

AuthN, AuthZ and PKI

PKI Labs

Lecture at FH Joanneum, Winter 2009/2010
Lab Walk-Through and Intro
Advanced Security Engineering 09

Dr. Elke Stangl, PKI Consultant | <http://punktwissen.at/>

Lab Startup and Overview

Overview on each Lab Exercise:
Goals, Intentions, Quick Walk-
Through

Labs

- Overview on **lab setup**
- Walk-through labs
 - **PKI demo:** Solution components, CA and certificate tools
 - Introduction to required **non-PKI components:** VMWare, AD, Windows 2008
- Lab details
- **Exercises** are described in **separate PPT document** (this document)

Startup

- When copying VMs select **I have moved the virtual machine**
- Do not select that you have copied the machine. This will trigger OS reactivation (hardware change!)
- Password for **Administrator** user(s)
answer.42
- Check **Windows activation state**:
 - Properties of My Computer
 - Scroll down → Check for info on activation

Windows activation

Windows is activated

Product ID: 92573-079-0354896-76781

 [Change product key](#)



[Learn more online...](#)

- In case you find: Automated activation will start in X days → get a new MSDN EDU key, change product key and re-activate. This should only be required if the machine had not been copied with the option 'moved' (see above)

Lab Environment | Machines

- Two virtual machines
 - Created with VMWare Workstation 6.5 (Setup instruction available)
 - Running **Windows 2008 Enterprise Edition**
 - Each server **has different roles** (Lab environment only – NOT an implementation best practice)
 - Both servers are members of a **Windows domain / Kerberos realm** (again not a best practice for a Root CA)
- Windows Domain
 - **GALA** (NetBIOS)
 - **gala.xy** (DNS)

Lab Environment | Machines (2)

- Machine **PKI-Lab-RootCA-Member**
 - Host name: ARTHTURDENT
 - Root CA ('offline')
 - Member of domain – Kerberos “client”
 - CA configuration “as if offline”
- Machine **PKI-Lab-IssuingCA-KDC**
 - Host name: TRILLIAN
 - Domain controller / Kerberos KDC server
 - Subordinate Issuing CA ('online')
 - Web server
 - LDAP server

Lab Environment | PWs, Network

- **Administrator accounts** (local/domain):
 - Password: answer.42
 - ARTHURDENT\Administrator
 - TRILLIAN\Administrator
 - GALA\Administrator
=Administrator@gala.xy)
- **Network**
 - Private class C subnet: 192.168.88.x
 - Static IPs, no gateway
 - Host-only networking
 - File transfer between host and guest should be done using darg-and-drop, no networking connection required
 - VMWare networking mode and IP settings may be changed if required as long as the two machines remain in the same network segment
- **Date / time**
 - Check for host / guest system time discrepancies
 - Change if required
 - A warning on system time and clock speed might be displayed on starup (HW dependent → check out the referenced VMWare knowledge base article)

Lab Environment | Software

○ Virtualization

- Machines created using VMWare Workstation 6.5
- Can be run with VMWare Workstation or VMWare Player
- Use drag&drop from guests to host in order to exchange files between guests

○ Installed software

- **Windows 2008 Enterprise Edition**
(MSDN, provided by FH Joanneum)
- All **Windows patches** (cut-off date see setup documentation TXT file)
- Wireshark sniffer

Lab Walkthrough

Overview on each Lab Exercise:
Goals, Intentions, Quick Walk-
Through

Important Tools

- **Management consoles:** Start, Administrative Tools
 - Certification Authority
 - Certificate Templates
 - Enterprise PKI
 - Internet Information Services Manager
 - Active Directory Users and Computer
- **Alternative: Start consoles from empty MMC:**
 - Start, Run..., MMC
 - Add/-Remove Snap-Ins
- **Command line tools**
 - Start, Run... <enter tool name>
 - Windows 2008 search form field

PKI / CA GUI Tools

- **Certification Authority MMC** (certsrv.msc)
 - CA configuration: CA object → Properties shows CA configuration such as
 - CA certificate(s)
 - URLs
 - Certificates' database:
 - Issued Certificates
 - Pending Certificates
 - Revoked Certificates
 - Failed Certificates
- **Local publication path**
C:\Windows\system32\certsrv\CertEnroll
- **Registry with config (Start regedit)**
HKLM/SYSTEM/CurrentControlSet/Services/CertSvc

Certificate GUI Tools

○ Certificates MMC

- MMC, Snap-In Certificates, select security principal: User, local computer (or services)
- Certmgr.msc → Always user context

○ Internet Explorer

- Options, Content, Certificates
- → OS store
- (IE cert. GUI will hardly be used)

Certificate / CA / Request CMD Tools

o certutil

- View stores
 - -store
 - -viewstore
- Verify paths with
 - -verify
 - -verify -urlfetch
 - -url

o certreq

- Create new key pair and request
 - -new
- Submit request to CA
 - -submit (-attrib)

Cert. Requests / Browser

- Enrollment URL

`http(s)://trillian.gala.xy/certsrv`

- Internet Explorer Hardening deactivated

- For users
- For admins

- **Site** `http(s)://trillian.gala.xy/`

added to Local Intranet Zone

- Security of Intranet zone set to low

Sniffer Introduction

- **Wireshark** network sniffer
- Define interface
- Capture traffic
- Inspect packet details

AD and Kerberos

- AD GUI tools
 - Active Directory Users and Computers / dsa.msc (Check 'Advanced')
 - Active Directory Sites and Services / dssite.msc (Show Services Node)
- LDAP Tools
 - `ldp.exe`
 - `adsiedit.msc`
- Kerberos tools
 - `klist`

Lab Goals

Overview Intentions and Goals

Lab 1: CA Hierarchy/Cert. Extensions

- Understand **PKI components** and **CA certificate extensions**
- Understand implications of **validity period configuration**.
- **Renew CAs** in a hierarchy with new keys
- **Publish CA certificates** and **CRLs** so that the certificate chain can be validated
- Provide **evidence** of new certificates and CRLs (hash values, dates) and a report of the validation of the full chain.

