

Projeto ICP da Escola Técnica da UFRGS



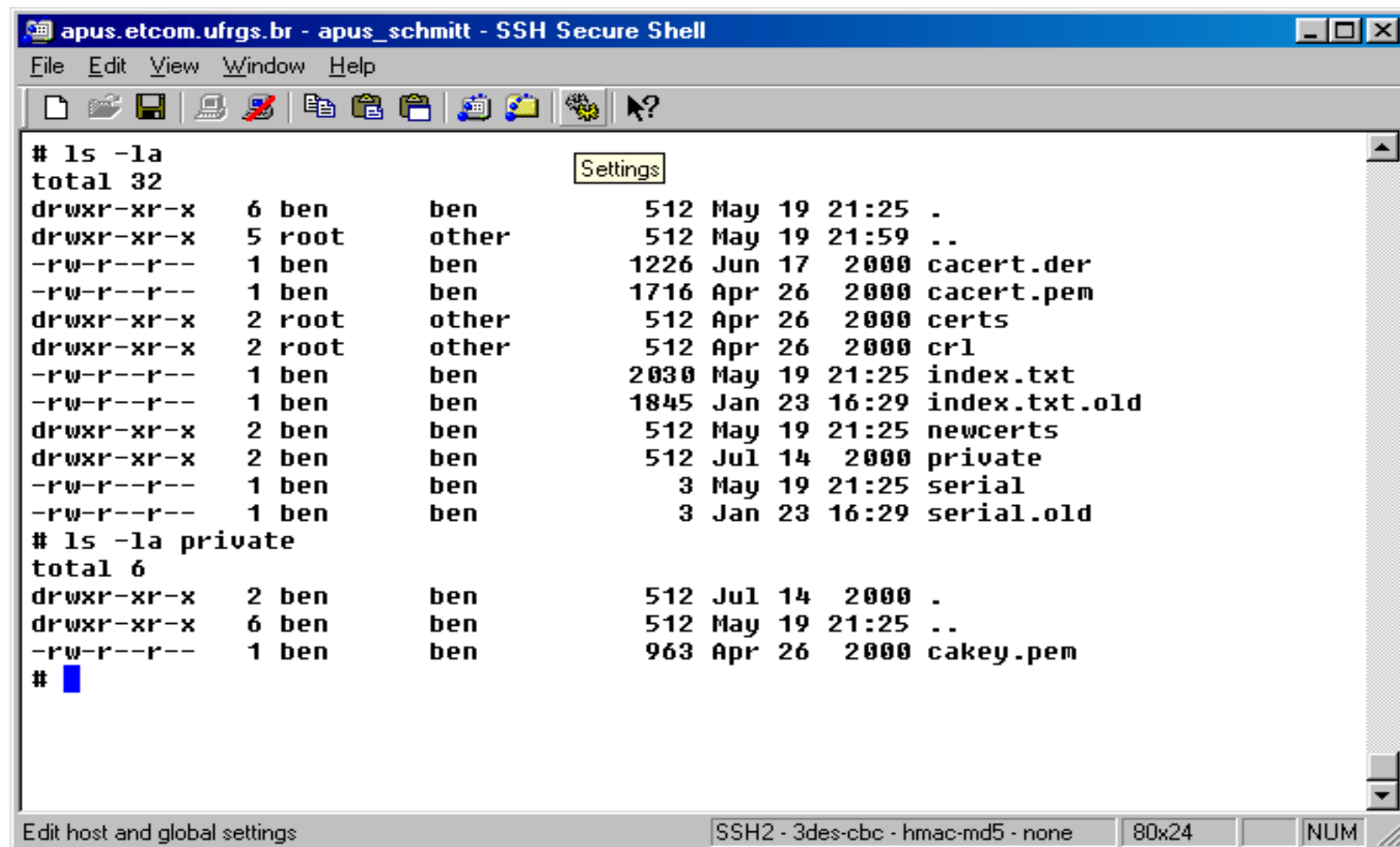
Prof. Marcelo Augusto Rauh Schmitt

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



The screenshot shows an SSH terminal window titled "apus.etcom.ufrgs.br - apus_schmitt - SSH Secure Shell". The terminal displays the output of two commands: `ls -la` and `ls -la private`. The first command lists files in the current directory, including `cacert.der`, `cacert.pem`, `certs`, `cr1`, `index.txt`, `index.txt.old`, `newcerts`, `private`, `serial`, and `serial.old`. The second command lists files in the `private` directory, including `.`, `..`, and `cakey.pem`. The terminal window has a menu bar (File, Edit, View, Window, Help) and a toolbar with various icons. A "Settings" button is visible in the top right of the terminal area. The status bar at the bottom shows "Edit host and global settings", "SSH2 - 3des-cbc - hmac-md5 - none", "80x24", and "NUM".

