



# Authentication, Authorization and Public Key Infrastructures

Lecture – Part 3

9.5.2008

Dr. Elke Stangl, PKI Consultant

[www.punktwissen.com](http://www.punktwissen.com)

1

## Questions? Open Issues?

2

## Agenda: Lecture 3

1. Wrap-up PKI basics, cover open issues
2. Smartcards and tokens (User AuthN and AuthZ)
  - Certificate Enrollment Processes
3. Real Life Example of a CA hierarchy: Life times, revocation lists, processes, digital signatures
4. Authentication protocols used in networking (Machine AuthN and AuthZ)
  - RADIUS
  - EAP/802.1x
  - IPsec
5. Overview on related technologies
  1. Federation, meta-directories, identity frameworks
  2. XrML certificates and rights management

3

## Wrap-Up: PKI Basics and Labs

4

## Certificates and Keys

- Certificate associates key material and identity.
- Private keys stored in protected store at the client.
- Public key is sent to certification authority together with a request.
- Signatures are used to prove the identity of a client ("PKI subscriber") to an application or person ("Relying party")

5

## Infrastructure and Processes

- Directories hold:
  - Public keys of certification authorities
  - Public keys of end entities
  - Revocation Lists
- Requests may be subject to additional processes:
  - Inspection by a registration officer
  - Out-of-band / face-to-face check of identity
- Identity management has to be in place BEFORE certificates can be issued.

6

# Lab Infrastructure

- Demo / overview on components used in the lab:
  - LDAP Directory = Windows Active Directory
  - Directory contains users
  - Directory server is also Kerberos server, user logon using Kerberos
  - Windows certification authority, hierarchy with two levels
  - Certificate attributes are governed by certificate templates → also stored in directory
  - Enrollment of certificates: Via web site or via MMC (management console)
- The next section will introduce additional tools (not in the lab version) to support smartcard related processes.

7

# Smartcards and Hardware Tokens

Strong User Authentication

8

## Smartcards and Certificates

- Smartcard = hardware storage of cryptographic key and certificates.
- Two-factor authentication
  - Something you have
  - Something you know
- Typically issued to users
- Example of smart card for a machine:
  - Hardware security module (HSM) of certification authority: Tamper-resistant – "self-destruction"

9

## Intention / Agenda

- Smartcards / token are often used for authentication in a general sense (corporate security badge).
- In most European countries "citizen cards" are issued to citizen which can be used to authenticate various applications.
- Solutions are difficult to plan due to different requirements of IT and other departments, such as facility management.
- This lecture covers the "crypto part"
- In the IT world / crypto world smart cards are used to authenticate against a broader range of applications than software certificates.

10

## Why Smart Cards?

- Protection of the private key!
- Software stores
  - Protected by additional key, generated from passphrase or operating system password / user identifier.
  - Subject to brute force attack against passwords → may be performed offline, on a copy of the key store data
- Hardware stores
  - Operating system / middleware of the card prevents export of the key.
  - Brute force attack requires the physical card / token.

11

## Why Smart Cards? (2)

- Different client applications may expect to find the private key in different key stores (Windows store, PKCS#11)
- Smart card interfaces are typically supported by a broader range of applications.
  - Note: There are also software key stores used as "virtual smart cards" which are comparable to smart cards with respect to application support.

12

## Why Smart Cards? (3)

- Software certificates are bound to a software "profile" of a user or machine.
- If users need their private keys / certificates at different machines, keys have to roam.
- Challenges in software key roaming:
  - Fail safe write to network location
  - Usage of directories: Increase in size of data stored in the directory.
  - Has to be supported by every client
- Smart cards roam "by design"

13

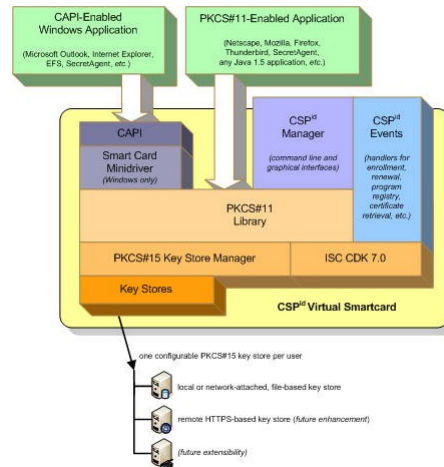
## Definition: Smart Cards

- Cryptographic chip → processor not only storage.
  - Combined devices available ("USB stick" + crypto chip)
- Programmable
- Secure storage for keys
- Shape may vary: credit card USB token
- A card / token may also hold different chips, such as RFID chips controlling physical access to buildings
- Require middleware to be used in operating systems and applications.

