Projeto ICP da Escola Técnica da UFRGS



Prof. Marcelo Augusto Rauh Schmitt

Objetivos

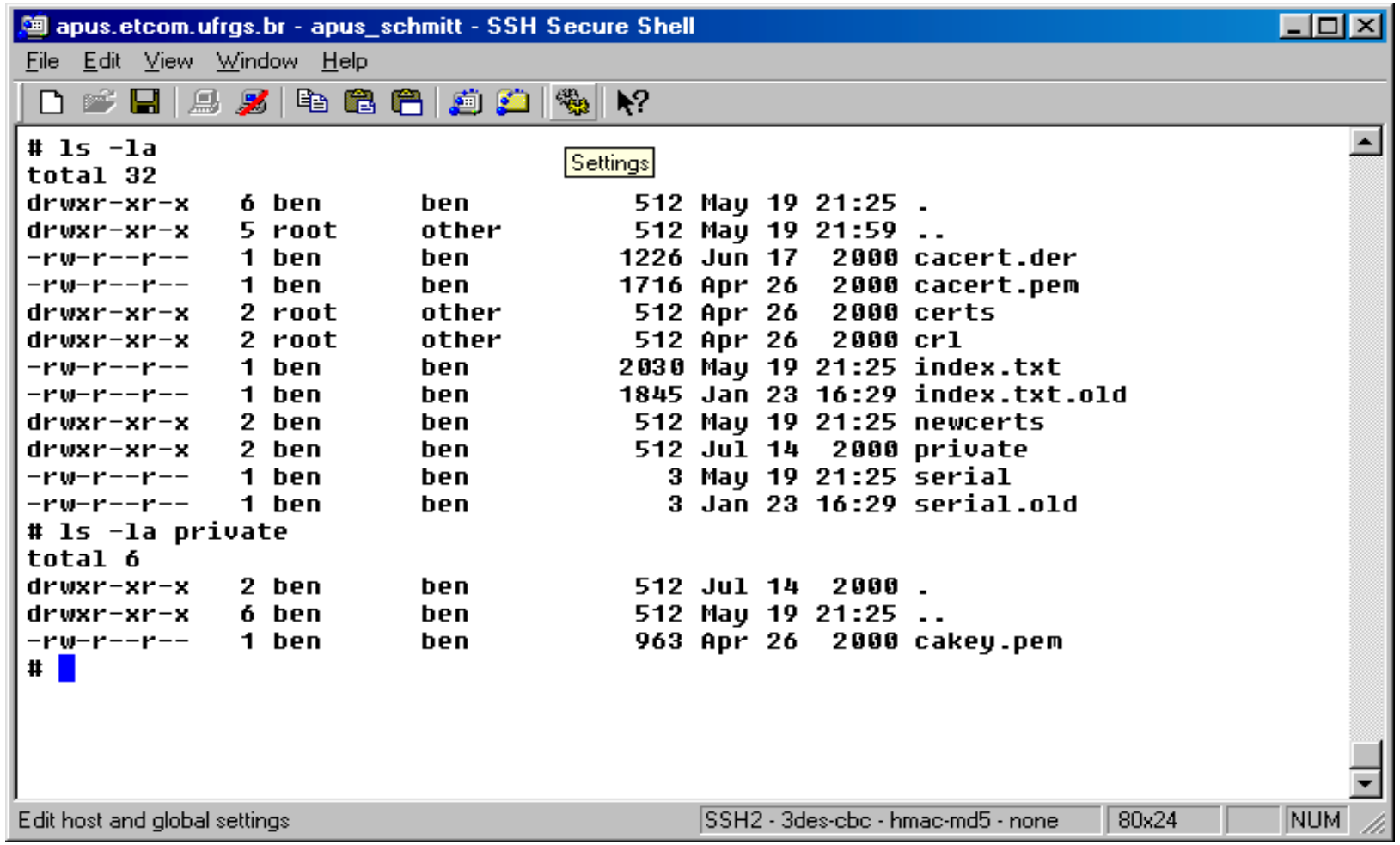
- Capacitar a Escola Técnica da UFRGS a ser uma autoridade certificadora (CA).

