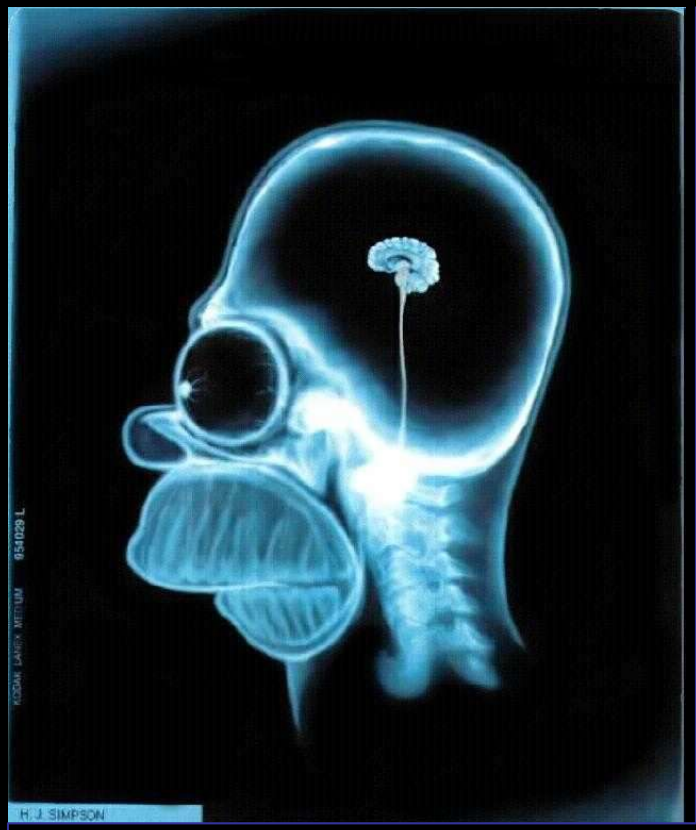


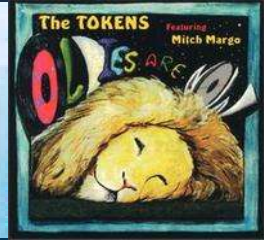
APLICAÇÕES PARA TOKENS E CARTÕES PROCESSADOS EM AMBIENTE DE SOFTWARE LIVRE

Nelson Murilo <nelson@pangeia.com.br>

Agenda

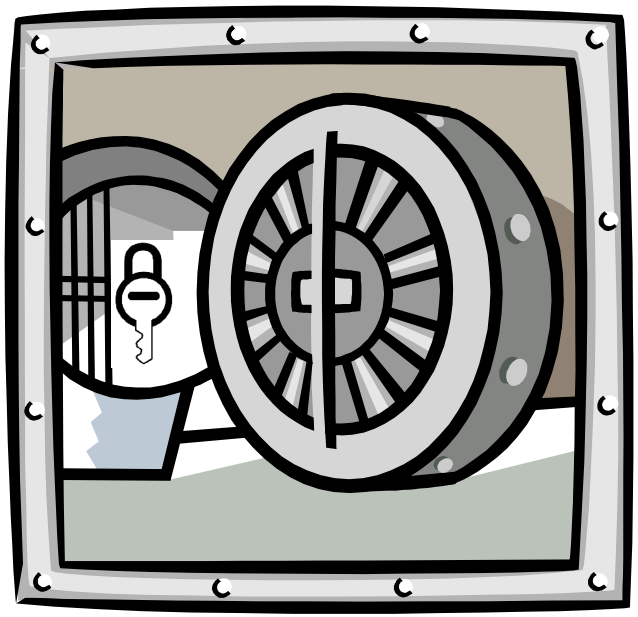
- Armazenamento
- Conceitos
- Aplicações
- Tipos de cartões/tokens
- Organização interna
- Ferramentas
- Exemplos de uso
- Futuro

Armazenamento

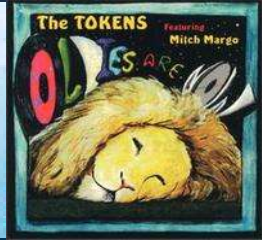


Problema:

Armazenamento da chave privada



Armazenamento

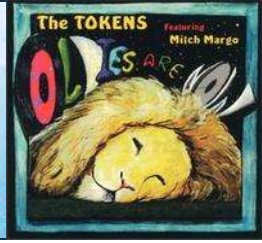


Soft Certificates

- A chave pode ser copiada
- Armazenada em HD's, disquetes, memórias USB e cartões de memória (Compact Flash, SD, SmartMedia,etc)