14

# Virtual Smartcards

- Example: CSPid by <http://www.infosecorp.com>
- "Looks like a smart card" to applications
- Software key storage file (encrypted) that can be accessed via various interfaces.



15

# Smart Card Usage

- Interactive logon → Kerberos tickets
- Logon to web application → certificate mapping
- Remote logon: VPN (Virtual Private Network)
- Code signing
- File or disk encryption
  - Note: Private keys should be recoverable – this depends on the smart card type

16

## Smart Card Selection Criteria

- Support of smart card middleware with different PKI clients / applications
- Cryptographic algorithms and key sizes
- Storage size: Number of keys that fit onto the smart card
- Combination of smart crypto chip with other chips on the same device
- Form factor: Usage as a company card (credit card shape) or combination with OTP token (one time password)
- Physical stability, life time

17

## Issuance of Smart Cards

- By the user himself or by a Registration Officers / Enrollment Agents
  - RO need to be trusted, because they issue authentication tokens to highly trusted persons.
  - Risk: A smart card permits an admin to logon as a user without the necessity of a password reset → the user does not notice the theft of credentials
- Submitted requests may required additional approval
- User might be permitted to renew the smart cards themselves. Example:
  - Initial issuance: By a registration officer
  - Renewal (\*). By the user himself as long as the user still has valid certificate.
  - (\*) Renewal = Issuance of new certificate (new request), but the new request is signed with the existing key.

18

## Processes and Roles

- The user and different administrators have different levels of permissions in the smart card lifecycle process
- Enroll for a card (for myself)
- Enroll for a card on behalf of another user
- Approve a pending request
- Retire a card
- Administrators act in roles based on some other kind of credentials (username / password or certificates).

19

## Registration Process and Identity

- (Remember general questions for lab 1)
- Automatic registration process can be based on credentials of the logged on user
  - User can be added to a group (without direct interaction with the user). On the next logon, the user is prompted to insert the card and enter the PIN
  - Issuance of strong authentication tokens is based on "weaker authentication".
- Chicken and egg problem: Issuance of tokens for identification has to be based on another process for identification

20

## Remember Lab 1

- Directory provides certificate templates (blueprints). Blueprints in lab 1 are used for issuing software certificates.
- To issue smart cards, "only" the key storage / cryptographic service provider needs to be changed.
- Templates are "published" at a certification authority before users and/or ROs can enroll for certificates
- New in this demo (because cards are used instead of software store): A card management / certificate management adds an additional interface: Exit module / policy module.

21

## Demo: Pre-Requisites

- Note: The card management software tool is not important – the tools just needs to provide support different processes and workflows.
- Middleware has to be installed
  - Cryptographic Service Provider
  - Tools for local management of the token / card
- User and/or registration officer need enrollment permissions (directory, database)
- A key pair is generated locally and the request is sent to a CA
  - Different tools might be used for submitting the request

22

## Card Management: Demo

- Microsoft Identity Lifecycle Manager is used to demonstrate typical card management functions
- Not only certificates and security principals need to be managed, but also the physical cards.
- Card lifecycle: Enrollment, renewal, replacement, retirement.
- Helpdesk task: PIN reset, issuance of temporary cards.

23

## Demo Details: Process Example

- Retire a card already managed by the card management system (otherwise not usable for other user) (as Administrator)
- Initialize the token: Erase existing key material (as Administrator)
- Enroll for new certificates: User self-service
- Approve a request a CA manager (=Administrator)
- Finish process as user by supplying additional information.
- Reminder – lab 2: Although less complicated, also SSL server certificate issuance needs some level of procedural control.

24

# Demo: Preparation of a Token

The screenshot shows the Microsoft Certificate Lifecycle Manager 2007 interface. The main window displays 'Review Details of a Smart Card Profile' for a smart card with serial number 0002DF0. The 'Smart Card Information' section lists details such as Provider (Aladdin Knowledge Systems Ltd), Card Type (Primary), Profile template name (\_Test 2 Smart Card Logon), and Smart card status (Active). An 'eToken Initialization Parameters' dialog box is open, showing options to initialize the eToken, create a user password, and create an administrator password. The 'Current Password' field is empty, and the 'Use Password' checkbox is unchecked.

