Fraunhofer-Institut für Digitale Medientechnologie IDMT

IDMT VPN Remote Access

Ives Steglich

Munich, 12. Oct 2004

Fraunhofer Institut
Digitale
Medientechnologie

Overview

Current Situation and Architecture

Goals and Requirements for Improvement

Proposed Soft- and Hardware

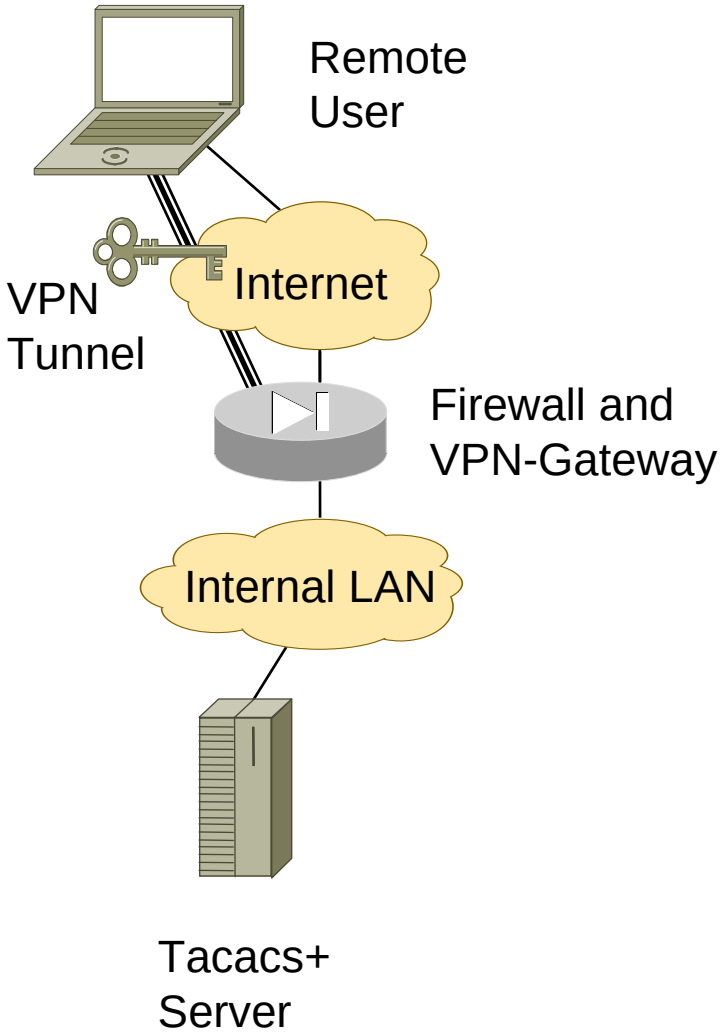
Proposed Architecture

How does the USB-Token work?

Usageprocess

Conclusions

Current Situation and Network Architecture



<u>Architecture</u>

Remote User
CISCO VPN Client

Firewall and VPN Gateway
CISCO PIX

<u>Steps to establish an connection</u>

1. VPN Tunnel initialization
   authenticated by shared secret

2. Access to internal Network
   authenticated by XAUTH trough tacacs+

Goals and Requirements for new Solution

Main Goals

1. remove the shared secret for remote users
2. keep the available infrastructure
3. use smartcards
4. be open for other usages
5. integration into the local LDAP
6. use open source whenever possible

Requirements from Goals and Architecture

- introduce certificates and administration
- setup an in-house pki
- pki must speak SCEP
- smartcards must be operable with linux and windows

Proposed Soft- and Hardware

Software for PKI

OpenCA

Reasons:

- understands SCEP
- can publish certs in LDAP
- open source
- good cooperation with development team

