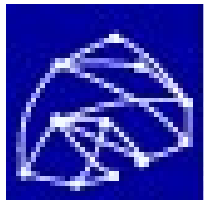


RNP - MCT

GT ICP-EDU II

Módulo de Hardware Seguro



RNP



UFSC



UNICAMP



UFMG

Material disponível em:
<http://www.labsec.ufsc.br>

Fortaleza, 05/2005

Prof. Ricardo Felipe Custódio
Prof. Ricardo Dahab
Prof. Jeroen van de Graaf
Prof. Daniel Santana de Freitas

Programa da Apresentação

- Histórico do GT
- Autenticação
- Cripto e ICP
 - Aplicações
- ICP-Brasil
- HSM
- Protótipo e Considerações Finais

Histórico

- GT ICP-EDU I (2003 – 2004)
 - Sistema de Gerenciamento de Certificados Digitais
 - Sítio com programa e documentação
 - <http://icpedu.labsec.ufsc.br>
- GT ICP-EDU II (2004 – 2005)
 - Proteção das Chaves Privadas das Aplicações
 - AC, AR
 - SSL, VPN
 - Instalação Padrão com serviços: AC, AR, SSL, ...

Objetivos ICP-EDU II

- HSM de Baixo Custo
 - < US\$ 1.000,00
- Pacote
 - OpenBSD
 - Web Seguro
 - AC, AR
 - SSH
 - Diretório OpenLDAP

Autenticação

- Informação compartilhada
 - Login/Senha
- Dispositivo Físico
 - Cartão, token
- Biometria
 - Impressão digital, reconhecimento de iris