Lab 2: Cert. Lifecycle / AuthN / AuthZ

- Create **new certificates** for
 - SSL web servers
 - SSL clients
- Configure **authentication** and **authorization** based on certificate mapping
- Evaluate **security of certificate mappings**

Lab 3: Kerberos Tickets

- **Inspection of Kerberos tickets**
 - Ticket granting tickets
 - Service tickets
- Validate that tickets are **created for specific services.**
- **Ticket flow and contents in the network sniffer**
- Changing Kerberos-related configuration to **provoke typical errors**
 - → troubleshoot using Kerberos tools and sniffer

Expected Output

- Lab description (these slides) contain **instructions** and **questions**
- Questions are **highlighted in red** and **assigned numbers**
- Categories of questions
 - **Documentation of output** as an indication that exercises actually have been done. Especially: certificates, hash values
 - Questions related to **one specific step** (E.g.: Why is error XY displayed here?)
 - **General questions** related to be content covered by the labs, but not related to a specific step
- Expected output
 - **Answers to questions** provided in document (TXT, DOC, DOCX, RTF, PDF)
 - **Attachment of additional files** if indicated in the question

Lab 1: CA Hierarchies

Lab Instructions
Certificate Chains and
X.509 Attributes

Lab 1: CA Hierarchy/Cert. Extensions

○ Intentions

- Become familiar with **typical components of a PKI solution** incl. directories
- Estimate admin. efforts, '**feel the process**'
- Understand **pre-requisites for client certificate enrollment**

○ Exercises

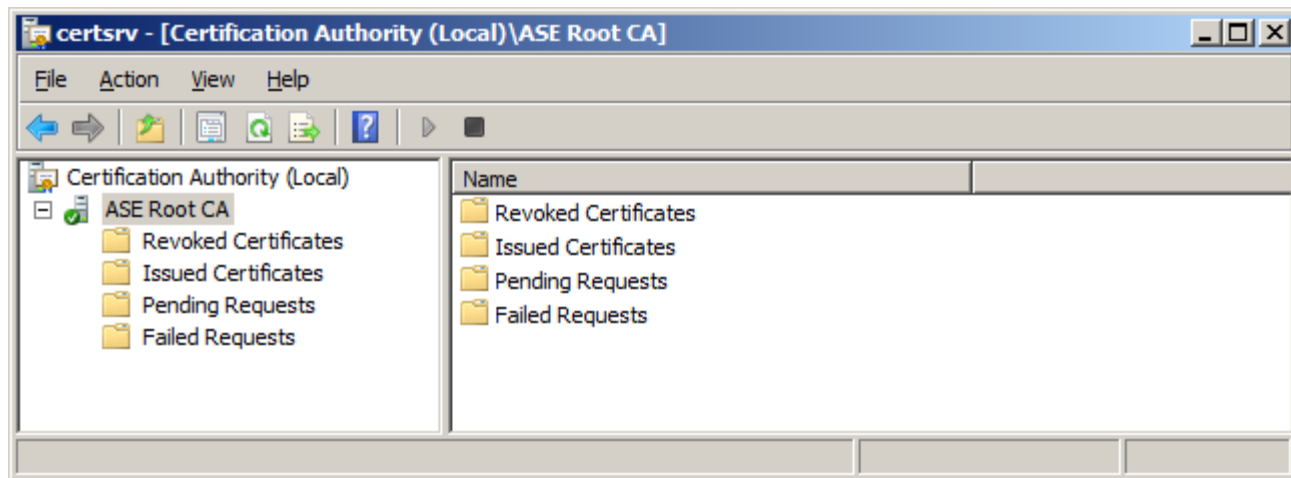
- **Inspect** PKI Configuration
- **Issuance** of Client Certificates
- **Renew** CA certificates
- **Validate** certificate paths

Lab 1 Initial State | Pre-Req's

- **Two-level CA hierarchy** installed
 - (Config. Scripts / Certs. and backup in C:\PKI-Lab)
- **CDP** and **AIA URLs** populated.
- Demo SSL certificate issued.
 - For that lab it is only important that **some end-entity certificate** has been issued.

Root CA Overview | Tools

- Start *PKI-Lab-RootCA-Member* and make yourself familiar with the CA management tools
- Note: The CA service on *PKI-Lab-IssuingCA-KDC* might not start immediately – this is per design of this lab. See instructions below
- CA MMC (GUI):
 - **Start, Administrative Tools, Certification Authority** or
 - **Start, Run, type `certsrv.msc`**



Root CA Overview | Tools (2)

- At the Root CA **click Start, Run**, type `cmd`
- `certutil` (View CA's database)
 - Fields cert. table: `certutil -schema`
 - Fields CRLtable: `certutil -schema CRL`
 - Display all CRLs: `certutil -view CRL`
 - Display some attributes of certificate with a specific request number (type without line break)
`certutil -view -restrict "RequestID=2"
-out "CommonName,NotBefore,NotAfter"`

PKI Status | Root CRL

- At the Root CA: Inspect the status of the current CRL, especially the attribute ***Next Update***
 - GUI: In the CA MMC, right-click ***Revoked Certificates, Properties..., View CRLs, View CRL***
 - Cmd: `certutil -view CRL`

PKI Status | Root CRL (2)

- Publish a new CRL locally at the Root CA. This has to be repeated if the CRL is expired or if it might expire while you are working on the labs.
- GUI: right-click ***Revoked Certificates, All Tasks..., Publish, Base CRL***
- Cmd: : `certutil -crl`
- Check the CRL(s) again to confirm that a CRL has been created.

PKI Status | Root Cert

- Inspect the Root CA certificate. Locate the CRT file at the Root CA in
`C:\Windows\system32\certsrv\CertEnroll`
- GUI: Double-click the file
- Cmd: `certutil <RootCACertFile>.crt`

[PKI-01-01]: Search for any extensions that include URLs. Does the certificate contain any URLs? If yes: Why are these URLs included? If no: Why are there no URLs?

PKI Status | Web Server

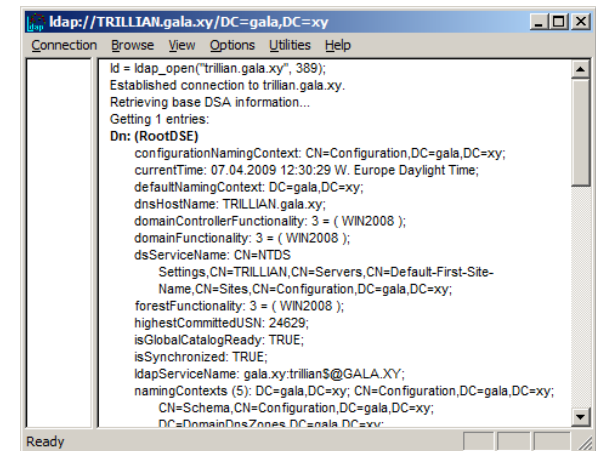
- Start the machine *PKI-Lab-IssuingCA-KDC*
- The Issuing CA also hosts a web server (We do not need the Issuing CA service now – neglect any 'per design' errors for this service for the time being)
- Check that this service is operational by running the following check at the Issuing CA machine
 - Start Internet Explorer and type: <http://trillian.gala.xy/>
 - A start page should be displayed
- The virtual directory used to publish certificates and CRLs (/CertEnroll) corresponds to the local folder
`C:\Windows\System32\certsrv\CertEnroll`
- Web server management is done
 - by the IIS Manager : **Start, Administrative Tools, Internet Information Services (IIS) Manager**
 - Or by editing the config files in
`C:\Windows\System32\inetsrv\config`