- Emitir certificados digitais
  - autenticação e criptografia
  - páginas e mensagens eletrônicas
  - escola e outras unidades da UFRGS

- Distribuir os programas desenvolvidos para entidades que desejem criar a sua própria estrutura.

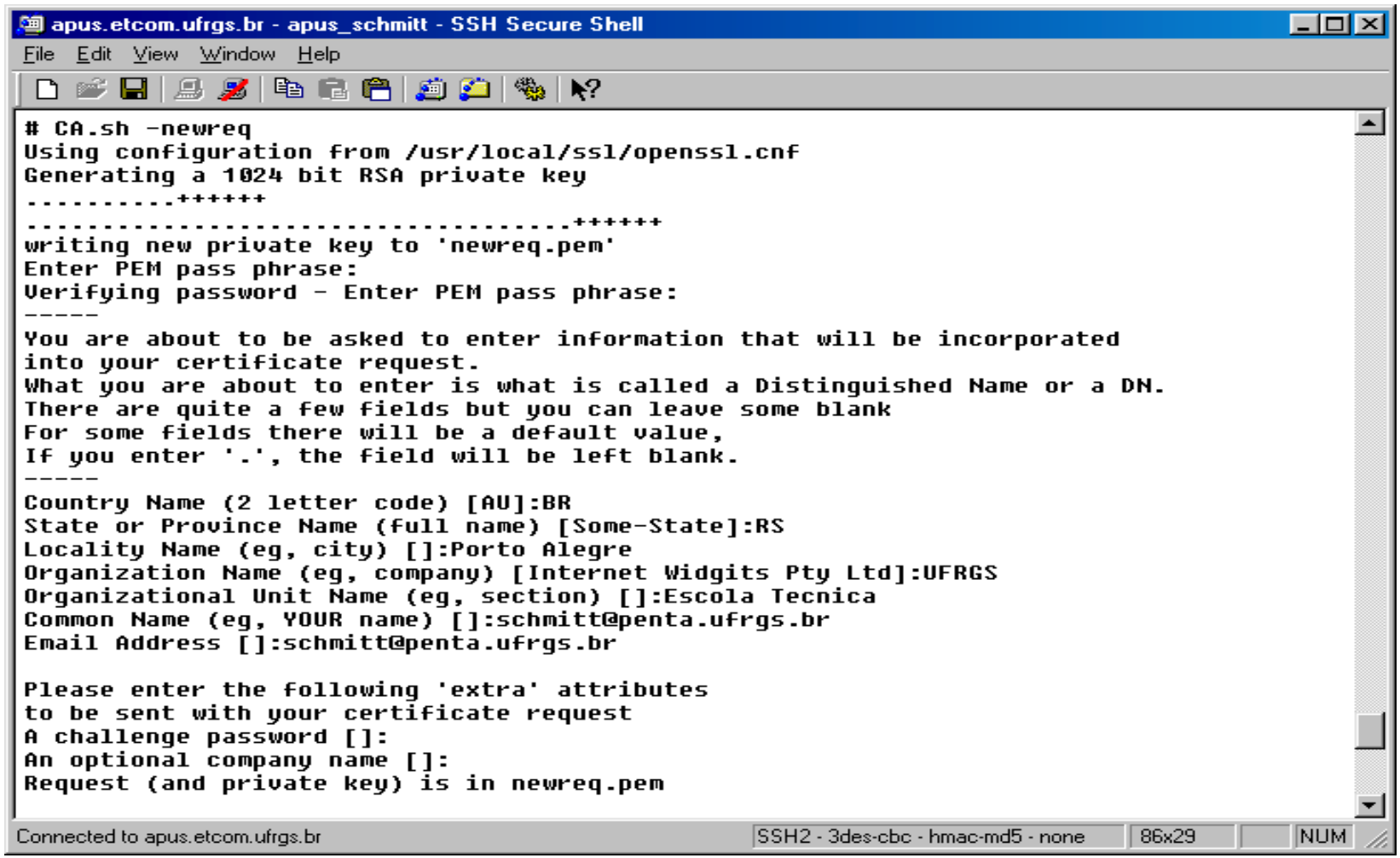
Trabalho inicial - OpenSSL

Arquivos



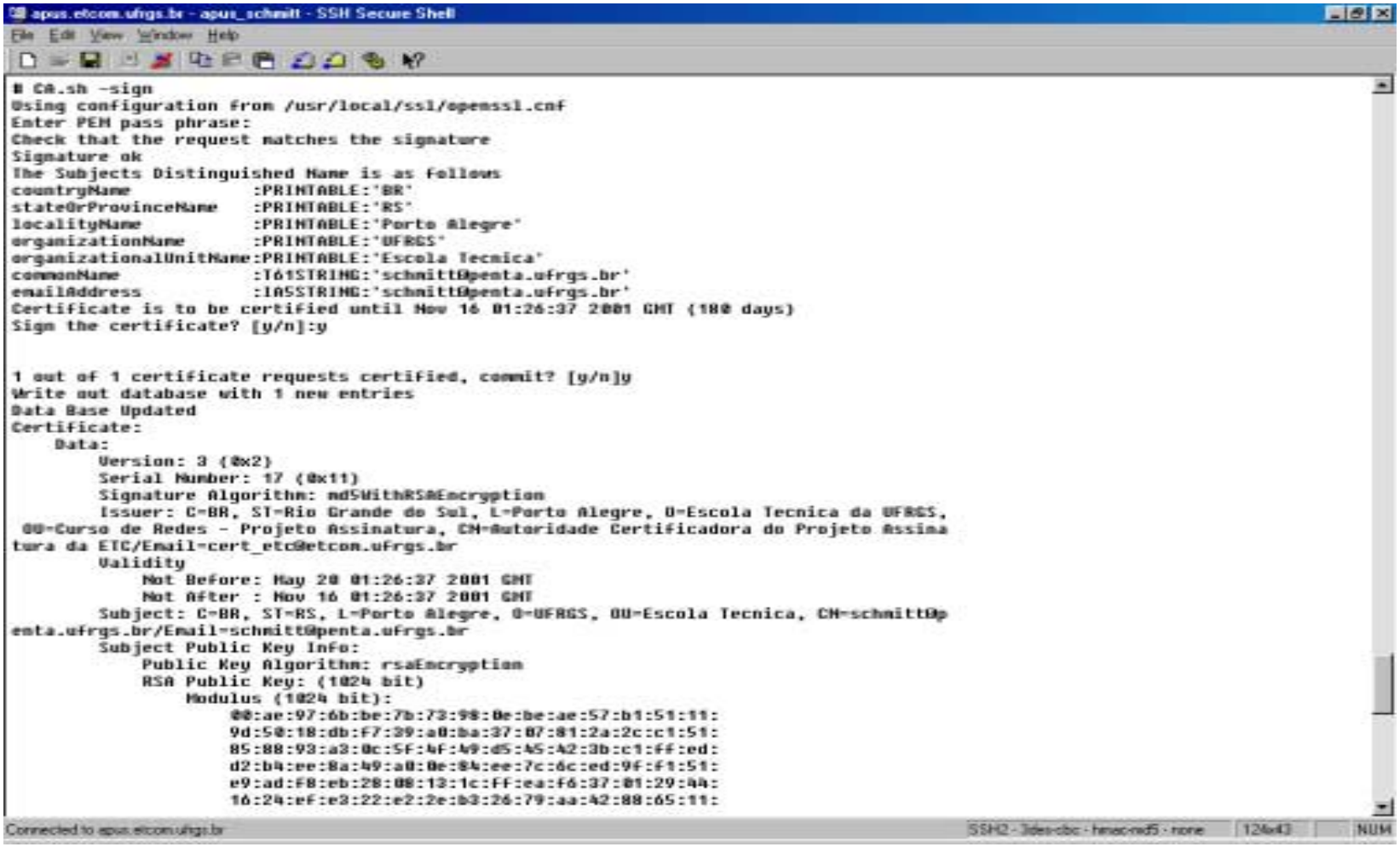
Trabalho inicial - OpenSSL

Geração das chaves

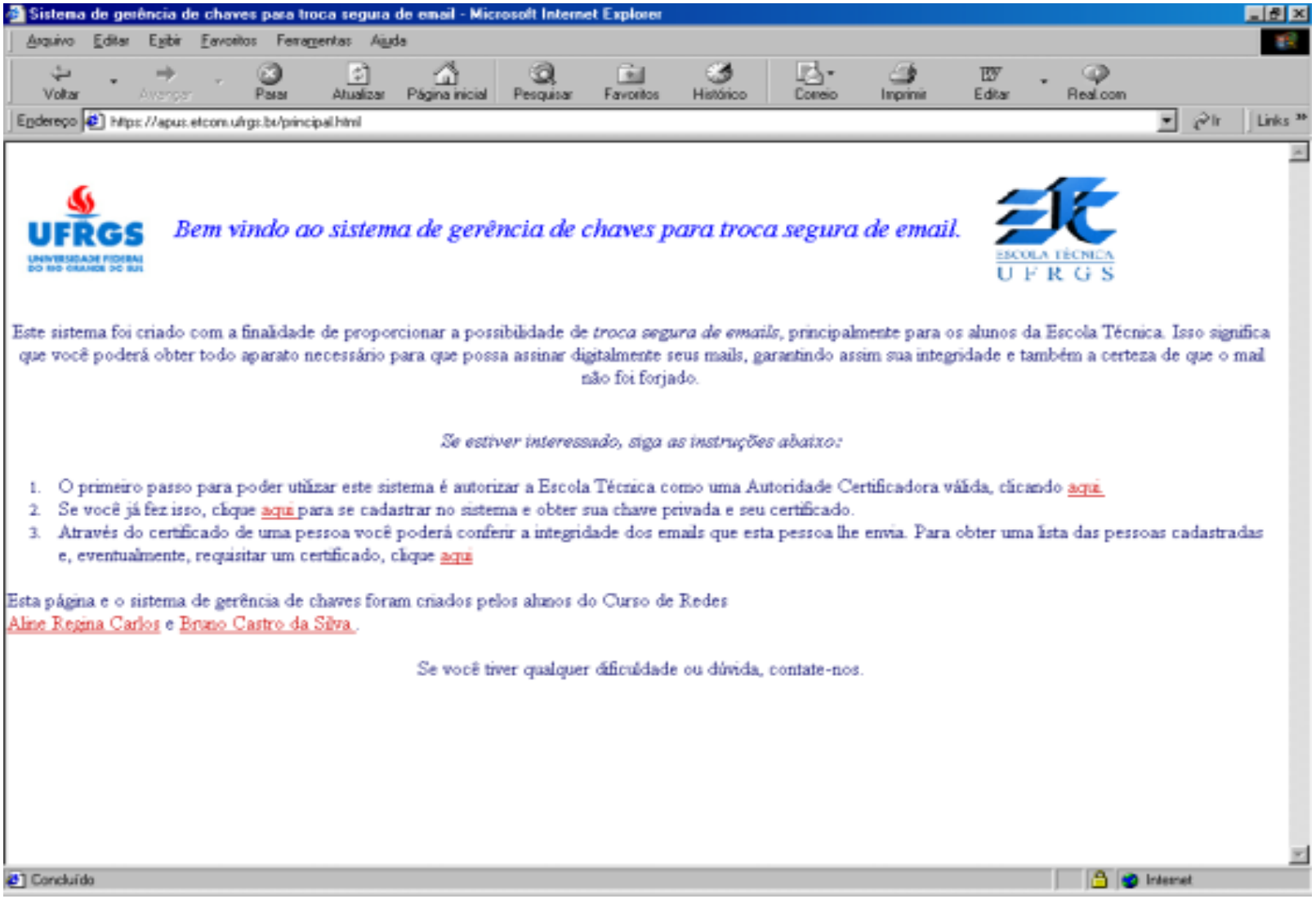