25

# Demo: Self-Enrollment

The screenshot shows the Microsoft Certificate Lifecycle Manager 2007 interface for self-enrollment. The 'Select a Profile Template' dialog is open, showing two options: '\_Test 2 Smart Card Logon' and 'eToken SC Logon 3'. The 'Data Collection' section is active, with a 'Sample Data Item' field containing 'Some other name' and a 'Comments' field containing 'I am requesting certs. for a card'. The 'Request Status' section shows the request type as 'Enroll', profile template as '\_Test 2 Smart Card Logon', and current status as 'Pending'. The 'Request Status' section also displays the enrollment agent required (checked), submitted date of request (Sunday, June 17, 2007 12:34:08 PM), completed date of request (Not complete), target user (GALAXYtest), originating user (GALAXYtest), and request priority (0).

26



# Demo: Correct CRL Error and Finish

**Enrollment Request Wizard** Help

Processing error: Error generating requested certificates. The operation completed successfully, 0x0 (WIN32: 0)

Your enrollment request is being processed. Do not remove your smart card from the reader.

Please wait ...

**Enrollment**  
Generating certificate requests and submitting them to the certificate authorities ...

Retry Cancel

**Certificate Revocation List**

General | Information

Certificate Revocation List Information

| Field                 | Value                            |
|-----------------------|----------------------------------|
| Issuer                | xy                               |
| Requestor             | Everything Issuing CA, gals, xy  |
| Creation date         | Sunday, 17. Jun 2007 10:13:20    |
| Next update           | Monday, 18. Jun 2007 10:13:20    |
| Signature algorithm   | SHA256                           |
| Authority Key Idem... | KeyID#1 at 17:50:23 to 46:50:... |
| CA Name               | xy                               |
| CA Number             | 01                               |
| Next CRL Publish      | Monday, 18. Jun 2007 10:29:29    |
| Valid                 | Monday, 18. Jun 2007 10:13:20    |

**Certification Authority**

Everything Issuing CA

| Request ID | Revocation Date  | Status      |
|------------|------------------|-------------|
| 67         | 25.05.2007 15:30 | Unspecified |
| 68         | 01.06.2007 15:33 | Unspecified |
| 69         | 01.06.2007 18:16 | Unspecified |
| 70         | 04.06.2007 10:20 | Unspecified |
| 71         | 04.06.2007 11:36 | Unspecified |
| 72         | 04.06.2007 17:36 | Unspecified |
| 73         | 04.06.2007 12:30 | Unspecified |
| 74         | 04.06.2007 13:41 | Unspecified |
| 75         | 04.06.2007 15:16 | Unspecified |
| 76         | 04.06.2007 16:54 | Unspecified |
| 77         | 04.06.2007 18:14 | Unspecified |
| 78         | 13.06.2007 10:40 | Unspecified |
| 79         | 13.06.2007 11:24 | Unspecified |

**Certificate Revocation List**

General | Information

Certificate Revocation List Information

| Field                 | Value                            |
|-----------------------|----------------------------------|
| Version               | V3                               |
| Issuer                | Everything Issuing CA, gals, xy  |
| Creation date         | Sunday, 17. Jun 2007 12:46:21    |
| Next update           | Monday, 18. Jun 2007 12:46:21    |
| Signature algorithm   | SHA256                           |
| Authority Key Idem... | KeyID#1 at 17:50:23 to 46:50:... |
| CA Name               | xy                               |
| CA Number             | 01                               |
| Next CRL Publish      | Monday, 18. Jun 2007 12:56:23    |
| Valid                 | Monday, 18. Jun 2007 01:06:21    |

**Request Complete** Help

The following summarizes the request that was just executed.

**Request Summary**  
For more details about the request, click the request type.

Request type: **Enroll**  
Request status: **Completed**  
Request originator: **GALAXYTest1**  
Date of submission: **Sunday, June 17, 2007 12:34:08 PM**

**Smart Card Summary**  
For more information, click the profile name.

Smart Card: **Aldin Knowledge Systems Ltd.:0002zfc**  
Status: **Active**

Main Menu

29

# Demo: Certs. on Token

**eToken Properties**

eToken

Advanced Initialization Refresh Help

eTokenUser [PRO]

Details Settings Certificates & keys Administrator

Test 1  
Exchange key <SmartCard\CO5000000248cc810...

Delete... Import CA Chain... Set as Default Key Protection... AIX Key

Version: V3  
Serial number: 14 a1 8a c0 00 00 00 00 55  
Signature algorithm: RSA\_SHA1RSA  
Issuer: xy, gals, Everything Issuing CA  
Valid from: Sunday, June 17, 2007 10:50:12 AM  
Valid to: Monday, June 16, 2008 10:50:12 AM  
Subject: xy, gals, I1PDemo, Test 1

Import Certificate... More... Refresh

Test 1  
Smart card credential  
test1@gala.xy

.....