Vantagens	Desvantagens
Flexível	Volátil
Cópia de segurança	Risco caso a senha seja copiada, fraca ou inexistente

Armazenamento

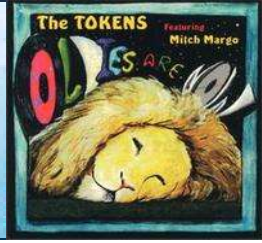


Hard Certificates

- A chave não pode ser copiada
- Armazenada em tokens e cartões processados

Vantagens	Desvantagem
Maior segurança	Em geral não existe backup
Pouco volátil	

Armazenamento



Private Key Object; RSA 1024 bits
label: Private Key
Usage: decrypt, sign, unwrap
Certificate Object, type = X.509 cert
label: /C=BR/O=ICP-Brasil/OU=MJ/CN=Nelson Murilo de Oliveira Rufino
Public Key Object; RSA 1024 bits
label: /C=BR/O=ICP-Brasil/OU=MJ/CN=Nelson Murilo de Oliveira Rufino
Usage: encrypt, verify

Usuário

Certificate Object, type = X.509 cert
label: /C=BR/O=ICP-Brasil/OU=CSPB-1/CN=Autoridade Certificadora do SERPRO
Public Key Object; RSA 2048 bits
label: /C=BR/O=ICP-Brasil/OU=CSPB-1/CN=Autoridade Certificadora do SERPRO
Usage: encrypt, verify

AR

Certificate Object, type = X.509 cert
label: /C=BR/O=ICP-Brasil/OU=Instituto Nacional de Tecnologia da Informacao - ITI/L=Brasilia/ST=DF/CN=Autoridade Certificadora Raiz Brasileira
Public Key Object; RSA 2048 bits
label: /C=BR/O=ICP-Brasil/OU=Instituto Nacional de Tecnologia da Informacao - ITI/L=Brasilia/ST=DF/CN=Autoridade Certificadora Raiz Brasileira
Usage: encrypt, verify

AC

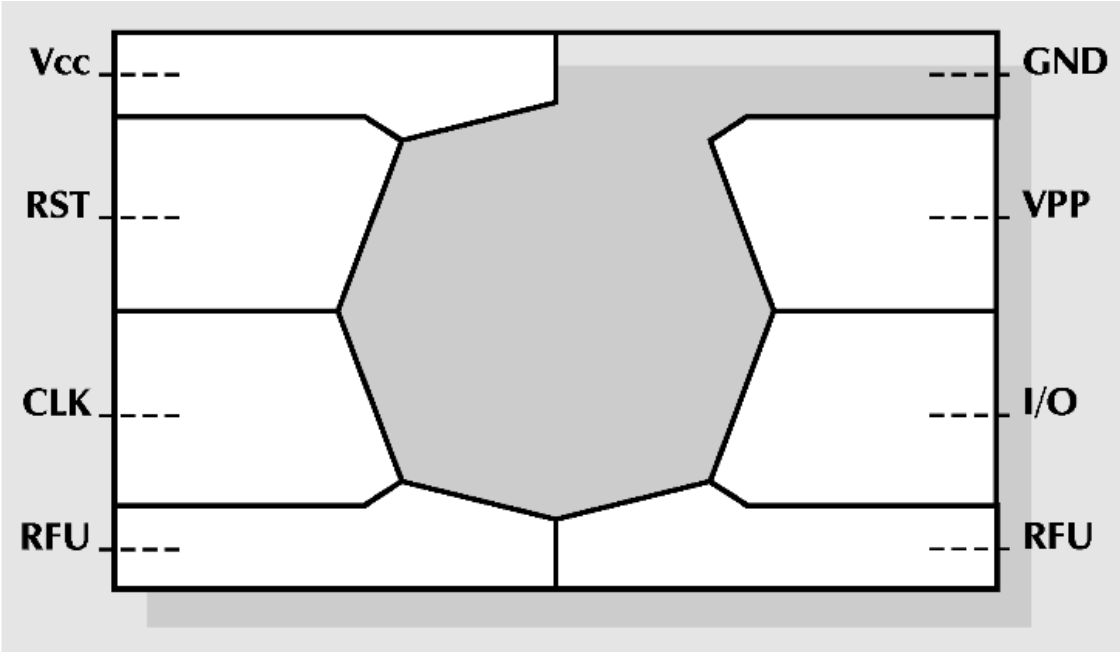
Conceitos

Norma ISO/IEC 7816

- Características físicas
- Dimensões e localização dos contatos
- Sinais elétricos e protocolos
- Linguagem padrão: *Structured Card Query Language (SCQL)*
- Requisitos mínimos de segurança
- ...