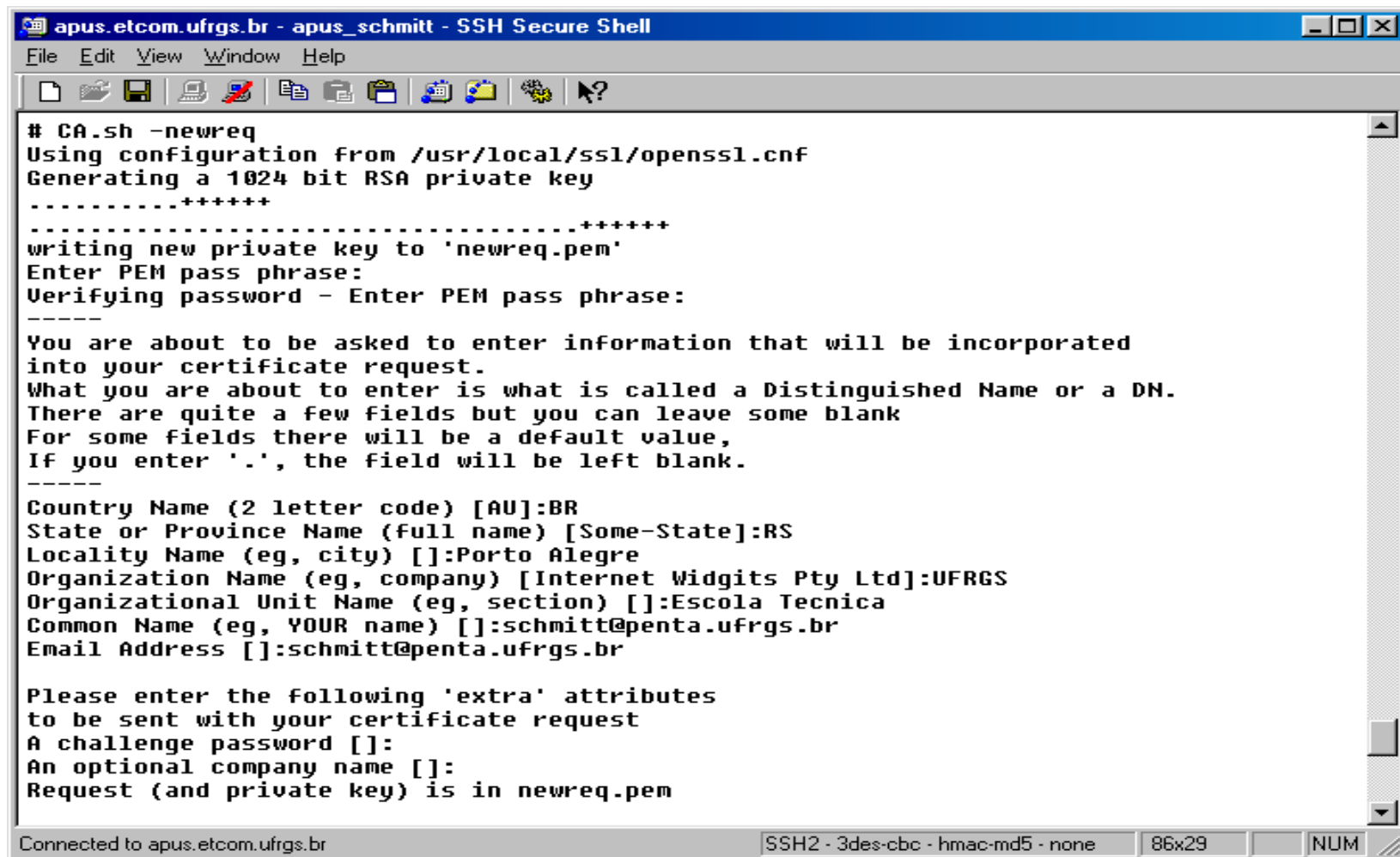
```
# ls -la
total 32
drwxr-xr-x  6 ben      ben      512 May 19 21:25 .
drwxr-xr-x  5 root    other    512 May 19 21:59 ..
-rw-r--r--  1 ben      ben     1226 Jun 17  2000 cacert.der
-rw-r--r--  1 ben      ben     1716 Apr 26  2000 cacert.pem
drwxr-xr-x  2 root    other    512 Apr 26  2000 certs
drwxr-xr-x  2 root    other    512 Apr 26  2000 cr1
-rw-r--r--  1 ben      ben     2030 May 19 21:25 index.txt
-rw-r--r--  1 ben      ben     1845 Jan 23 16:29 index.txt.old
drwxr-xr-x  2 ben      ben      512 May 19 21:25 newcerts
drwxr-xr-x  2 ben      ben      512 Jul 14  2000 private
-rw-r--r--  1 ben      ben        3 May 19 21:25 serial
-rw-r--r--  1 ben      ben        3 Jan 23 16:29 serial.old

# ls -la private
total 6
drwxr-xr-x  2 ben      ben      512 Jul 14  2000 .
drwxr-xr-x  6 ben      ben      512 May 19 21:25 ..
-rw-r--r--  1 ben      ben     963 Apr 26  2000 cakey.pem

#
```

