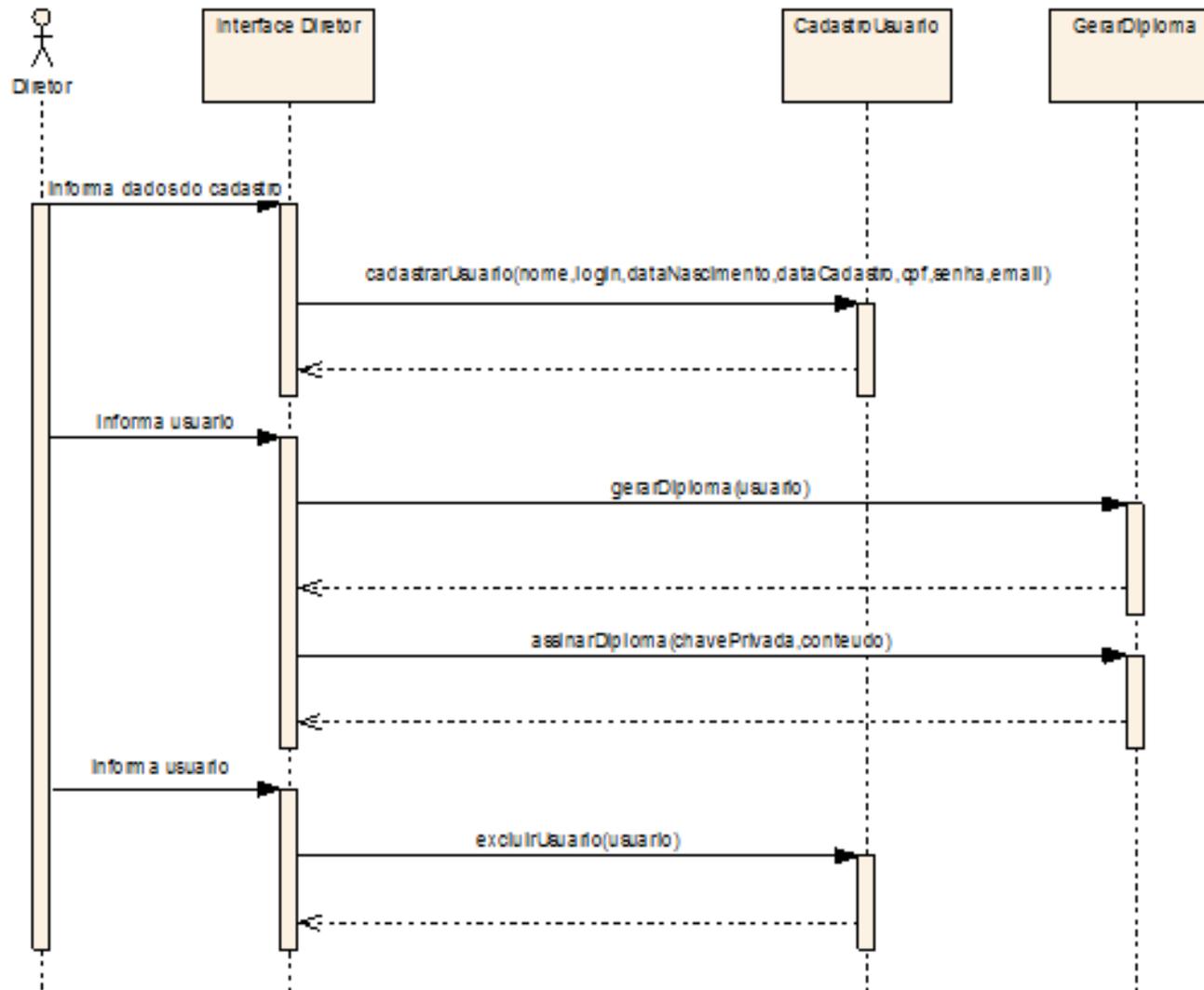


Diagrama de Seqüência





Implementação

Tecnologias e ferramentas utilizadas

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



Operacionalidade



Operacionalidade do Certificado Digital

Operacionalidade do Certificado Digital

Certificado Digital do Servidor (auto assinado)