Conceitos

Características físicas

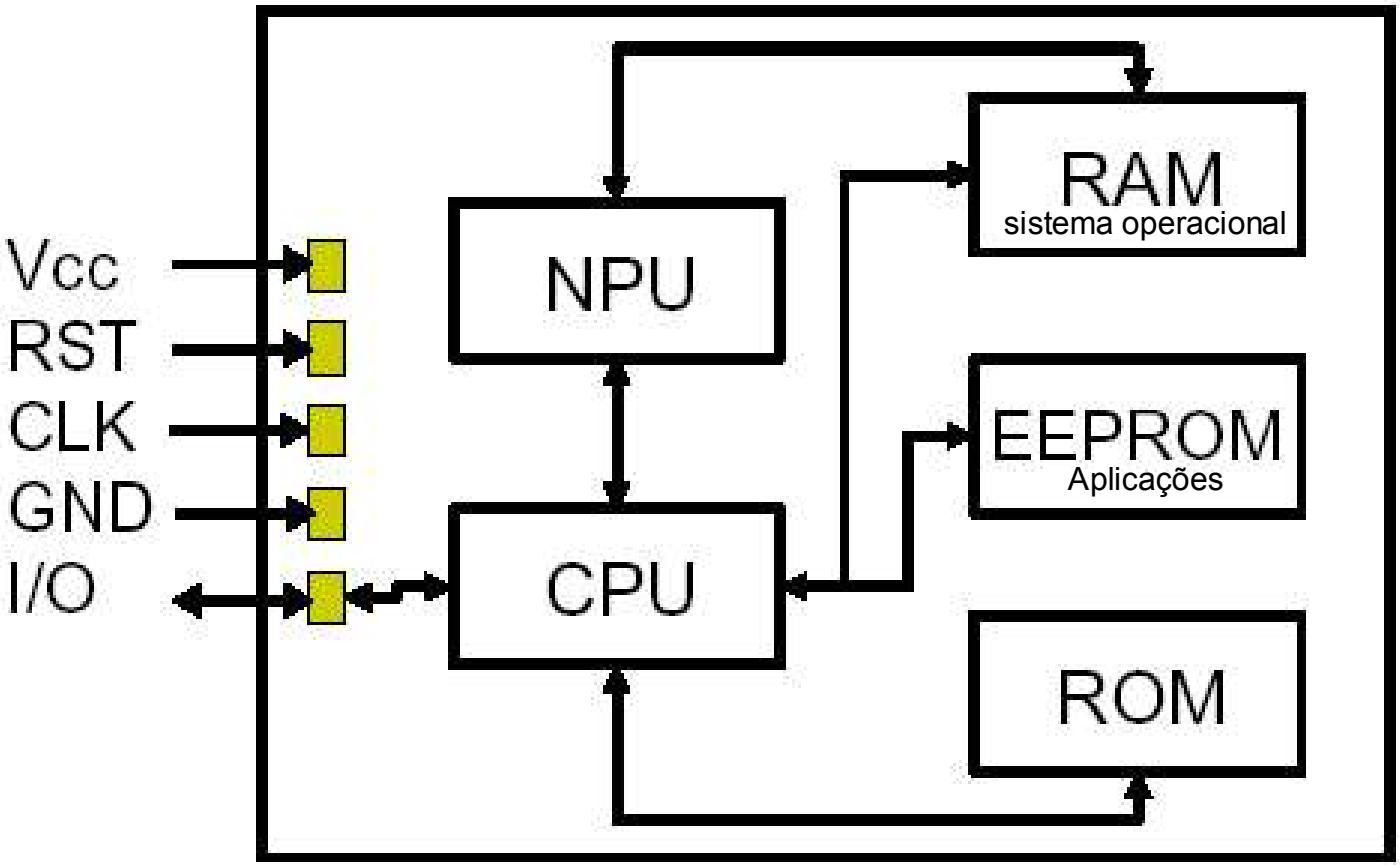


Vcc - Fonte de alimentação do chip
RST – Reset
CLK – Relógio
RFU – Reservado p/ uso futuro