**Windows Security**

Enter your credentials  
These credentials will be used to connect to 192.168.0.33.

galaxy/administrator  
Password

Use another account

Test 1  
Smart card credential

Remember my credentials

OK Cancel

**Log On to Windows**

Microsoft  
**Windows Server 2003**  
Enterprise Edition

Copyright © 1985-2003 Microsoft Corporation

PIN: .....

OK Cancel Shut Down... Options <<

30

## Card Management Essentials

- Either the user has to be given permissions to enroll on his/her own ("self-service") or an "officer" has to create cards for the user.
- Renewal may be different from initial enrollment.
- Cards may be lost or physically damaged and need to be retired and replaced. The certificate has then to be revoked (and the correct revocation reason should be supplied).
- If a card is only lost temporarily, the certificate may be suspended (revocation reason on hold) and reinstated later. During the suspension period users may be issued temporary replacement cards.

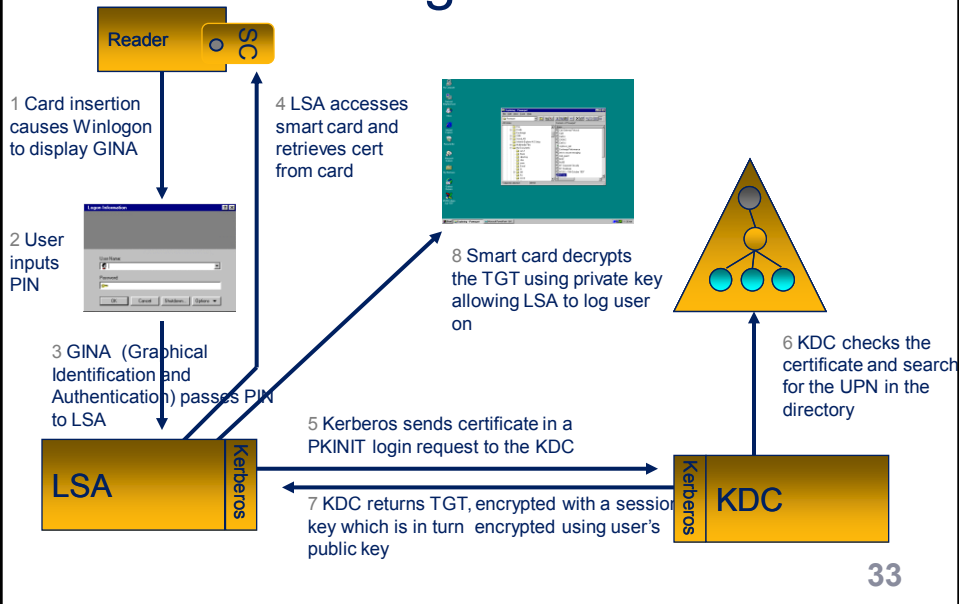
31

## Example: Austrian Citizen Card

- Issued to citizen by trusted registrars (e.g. banks). No self-service
- The user is responsible for notifying the certification authority service center when the card is lost, stolen or damaged.
- Cards may contain qualified or advanced signatures: Distinguished by certificate policies and practices = different processes used in generating and managing keys of CAs and end-entities.

32

# Smart Card Logon and Kerberos



## Mutual Authentication

- Kerberos Distribution Center (Domain Controller) also authenticates to the user.
- The user can be sure to talk to a trusted authentication server!
- Note: Machine certificates need to be issued to domain controllers:
  - Automatic enrollment recommended
  - Risk of interruption of authentication services high.

## Remember Lecture 1: Attributes

- Demo: Certificates needed for smart card logon
- Special attributes are validated:
  - User:  
Extended Key Usage = Smart Card Logon
  - Domain Controller (At least one of these)  
Extended Key Usage = Smart Card Logon  
Subject Alternative Name = GUID  
(GUID: special ID in the directory)

35

## Remember Lecture 1: Revocation Lists

- Smart card logon enforces the validation of revocation lists.
- Consequences: Smart card logon breaks immediately if any revocation list in the certificate chain is either not there or expired
- Logon to a web application: CRL checking depends on browser settings.

36

## Example of a Real-Life PKI

Signing PDF Documents with  
smart cards using Time Stamps

37

## Intentions for Choosing this Scenario

- Demonstration of PKI principles
- Life Times and Long-Time Planning in real world.
- Certificates involved can be downloaded from the internet and inspected
- Different certificate chains involved (real-world complexity)

38

## Digital Signatures on PDFs

- [http://www.adobe.com/devnet/acrobat/pdfs/digisig\\_in\\_acrobat.pdf](http://www.adobe.com/devnet/acrobat/pdfs/digisig_in_acrobat.pdf)  
(This is also a signed document)
- Provide proof of: Integrity of the document and authenticity of the creator.
- Hash value of document is encrypted using the user's private key
- Additional challenge: Signatures may need to be verified years after all included services have "died".
  - The point of time the signature has been made needs to be compared to end of life dates or revocation dates.