Informações sobre o Certificado

Este certificado destina-se ao(s) seguinte(s) fim(ns):

- Todas as configurações de emissão
- Todas as diretivas de aplicativo

Emitido para: 127.0.0.1

Emitido por: 127.0.0.1

Válido a partir de 06/ 05/ 2011 **até** 03/ 05/ 2021

Operacionalidade do Certificado Digital

Detalhes do Certificado Digital do Servidor (auto assinado)

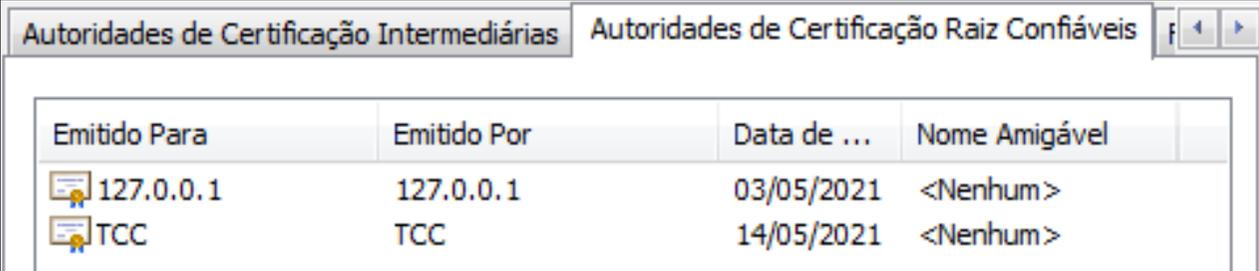
The screenshot shows a web browser window with the address bar displaying `https://127.0.0.1/ambiente_seguro/index.php?pg=verificar`. A security warning dialog box is open, providing details about the self-signed certificate. The dialog box contains the following information:

- 127.0.0.1**: A identidade deste site foi confirmada por 127.0.0.1. [Informações do certificado](#)
- 256 bits**: Sua conexão com 127.0.0.1 tem uma criptografia de 256 bits. A conexão usa a TLS 1.0. A conexão foi criptografada utilizando AES_256_CBC, com SHA1 para mensagem de autenticação e DHE_RSA como o mecanismo de troca de chaves. A conexão está compactada com DEFLATE. O servidor não é compatível com a extensão de renegociação TLS.
- Informações do site**: Você visitou este site pela primeira vez em 23/05/2011. [O que significam?](#)

The background page is titled "OPÇÕES UTILIZANDO CERTIFICADOS DIGITAIS" and includes a login form with fields for "Usuário:" and "Senha:", a "Login" button, and an "Autenticar (Certificado)" button. The footer of the page reads "TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1" and "ORIENTADOR PAULO FERNANDO DA SILVA".

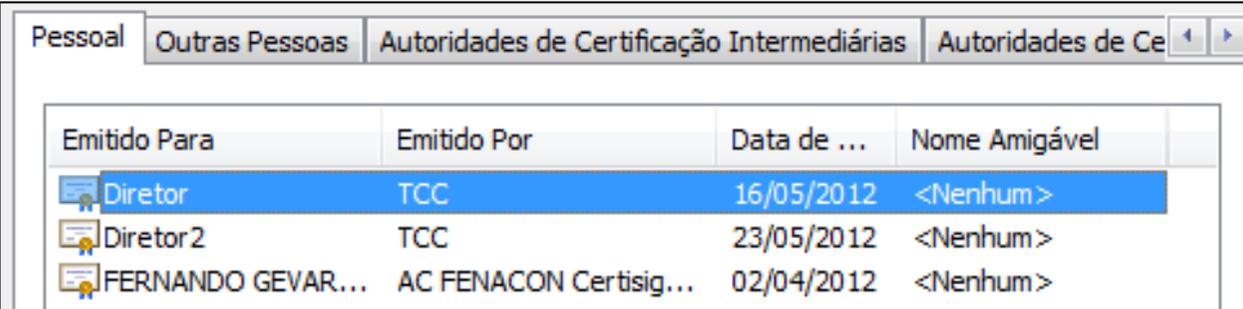
Operacionalidade do Certificado Digital

Repositório de autoridades de certificação raiz confiáveis



Emitido Para	Emitido Por	Data de ...	Nome Amigável
127.0.0.1	127.0.0.1	03/05/2021	<Nenhum>
TCC	TCC	14/05/2021	<Nenhum>