PKI Status | LDAP Server

- The Issuing CA also hosts a LDAP server
- Check that this service is operational by running the following check at the Issuing CA machine
- **Start, Run**, type `ldp`
- Select Connection, Connect
- Type `trillian.gala.xy`
(Leave 389, do not check SSL)
- The server should reply a text output starting with

```
ld = ldap_open("trillian.gala.xy", 389);
Established connection to trillian.gala.xy.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
```



PKI Status | Issuing CA

- Start the machine PKI-Lab-IssuingCA-KDC
- Check if the Issuing CA is operational by trying to run either the **CA MMC** (GUI) or `certutil -view` to check the contents of the CA database
- If the CA service is not operational, there is most likely a problem related to validation of the certificate path of the CA's own Issuing CA certificate
 - This 'error' is added on purpose, because it is one of the most frequent problems observed in read-live PKIs.

PKI Status | CA Cert. Path

- At the Issuing CA start cmd
- Navigate to
`C:\Windows\system32\certsrv\CertEnroll`
- There are two CRT files in this folder. Double-click both and identify the Issuing CA certificate.
- Run a full path validation test using
`certutil -verify -urlfetch <IssuingCACertFile>.crt`
- **[PKI-01-02]:** Paste the output of this dump into documentation. Add comments to all references to the URL <http://trillian.gala.xy> and explain
 - Where these URLs are retrieved from
 - Why these URLs are evaluated(Remember how path validation works)

Publish Root CA CRL

- Create a temporary folder on your host machine that will be used as a temp. folder for exchanging files between Root and Issuing CA
 - (This replaces removable media used with real-live CA hierarchies)
- Copy the CRL file created in this folder at the Root CA before
`C:\Windows\System32\certsrv\CertEnroll`
- To the folder `C:\Windows\System32\certsrv\CertEnroll` at the Issuing CA
 - This folder is also the virtual web directory
- Repeat the path validation check and dump the output again
- If the Issuing CA could not be started before: Start the CA service now running `net start certsvc`
- **[PKI-01-03] Which step is missing here? (Hint: Investigate the path validation dump and check which version of the CRL can be found at which publication point. CRLs have a sequence number). Why does the CA service still start?)**

Test End-Entity Certificate

- Create a new certificate for the Administrator
 - **Start, Run**, type `certmgr.msc`
 - Right-click on **Personal, All Tasks..., Request new certificate...**
 - **Next**
 - Check: **ASE SSL Client**
 - **Enroll**
- Locate the certificate in **Personal/Certificates** (Double-click the certificates and check the validity dates in the Details tab)
- Export the certificate
 - Double-click
 - **Copy to File...**
 - **Next, Next (No private key)**
 - Select **BASE64** encoding (uncritical)
 - Choose a file name (**Browse folders** to see all folders)

PKI Status | Full Certificate Chain

- Run again a full check of the chain, this time starting at the end-entity certificate and save the dump ([command] > [dump])
`certutil -verify -urlfetch <EndEntityCertFile>.cert`
- Run a simplified version of the check that does not query all URLs
`certutil -verify <EndEntityCertFile>.cert`
Note the last lines of the dump which indicate a summary on revocation checking
- **[PKI-01-04]** Copy both dumps to the documentation. Add comments to the dump explaining how URLs are used to validate certificates.

Inaccessible CRLs(?)

- Stop the web server running
`net stop w3svc`
- Repeat both checks using `certutil -verify (-urlfetch)` described in the previous slide
- **[PKI-01-05]** Copy the new versions of both dumps to the documentation. Point out the difference. Did the summary on revocation checking displayed at the bottom of the `certutil -verify` dump change? Why or why not?
- Start the web server again by running
`net start w3svc`

Prep. For Renewal Root CA | Backup

- Create a backup of the CA databases and key configuration
 - Create an empty folder
 - Run `certutil -backup <BackupFolder>`
 - You will be prompted for a password to protect the key backup (can be left empty)
- Create a backup of the CA configuration
 - Start, Run, regedit
 - Navigate to
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc`
 - Right-click the CertSvc key and select **Export**
 - Choose a name for the exported .REG file

Prep. For Renewal Root CA | Test Certs.

- In order to test the effect of renewal a non-expired and non-revoked end-entity certificate will be required.
- If a proper certificate does not exist, create a new one (see description of enrollment for user certificate earlier)
- Plan to complete the renewal and subsequent tests before this certificate will be expired.

Renew Root CA

- Start the Root CA machine
- Renew once with a new key running
`certutil -renewcert`
- Restart the CA service running
`net stop certsvc & net start certsvc`
- Renew once more with the same key running
`certutil -renewcert ReuseKeys`
- Restart the CA service running
`net stop certsvc & net start certsvc`
- You can renew the CA more often if you wish. It is just important that it should be renewed
 - At least once with the same key
 - At least once with a new key

Confirm Renewal

- **Start, Run**, type `certsrv.msc`
- Right-click the CA, **Properties**
- Three certificates should be displayed in the list
- Navigate to
`C:\Windows\System32\CertSrv\CertEnroll`
- **[PKI-01-06]** ZIP all files in the CertEnroll folder and attach this ZIP file to the documentation.

Understand Renewal

- The CertEnroll folder shows different types of files:
 - ...(x).CRT (*)
 - ...(x-y).CRT
 - ...(x).CRL
- **[PKI-01-07]** There is not a (x).CRL file for every (x).CRT file. Why? Inspect the (x-y).CRT certificate files and compare them to the (x).CRT files. What is the difference? What might be the purpose of these certificates?
- Hint for both questions: Check the AKI and SKI extensions.
- (*) Due to this issue <http://support.microsoft.com/kb/927169/en-us> some certificates might contain URLs – these can be ignored, they are not important for these exercises.