Deve haver confiança mútua

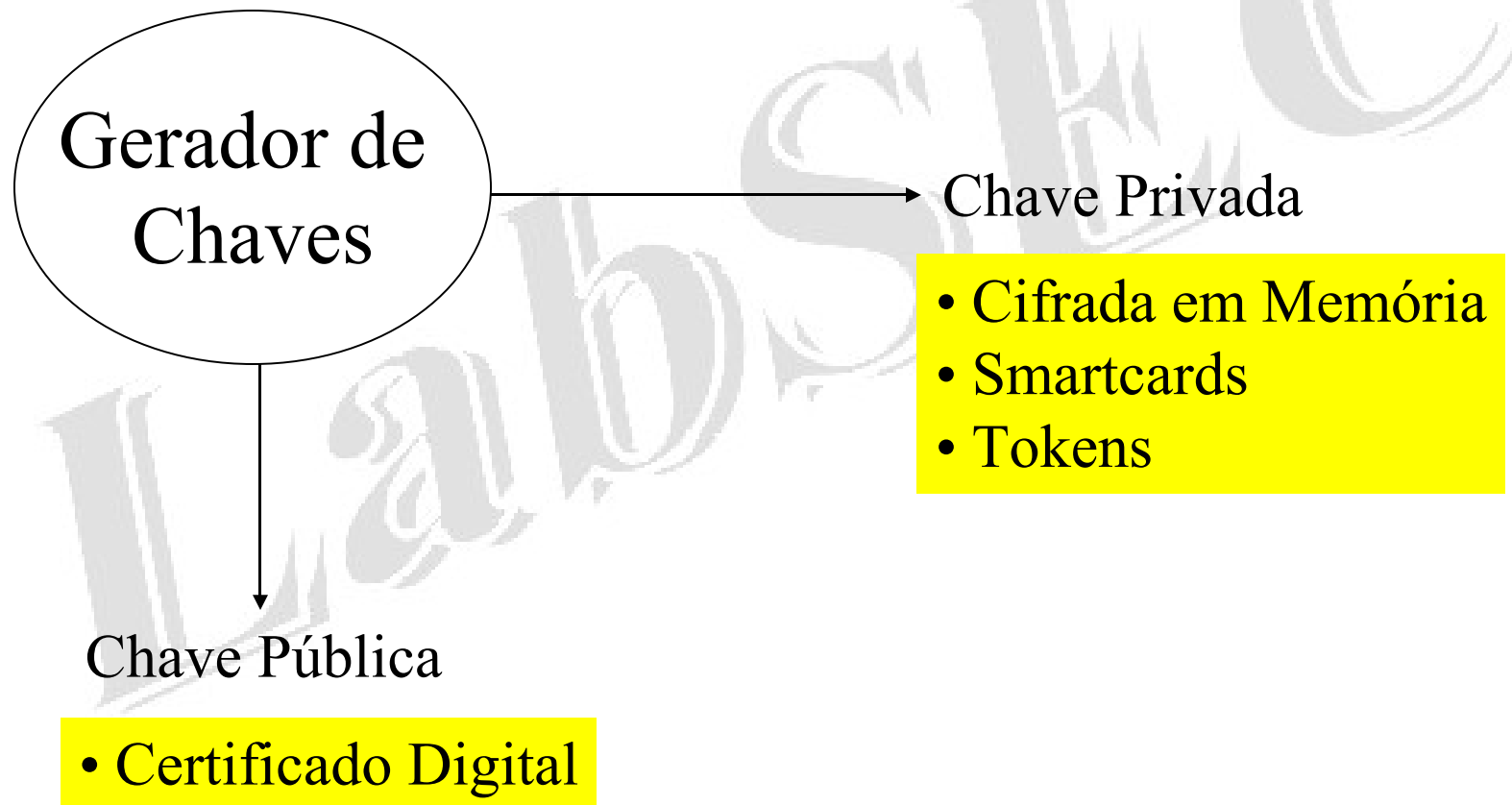
Criptografia Assimétrica

Alice

Beto



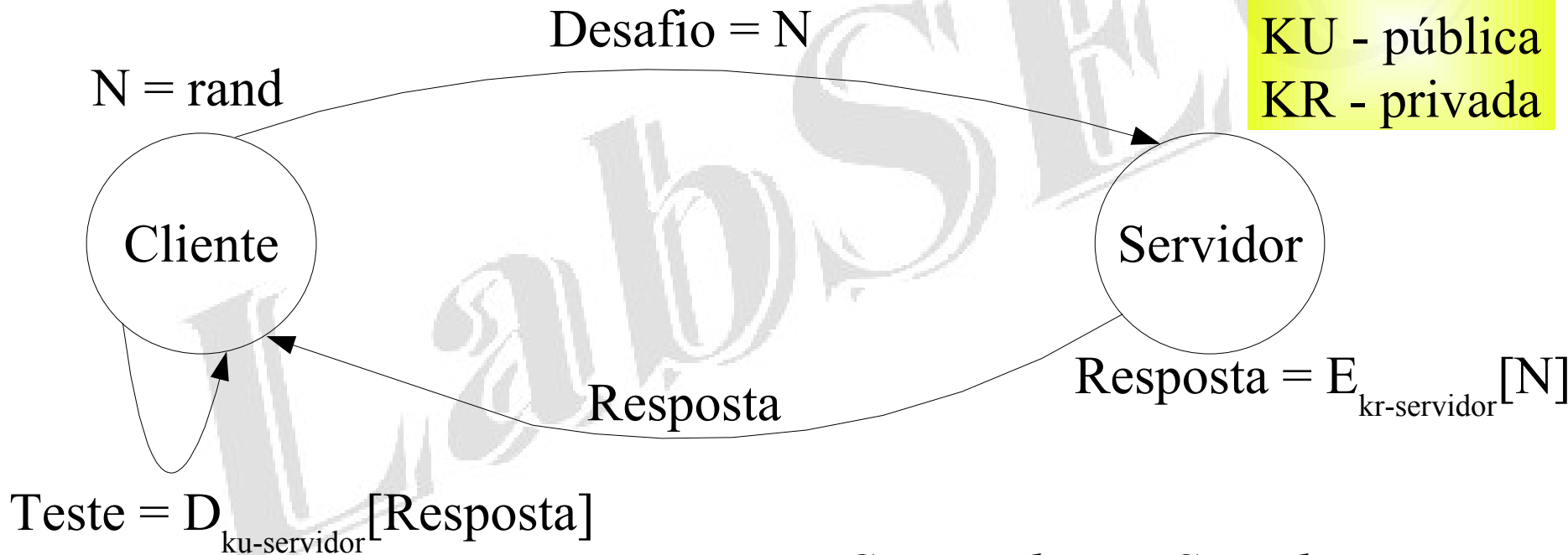
Alice e Beto Geram suas Chaves



Criptografia Assimétrica

autenticação

Par de Chaves
KU - pública
KR - privada