Trabalho inicial - OpenSSL

Geração das chaves



```
apus.etcom.ufrgs.br - apus_schmitt - SSH Secure Shell
File Edit View Window Help
.....
# CA.sh -newreq
Using configuration from /usr/local/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:RS
Locality Name (eg, city) []:Porto Alegre
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UFRGS
Organizational Unit Name (eg, section) []:Escola Tecnica
Common Name (eg, YOUR name) []:schmitt@penta.ufrgs.br
Email Address []:schmitt@penta.ufrgs.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request (and private key) is in newreq.pem

Connected to apus.etcom.ufrgs.br
SSH2 - 3des-cbc - hmac-md5 - none
86x29
NUM
```

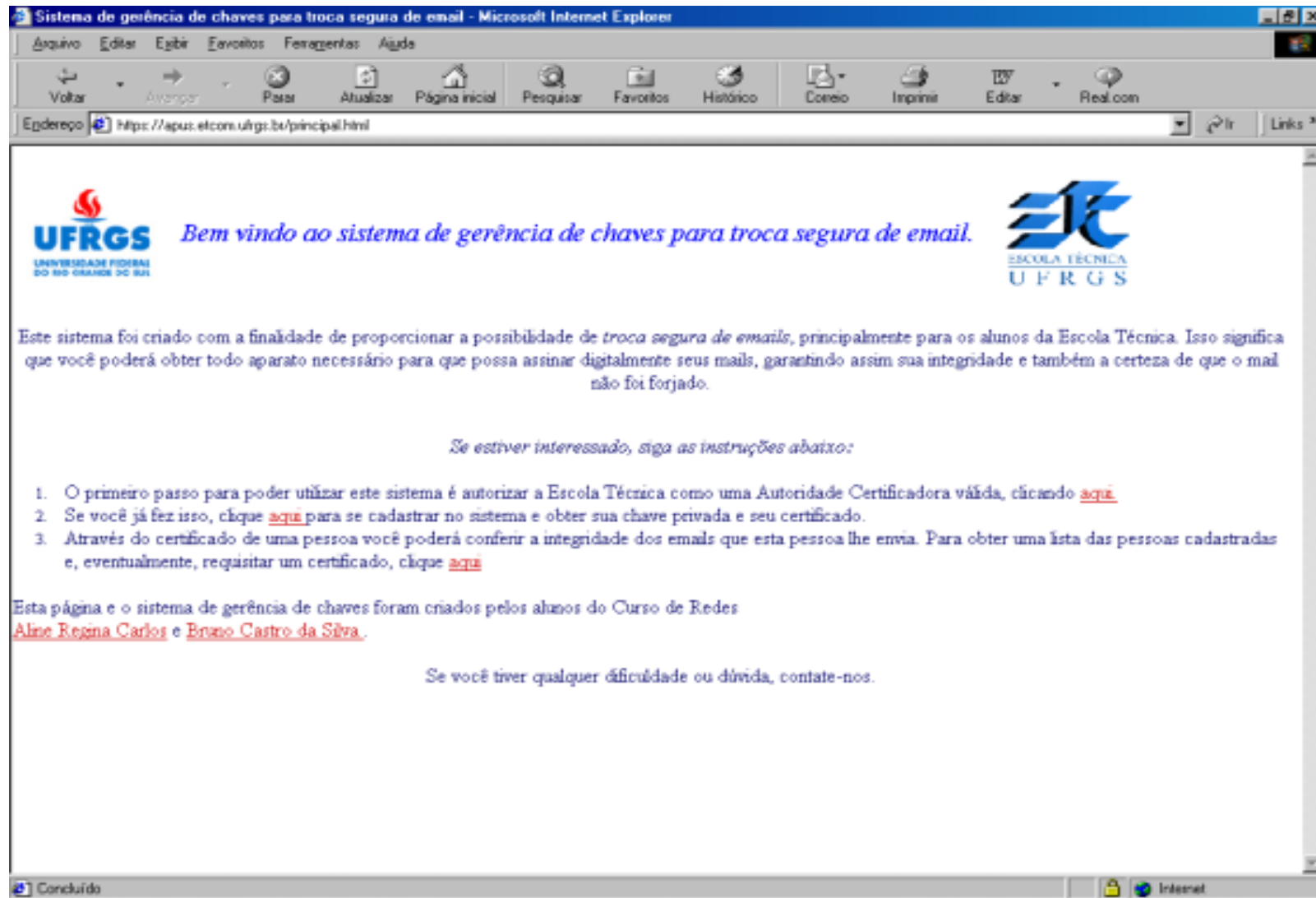
```

ap@ap.usf.br: ~$ ssh-keygen -s -C ap@ap.usf.br -i /usr/local/ssl/openssl.cnf