Repositório pessoal de certificados



Emitido Para	Emitido Por	Data de ...	Nome Amigável
Diretor	TCC	16/05/2012	<Nenhum>
Diretor2	TCC	23/05/2012	<Nenhum>
FERNANDO GEVAR...	AC FENACON Certisig...	02/04/2012	<Nenhum>

Operacionalidade do Certificado Digital

Opções de instalação do certificado do diretor



Assistente para Importação de Certificados

Senha

Para manter a segurança, a chave privada foi protegida com uma senha.

Digite a senha da chave privada.

Senha:

Ativar proteção de chaves privadas fortes. Se ativar esta opção, você será avisado todas as vezes que uma chave privada for usada por um aplicativo.

Marcar esta chave como exportável. Isso possibilitará o backup e o transporte das chaves posteriormente.

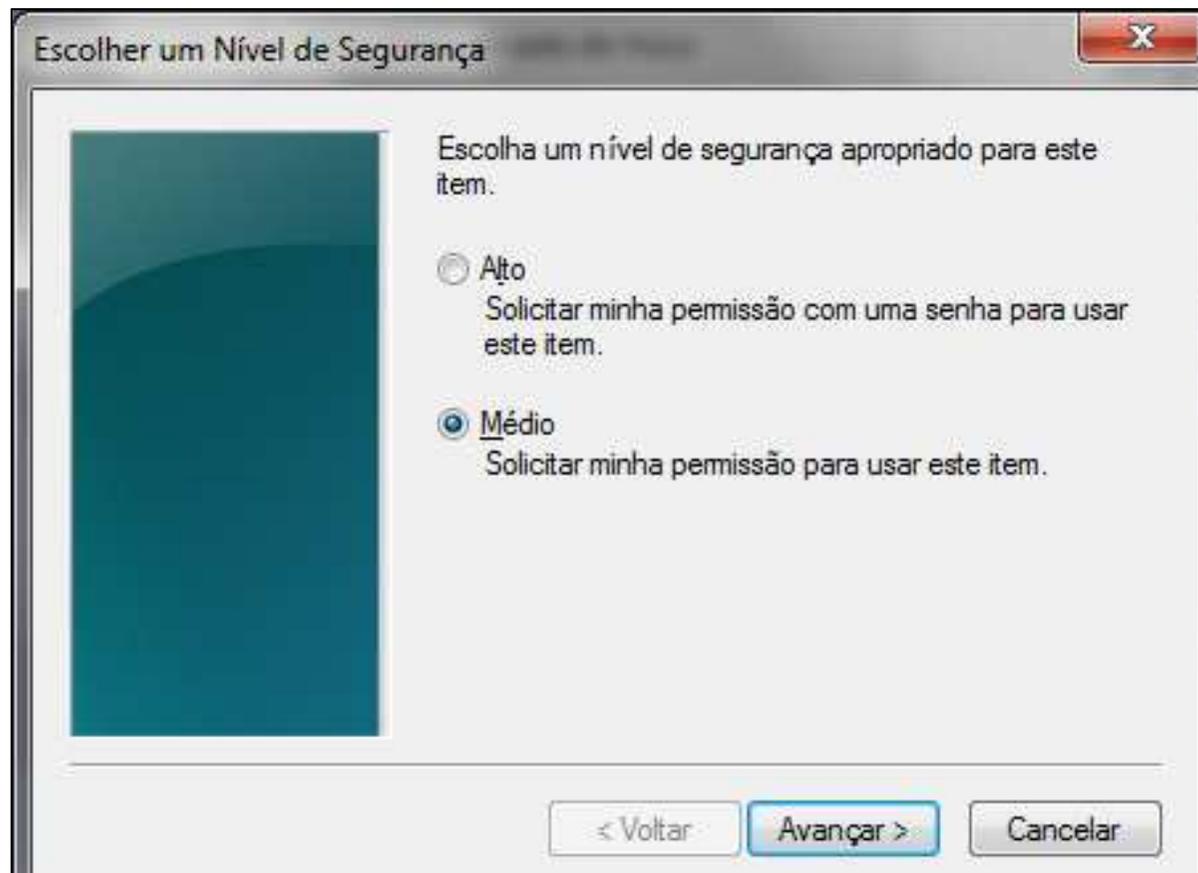
Incluir todas as propriedades estendidas.