39

## Signature Options

- Choice of user certificate
  - Certificate may need to fulfill different legal requirements, depending on the type of document. Official authorities publish lists of suitable certification authorities (e.g. <http://signatur.rtr.at/en/providers/services.html>)
  - Electronic invoices in Austria → Advanced signature
  - Electronic invoices in Germany → Qualified signature.
- Choice of application used for creating signatures: Adobe Acrobat,... ("subscriber")
- Choice of application used for verification of signatures ("relying party")
- Choice of way the time is calculated
  - User's computer's system time
  - Time stamp created by Time Stamping authority

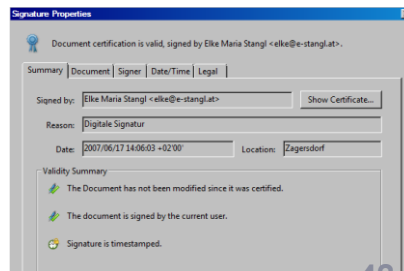
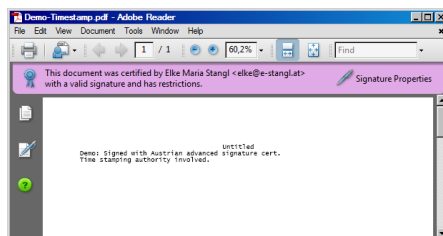
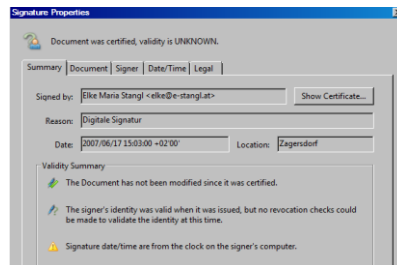
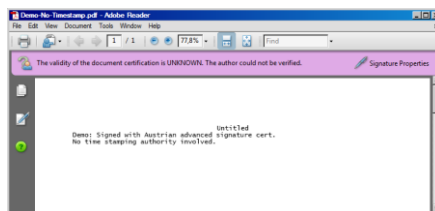
40

# Example: Citizen Card used for PDF Signature

- Demo documents provided together with these slides
  - With time stamp
  - Without time stamp
- Cached (expired) CRLs provided as well
  - Demo: Inspection of CRLs, details: cerutil <cer>.crl
- When validating machine is offline and/or CRLs are outdated (e.g. after CA service is terminated)...
  - Expired CRLs are available and are copied into Adobe Acrobat's CRLCache folder (C:\<ProfileFolder>UserName>\AppData\Roaming\Adobe\Acrobat\8.0\Security\CRLCache)
  - Validation only works when time stamps have been used
  - The validating application / relying party (Adobe Acrobat Reader) is using the expired CRLs

41

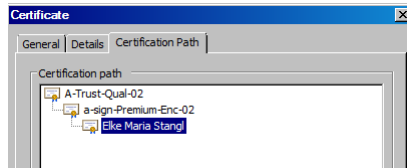
## Demo: Summary



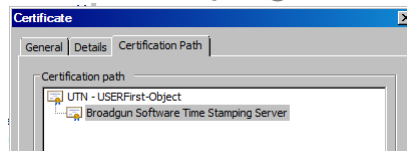
42

## Involved CA Hierarchies

- User Certificate



- Time Stamping Server



43

## Life Time Nesting

- (see also: PKI section in lecture 1 – CA hierarchies)
- Demo: Inspection of CA certificates (distributed with these slides)
  - Issuing CA and Root CA have the same validity period
  - Issuing CA's end of life is after Root CA's end of life
- Some CAs enforce strict life time nesting
  - Subordinate CA may not live longer than the parent CA
  - If CA life times would be chosen according to the demo certificates and never renewed, a user certificate issued near Dec. 2014 would be issued with a life time shorter than the intended one.

44

# Authentication for Network Protection

Machine Authentication:  
802.1x, VPNs, IPsec....