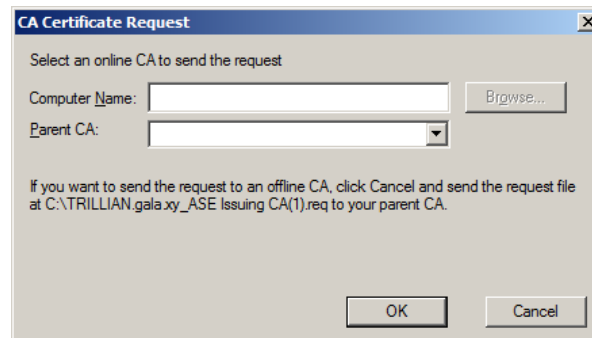
Publish CA Cert. and CRL

- Transfer ALL (x).CRT and (y).CRL files created at the Root CA in
`C:\Windows\system32\certsrv\CertEnroll`
- to the following folder at the Issuing CA (and web server)
`C:\Windows\system32\certsrv\CertEnroll`

Renew Issuing CA

- At the Issuing CA
- Renew once with a new key running
`certutil -renewcert`
 - Note: You cannot run this command twice without errors. Either complete the renewal process or run the following command to discard an outstanding request:
`certutil -renewcert -f`

- This popup is presented
Click **Cancel**



- **[PKI-01-08]** Why is the request not sent to the Root CA directly (in real-life scenarios – in the lab this is theoretically possible)

Inspect and Process the Request

- Locate the request at `C:\`
- At the Issuing CA, inspect the request running `certutil -v <RequestFile>.req`
- Copy the request file to the Root CA
- At the Root CA submit the request using `certreq -submit -config "arthurdent\ASE Root CA" <RequestFile>.req`
- Start `certmsrv.msc` and locate the request in the **Pending** queue
- Right-click the request and select **Issue...**
- Locate the certificate in **Issued** Certificates

Export the Certificate (2)

- Export the certificate using (*different options*)
The MMC: Double-click, Details, Export.... (same as used earlier)

or

- Export the certificate using the command line
 - Identify the number of the request
`certutil -view -out "RequestID,CommonName, NotBefore" Log`
(Log restricts output to issued and failed and excludes pending requests)
 - and run and dump the following command
`certutil -view -out RawCertificate -restrict
RequestID=<YourRequestID>`
The dump of the command is the BASE64 encoded certificate. Save the dump as .CER or .CRT file

For either option continue with...

- Double-click the certificate and check the attributes
 - Verify that the key has changed or not changed (depending on renewal choices)
 - Start and end dates

Process Certificate at the Issuing CA

- Copy the certificate file created in the previous step to the Issuing CA
- Run a check against the new cert. and save the dump
`Certutil -verify -urlfetch <RenewedIssuingCACert>.cert`
- Do a second check by simply double-clicking the certificate at the Issuing CA – an error will be displayed.
- **[PKI-01-09]** Copy this dump to the documentation and compare it to the analysis of the original Issuing CA certificate. Hint: Not all URLs are populated, so URL errors are expected. But in addition you have to watch out for another error – this is the error that is also reflected in the GUI certificate viewer. What has not been done yet to provide the Issuing CA with all information?

Analysis of Error

- Try to install the new certificate at the Issuing CA using `certutil -installcert <NewCACert>.cer`
- A popup is displayed that should give you more information on what is still missing
- **[PKI-01-09-continued]** If the answer was not clear yet – can you explain now which step is missing? If yes – can you explain why a different error had been displayed before?
Hint: Remember that the machine or user checking a cert. always tries to build different certificate chains – based on different attributes in the certs. Including names. And it desperately tries to find some path to a trusted root CA.

Root CA Certificate LDAP Pub.

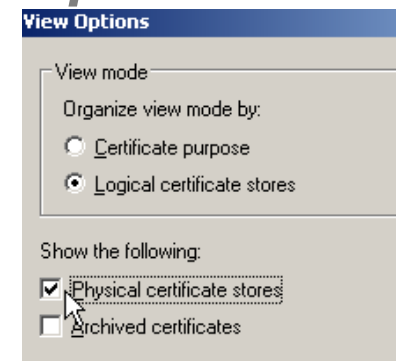
- Note: The Issuing CA machine is also as a 'certificate client' – Root CA certificates are distributed to this machine in the same way as they would be distributed to clients.
- Publish the files to the LDAP server (Issuing CA machine)
 - For all (x).CRT files run (*)
`certutil -dspublish -f <RootCACert>.crt RootCA`
(Note that RootCA is a parameter, not a name)
 - For all (x).CRL files run
`Certutil -dspublish -f <RootCACRL>.crl`
- (*) This command publishes the cert. to two locations
 - A n LDAP locations ('AIA') that clients need to chase actively
 - A trusted root store ('Certification Authorities') that will allow clients to download the certificate to their local trusted root stores.

Root Certificate Download

- Publish the trusted does not trust the certificates in Active Directory immediately
- Certificates have to be downloaded to the client-side store of trusted certificates – even if the machine itself is the domain controller hosting the directory
- Download is forced at the same time so-called group policies are refreshed. To trigger the download run
`gpupdate /force`

Client-Side Store of the Issuing CA

- Run the following command to inspect the client-side store
`certutil -store -enterprise root`
- Verify that the renewed Root CA certificate(s) have been downloaded successfully.
- **[PKI-01-10] Copy the dump the documentation. Why does the dump include this line: Cannot find the certificate and private key for decryption. Is this really an error?**
- For your information: The command provides the same information as: **Start, Run, Type MMC, File, Add/Remove Snap-Ins, Select Certificates, select Local Computer**
 - Click on cert. symbol, Options,
 - Physical Store
 - Navigate to Trusted Root Certificates
 - Sub-container Enterprise (= downloaded from the LDAP objects just investigated)
 - If the Root Certificate(s) are not there, run `gpupdate /force`



Finalize Installation

- Re-run the installation command at the Issuing CA – this should now finish without errors
`certutil -installcert <NewCACert>.cer`
- Re-start the CA service
`net stop certsvc & net start certsvc`
- Check the contents of the folder
`C: \Windows\system32\certsrv\CertEnroll`
You should see at new CRL with a suffix (<number>) per renewal with a new key.
- **[PKI-01-11]** ZIP the contents of the CertEnroll folder at the Issuing CA and submit it together with the documentation.

If Installation Fails...

- although `certutil -verify` reports OK and the Root CA cert. is visible in the output of `certutil -store -enterprise root` (issue/bug with virtual machines & fast testing)
- → Import both the Root CA cert and CRL manually to the the Issuing CA's local machine store for trusted roots
 - `certutil -addstore root <NewRootCACert>.cer`
 - `certutil -addstore root <NewRootCACert>.crl`
- Re-run the installation of the Issuing CA cert

Final Check

- Enroll for a new user certificate as the administrator and export the certificate to a file
- Run `certutil -verify` and `certutil -url` against the new user certificate. Check the output for errors.
- Check for errors in `pkiview.msc`
Note: `pkiview.msc` always used the most recent certificate of type 'CA Exchange' to read the most current URLs

Full Validation of New Chain

- Enroll a new test certificate for the logged on administrator at the Issuing CA (as described before the renewal section: `certmgr.msc`, *Personal, All Tasks, Request a New Certificate...*)
- Export the certificate to a CER file and run `certutil -verify -urlfetch <NewUserCert>.cer`
- **[PKI-01-12]** Copy the dump to the documentation. Compare the dump to the dump created for an end-entity certificate that had been created before renewal. Why are some URLs different?