Saiba mais sobre [como proteger chaves privadas](#)

< Voltar Avançar > Cancelar

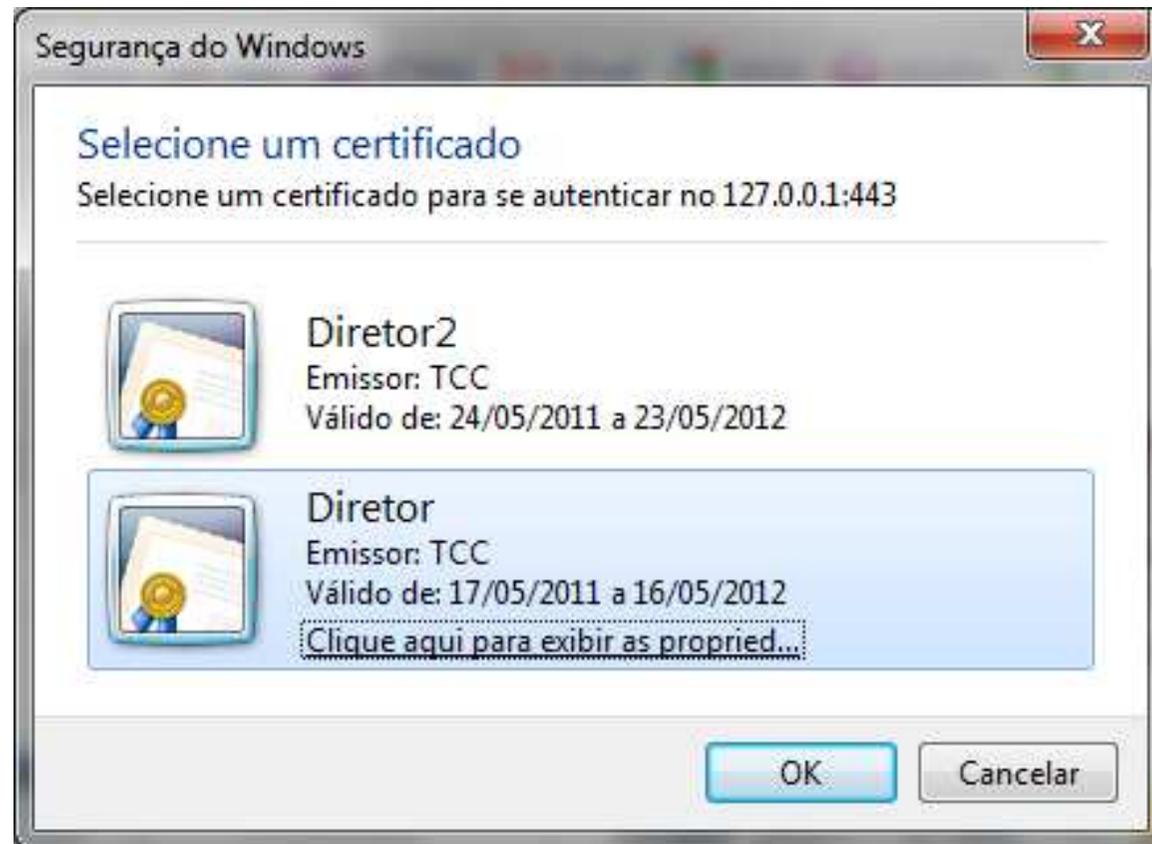
Operacionalidade do Certificado Digital

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

Operacionalidade das Funcionalidades Gerais

Cadastro de Usuários

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Diretor	Cadastrar Usuário	Seja Bem Vindo(a) Diretor! Sair
Página Inicial	Nome Completo: <input type="text" value="PROF"/>	
Cadastrar Usuário	Data de Nascimento: <input type="text" value="10"/> / <input type="text" value="09"/> / <input type="text" value="1988"/>	
Excluir Usuários	CPF: <input type="text" value="4294967295"/>	
Gerar Diploma Virtual	Sexo: <input checked="" type="radio"/> Masculino <input type="radio"/> Feminino	
Excluir Diploma Virtual	E-mail: <input type="text" value="prof@gmail.com"/>	
Geral	Tipo/Nível do Usuário: <input type="radio"/> Aluno <input checked="" type="radio"/> Professor	
Verificar Diploma	Usuário: <input type="text" value="proff"/> (5 a 12 caracteres)	
	Senha: <input type="password" value="....."/> (4 a 12 caracteres)	
	Confirmar Senha: <input type="password" value="....."/> (4 a 12 caracteres)	
	Lembrete de Senha: <input type="text"/>	
	<input type="button" value="Cadastrar Usuário"/>	

Operacionalidade das Funcionalidades Gerais

Excluir de Usuários

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Diretor

- Página Inicial
- Cadastrar Usuário
- Excluir Usuários
- Gerar Diploma Virtual
- Excluir Diploma Virtual

Geral

- Verificar Diploma

Excluir Usuários

Nome	CPF	Tipo Usuario	Excluir
PROF	4294967295	Professor	X
ALUNO1	198798	Aluno	X
ALUNO2	9879879	Aluno	X
ANDREY	9879897	Aluno	X

Seja Bem Vindo(a)
Diretor! [Sair](#)

FURB - UNIVERSIDADE REGIONAL DE BLUMENAU | TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1