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BR'
stateOrProvinceName   :PRINTABLE:'RS'
localityName          :PRINTABLE:'Porto Alegre'
organizationName       :PRINTABLE:'UFERS'
organizationalUnitName:PRINTABLE:'Escola Tecnica'
commonName            :T61STRING:'schmitt@penta.ufers.br'
emailAddress          :IASSTRING:'schmitt@penta.ufers.br'
Certificate is to be certified until Nov 16 01:26:37 2001 GMT (180 days)
Sign the certificate? [y/n]:y

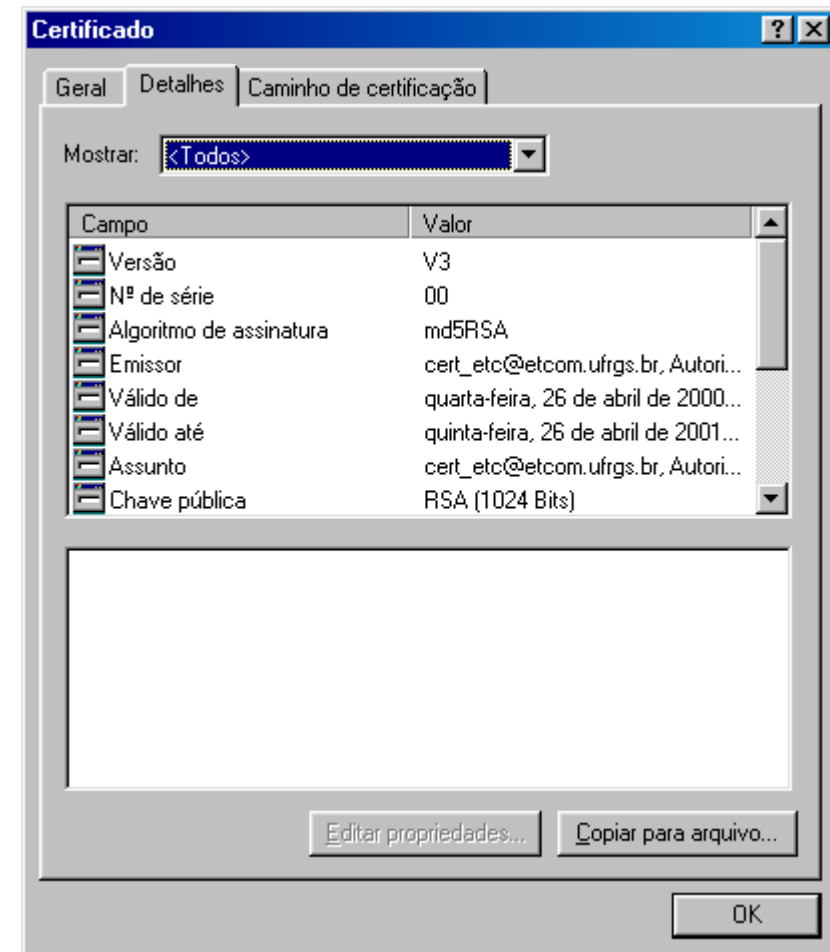
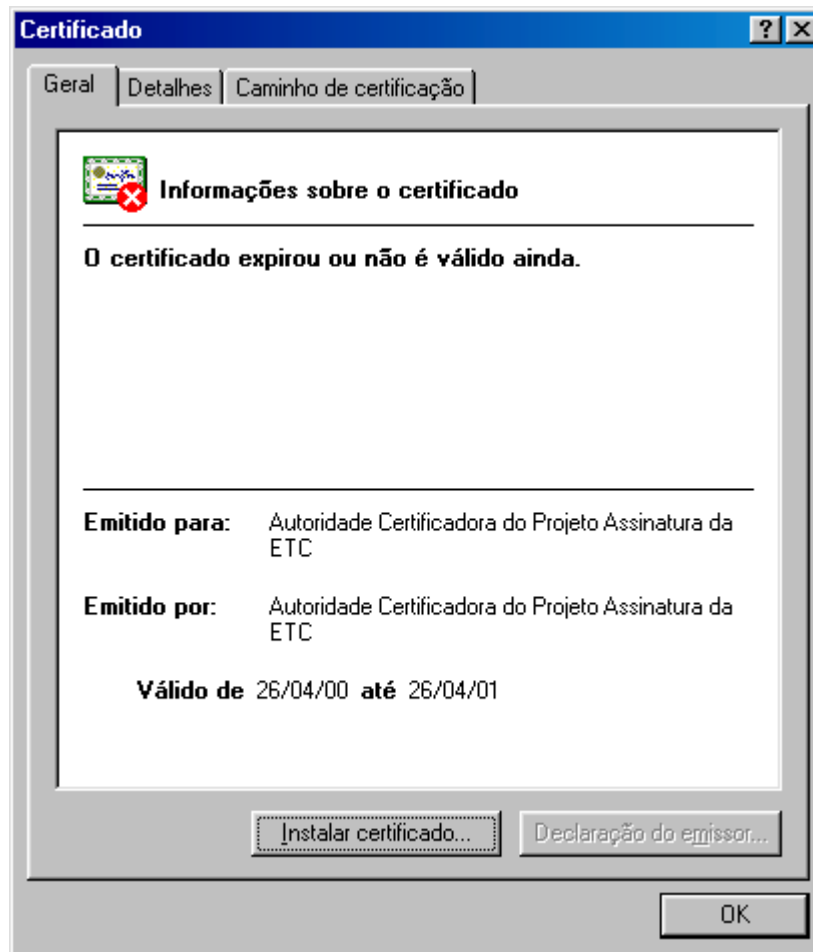
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 17 (0x11)
        Signature Algorithm: md5WithRSAShEncryption
        Issuer: C=BR, ST=Rio Grande do Sul, L=Porto Alegre, O=Escola Tecnica da UFERS,
        OU=Curso de Redes - Projeto Assinatura, CN=Autoridade Certificadora do Projeto Assina-
        tura da EIC/Email=cert_eic@etcon.ufers.br
        Validity
            Not Before: May 20 01:26:37 2001 GMT
            Not After : Nov 16 01:26:37 2001 GMT
        Subject: C=BR, ST=RS, L=Porto Alegre, O=UFERS, OU=Escola Tecnica, CN=schmitt@p-
        enta.ufers.br/Email=schmitt@penta.ufers.br
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ae:97:6b:be:7b:73:98:0e:be:ae:57:b1:51:11:
                    9d:50:18:db:f7:39:a0:ba:37:07:81:2a:2c:c1:51:
                    85:88:93:a3:0c:5f:4f:49:d5:a5:a2:3b:c1:ff:ed:
                    d2:b4:ee:8a:49:a0:0e:84:ee:7c:dc:ed:9f:f1:51:
                    e9:ad:f8:eb:28:08:13:1c:ff:ea:f6:37:01:29:44:
                    16:24:ef:e3:22:e2:2e:b3:26:79:aa:42:88:65:11:

```

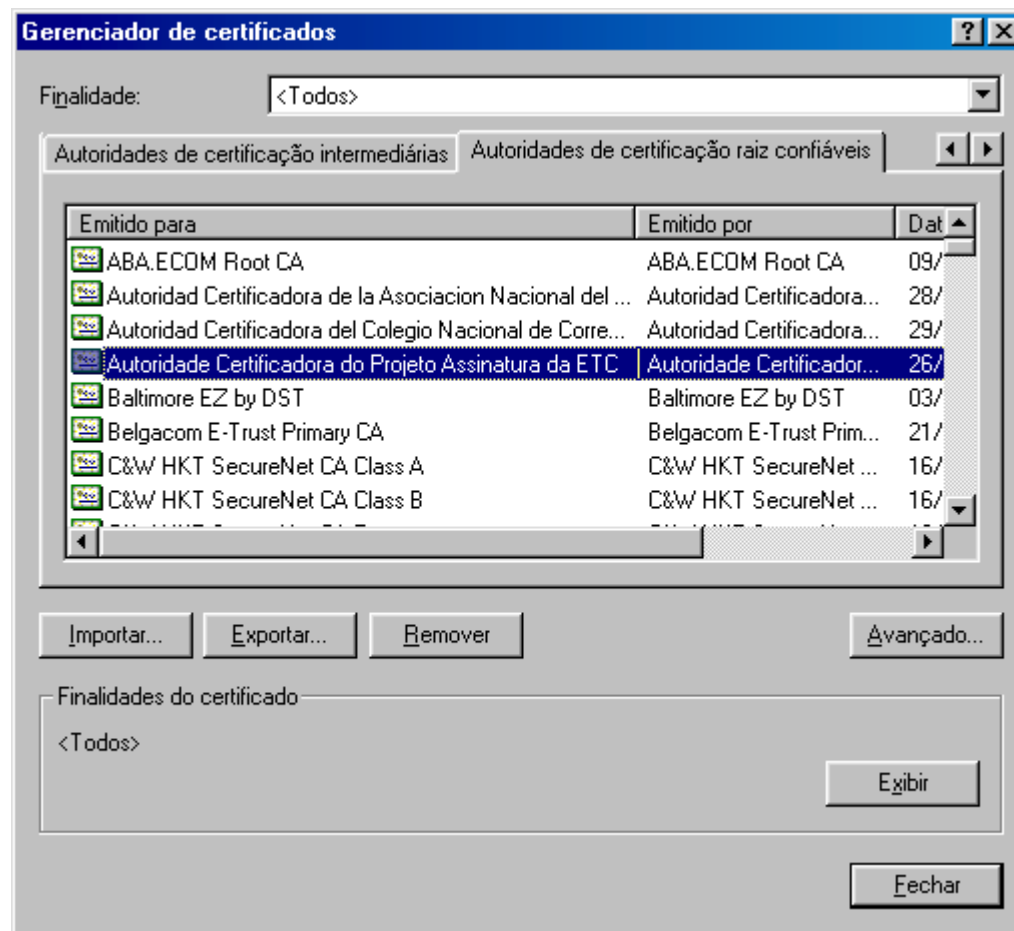
Páginas para emissão de certificado



Páginas para emissão de certificado



Páginas para emissão de certificado



Páginas para emissão de certificado

Cadastro no sistema de gestão de chaves - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Voltar Avançar Parar Atualizar Página inicial Pesquisar Favoritos Histórico Correio Impressão Editor Real.com

Endereço <https://apex.etcom.ufrgs.br/seguco/cadestra.html> Links



UFRGS
UNIVERSIDADE FEDERAL
DO RIO GRANDE DO SUL



ESCOLA TÉCNICA
UFRGS

Cadastro no sistema de gestão de chaves.