Implications of Renewal on URLs

- **[PKI-01-13]** Consider all the files that have been created on renewing the Root CA and the Issuing CA in the respective CertEnroll folders.
 - Why is it not sufficient to just publish the files with the highest index (x)?.
 - If a CA had been operational for some time and issued many certificates – what would happen if after renewal only the CRLs with the highest index are published to web and LDAP server?
 - If you have now renewed your CA several times in the lab before you have issued the first user or machine certificate: Which files are the ones that are really required? (Note that in real life you would anyway always advise admins to publish all files in order to avoid errors).

Lab 2: Certificate Enrollment

SSL Certificate Enrollment and Certificate Mapping

Lab 2: Enrollment, Cert. Mapping

○ Intentions

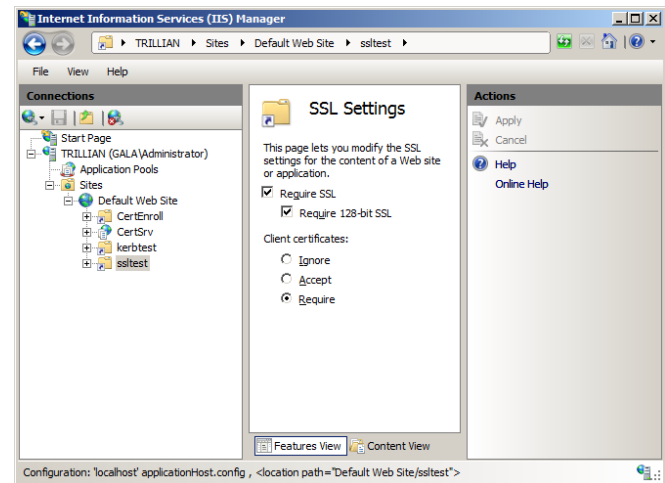
- Understand how certificates are used for **mutual authentication**
- Understand how **security principals / directory entries** are **linked to certificates for authentication**
- See an example for the **separation of authentication and authorization**

○ Exercises

- Creation a **certificate for a web server**
- Creation of a **certificate for a web client**
- Analyze security of **certificate mapping**

Lab 2: Initial State | Pre-Req's

- FYI only – configured already
- Configured via IIS Manager or
`C:\Windows\System32\inetsrv\config\applicationHost.config`
- SSL server certificate is configured, but might be expired already
- SSL can optionally be used for any virtual directory, but is not enforced at the root directory of the Default Web Site
- Client certs. are accepted, but not enforced at the root directory of the Default Web Site
- Client certificate mapping based on Active Directory mapping is available as AuthN method for all web directories
- For one virtual directory /ssltest,
 - SSL is required and
 - the usage of client certificates is enforced.



Lab 2: Initial State | Pre-Req's (2)

- AD based mapping enabled at web server level

```
<system.webServer>  
  <security>  
    <authentication>  
      <clientCertificateMappingAuthentication enabled="true" />
```

- Mapping is activated for specific directories in the applicationHost.config file

```
<location path="Default Web Site">  
  <system.webServer>  
    <security>  
      <access sslFlags="SslNegotiateCert" />  
    .....
```

```
<location path="Default Web Site/ssltest">  
  <system.webServer>  
    <security>  
      <access sslFlags="Ssl, SslNegotiateCert, SslRequireCert, Ssl128" />  
      <authentication>  
        <windowsAuthentication enabled="false" />  
        <anonymousAuthentication enabled="false" />  
        <clientCertificateMappingAuthentication enabled="true" />
```

Lab 2: Initial State | Pre-Req's (3)

- Both the web servers root (`C:\inetpub\wwwroot`) and the test directory contain a file with the name `noadminaccess.htm`
- NTFS file system permissions do only include an access control entry for the user 'IUSR' – the user for anonymous access.
- Not even the admins have access to this file

Enroll for a New Server Cert.

- At the Web Server (Issuing CA) create a file named `ssl.inf` with the following content

```
[Version]
Signature=$Windows NT$

[NewRequest]
RequestType=PKCS10
Subject="CN=trillian.gala.xy"
KeyLength=2048
KeyUsage=0xa0
MachineKeySet=TRUE
ProviderName="Microsoft RSA SChannel Cryptographic Provider"
ProviderType=12
KeySpec=1
```

Enroll for a New Server Cert. (2)

- Create key pair and request running

```
certreq -new ssl.inf ssl.req
```

- Submit the request to the CA

```
certreq -submit -attrib
```

```
"CertificateTemplate:ASE Web Server" -  
config "trillian.gala.xy\ASE Issuing CA"  
ssl.req ssl.cer
```