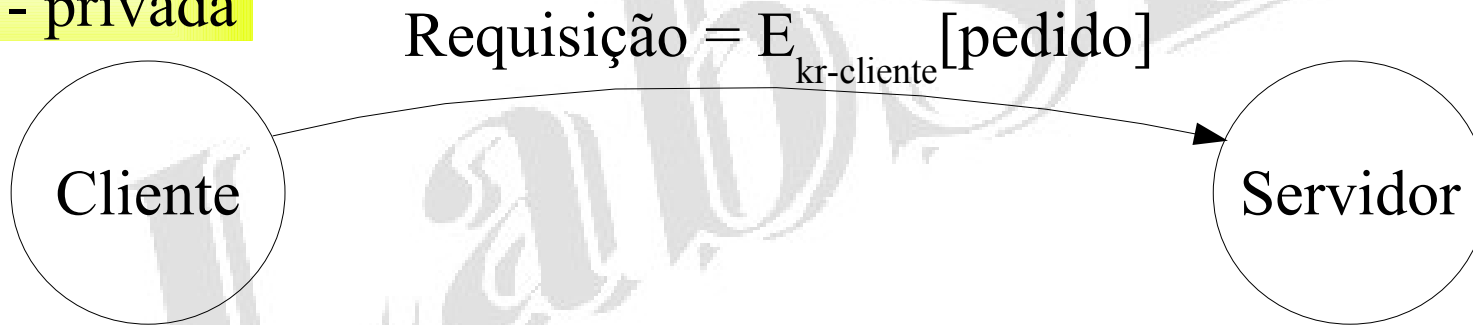
Teste = N ?

Como saber se Servidor possui a Chave Privada?

Criptografia Assimétrica

assinatura

Par de Chaves
KU - pública
KR - privada



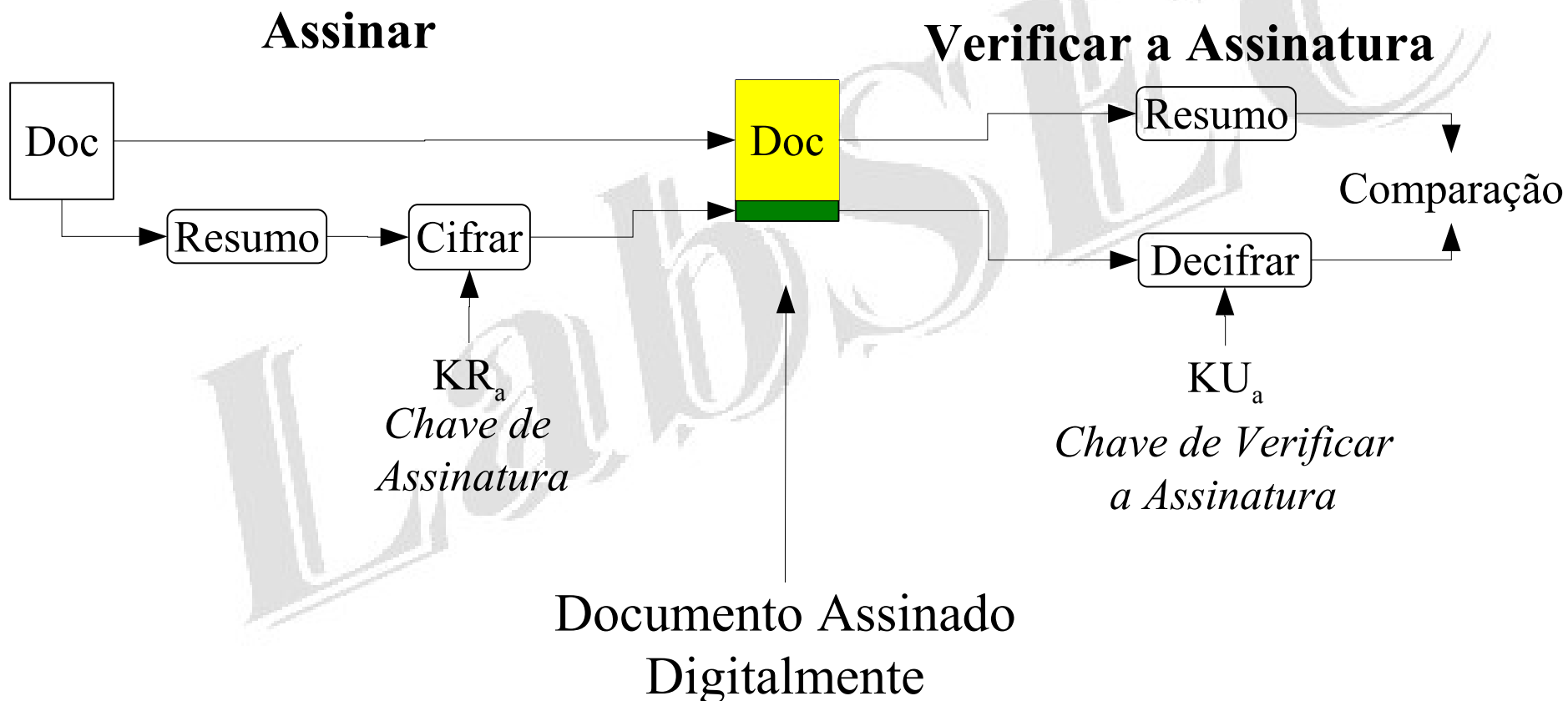
*Como saber se
pedido é do alegado
cliente?*

Utilidade

Para que Serve?