Preencha os dados abaixo para obter sua chave privada e o certificado assinado pela **Escola Técnica**.

Obs.: os arquivos gerados serão automaticamente enviados para o endereço de email que você informar, juntamente com as instruções de como utilizá-los.

Nome completo:

Email:

Selecione o curso no qual voce esta matriculado:

Selecione o semestre que esta cursando:

Obs.: se você não escolheu Não sou da Escola Técnica no campo Curso, selecione Não estou matriculado em nenhum curso.

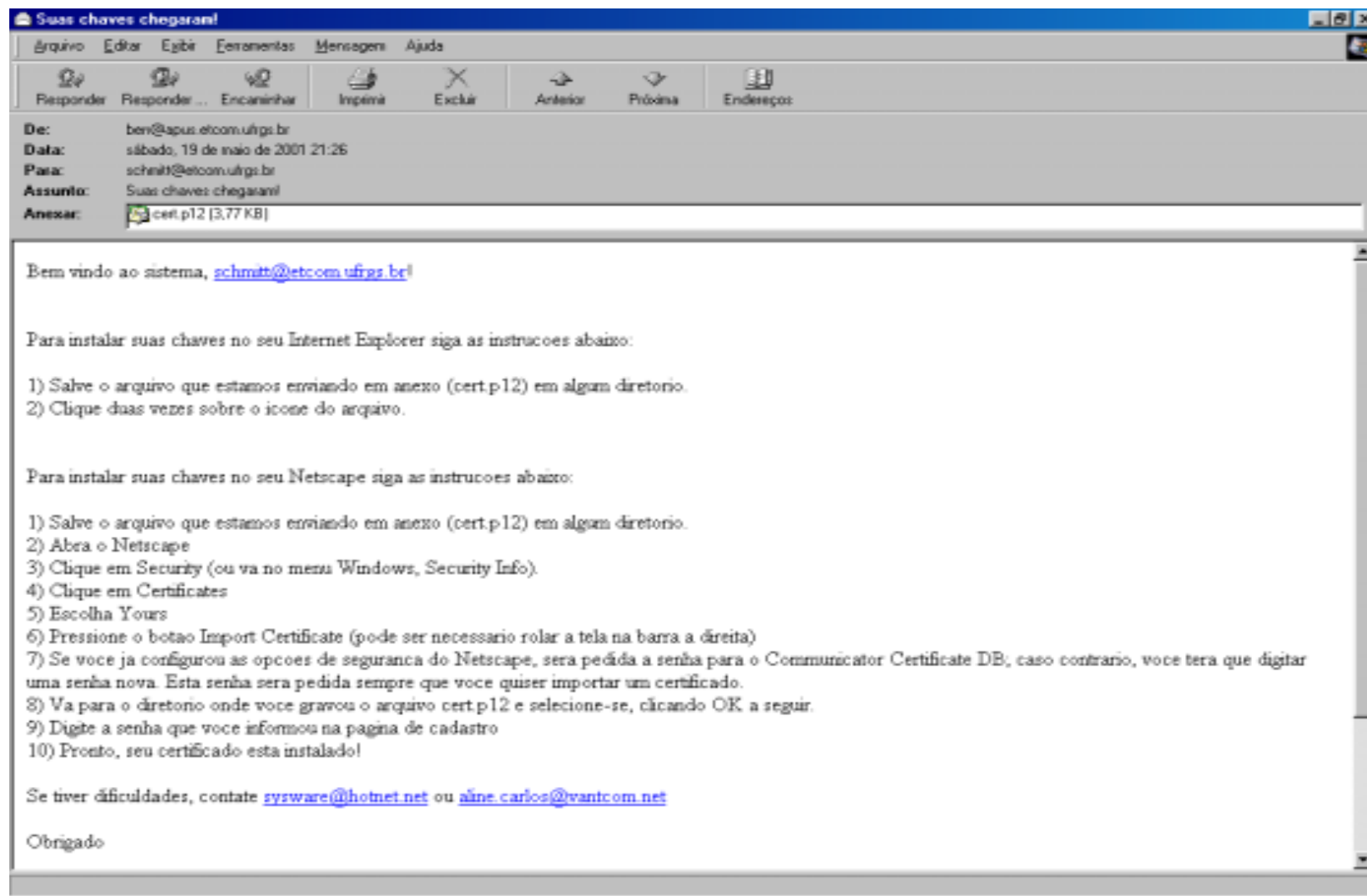
Agora você precisa informar uma senha que será pedida novamente quando você estiver instalando as chaves no seu computador. A senha é sua e não deve ser fornecida a outra pessoa; deve conter no mínimo 5 caracteres.