- Install the certificate

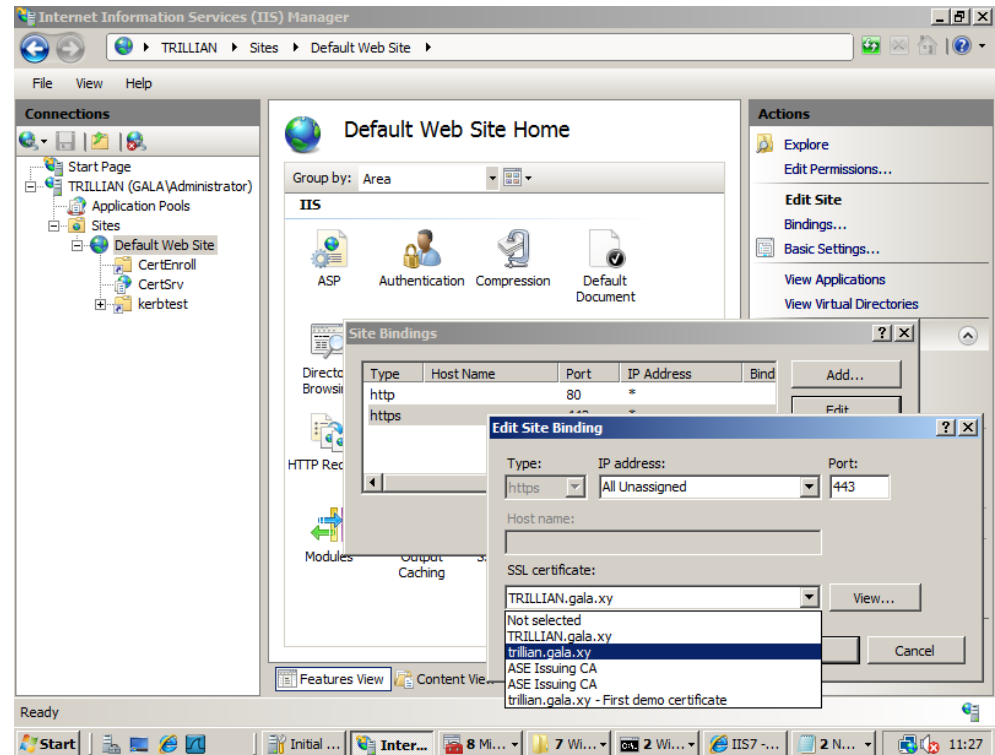
```
certreq -accept ssl.cer
```

Use the Cert. With the Web Server

- (A GUI version of this configuration can be found on the next slide)
- Run the following at the web server to retrieve the (default) IIS app. Id
`netsh http show sslcert`
- Copy the appid in the output
IIS always uses {4dc3e181-e14b-4a21-b022-59fc669b0914}
- Copy the hash value of the new certificate by running `certutil -store my` and copy the value following `Cert Hash(sha1)` :
- Delete previous configuration (0.0.0.0 → any IP. Netsh is required because SSL is handled by the HTTP.sys driver (kernel mode), not by the application
`netsh http delete sslcert ipport=0.0.0.0:443`
- **Configure the certificate**
`http add sslcert ipport=0.0.0.0:443`
`certhash=<CertHashWithout Blanks>`
`appid=<IDasDeterminedBefore>`
- **Configuration example (do not simply copy – use your own hash, IP address and appid)**
`http add sslcert ipport=0.0.0.0:443`
`certhash=af1b937017c0c73e15a1a4de5756ebe51406e7dd`
`appid={4dc3e181-e14b-4a21-b022-59fc669b0914}`

GUI Alternative

- *(This is an alternative to the cmd config described on the previous slide)*
- **Start, Administrative Programs, IIS Manager**
- Left pane: **Default Web Site**
- Right pane:
 - **Bindings...**
 - **https**
 - **Edit**
 - Select new certificate
 - Check certificate using **View...**



Enroll for a New User Cert.

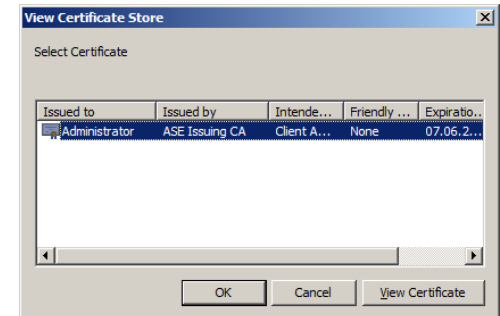
- At the client / member server (Root CA) create a file named `client.inf` with the following content

```
[Version]
Signature=$Windows NT$

[NewRequest]
RequestType=PKCS10
KeyLength=2048
KeyUsage=0xa0
MachineKeySet=FALSE
ProviderName="Microsoft Enhanced Cryptographic Provider v1.0"
ProviderType=1
KeySpec=1
```

Enroll for a New User Cert. (2)

- Logon as GALA\Administrator to the Root CA (Client)
- Create key pair and request running
`certreq -new user.inf user.req`
- Submit the request to the CA
`certreq -submit -attrib "CertificateTemplate:ASE SSL Client" -config "trillian.gala.xy\ASE Issuing CA" user.req user.cer`
- Install the certificate
`certreq -accept user.cer`
- Check that certificate is there
`certutil -viewstore -user my`

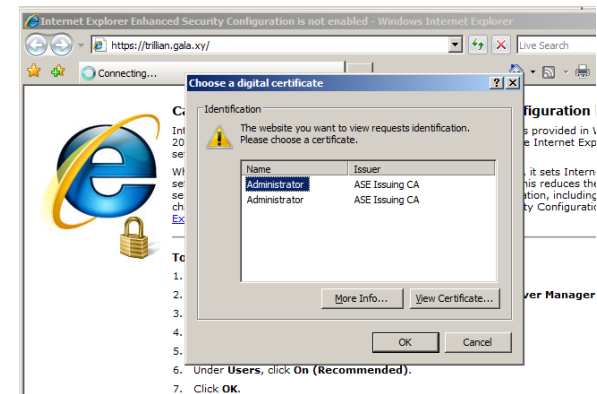


Certificate Documentation

- **[PKI-02-01]** Export both the new user and the new server certificate and submit these files together with the documentation

Test SSL Certificates

- (Always re-)start Internet Explorer
- Enter <https://trillian.gala.xy>
- If there is more than one cert. in the user's store, a popup is displayed
- For the root of the web server, <https://trillian.gala.xy> the cert. popup can be cancelled or a certificate can be presented – check out the difference, for the virtual directory /ssltest an error will be displayed (<https://trillian.gala.xy/ssltest>)
- Revoked or expired certificates will also cause an error.



Effect of Revocation

- Identify a working user certificate (not expired and not revoked and complete one successful authentication (see previous slide))
- Revoke the certificate
 - At the Issuing CA start `certsrv.msc`
 - Navigate to **Issued Certificates**
 - Find the certificate (compare serial numbers and time values)
 - Right-click the certificate and select **Revoke**
 - Select the Reason Code **Certificate Hold** - this provides you with the option to un-revoke the certificates
- Publish the CRL. At the Issuing CA run `certutil -crl`

Effect of Revocation (2)

- Try to authenticate to the website using a revoked certificate
- The same error will be displayed both for <https://trillian.gala.xy> and for <https://trillian.gala.xy/ssltest>

General Comments on Mapping

In the following, you will explore the cert. mapping functionality step-by-step. Note the following:

- Mapping = The web server uses the permissions of a system user to check the authorization status. The certificate presented by a user is "replaced" by that user when the web server evaluates the authorization.
- Mapping can be done on a mapping table maintained at the web server or by a central table – in this case a mapping in the LDAP directory will be used based on the User Principal Name in the certificate. User certificate is mapped to a user if the UPN in the certificate is equal to the UPN attribute in the directory.
- The revocation status is always evaluated when a certificate is presented.
- Note that requiring a client certificate does not yet mean that the certificate is mapped to a specific user with specific credentials.

Tests and Results

- **[PKI-02-02]** Document the results of the following tests (Screenshots and table)

ID	URL	Certificate Selected
1	https://trillian.gala.xy/	Valid
2	https://trillian.gala.xy/	Revoked
3	https://trillian.gala.xy/ssltest	Valid
4	https://trillian.gala.xy/ssltest	Revoked
5	https://trillian.gala.xy/noadminaccess.htm	Valid
6	https://trillian.gala.xy/noadminaccess.htm	Revoked
7	https://trillian.gala.xy/ssltest/noadminaccess.htm	Valid
8	https://trillian.gala.xy/ssltest/noadminaccess.htm	Revoked

Tests and Results (2)

- **[PKI-02-02-cont'd]** Use your results to prove the following
 - "The revocation state of the certificate is evaluated before a (potential) mapping is evaluated"
 - "Mappings do not work if the web server does allow anonymous access"

Security of a Mapping

- **[PKI-02-03]** Directory based mappings are not equal to 1:1 mappings of a binary certificate file to a user. An attribute of the user object in the directory (`userPrincipalName`) is mapped to a 'Principal Name' in the Subject Alternative Attribute in the certificate. How can such a mapping of name strings still be made secure? What are the implications for the process of certificate issuance?