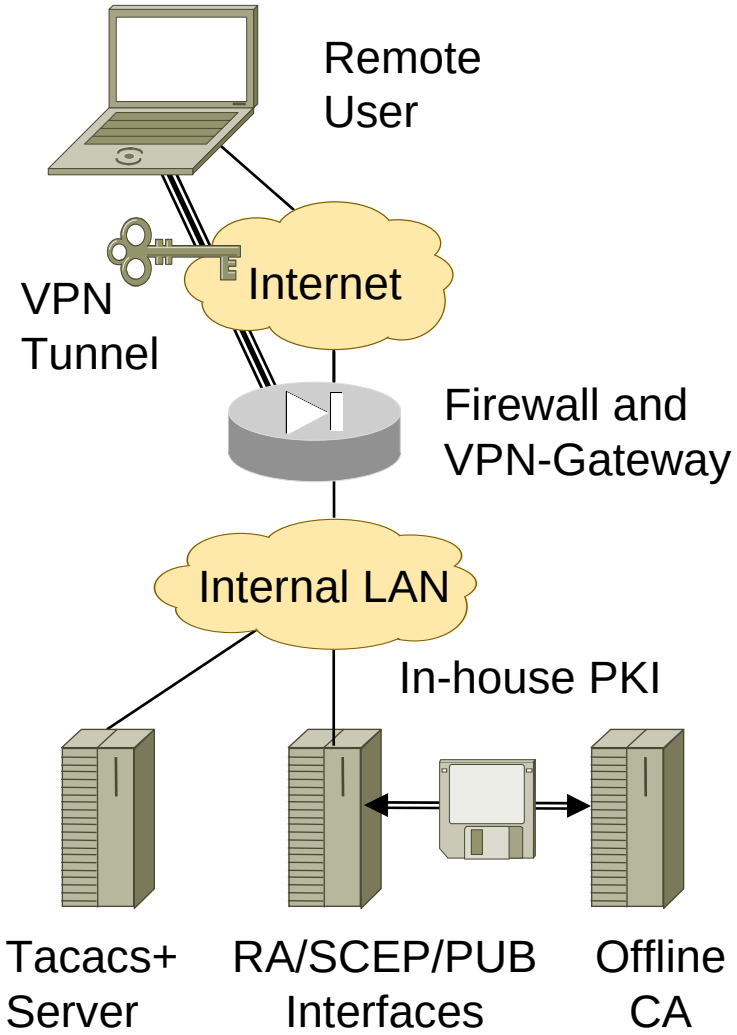
Hardware for Smartcards

Aladdin eToken Pro

Reasons:

- works with Microsoft Crypto API
- PKCS#11 library for linux available
  (but hard to get, not offically distributed)
- enables OpenCA administration from Linux
  and Windows (Mozilla, IE)

Proposed Architecture



OpenCA-Setup

One Server with RA, PUB and SCEP Interfaces
One Server with the CA (offline)

Access to RA-Interface certificatebased
stored at Smartcards

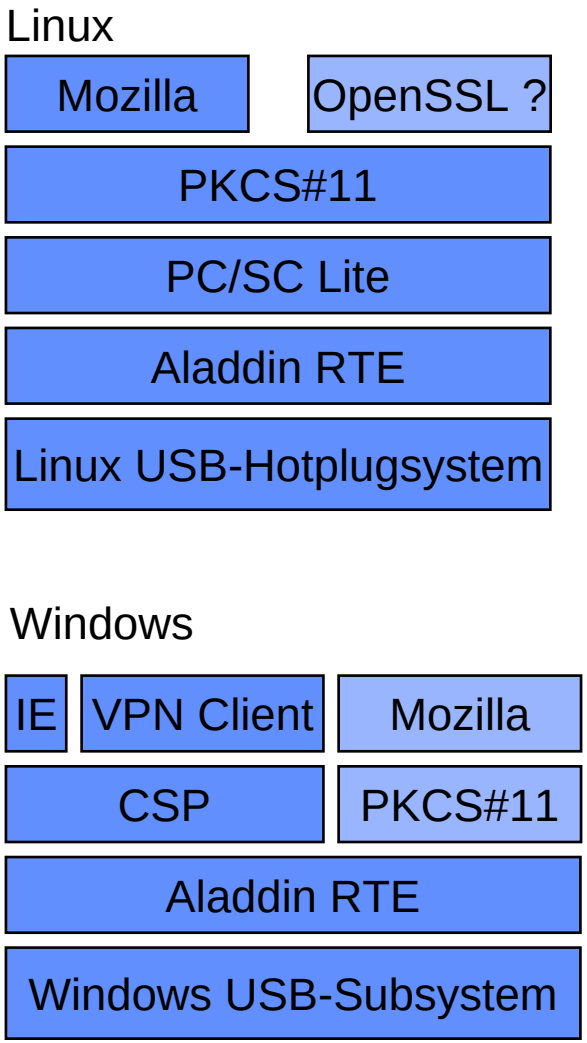
PIX-Setup

Remote Users Authentication with RSA Certs

Client Setup

VPN-Gateway identification with Certs
Own Authentication with RSA Certs

How does the USB-Token work?