GND – Contatos elétricos com o leitor
Vpp – Alimentação do módulo de programação
IO – Porta serial
RFU – Reservado p/ uso futuro

Conceitos

Características físicas



NPU - Numerical Processing Unit

Conceitos

Sinalização e operação

Connecting to card in reader Towitoko Chipdrive USB 0 0...
Using card driver: Schlumberger Multiflex/Cryptoflex
Card ATR: 3B 95 18 40 FF 62 01 02 01 04 ;..@.b....

Using card driver: Schlumberger Multiflex/Cryptoflex
Card ATR: 3B 95 15 40 FF 68 01 02 02 04 ;..@.h....

Using card driver: EMV compatible cards
Card ATR: 3B 6F 00 00 80 31 C0 52 02 77 64 02 19 04 32 83 ;
o...1.R.wd...2.83 90 00

Using card driver: EMV compatible cards
Card ATR: 3B 68 00 00 6A E1 10 00 00 4F 54 53 ;h..j....OTS

Conceitos

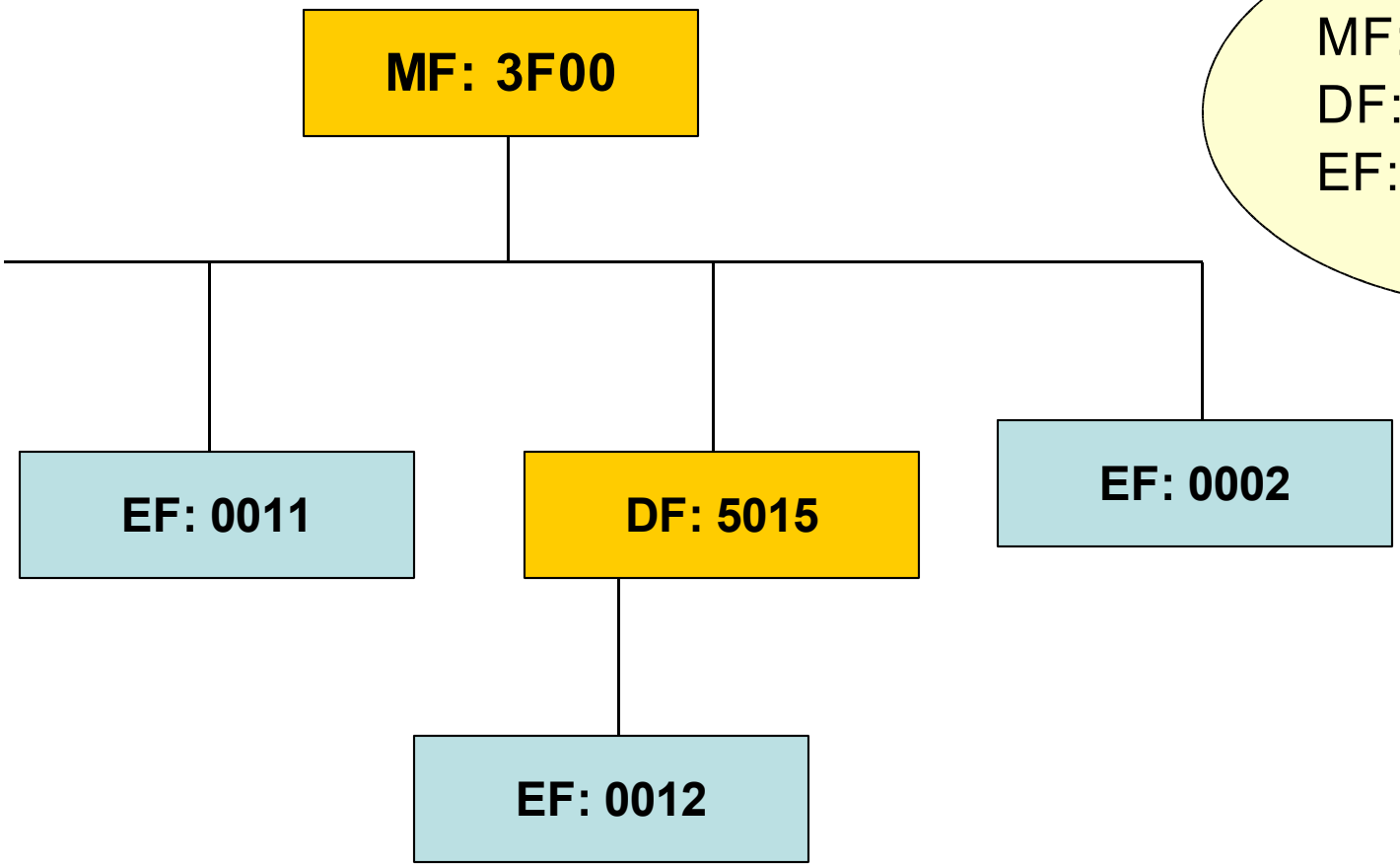
Componentes de software

- **Sistema operacional** (starcos, tcos, miocos, setcos, etc)
  - Autenticação (Chave de transporte/Transport key)
  - Controle de acesso (PIN/PUK)
- **Sistema de arquivos**
  - Diretórios e arquivos
  - Permissões (criação, leitura, acesso, etc)

Conceitos

Sistema de arquivos

MF: Master File
DF: Dedicated File
EF: Elementary File



Conceitos

Sistema de arquivos

Tipo de arquivo elementar

- Transparente: Arquivos comuns
- Linear fixo: Arquivos com registro de tamanho fixo
- Linear variável: Registro de tamanho variável
- Cíclico: Arquivo com apontador para o registro corrente (p.e.: arquivos de logs)

Conceitos

Sistema de arquivos

```