- Assinatura Digital
- Autenticação, Autorização
- Confiança nos Documentos Eletrônicos
 - Documentos Papel -> Documentos Eletrônicos
- Aumentar a confiança nas transações eletrônicas
- Sigilo da Informação

Como é feita a Assinatura Digital?



Como Confiar na Chave Pública?

- Cliente gera o par de Chaves
- Chaves protegidas por hardware
- Certificados Digitais emitidos por terceiras partes confiáveis
- Âncora de Confiança (AC RAIZ)
- Âncora de Tempo
- Âncora de Plataforma Computacional

Componentes de uma ICP

Gera Par de Chaves

Verifica os
Dados e
Assina a
Requisição

Requisição
c/ Dados

AR

HSM

Usuário

Requisição
Assinada pela AR

Chave
Privada

Smartcard

Certificado
Digital

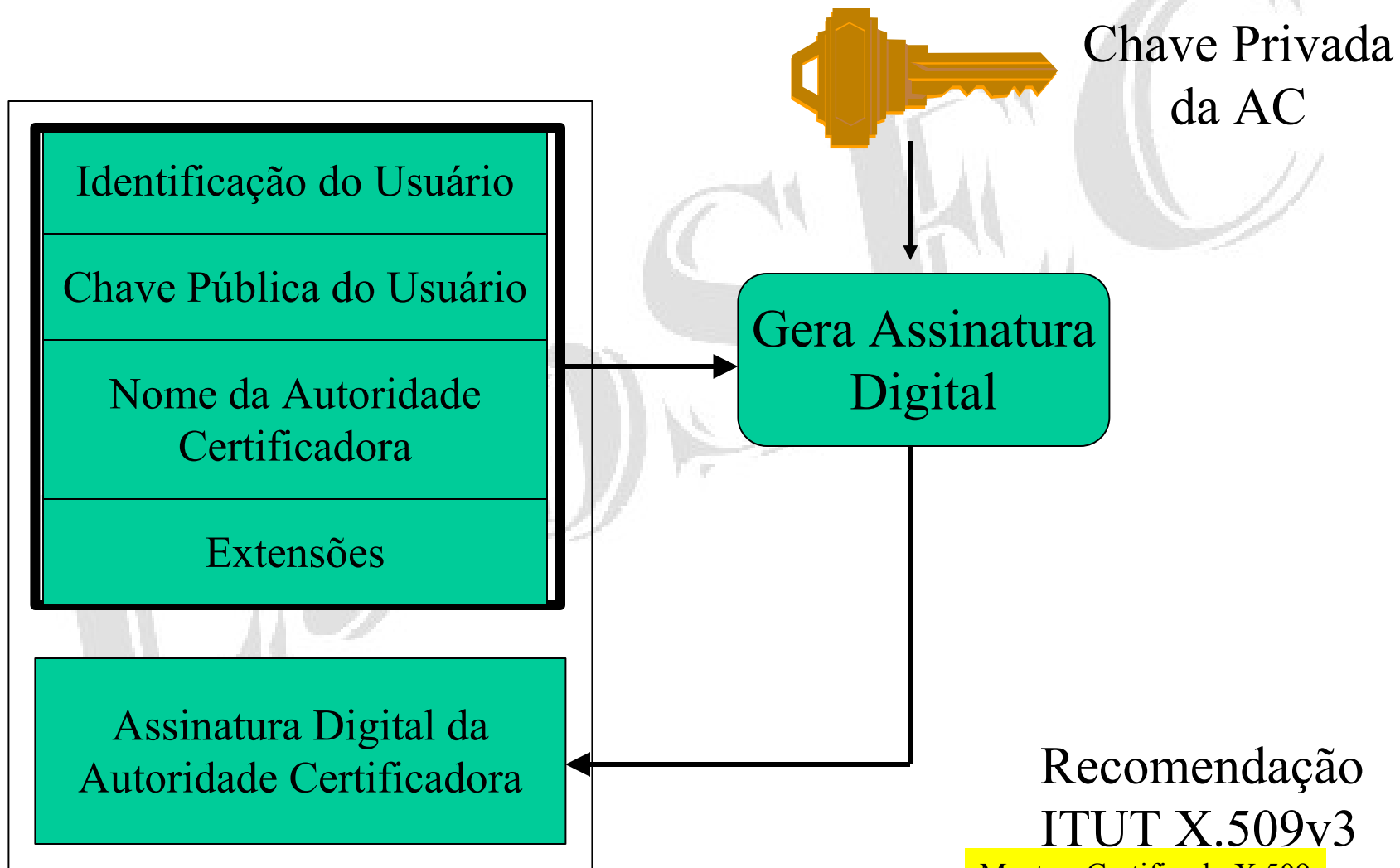
AC

HSM

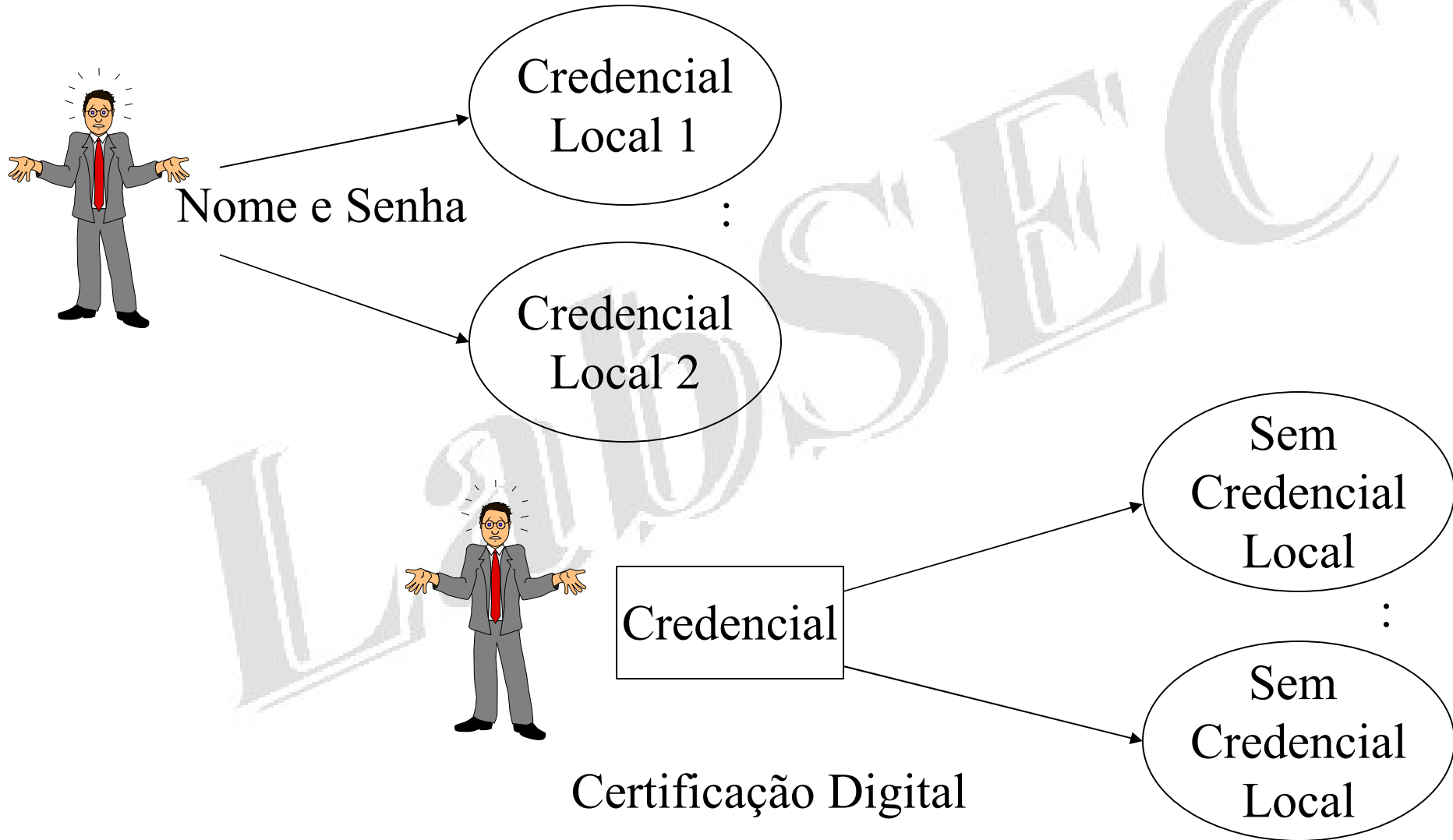