ACADÊMICO FERNANDO GEVARD | ORIENTADOR PAULO FERNANDO DA SILVA

Operacionalidade das Funcionalidades Gerais

Excluir de Diplomas

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Diretor

- [Página Inicial](#)
- [Cadastrar Usuário](#)
- [Excluir Usuários](#)
- [Gerar Diploma Virtual](#)
- [Excluir Diploma Virtual](#)

Geral

- [Verificar Diploma](#)

Excluir Diplomas

Nome	CPF	Tipo Usuario	Excluir
aluno1	198798	Aluno	<input type="button" value="Excluir"/>
aluno2	9879879	Aluno	<input type="button" value="Excluir"/>

Seja Bem Vindo(a)
Diretor! [Sair](#)

FURB - UNIVERSIDADE REGIONAL DE BLUMENAU | TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1
ACADÊMICO FERNANDO GEVARD | ORIENTADOR PAULO FERNANDO DA SILVA

Operacionalidade das Funcionalidades Gerais

Criar Nova Prova

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Professor	Criar Nova Prova	Seja Bem Vindo(a) Proff! Sair
Página Inicial	Assunto: <input type="text" value="Multiplicação"/>	
Criar Prova	Observação: <input type="text" value="Observação1"/>	
Excluir Prova		
Criar Questões para Prova		
Excluir Questões		
Selecionar Alunos para Prova		
Gerar Relatório		
Geral		
Verificar Diploma	<input type="button" value="Cadastrar Prova"/>	

FURB - UNIVERSIDADE REGIONAL DE BLUMENAU | TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1
ACADÊMICO FERNANDO GEVARD | ORIENTADOR PAULO FERNANDO DA SILVA

Operacionalidade das Funcionalidades Gerais

Excluir Prova

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Professor

- Página Inicial
- Criar Prova
- Excluir Prova
- Criar Questões para Prova
- Excluir Questões
- Selecionar Alunos para Prova
- Gerar Relatório

Geral

- Verificar Diploma

Excluir Prova

Assunto	Observação	Data Cadastro	Excluir
Multiplicação	Observação1	2011-05-10	X
Adição	Observação2	2011-05-10	X
Subtração	Observação3	2011-05-10	X
Divisão	Observação4	2011-05-10	X