# pkcs15-tool -k
Card has 1 private key(s).

Private RSA Key [Private Key]
        Com. Flags  : 3
        Usage       : [0x32E], decrypt, sign, signRecover,
    unwrap, derive, nonRepudiation
        Access Flags: [0x1D], sensitive, alwaysSensitive,
    neverExtract, local
        ModLength   : 1024
        Key ref     : 0
        Native      : yes
        Path        : 3F00501530450012
```

Conceitos

Path : 3F00501530450012

 # opensc-explorer
OpenSC Explorer version 20031003
Connecting to card in reader Towitoko Chipdrive Micro 0 0...
Using card driver: Schlumberger Multiflex/Cryptoflex
OpenSC [3F00]> **ls**

FileID	Type	Size
0011	wEF	38
0002	wEF	8
[5015]	DF	1244
2F00	wEF	128

OpenSC [3F00]> **cd 5015**
OpenSC [3F00/5015]> **cd 4500**
OpenSC [3F00/5015/4500]> **ls**

FileID	Type	Size
0012	wEF	23

Conceitos

X.509 Certificate [/C=BR/O=ICP-Brasil/OU=MJ/CN=Nelson Murilo de Oliveira Rufino]

Authority: no

Path : 3F0050155501

X.509 Certificate [/C=BR/O=ICP-Brasil/OU=Instituto Nacional de Tecnologia da Informacao - ITI/L=Brasilia/ST=DF/CN=Autoridade Certificadora Raiz Brasileira]

Authority: yes

Path : 3F0050155502

X.509 Certificate [/C=BR/O=ICP-Brasil/OU=CSPB-1/CN=Autoridade Certificadora do SERPRO]

Authority: yes

Path : 3F0050155503

Conceitos

Public-Key Cryptograpy Standards (PKCS)

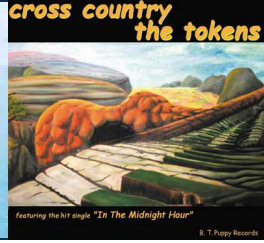
- PKCS #7 Mensagens criptografadas
- PKCS #11 API
- PKCS #12 Intercâmbio de informações
- PKCS #15 Armazenamento