Lab 3: Kerberos Tickets

Kerberos Protocol Details and Troubleshooting

Lab 3 Kerberos Tickets

○ Intentions

- Follow the **flow of tickets** to validate the theoretical **introduction to the protocol** provided in the lecture
- Test your understanding of Kerberos by **troubleshooting two common errors** (simple root cause, still not always easy to find)

○ Exercises

- Inspect tickets using `klist` and Wireshark.
- Troubleshooting and analysis of typical errors

Lab 3 Initial State | Pre-Req's

- Can be done independently from other labs
 - This lab does not rely on certificates
 - There is only a slight interrelation with lab 2: A virtual directory has been created for Kerberos testing – this directory should not be re-configured (Anonymous authentication disabled, only Windows Integrated authentication)
- Both machines are members of the same Kerberos realm (Windows domain in this case)
- The domain user GALA\Administrator is used
- An additional user '**TestKerberos**' has been created (same PW as admin – it is not required to logon in the context of this user. Users can be managed using the tool `dsa.msc` (**Start, Run**, type `dsa.msc`))
- An additional virtual directory **kerbtest** has been created that does only allow for Windows Integrated authentication (not for anonymous / certs.)
- Windows 2008 Internet Explorer Hardening has been disabled (configured already, just FYI)
 - **Start, Server Manager**
 - Scroll to **Security Information**
 - Click **Configure IE ESC**
 - Select **Off** for both **users** and **administrators**

Lab 3 Initial State | Pre-Req's (2)

- All names used in the lab have been added to the Internet Explorer Local intranet Security Zone of the member server (configured already, just FYI)
 - **Start, Internet Explorer**, menu **Tool, Internet Options**
 - Tab **Security**, select **Local Intranet**
 - **Sites, Advanced**
 - URLs added at both machines: ***http(s)://trillian(.gala.xy)***
 - URLs added at TRILLIAN ***http(s)://marvin(.gala.xy)***
- Web Server Logging enabled (configured already, just FYI)
 - **Start, Administrative Tools, IIS Manager**
 - Click symbol for server TRILLIAN
 - Middle pane, **Features View** tab, click Logging
 - Logs in **W3C format** are stored to **%SystemDrive%\inetpub\logs\LogFiles**

Kerberos and Logging Tools

- Klist command line tool (part of operating system)
 - **Start, Run**, type `klist`
- Wireshark network sniffer
 - **Start, All Programs**
 - **Wireshark** (folder)
 - **Wireshark** (program)
- LDAP editor:
 - **Start, Run**
 - Type `adsiedit.msc`
- Web server log files
 - **Start, Run**, type log folder path
 - `C:\inetpub\logs\LogFiles\W3SVC1`

Scenarios to be Tested (Overview)

- The same analysis will be done for the following three scenarios (Details on the data to be collected and analyzed are listed below)
 - Baseline "good" scenario: Kerberos working as expected
 - Name resolution error breaking Kerberos
 - Service Principal Name error breaking Kerberos
- Considering the background information on Kerberos provided in the lecture, it should be explained
 - Which Kerberos tickets are issued
 - Why the above mentioned errors break Kerberos

Tests to be Done

- The following tests will be done for three different scenarios
- Start both virtual machines (only need to be done before testing the first scenario – machines do not need to be rebooted)
 - First start the KDC server (Issuing CA)
 - Then start the member server (Root CA)
- Logon to the member server as GALA\Administrator
- Make changes to name resolution or directory attributes as described below in the scenario details.
- Delete all Kerberos tickets
 - **Start, Run**, type `cmd`
 - `Klist purge`
- Confirm that there are no tickets (neither TGTs nor service tickets) running
 - `Klist tgt`
 - `Klist tickets`

Tests to be Done (2)

- If Internet Explorer is running → close the browser
- At the member server start to capture packets
 - Start **Wireshark**
 - Menu **Capture, Interfaces**
 - Click the **Start** button
- Start Internet Explorer
- Enter the address described in the scenario details in the address bar. Depending on the scenario this is either
 - <http://trillian/kerbtest>
 - <http://marvin/kerbtest>
- Wait until the default page appears
- If you are prompted for credentials try to logon as GALA\Administrator
- In **Wireshark**, select **Capture, Stop**
- Save the capture file using **File, Save As**
- Inspect the tickets and save the dumps of the following commands
 - `Klist tgt`
 - `Klist tickets`

Tests to be Done (3)

- Packets in Wireshare should be analyzed by unfolding the full tree of information to reveal the details of the HTTP or Kerberos specific messages

The screenshot shows a Wireshark capture of a network packet. The packet list pane shows a sequence of packets: a Kerberos message (49681), a TCP reset (49681), an unauthorized HTTP request (49681), and a successful GET request (49680). The selected packet (No. 57) is a GET request for /kerbttest/ HTTP/1.1. The packet details pane shows the following structure:

- Ethernet II, Src: Microsof_46:38:2b (00:03:ff:46:38:2b), Dst: Microsof_45:38:2b (00:03:ff:45:38:2b)
- Internet Protocol, Src: 192.168.77.100 (192.168.77.100), Dst: 192.168.77.101 (192.168.77.101)
- Transmission Control Protocol, Src Port: 49680 (49680), Dst Port: http (80), Seq: 1132, Ack: 2267
- Hypertext Transfer Protocol
 - GET /kerbttest/ HTTP/1.1\r\n
 - Request Method: GET
 - Request URI: /kerbttest/
 - Request Version: HTTP/1.1
 - Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-ms-application, app
 - Accept-Language: de-at\r\n

The packet bytes pane shows the raw data of the request, including the NTLMSSP/GSSAPI data (414 bytes).