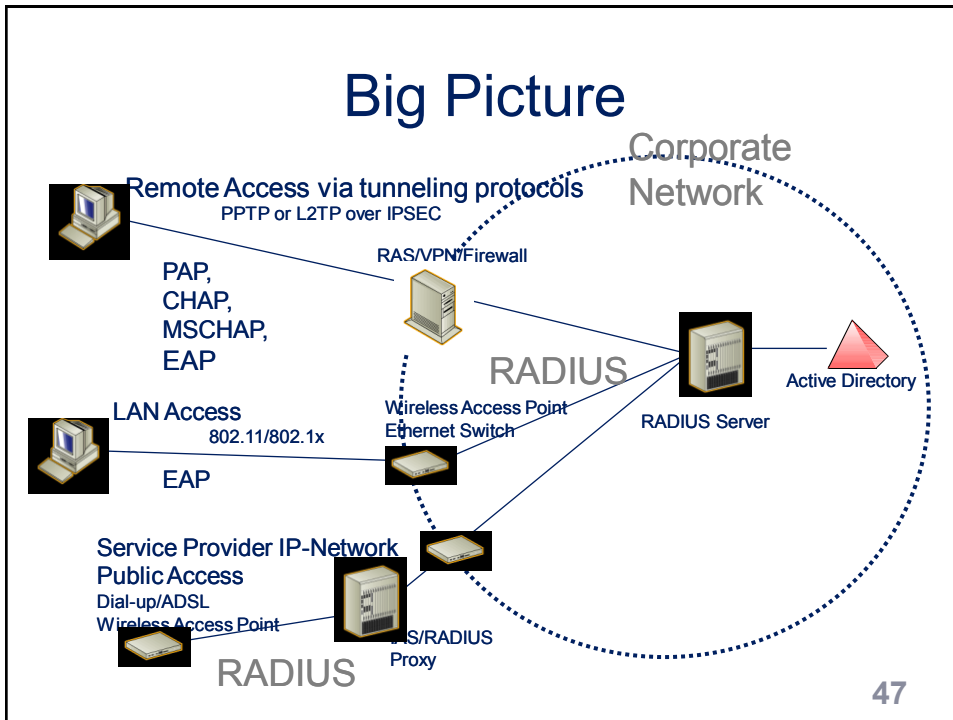
.... Viewed from AuthN/AuthZ perspective

45

## Intention / Agenda

- "Interconnected, mobile world"
- Mobile workers need access to different networks / companies
  - One person has cards / tokens / certificates issued by different companies
- An organization might not only ask for the user's identity, but also ask "where users come from" = which device or connection method they use to access the network.
- Different solutions / technologies / standards are used to fulfill nearly the same or similar requirements → confusion.
- A new way to look at networking topology or applications → Authentication topology.

46



- ## Big Picture
- Network perimeter is extended to wireless and remote access
  - Not only users should be forced to authenticate at the perimeters, but also computers and other – mobile ! - devices
  - Common central AuthN infrastructure (at least: not too many parallel systems used for AuthN)
- 48

## Users versus Machines

- Users and machines can be / should be both treated as end-entities.
  - Should users be allowed to access the trusted network via untrusted devices?
- Machines are security principals!
- Aspects to consider
  - Risk mitigation versus administrative overhead
  - Management of machines: Do you know which machines are "external" or "internal?"

49

## Network versus Applications

- In a traditional approach to PKI, network protection is sometimes separated from application protection.
  - Machine certificates versus user certificates
  - Different kinds of user certificates
- Depending on AuthN/AuthZ design the same user certificates could be used
  - Multi-purpose user certificates versus: different certificate for apps./network
- Caveat: Limitations due to network access clients (2048bit...)

50

## Technologies Overview

- **802.1x**: Authentication framework that permits network access only after a machine and/or user has been successfully authenticated.
- **VPN** (Virtual Private Network): Traversing untrusted networks using tunneling. Setup of the tunnel is typically dependent on strong authentication.
- **IPsec**: Extension of TCP/IP that provides machine-to-machine encryption and/or integrity. Setup of IPsec communication is bound to AuthN
- All of these technologies could use X.509 certificates!

51

## The "Connect As..." Problem

- If a user has valid credentials with permissions to logon to a machine, he can access this machine from any other machine
- Only solution: Usage of IPsec policies as IP filters
  - You do not even need to negotiate security
  - IPsec is based on authentication: If a machine does not have proper credentials access is blocked due to failing
  - "IPsec without IPsec"
- Note: Encryption is not required

52

## Different solutions, overlapping goals

- Requirements
  - Keeping untrusted and/or unmanaged machines out of the network. Same with users.
  - Locking down the network by relying on the lower level of networking protocols. If authentication and authorization at a particular device is unsuccessful.
- Common features of IPsec, VPN, 802.1x
  - Certificates are an option (for users and machines – incl. recent extensions for IPsec)
  - Authentication is the purpose or part of the protocol
- Users and machines should be authenticated against a central repository of security principals
- Different access devices implement different authorization rules