Seja Bem Vindo(a)
Proff! Sair

FURB - UNIVERSIDADE REGIONAL DE BLUMENAU | TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1
ACADÊMICO FERNANDO GEVARD | ORIENTADOR PAULO FERNANDO DA SILVA

Operacionalidade das Funcionalidades Gerais

Criar Nova Questão

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Professor	Criar Nova Questao		Seja Bem Vindo(a) Proff! Sair
Página Inicial	Prova:	<input type="text" value="Multiplicação"/>	
Criar Prova	Pergunta:	<input type="text" value="3*3?"/>	
Excluir Prova			
Criar Questões para Prova			
Excluir Questões			
Selecionar Alunos para Prova			
Gerar Relatório			
Geral			
Verificar Diploma			
	<input type="button" value="Cadastrar Questão"/>		

Operacionalidade das Funcionalidades Gerais

Excluir Questões

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Professor

- Página Inicial
- Criar Prova
- Excluir Prova
- Criar Questões para Prova
- Excluir Questões
- Selecionar Alunos para Prova
- Gerar Relatório

Geral

- Verificar Diploma

Excluir Questões

Prova	Pergunta	Excluir
Multiplicação	3*3?	<input checked="" type="checkbox"/>
Multiplicação	3*4?	<input checked="" type="checkbox"/>
Multiplicação	3*5?	<input checked="" type="checkbox"/>
Adição	2+2?	<input checked="" type="checkbox"/>
Adição	2+3?	<input checked="" type="checkbox"/>

Seja Bem Vindo(a)
Proff! Sair

Operacionalidade das Funcionalidades Gerais

Selecionar Alunos para Prova

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Professor

- Página Inicial
- Criar Prova
- Excluir Prova
- Criar Questões para Prova
- Excluir Questões
- Selecionar Alunos para Prova
- Gerar Relatório

Seja Bem Vindo(a) Proff! Sair

Selecionar Aluno para Prova

Prova: Multiplicação ▾

Aluno: aluno1 ▾

Selecionar Aluno

Geral

Verificar Diploma

Alunos cadastrados

Prova	Aluno	Respondida?	Excluir
Adição	aluno2	Não	✘
Adição	aluno1	Sim	
Divisão	aluno2	Não	✘
Divisão	aluno3	Não	✘
Divisão	aluno1	Sim	
Multiplicação	aluno2	Não	✘
Multiplicação	aluno1	Sim	



Operacionalidade da Assinatura Digital e Verificação

Operacionalidade da Assinatura Digital e Verificação

Gerando um Diploma

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Menu Diretor	Selecione a sua chave privada:	Seja Bem Vindo(a) Diretor! Sair
Página Inicial	<input type="button" value="Escolher arquivo"/> Nenhum a...cionado	
Cadastrar Usuário		
Excluir Usuários		
Gerar Diploma Virtual		
Excluir Diploma Virtual		
	Selecione o Aluno a receber o diploma: <input type="text" value="aluno1"/>	
Geral	<input type="button" value="Gerar e Assinar Diploma"/>	
Verificar Diploma		

Operacionalidade da Assinatura Digital e Verificação

Diploma Gerado

```
aluno1_diploma_assinado.txt
1 Diploma Virtual Assinado Digitalmente
2
3 Nome do aluno: ALUNO1
4 Data de Nascimento: 1999-1-1
5 CPF: 198798
6 Nome do Diretor: DIRETOR
7
8 Obs: Se este diploma for adulterado, a verificação da assinatura falhará.
9
10 Assinatura do Diretor:
11 US·T@)ÅNRSO²Ž-@Y-ef·ED'Íf@%à;.^)SOHC\²zS,2Øc2,,ETXVÉ2ÛzENOSû}zE?J4GS%:;US
```

Operacionalidade da Assinatura Digital e Verificação

Download do Diploma (pelo Aluno)