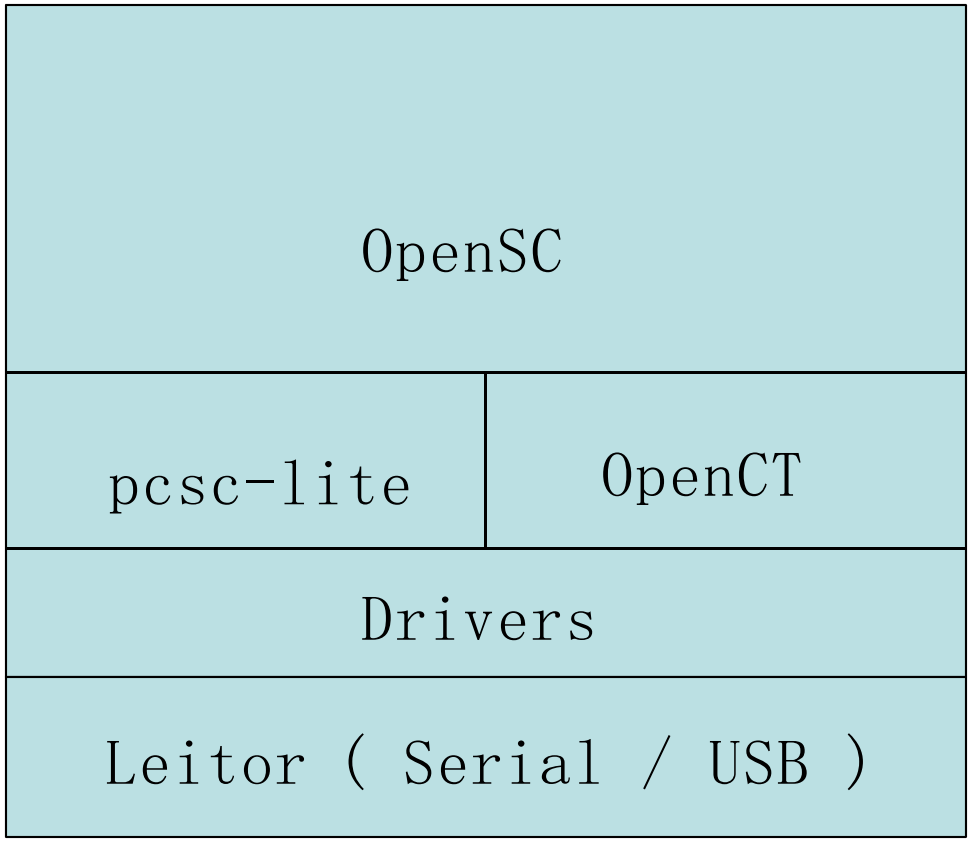
http://www.rsasecurity.com/rsalabs/pkcs

Tipos

Cartão	Token
Permite identificação visual	Facilidade de transporte
Necessita de leitor (serial / usb)	Interface USB
Mais robusto	Mais frágil, por conta do manuseio

Ambiente





pangeia

Aplicações

- Armazenamento máximo de 1GB
  (256MB em cartão magnético)
- Permite cópia e armazenamento de arquivos, como chaves e certificados (X.509, OpenPGP, etc)
- Permite cifração dos objetos armazenados
- Permite geração do par de chaves (RSA)

Aplicações

Possibilidades de uso

- Autenticação
  - Logon, senha única, etc
  - Aplicações WEB
  - Correio eletrônico

Assinatura/conferência de documentos
  - Correio eletrônico
  - Workflow / GED

Aplicações

- **Autenticação**
  - OpenSSH
  - PAM (login, su, passwd, etc)
  - GnuPG
  - Mozilla
  - Stunnel
  - Boot (linux e *bsd)
- **Assinatura/conferência de documentos**
  - Mozilla
  - Programas com suporte GnuPG

Exemplos de uso


```
$ head -2 /etc/pam.d/su
#%PAM-1.0
auth  required /lib/security/pam_opensc.so
$
$ su
Using card reader Towitoko Chipdrive USB 0 0
Enter PIN1 []: ********
#
```

Exemplos de uso


```
$ eval `ssh-agent`
Agent pid 13751
$ ssh-add -s 0
Enter passphrase for smartcard: ********
Card added: 0
$ ssh 10.61.3.120
Last login: Wed Nov  5 14:09:50 2003 from
10.61.5.79
Linux 2.6.0-test8.
$
```