Trabalho inicial - OpenSSL

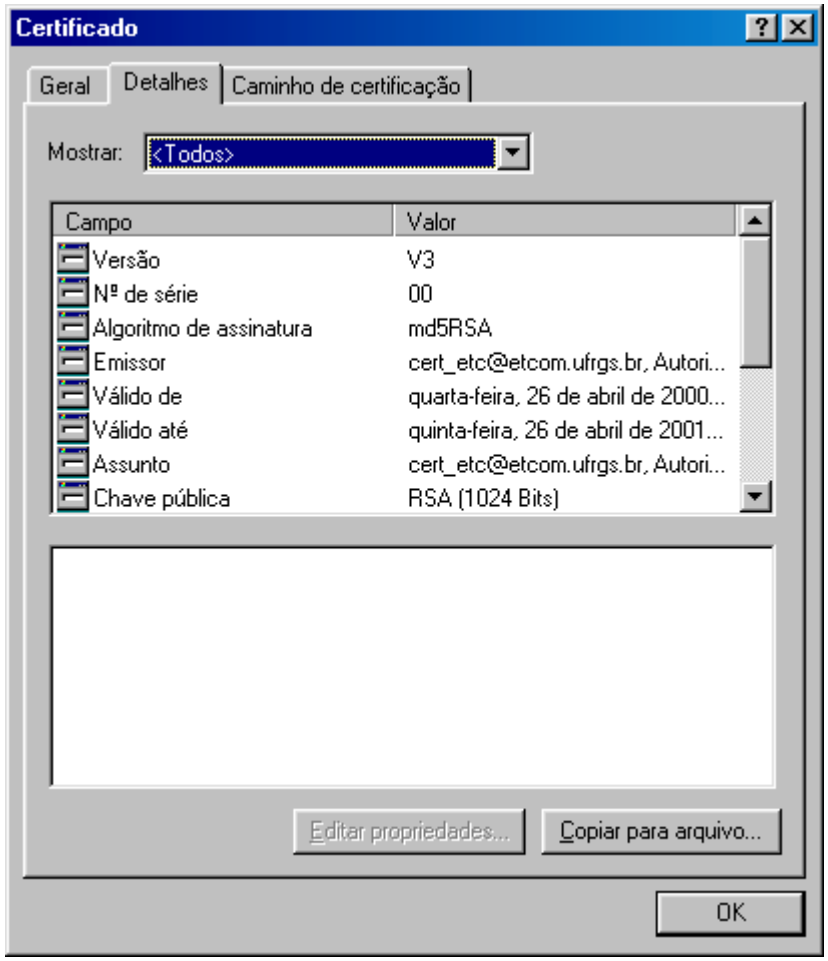
Geração do certificado



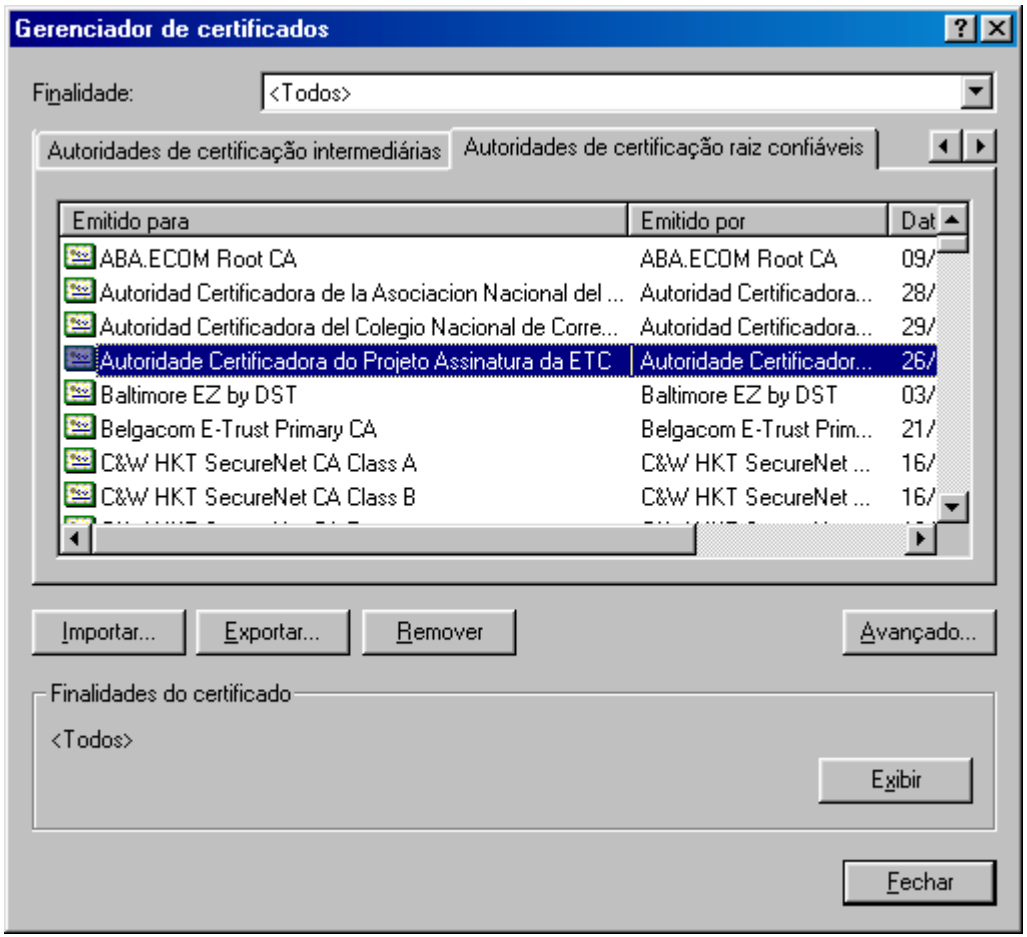
Páginas para emissão de certificado



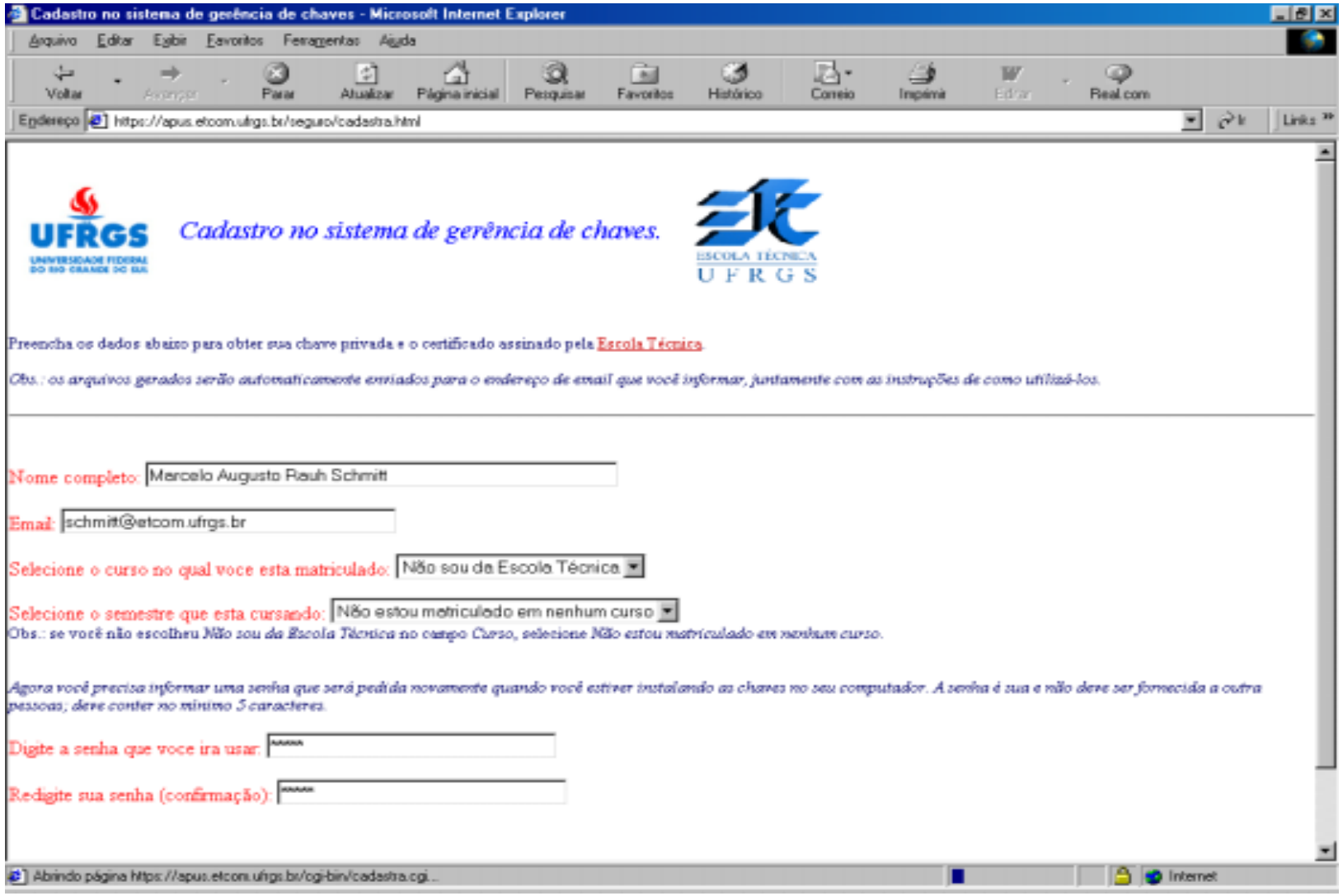