53

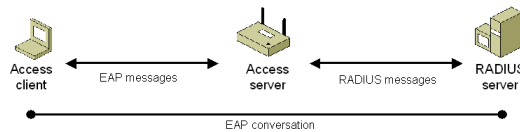
## 802.1x Scenarios

- Prevent guests to access a corporate network (meeting rooms) via wired or wireless LANs.
  - Guest machines may be directed to a guest LAN which provides internet access.
  - This is more than protection by user accounts: This prevents machine from sending a single (malicious?) packet into a corporate subnet.
- Securing wireless LANs, even if the wireless network adapter does not provide strong encryption (WEP)
  - 802.1x includes methods for changing (otherwise unsafe) encryption keys and distributing individual keys to different machines.

54

## Network Protection by EAP/802.1x

- EAP – Extensible Authentication Protocol: Framework for authentication, encapsulated authentication messages provided by underlying protocols
  - EAP-TLS: Transport Layer Security → Certificates
  - PEAP: Protected EAP → Passwords
  - LEAP: Lightweight EAP → Passwords (CISCO)
- 802.1x – how to pass EAP over wired or wireless LANs (802.11a,b,g,... covers the Ethernet part)
- Involved parties:
  - Supplicant = client
  - Authenticator = Network access device (switch, access point)
  - RADIUS server (to be explained)
  - Central authentication server



55

## 802.1x Authentication Process

- RADIUS server sends his certification to the supplicant (public key included)
  - Supplicant authenticates the server
  - Authentication communication is secured (similar to SSL)
- Access device asks machine: Who are you? → Machine sends name or cert.
- Access device says: Prove it! → Machine sends response to a challenge (password based) or signed data (cert. based method)
- Machine is granted network access, IP address is assigned
- Machine has network access: Can be reached from other devices on the network (virus updates, system management)

56

## 802.1x AuthN Process (2)

- Access device asks user: Who are you? → User sends name or cert.
- (Now the network access may be interrupted)
- Access device says: Prove it! → User sends response to a challenge (password based) or signed data (cert. based method)
- Network access is established again
- Note: Machine or user could be authenticated – or both. It is the client that decides to start and AuthN sequence in the context of either machine or user.

57

## 802.1x is NOT...

- Encryption of the communication between client and servers on the network: ONLY the authentication traffic is encrypted.
- A measure to force both machine AND user to authenticate.

58

## Certificates in 802.1x / EAP

- EAP: Extensible Authentication Protocol
- Authentication framework → Details are subject to implementation
- Users and machines may authenticate using...
  - Passwords: PEAP (Protected EAP)
  - Certificates: EAP-TLS (Transport Layer Security)

59

## RADIUS

- Remote Dial-In User Service
- Vendor-independent: Authentication service used in heterogeneous environments
- Different kinds of user databases can be used for authentication
- Used with 802.1x and VPN
- Can also act as an authentication proxy and send request to different RADIUS servers for final authentication (e.g. based on the domain suffix of the user name)

60

## RADIUS and 802.1x

- Switches and WLAN access points send AuthN requests to RADIUS servers.
- The RADIUS server then authenticates the user (or machine) against an "authentication database" or directory.
- RADIUS servers have to be available at every location.
  - Note: If RADIUS servers are centralized, users might not be able to access their local network.

61

## Network Protection by VPN

- Cross untrusted networks by secure tunnel
  - Example in Austria: ADSL internet access
- Machine certificate can be used to secure communications (IPsec)
- User certificate can be used to authenticate the user (L2TP)
- Can be (mis)used to protect wireless connections.
- VPN types:
  - Site-to-site (server-to-server) VPN: Connect branch offices to central locations via the internet
  - Client-to-server: Connect remote mobile workers to the corporate network.

62

## Network Protection by IPsec

- IPsec: Protocol 50/51 (not TCP or UDP), additional headers added to packets
- IPsec is not only used for encryption (IPsec-ESP), but also for authentication (IPsec-AH or IPsec-ESP-Null)
- IPsec is not only used for tunneling
- Only trusted devices are accepted as IPsec partner host:
  - Trusting in the same CA
  - Member of the same Kerberos realm (or Kerberos trusted realms).