General

- uses proprietary format from Aladdin
- therefore needs specific drivers
- not PKCS#15 compatible
  (but can be used parallel if space is left on token
  PKCS#15 doesn't works with Microsoft Crypto API)

Linux

- based on PC/SC-Lite
- works with Mozilla through PKCS#11
- doesn't work right now with OpenSSL engine
- hotplugable

Windows

- works with Mozilla through PKCS#11
- works with Microsoft Crypto API
- hotplugable

Fraunhofer IDMT Institut Digitale Medientechnologie

Usageprocess

Token Initialization

- has to be done at Linux
- key generation with Linux+Windows
- certificate Iistallation with Linux+Windows
- only one Login for User and Admin possible

Process

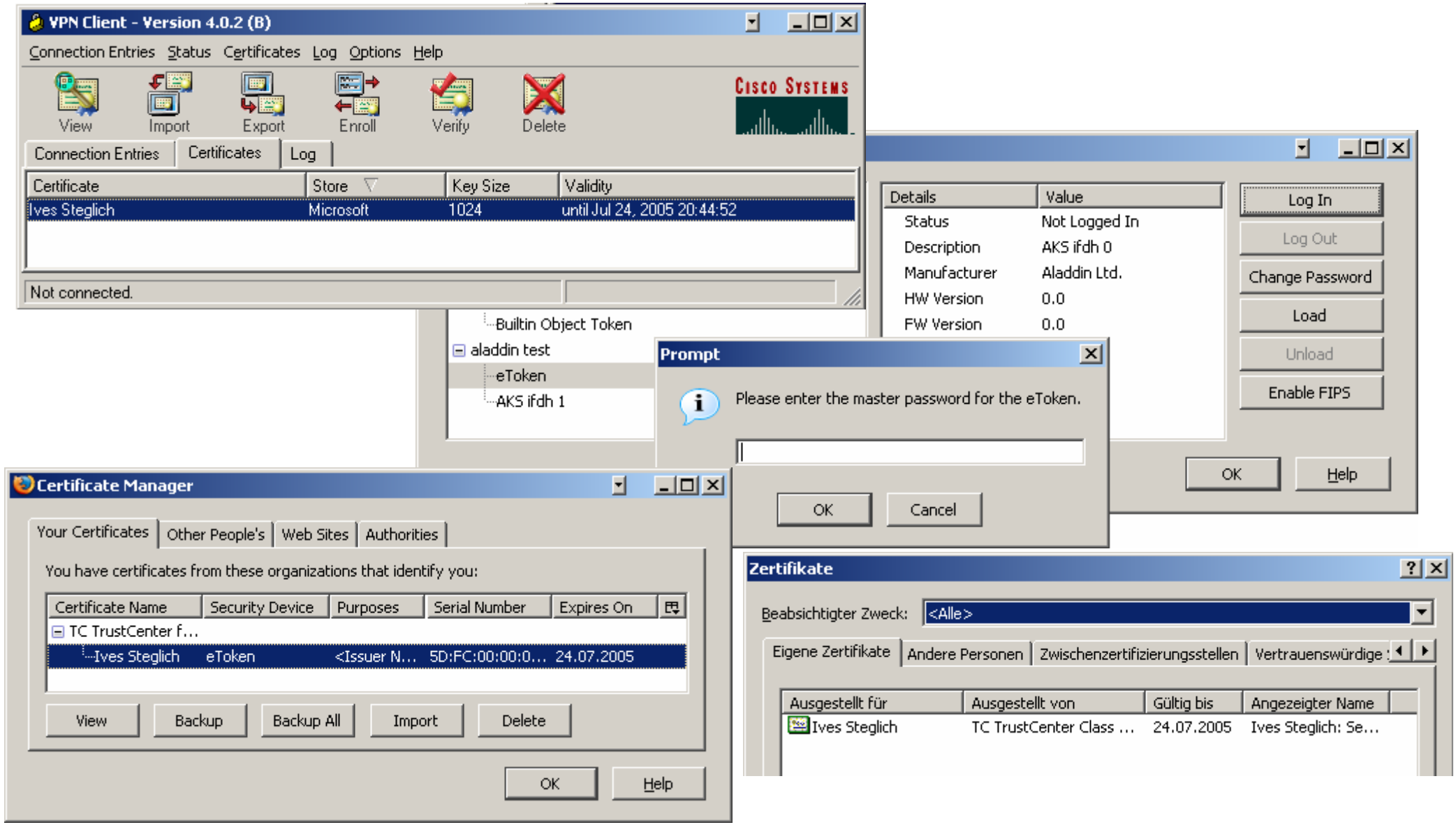
- Two Options:
  - batch-orientied serverside-key-generation
    (p12 files import through Mozilla or Win-System)
  - token-based-key-generation
    (through users themselves)