The screenshot shows a Wireshark capture of a network packet. The packet list pane shows a sequence of packets: a Kerberos message (49681), a TCP reset (49681), an unauthorized HTTP request (49681), and a successful TGS-REP message (49679). The selected packet (No. 60) is a TGS-REP message. The packet details pane shows the following structure:

- Reassembled TCP Segments (1556 bytes): #58(1460), #59(96)]
- Kerberos TGS-REP
 - Record Mark: 1552 bytes
 - Pvno: 5
 - MSG Type: TGS-REP (13)
 - Client Realm: GALA.XY
 - Client Name (Principal): Administrator
 - Name-type: Principal (1)
 - Name: Administrator
 - Ticket
 - Tkt-vno: 5
 - Realm: GALA.XY
 - Server Name (Service and Instance): LDAP/TRILLIAN.gala.xy/gala.xy

The packet bytes pane shows the raw data of the TGS-REP message, including the reassembled TCP segments (1556 bytes).

Data to be Copied to Documentation

- **[PKI-03-01]** Attach the capture and the ticket dumps of scenario 1 to the documentation.
- **[PKI-03-02]** Attach the capture and the ticket dumps of scenario 2 to the documentation.
- **[PKI-03-03]** Attach the capture and the ticket dumps of scenario 3 to the documentation.

Scenario 1: Base Line

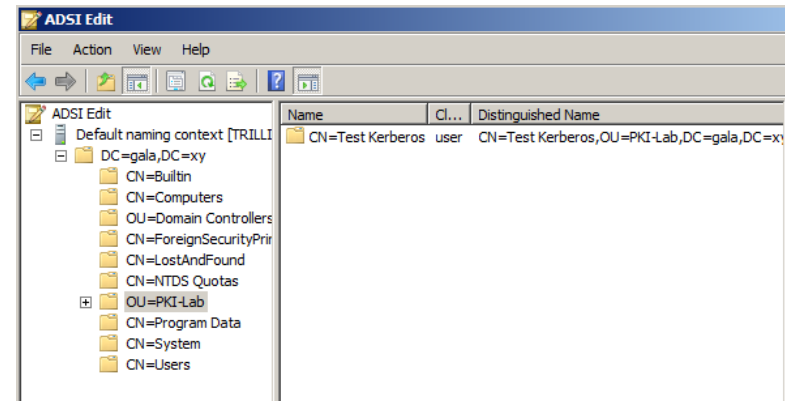
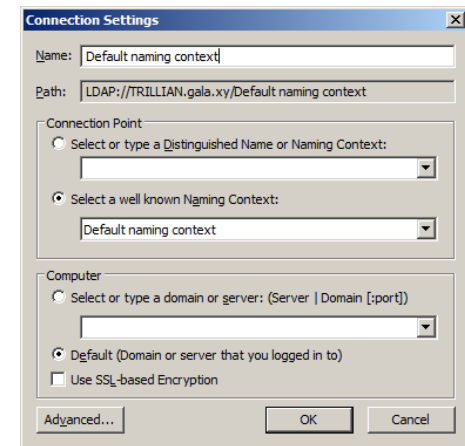
- No changes required
- Name to be used: <http://trillian/kerbtest>
- If you want to repeat the test, make sure that you undo the modification made to a directory object in scenario 3

Scenario 2: Name Resolution

- Name resolution: An alternative name is configured in the local hosts file.
 - If you have changed to IP addresses of the machines navigate to:
`C:\Windows\System32\drivers\etc`
 - Open the file `hosts` with *notepad*
 - Edit the line in the file referring to the machine `marvin` and change the IP address. Default
`192.168.88.88 marvin`
- Name to be used: <http://marvin/kerbtest>

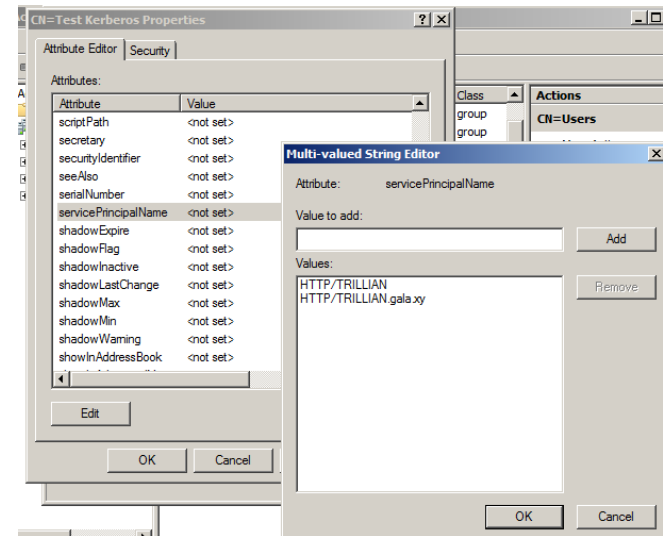
Scenario 3: Service Princ. Name

- At the KDC server...
- Start the LDAP editor
 - **Start, Run**
 - Type `adsiedit.msc`
- Menu **Action, Connect To...**
- Leave the defaults (Domain Naming Context)
- In the left pane open the tree subordinated to the Default Naming Context and locate the User
 - **CN=gala,CN=xy**
 - **OU=PKI-Lab**
 - **CN=Test Kerberos**



Scenario 3: SPN (2)

- Right-click **CN=Test Kerberos**
- **Properties**
- Scroll down to the attribute **servicePrincipalName**
- Add the names
 - HTTP/TRILLIAN.gala.xy
 - HTTP/TRILLIAN



Compare SPNs

- In adsiedit.msc, identify the SPNs assigned to the web server
- In the left pane open the tree subordinated to the Default Naming Context and locate the machine account
 - ***CN=gala,CN=xy***
 - ***CN=Domain Controllers***
 - ***CN=TRILLIAN***

Analyze "Good" Tickets

- **[PKI-03-04] Scenario 1: Analyse the tickets in the klist dump of the "good" baseline and the corresponding capture.**
 - Compare the tickets issued to the explanations of the protocol given in the lecture
 - Identify the packets that indicate the issuance and TGTs and service tickets.
Kerberos section of this lecture.
 - Identify the service ticket issued for the web service. Hint search for the service principal name in the packet contents and the ticket description in the klist dump.
 - Explain why the web server is able to decrypt the Kerberos service ticket. How does the KDC know which encryption ticket to choose to encrypt the ticket?

Analyze Name Problem

- **[PKI-03-05] Scenario 2**
 - Summarize the difference to scenario 1 by comparing dumps and tickets
 - Which tickets have been issued, which are missing?
 - Is the website displayed correctly? Hint: Windows and Internet Explorer may fall back to the "older" authentication method, NTLM. Check the HTTP related packets.
 - Re-visit the explanations on the protocol: Can you explain why this error exactly occurs? What could be done to allow Kerberos authentication when the name marvin is used. Hint: It might help to work on scenario 3 first and then return to this question.

Analyze SPN Problem

- **[PKI-03-06] Scenario 3**
 - Again compare tickets and capture to the good baseline scenario.
 - Explain why Kerberos is failing this time. What is the difference to the error associated with scenario 2?