Isolada

Documentos, Procedimentos
Sala Cofre, Equipamentos

Certificado Digital = Identidade Digital

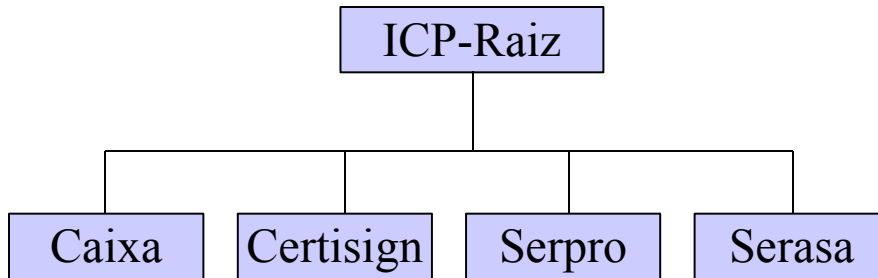


Tipos de Autenticação

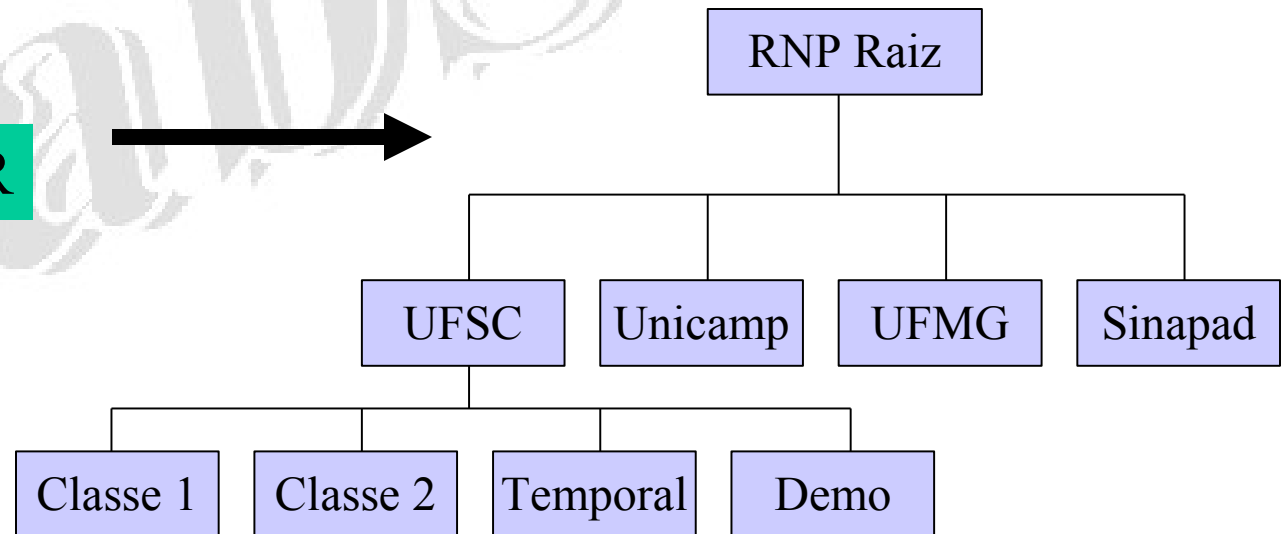


Modelo ICP-Brasil

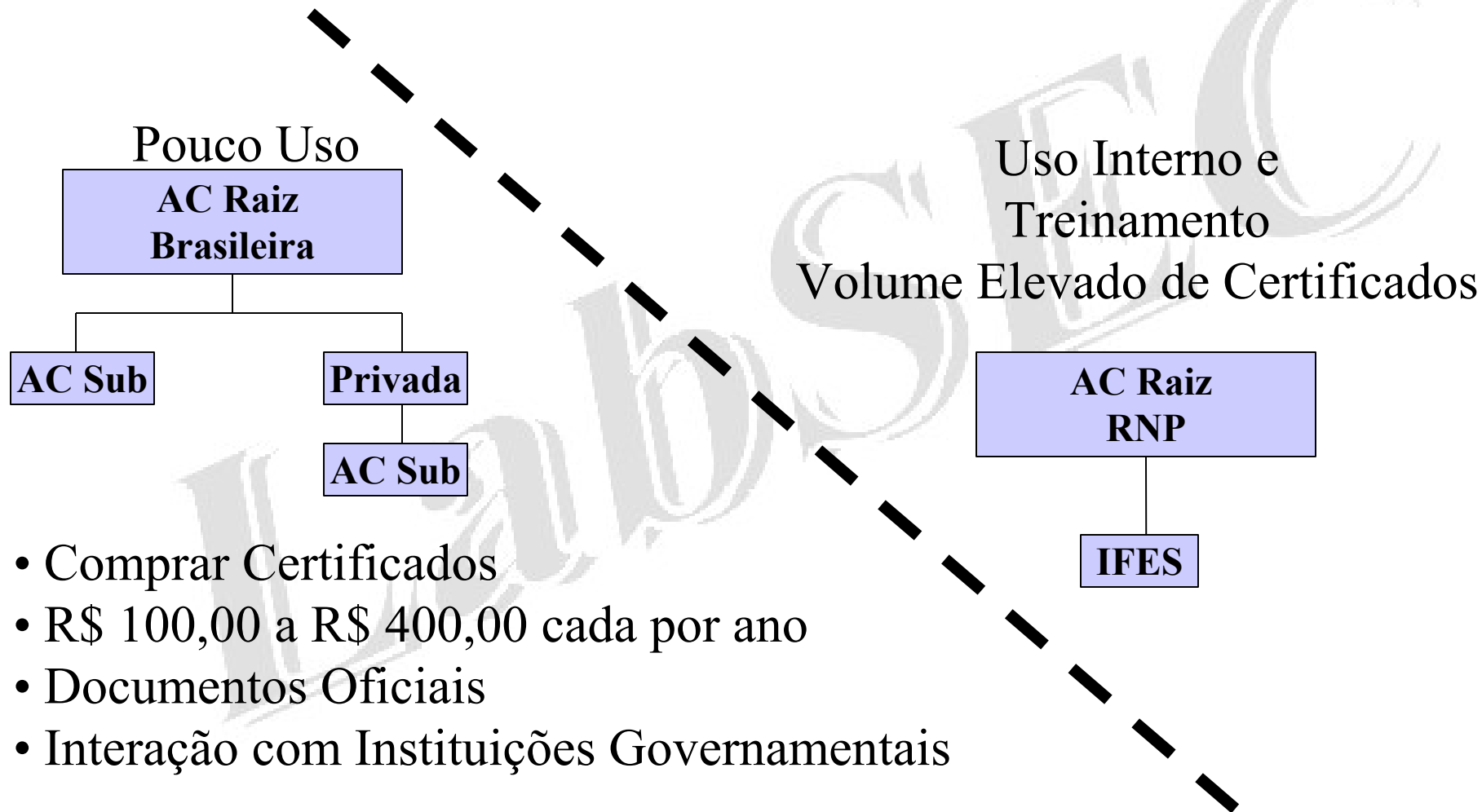
MP 2.200-2



RNP GT ICP-EDU
Sistema CRIADOR



Certificação nas Universidades



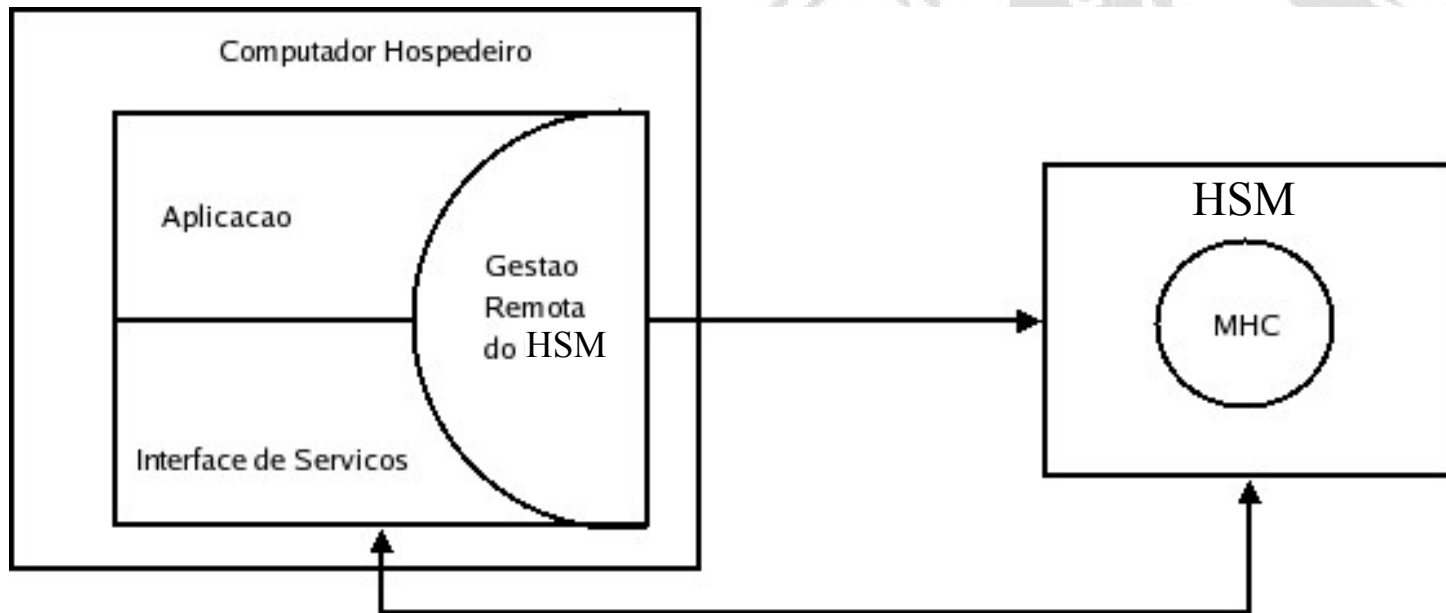
GT ICP-EDU II

Módulo de Hardware Criptográfico

Requisitos

- Autoridades Certificadoras
 - Proteção das chave criptográficas
 - Controle de acesso às chaves criptográficas
 - Aceleração é um “Conforto”
 - Os ataques são controlados pelo ambiente
- Aplicações
 - Proteção das chave criptográficas
 - Aceleração é uma necessidade
 - O ambiente é hostil