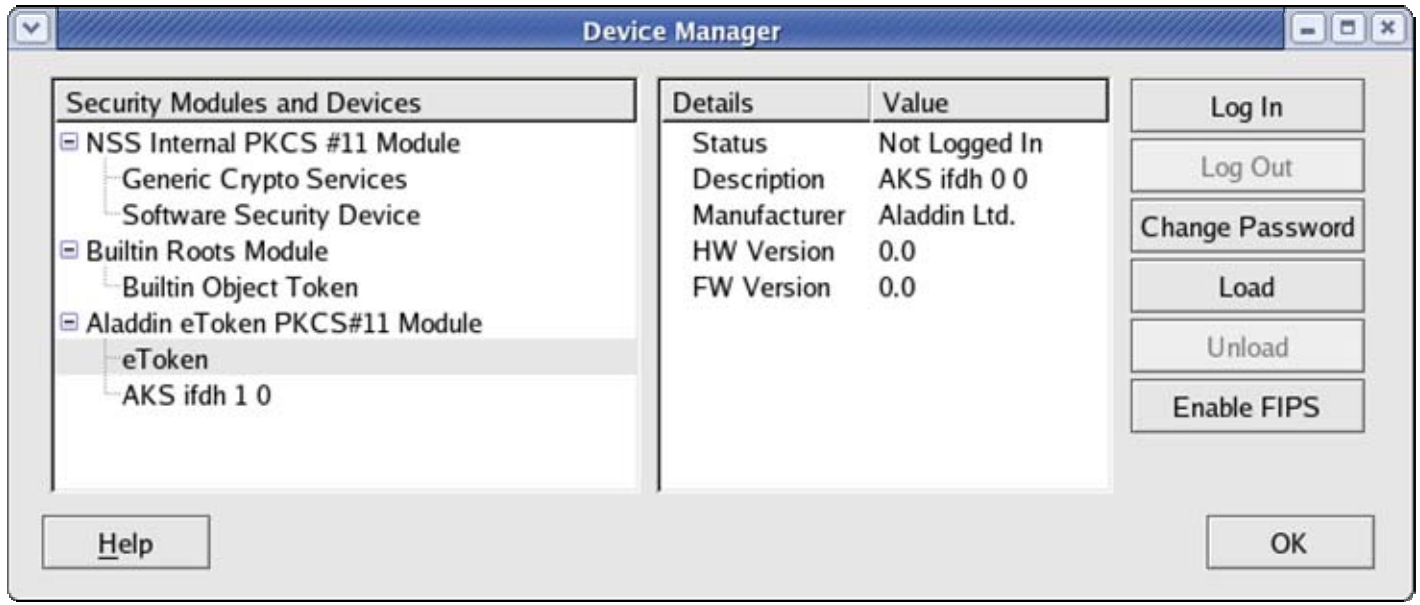
- Administration:
  - requests initiated through users
  - granted at RA through ‘Groupleaders’
  - certs issued through CA-Operator

Fraunhofer IDMT Institut Digitale Medientechnologie

Conclusions

- Authentication for Remote-VPN-Access
- Option to skip one step during VPN-Login
- Transparent usage with Linux and Windows
- Encrypt, Decrypt and Sign E-Mails
- Authentication for webbased services
  (PKI-Access and Administration)
- Dezentralized Management
- LDAP Storage and Access to Certificates
- Still not perfect
- Overview about smartcards providing PKCS#11 libs:
  http://jce.iaik.tugraz.at/products/14_PKCS11_Wrapper/
  tested_products/index.php


VPN Client - Version 4.0.2 (B)
Connection Entries Status Certificates Log Options Help
View
Import
Export
Enroll
Verify
Delete
Cisco Systems
Connection Entries
Certificates
Log
Certificate
Store
Key Size
Validity
Ives Steglich
Microsoft
1024
until Jul 24, 2005 20:44:52
Not connected.
Builtin Object Token
aladdin test
eToken
AKS ifdh 1
Details
Value
Status
Not Logged In
Description
AKS ifdh 0
Manufacturer
Aladdin Ltd.
HW Version
0.0
FW Version
0.0
Log In
Log Out
Change Password
Load
Unload
Enable FIPS
OK
Help
Prompt
Please enter the master password for the eToken.
OK
Cancel
Certificate Manager
Your Certificates
Other People's
Web Sites
Authorities
You have certificates from these organizations that identify you:
Certificate Name
Security Device
Purposes
Serial Number
Expires On
TC TrustCenter f...
Ives Steglich
eToken
<Issuer N...
5D:FC:00:00:0...
24.07.2005
View
Backup
Backup All
Import
Delete
OK
Help
Zertifikate
Beabsichtigter Zweck:
<Alle>
Eigene Zertifikate
Andere Personen
Zwischenzertifizierungsstellen
Vertrauenswürdige
Ausgestellt für
Ausgestellt von
Gültig bis
Angezeigter Name
Ives Steglich
TC TrustCenter Class ...
24.07.2005
Ives Steglich: Se...



Fraunhofer IDMT Institut Digitale Medientechnologie

Thanks for your attention!

Questions?

Fraunhofer IDMT Institut Digitale Medientechnologie