Digite a senha que voce ira usar:

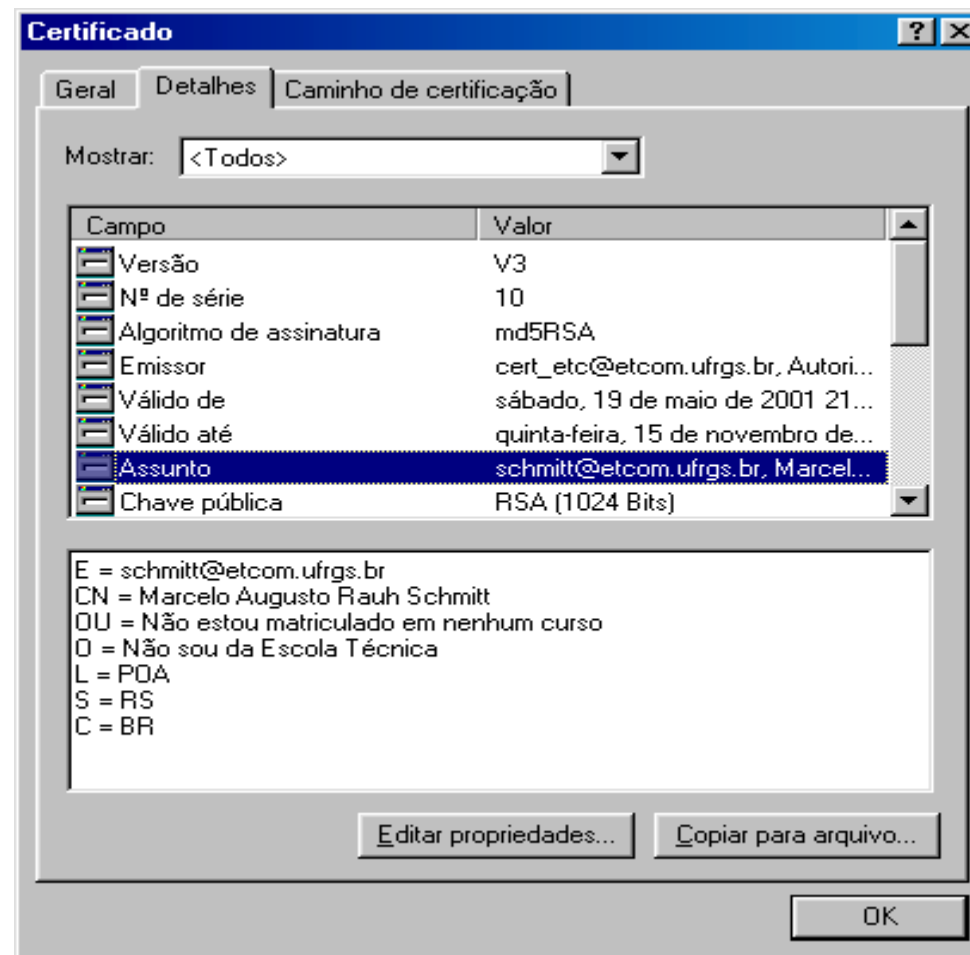
Redigite sua senha (confirmação):

Abrindo página <https://apex.etcom.ufrgs.br/cgi-bin/cadestra.cgi...> Internet

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