Ambiente de um HSM



Normas de Construção de HSM

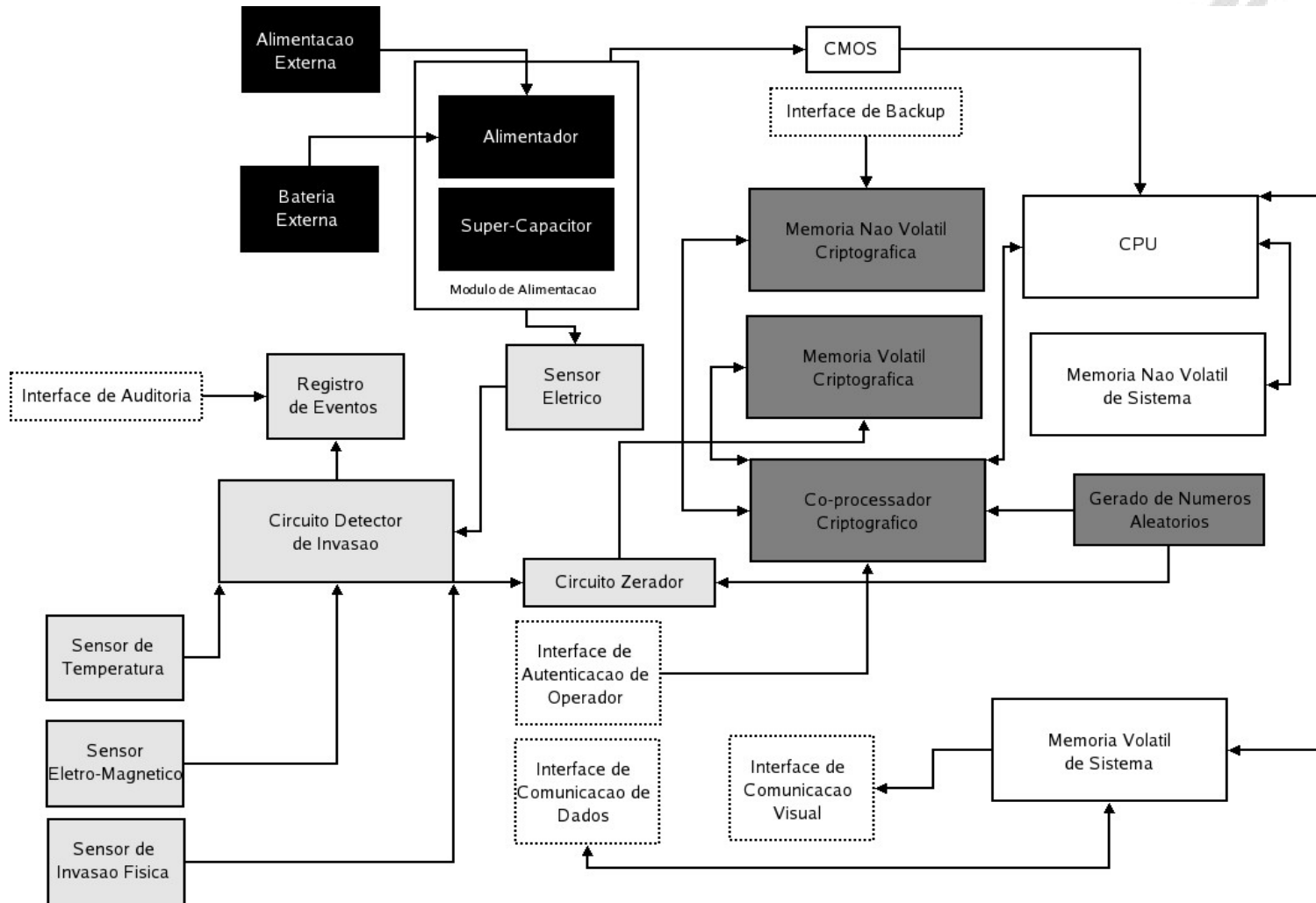
- FIPS PUB 140-2
 - NIST
 - Hardware
- Critérios Comuns
 - ISO15408
 - Ambiente
 - Procedimentos

Equipamentos de Mercado

- Avaliados pelo NIST como compatível com FIPS PUB 140 níveis 3 e 4
- Avaliação pelo certificado de homologação
 - Manuais quando disponível
 - Exceção para nCipher e Eracom (acessíveis)
- Requisitos
 - Compatível com OpenSSL
 - Voltado à proteção de chaves



Proposta de Hardware



Estrutura do Gerenciamento de Chaves Criptográficas

- Atores
 - Administradores
 - Operadores
 - Auditores
- Propriedades
 - proteção de chaves
 - processos criptográficos
 - registros de eventos
 - compartilhamento de segredo

Funcionalidades

- Cria Administradores e Operadores
- Geração de Chave de Aplicação
- Uso da Chave
- Cria Auditores
- Troca Administradores e Operadores
- Cria Cópia de Segurança
- Recupera Cópia de Segurança
- Lista de Certificados Confiáveis

Administradores

- criar operadores
- criar chaves
- criar auditores
- gerenciar operadores
- importar certificados
- importar LCR
- configurar equipamento

Operadores

- Uso das Chaves
 - controle de acesso
 - compartilhamento de segredos
- Rastreamento
 - dados não exportáveis
 - encadeamento de XOR
- Confia parcialmente nos administradores

Audidores

- Especialização de Operadores
 - não é guardada a chave não exportável
 - Administradores não podem delegar novamente as chaves
- Possui uma chave de Aplicação
 - Ku_{audit} e Kr_{audit}
- Os registros são cifrados com Ku_{audit} .
 - Controle de acesso aos registros
 - Imprevisibilidade de alterações

Protótipo

- Hardware de prateleira
- Sensores simples
- Software livre
- Aceleração criptográfica
- Voltado para ambiente de redes

Características do Protótipo

- Hardware
 - Soekris e PC-104
- Sistema Operacional
 - OpenBSD + Patches
- Bibliotecas
 - OpenSSL, OpenCT, OpenSC, ShareSecret, SQLite
- Software Gestor
 - OpenHSMD
 - Desenvolvido no LabSEC
 - Licença BSD

Protótipo





FreeHSM - (disconnected from HSM server)

Connections Help

Certificates Configuration

A suitable description for certificates

Country name (2 letter code)

State or Province Name (full name)

Locality Name (eg, city)

Organization Name (eg, company)