Páginas para emissão de certificado



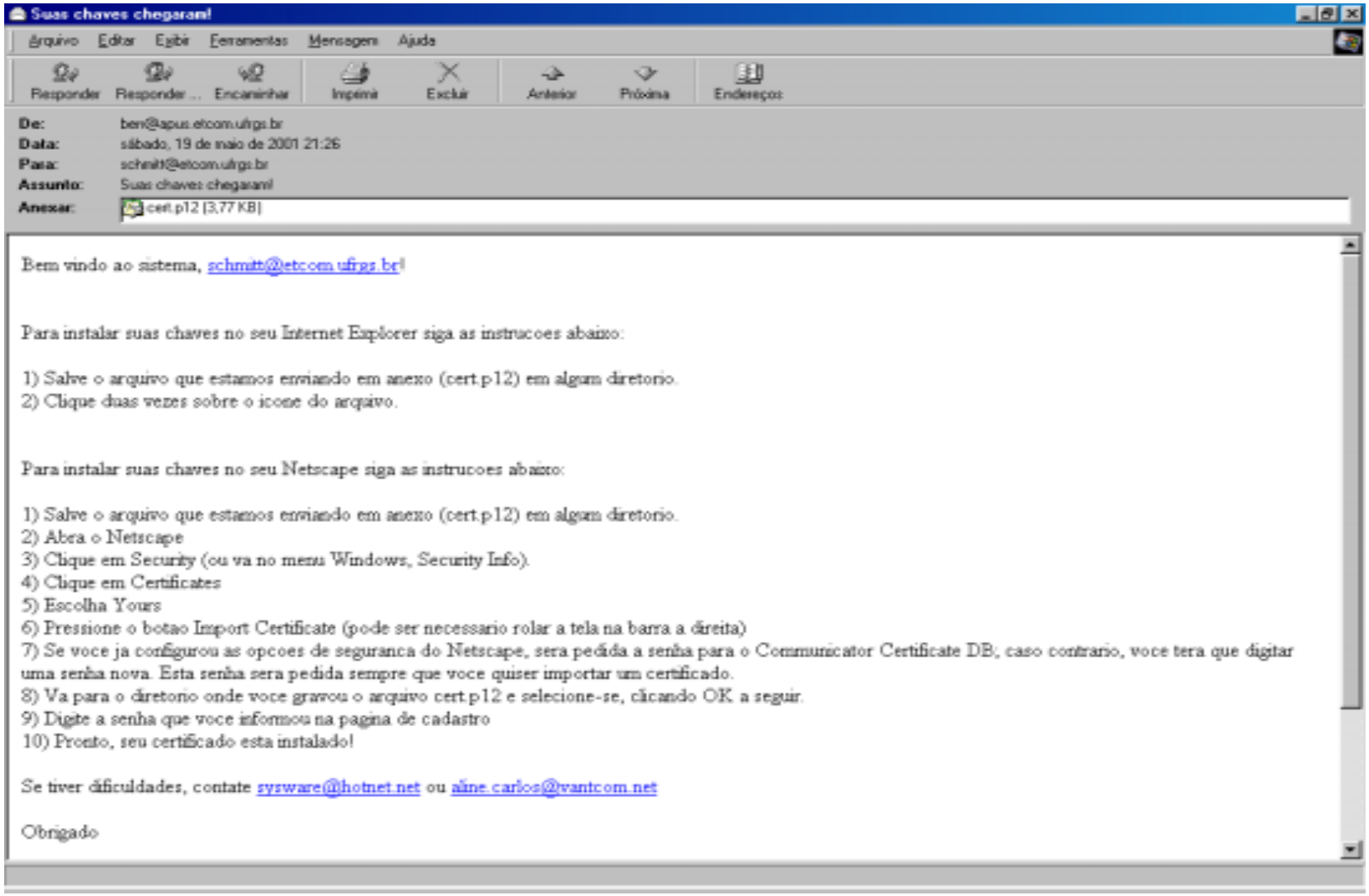
Páginas para emissão de certificado



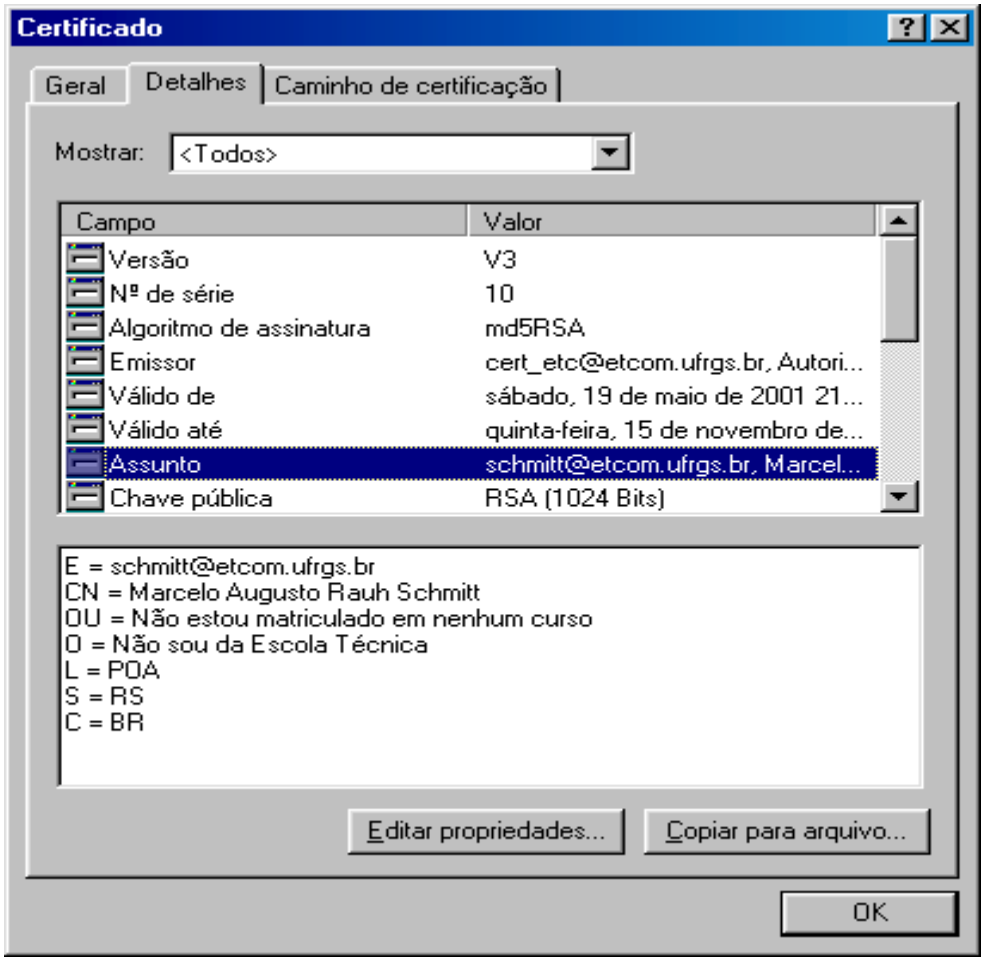
Páginas para emissão de certificado



Páginas para emissão de certificado



Páginas para emissão de certificado



Problemas detectados

- Necessidade de se ter várias Autoridades Certificadoras
- Necessidade de se gerenciar as várias Autoridades Certificadoras
- Necessidade de se controlar a emissão de certificados
- Esquema de arquivos do OpenSSL inseguro

Fase atual

- Criação de programas para gerenciar as Autoridades Certificadoras
- Criação de programa para gerenciar a emissão de certificados
- Utilização de MySQL e nova estrutura de arquivos para gerenciar Autoridades Certificadoras e Certificados

Próxima fase

- Distribuição de certificados
  - LDAP
  - WEB
- Listas de revogação
- Utilização na Escola Técnica da UFRGS