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

<p>Menu Aluno</p> <p>Página Inicial</p> <p>Executar Prova</p>	<p>BEM VINDO!</p> <p>Você possui um diploma virtual assinado digitalmente, clique abaixo para baixar!</p> <p>Efetuar Download do Diploma!</p>	<p>Seja Bem Vindo(a) Aluno1! Sair</p>
<p>Geral</p> <p>Verificar Diploma</p>		

FURB - UNIVERSIDADE REGIONAL DE BLUMENAU | TRABALHO DE CONCLUSÃO DE CURSO | SEMESTRE 2011/1
ACADÊMICO FERNANDO GEVARD | ORIENTADOR PAULO FERNANDO DA SILVA

Operacionalidade da Assinatura Digital e Verificação

Verificação do Diploma (Autenticidade e Integridade)

AVACD - AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Geral
Verificar Diploma

Selecione o diploma que deseja verificar:

Nenhum a...cionado

Usuário:

Senha:

Para autenticar-se com um certificado digital, clique no botão abaixo:



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

Operacionalidade da Auditoria

Arquivo responsável por armazenar as trilhas de auditoria:

```
log.txt
1 [26/05/2011 11:07:49] - Usuario: diretor - logado com sucesso!
2 [26/05/2011 11:09:03] - Usuario: diretor - cadastrou o usuário fernando com sucesso.
3 [26/05/2011 11:09:13] - Usuario: diretor - excluiu o usuario FERNANDO com sucesso!
4 [26/05/2011 11:10:26] - Usuario: diretor - gerou o diploma do aluno (aluno2) com sucesso!
5 [26/05/2011 11:10:29] - Usuario: diretor - excluiu o diploma do aluno aluno1 com sucesso!
6 [26/05/2011 11:11:02] - Usuario: diretor - efetuou logout com sucesso!
7 [26/05/2011 11:11:20] - Usuario: diretor - verificou um diploma (válido) com sucesso!
8 [26/05/2011 11:12:06] - Usuario: proff - logado com sucesso!
9 [26/05/2011 11:12:22] - Usuario: proff - criou a prova (assunto: Matemática) com sucesso!
10 [26/05/2011 11:12:36] - Usuario: proff - excluiu a prova (assunto: Divisão) com sucesso!
11 [26/05/2011 11:12:44] - Usuario: proff - criou a questão (1+1?) com sucesso!
12 [26/05/2011 11:12:55] - Usuario: proff - criou a questão (1+2?) com sucesso!
13 [26/05/2011 11:13:03] - Usuario: proff - excluiu a questao (1+2?) com sucesso!
14 [26/05/2011 11:13:11] - Usuario: proff - selecionou o aluno (aluno1) para realizar a prova (assunto: Matemática)
15 [26/05/2011 11:13:13] - Usuario: proff - selecionou o aluno (aluno2) para realizar a prova (assunto: Matemática)
16 [26/05/2011 11:13:17] - Usuario: proff - excluiu o aluno (aluno2) de executar a prova (assunto: Matemática)
17 [26/05/2011 11:13:27] - Usuario: proff - efetuou logout com sucesso!
18 [26/05/2011 11:13:34] - Usuario: aluno1 - logado com sucesso!
19 [26/05/2011 11:13:44] - Usuario: aluno1 - executou a prova (assunto: Matemática) com sucesso!
20 [26/05/2011 11:13:48] - Usuario: aluno1 - efetuou logout com sucesso!
21 [26/05/2011 11:14:35] - Usuario: aluno2 - logado com sucesso!
22 [26/05/2011 11:14:38] - Usuario: aluno2 - efetuou download do seu diploma virtual assinado!
23 [26/05/2011 11:14:40] - Usuario: aluno2 - efetuou logout com sucesso!
24 [26/05/2011 11:14:49] - Usuario: proff - logado com sucesso!
25 [26/05/2011 11:14:56] - Usuario: proff - gerou relatório da prova (assunto: Matemática) com sucesso!
26 [26/05/2011 11:15:00] - Usuario: proff - efetuou logout com sucesso!
27 [26/05/2011 11:15:05] - Usuario: - verificou um diploma (válido) com sucesso!
28 [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

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 (<i>hash</i>)	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

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.

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.



Obrigado!