Previous Next

System Configuration

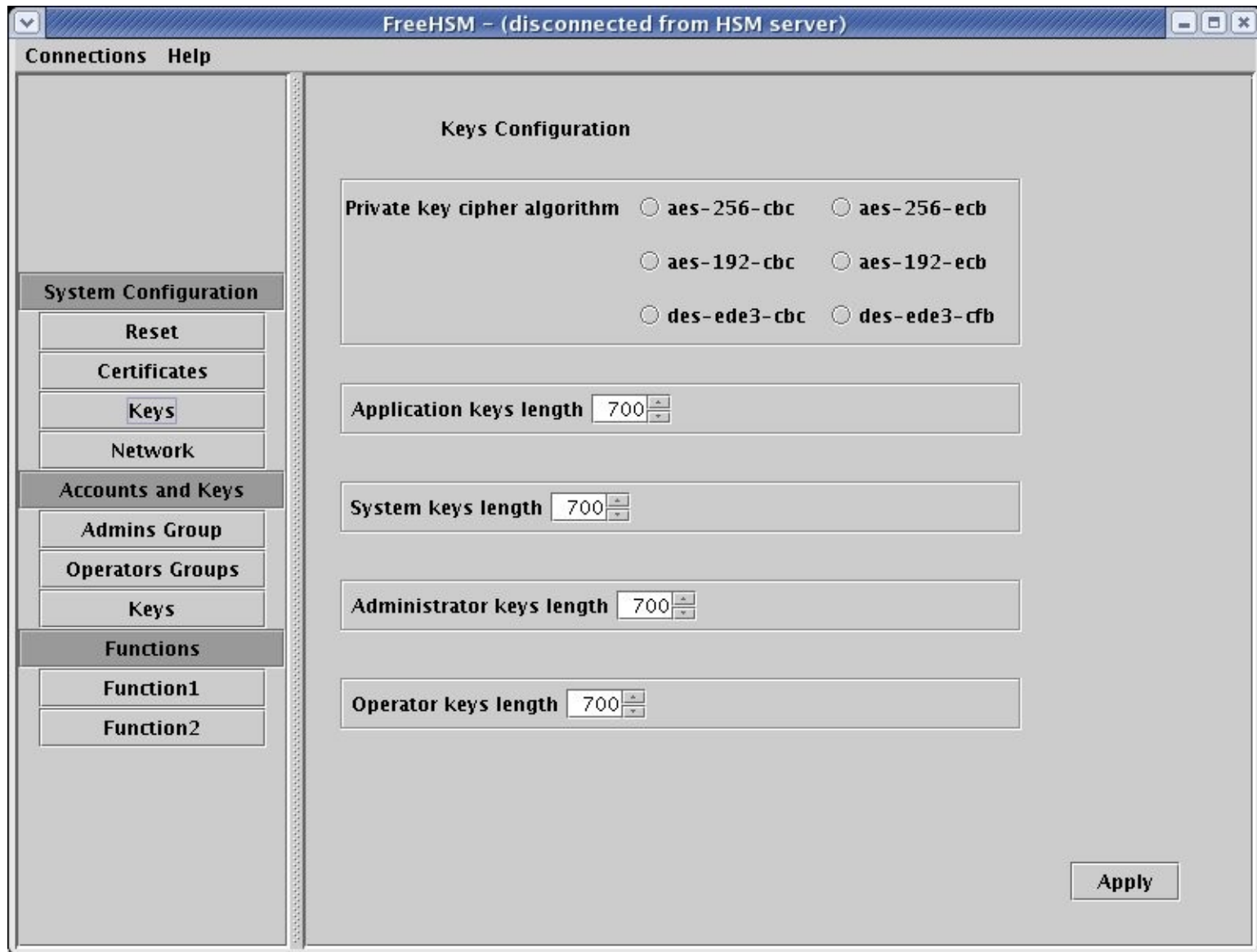
- Reset
- Certificates**
- Keys
- Network