Exemplos de uso

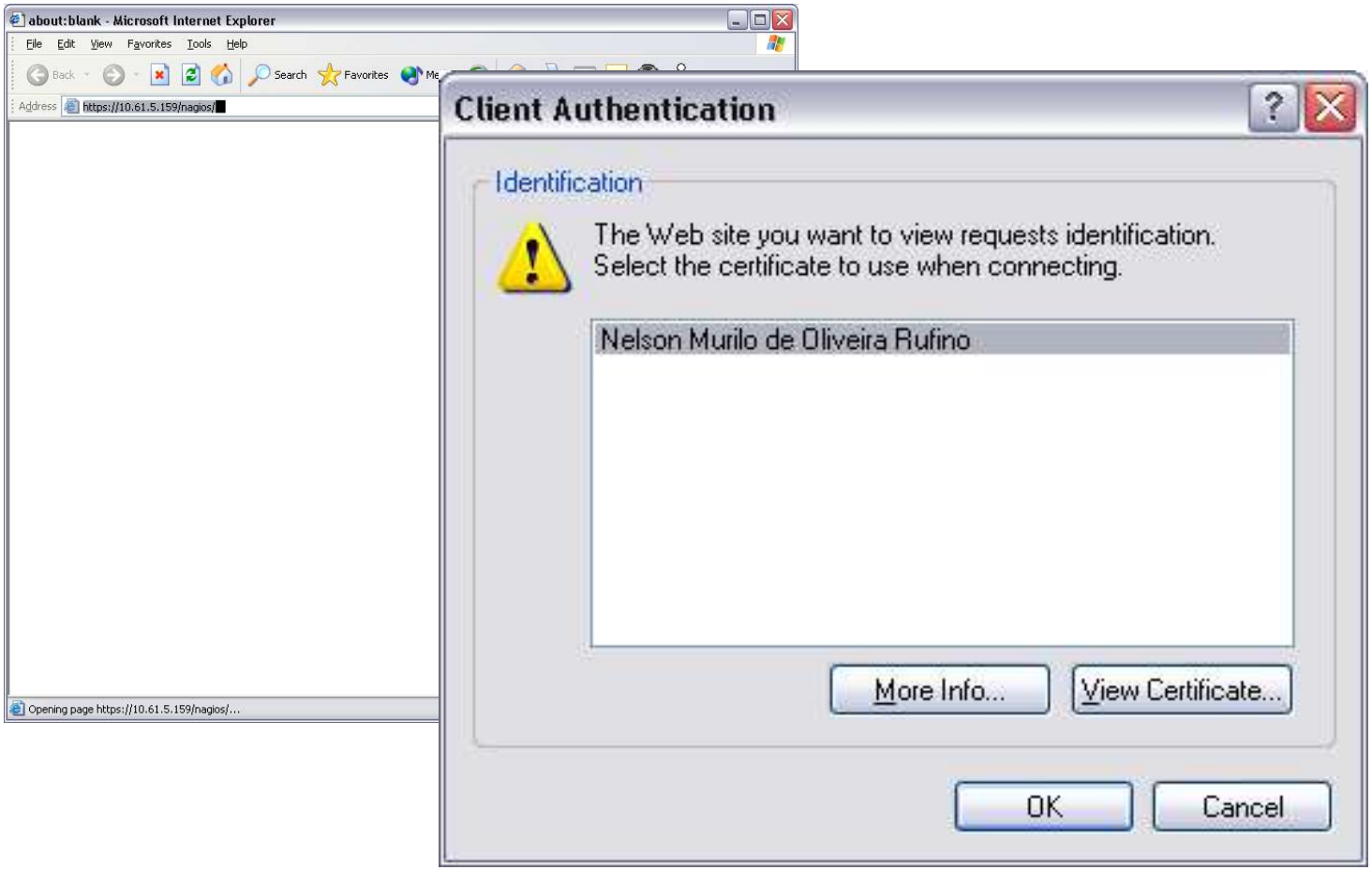
$ ssh nelson@10.61.3.120

Nov 5 15:00:01 abutre ssh-agent[13751]:
error: Unable to lock smartcard: Card removed
Agent admitted failure to sign using the key.
nelson@10.61.3.120's password:

Exemplos de uso


```
$ ssh  -I 0 10.61.5.159
Please enter PIN: *********
Last login: Tue Nov 25 14:04:02 2003 from
10.61.5.56
OpenBSD 3.3 (GENERIC) #0: Tue Apr 29
08:10:04 AMT 2003
$
```

Exemplos de uso



pangeia

Exemplos de uso

about:blank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address https://10.61.5.159/nagios/

Go Links

Opening page https://10.61.5.159/nagios/...