63

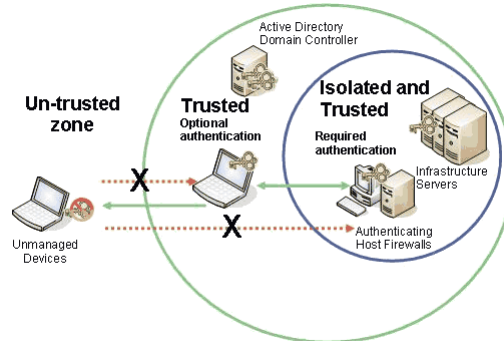
## Authentication in IPsec

- Communicating hosts need to be part of the same "trust infrastructure".
- IPsec policy: similar to a router access rule or a firewall rule
  - Filter List: Source → Destination, protocol, port
  - Filter Rule: Permit / Deny / Negiate (algorithm)
- Diffie-Hellman used for negotiating a secure symmetric key
- Authentication required for negotiating on keys:
  - Pre-Shared Secret
  - Kerberos tickets
  - X.509 certificates

64

# IPsec Defines Logical Perimeter

- Each host in the protected zone refuses communication that is not IPsec



65

## Overview on Related Technologies

Identity Buzz Words

66

## Problem: Interconnected World

- Kerberos only works within a Kerberos realm or within different trusted realms
- Certification authorities have to mutually cross-trusted
- → Any universal AuthN solution is based on manual establishment of "cross-trusts"
- Standardization bodies try to define interfaces and standards.

67

## Single-Sign On

- Marketing buzz word
- SSO can mean completely different things
- Client-based SSO:
  - One client has a "credential store" which contains credential for different services, such as certificates for VPN access, usernames and passwords for web sites, logon certificates for Kerberos logon.
  - Every platform uses its own AuthN and AuthZ
- "Real" SSO:
  - Client is authenticated once using a single set of credentials (e.g. certificates) and authorized on the bases of this authentication by different systems.

68

## Meta-Directories

- Identity manager's dream: The universal directory containing ALL relevant objects and attributes
  - Not realistic
- "Meta-Directory" also used to describe a service synchronizing different directories
- Defining master and slave directories, e.g.
  - User names: HR system → Active Directory / Novell
  - Telephone numbers: Phone system management → all other systems
- User Certificates may e.g. be published by a certification authority to an LDAP directory (attribute: userCertificate) and replicated to other directories

69

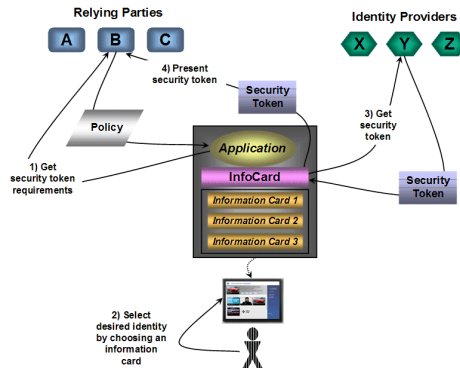
## InfoCard / CardSpace

- Generalized identity
  - **Security tokens** can contain different claims.
  - **Claims:** Identity data (user name...) plus – typically – something that is used to authenticate, such as digital signatures.
  - **SAML:** XML standard, Security Assertion Markup Language
- CardSpace can contain
  - SAML token, X.509 cert., Kerberos ticket
- <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>

70

## InfoCard / CardSpace (2)

- Protocols for exchange of policies and identity information: WS-\*
- Passwords defined by the user: Self-issued identity provider



71

## Federation in General | Higgins

- Federation refers to the general concept of presenting security tokens issued by a token provider to another system.
  - <http://msdn2.microsoft.com/en-us/library/ms951235.aspx> (by IBM)
- Higgins: Open source project, goals similar to InfoCard
  - <http://www.eclipse.org/higgins/faq.php>
- Interoperability: Work in progress
  - <http://www.identityblog.com/>

72

## Information Rights Management

- Author defines access rights.
- Rights are enforced by encrypting the content at a server.
- Content is read ("consumed") after readers have acquired licences from the server.
- Licences permit to decrypt the content
- <http://www.microsoft.com/windowsserver2003/techinfo/overview/rmenterprise.msp>

73

## XrML Certificates used in RM

- X.509 certificates have not been defined for AuthZ purposes (though sometimes used for – e.g. by building access rules based on naming attributes)
- Requirement in rights management: Authorization information (Access right, use licence) should be bound to content
  - Fundamentally different from classic implementations of access rights and permissions.

74

## X.509 vs. XrML | PKI vs. RM

- X.509 certificates and keys are primarily considered the user's property and used in end-to-end communication.  
RM rather protects the content belonging to an organization or enforces an orgs. Information policies
- In RM the user do not need to have the keys – keys are primarily managed by servers.