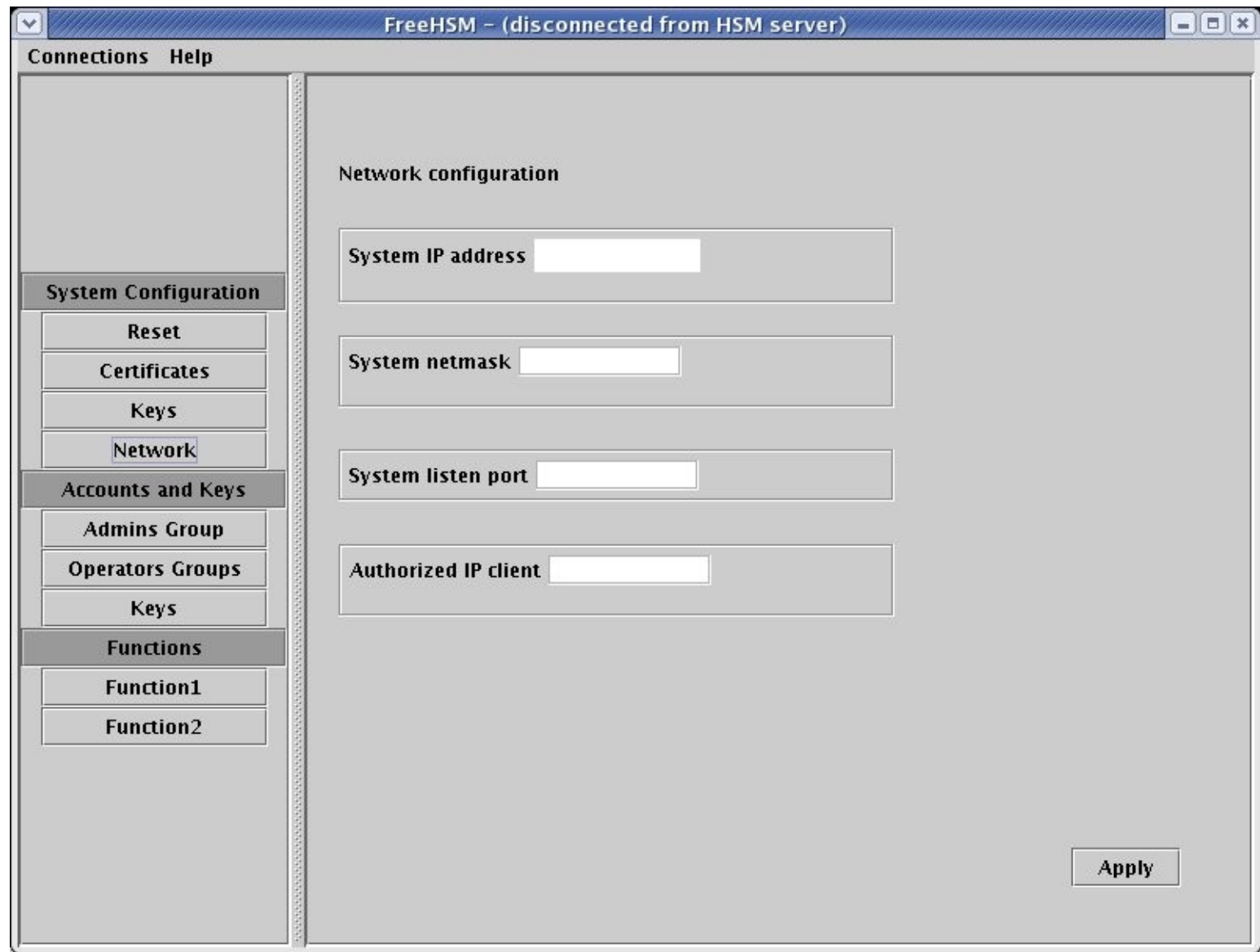
Accounts and Keys

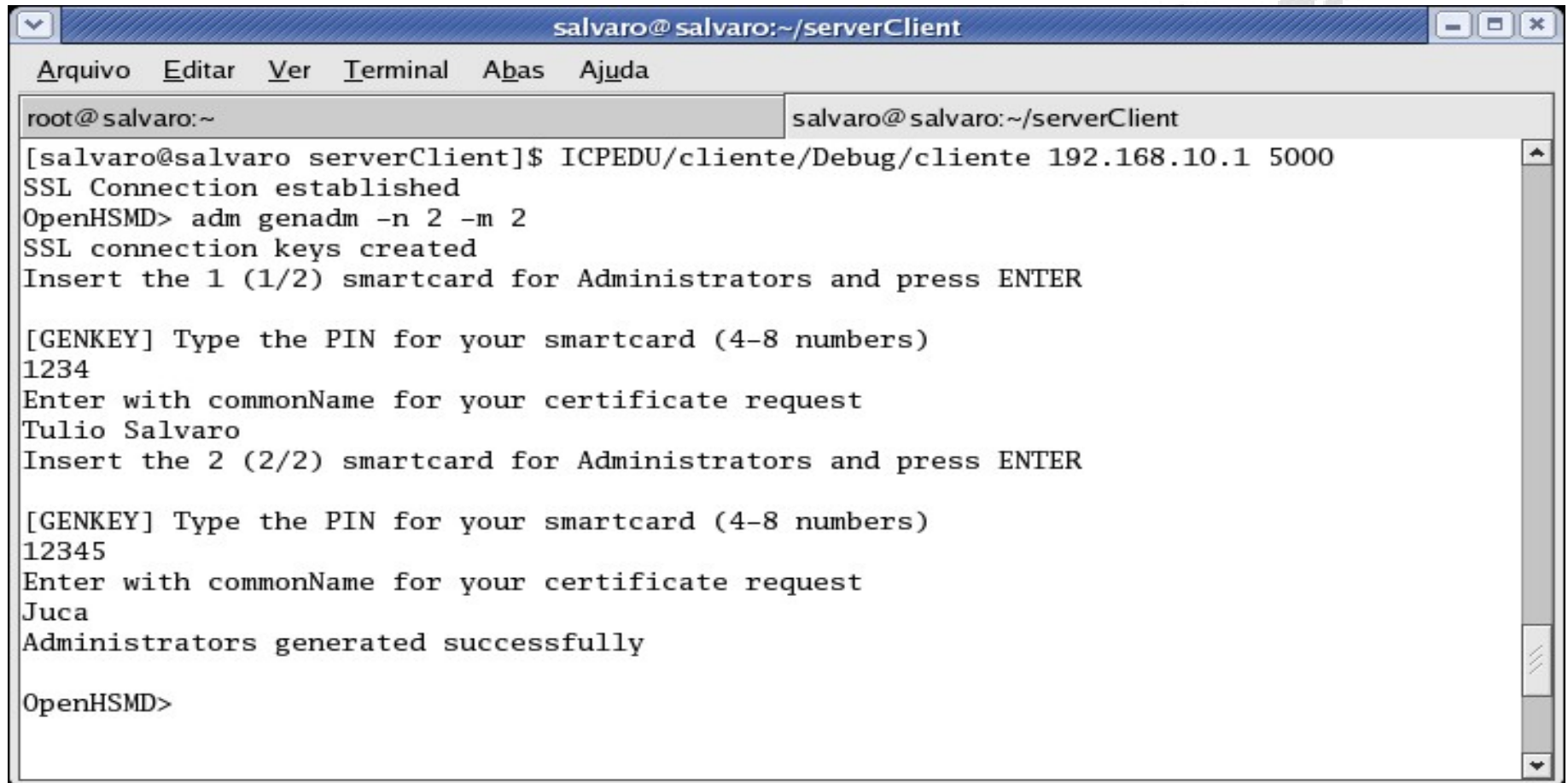
- Admins Group
- Operators Groups
- Keys

Functions

- Function1
- Function2







```
salvaro@salvaro:~/serverClient
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
root@salvaro:~
[salvaro@salvaro serverClient]$ ICPEDU/cliente/Debug/cliente 192.168.10.1 5000
SSL Connection established
OpenHSMD> adm genadm -n 2 -m 2
SSL connection keys created
Insert the 1 (1/2) smartcard for Administrators and press ENTER

[GENKEY] Type the PIN for your smartcard (4-8 numbers)
1234
Enter with commonName for your certificate request
Tulio Salvaro
Insert the 2 (2/2) smartcard for Administrators and press ENTER

[GENKEY] Type the PIN for your smartcard (4-8 numbers)
12345
Enter with commonName for your certificate request
Juca
Administrators generated successfully

OpenHSMD>
```

```
salvaro@ salvaro:~/serverClient
Arquivo Editar Ver Terminal Abas Ajuda
root@ salvaro:~
salvaro@ salvaro:~/serverClient
salvaro@ salvaro:~/serverClient
Arquivo Editar Ver Terminal Abas Ajuda
root@ salvaro:~
salvaro@ salvaro:~/serverClient
[salvaro@salvaro serverClient]$ ICPEDU/cliente/Debug/cliente -v 192.168.10.1 5000
SSL Connection established
OpenHSMD>
OpenHSMD>
OpenHSMD> adm genadm -n 2 -m 2
Checking if HSM already configured
** ERROR -> HSM without configurations
OpenHSMD>
```

```
salvaro@salvaro:~/serverClient
Arquivo Editar Ver Terminal Abas Ajuda
root@salvaro:~ salvaro@salvaro:~/serverClient
[salvaro@salvaro serverClient]$ ICPEDU/cliente/Debug/cliente 192.168.10.1 5000
SSL Connection established
OpenHSMD> hsm init
# Certificates configuration
Enter values for the following parameters:
* A suitable description for the certificate:
Comentario
* Country name (2 letter code):
BR
* State or Province Name (full name):
Santa Catarina
* Locality Name (eg, city):
Florianopolis
* Organization Name (eg, company):
UFSC
* Organizational Unit Name (eg, section):
LabSEC
* Common Name (eg, your name or your server's hostname):
GT ICP EDU II
*Days until HSM's certificate expires (eg, 700):
500
* Days until administrator's certificate expires (eg, 700):
500
* Days until operator's certificate expires (eg, 700):
500
* Days until SSL certificate expires (eg, 700):
500
# Keys configuration
Enter values for the following parameters:
* Private key cipher algorithm (eg, aes-256-cbc):
aes-256-cbc
* Application key length (eg, 1024):
1024
* Application key length (eg, 1024):
1024
* HSM's key length (eg, 1024):
1024
```

```
salvaro@salvaro:~/serverClient
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
root@salvaro:~ | salvaro@salvaro:~/serverClient
* Administrator's keys length (eg, 1024):
1024
* Operator's keys length (eg, 1024):
1024
# Network configuration
Enter values for the following parameters:
* HSM's IP Adress (eg, 150.162.1.1):
192.168.10.1
* HSM's netmask (eg, 255.255.255.0):
255.255.255.0
* HSM's listen port (eg, 5000):
5000
* Authorized HSM client's IP Adress (eg, 150.162.1.1):
192.168.10.2
HSM Configured successfully. Rebooting now
[salvaro@salvaro serverClient]$
```

Considerações Finais

- Próximos Passos
 - Hardware Próprio
 - Previsão 2005
 - Implantação de ICPs nas Universidades
 - Treinamento / Capacitação
 - ICP da RNP usando Sala Cofre
- HSM marca RNP

Questões?