Internet

Cryptographic Service Provider

Nelson Murilo de Oliveira Rufino

Enter User Pass Phrase:

OK Cancel

pangeia

Exemplos de uso

Mozilla {Build ID: 2003102905}

File Edit View Go Bookmarks Tools Window Help Debug QA

https://[redacted]/nagios/

User Identification Request

This site has requested that you identify yourself with a certificate:

nagios.dpf.gov.br

Organization: "DPF"

Issued Under: "DPF"

Choose a certificate to present as identification:

OpenSC Card:/C=BR/O=ICP-Brasil/OU=MJ/CN=Nelson Murilo de Oliveira Rufino [05...

Details of selected certificate:

Issued to:
  Subject: CN=Nelson Murilo de Oliveira Rufino, OU=MJ, O=ICP-Brasil, C=BR
  Serial Number: 05:71
  Valid from 07/11/2003 14:31:43 to 07/11/2004 20:59:00
Issued by:
  Subject: CN=Autoridade Certificadora do SERPRO, OU=CSPB-1, O=ICP-Brasil, C=BR

OK Cancel Help

Connected to 200.[redacted]...

pangeia

Exemplo de uso

Nagios - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address https://10.61.5.159/nagios/ Go Links

Nagios

General
- Home
- Documentation

Monitoring
- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting
- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications

Tactical Monitoring Overview
Last Updated: Tue Nov 4 14:35:47 BRST 2003
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as *nagiosadmin*

Monitoring Performance

Check Execution Time:	0 / 4 / 0.750 sec
Check Latency:	0 / 0 / 0.000 sec
# Active Checks:	20
# Passive Checks:	0

Network Outages
0 Outages

Network Health
Host Health:
Service Health:

Hosts

0 Down	0 Unreachable	17 Up	0 Pending

Services
0 Critical

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Ch
Disabled N/A	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services

Done Internet

pangeia

Futuro

pangeia

Futuro

Problema:

Necessidade de contato

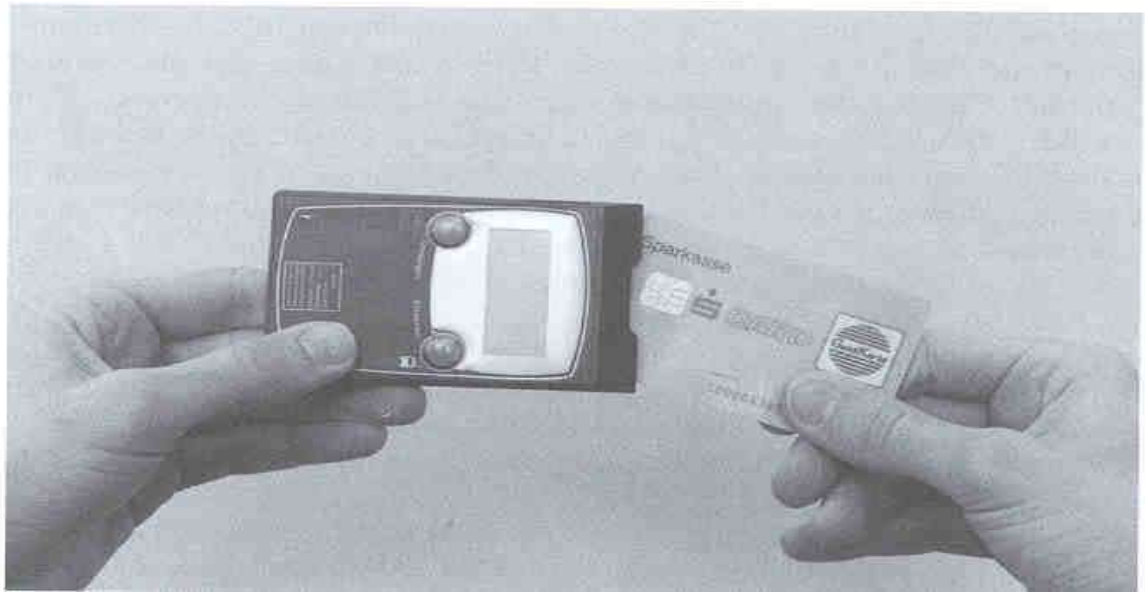
Solução:

Cartões sem contato (RF em geral)

http://www.ibutton.com
http://www.smartid.com.sg
http://www.st.com

Futuro

Compatiblidade com “legado”



Referências

OpenCT e OpenSC
http://www.opensc.org

M.U.S.C.L.E
http://www.linuxnet.com

pcsc-lite
http://alioth.debian.org/projects/pcsclite

Dúvidas ?

Obrigado

Nelson Murilo
<nelson@pangeia.com.br>