



Guide to setting up Windows Smart Card Logon using EJBCA

PKI Configuration Guide

Table of contents

1	Configuring the PKI.....	2
1.1	Creating the CA.....	2
1.2	Define a certificate that fulfills all the MS DC requirements.....	3
1.2.1	Create Certificate Profile "DomainController"	3
1.2.2	Create End Entity Profile "DomainController"	5
1.3	Create profiles for end users	6
1.3.1	Create new certificate profile "MSSmartCardLogon"	6
1.3.2	Create new end entity profile "MSSmartCardLogon"	7
1.4	Issue Domain Controller Certificate s for all DCs.....	8
1.4.1	Add end entity "DomainController-001"	8
1.4.2	Fetch certificate.....	9
1.5	Fetch CA certificate.....	10
1.6	Create an end user	11
1.6.1	Add a "MS SmartCardLogon" end entity	11

1 Configuring the PKI

This configuration guide is part of the Windows Smart Card Logon Guide. This document is provided for PKI administrators to configure EJBCA for issuing certificates to domain controllers and smart card users.

Configuring the PKI involves a few steps:

- Creating the CA
- Creating certificate profiles
- Creating end-entity profiles

All of these steps are done in the EJBCA Administration GUI at “<https://ca-machine:8443/ejbcadminweb/>” if nothing else is stated.

1.1 Creating the CA

1. Login to EJBCA Administration GUI
2. Click “Edit Certificate Authorities”
3. Create "MS_SCL_CA_v1"
4. Choose appropriate values for the CA. In this example we use the following:

Type of CA	X509
CA Token Type	Soft
Signing Algorithm	SHA1WithRSA
Key Size	2048
Subject DN	CN=MS SCL CA v1, O=PrimeKey Testing, C=SE
Always use UTF8 strings in subject DN	<input type="checkbox"/>
Signed By	Self Signed
Certificate Profile	ROOTCA
Validity (Days)	3650

The CA is a RootCA (self-signed), uses 2048 bit RSA, DN="CN=MS SCL CA v1,O=PrimeKey Testing,C=SE", validity 3650 days, 24h CRL update interval.

CRL Expire Period (Hours)	24
CRL Issue Interval (Hours)	
CRL Overlap Time (Minutes)	
CRL Publishers	
Default CRL Dist. Point (Used as default value in certificateprofiles using this CA.)	<input type="text" value="http://ca.testing.primekey.se:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=MS SCL C"/> <input type="button" value="Generate"/>

Press "Generate" to generate the CRL Distribution Point (CDP). Edit the address to point to the CA's DNS name (ca.testing.primekey.se).

As an alternative, you can copy the CRL to another location from the PKI service provider and use this URL as CDP. This can make the system more resilient to network outages. To set up a local CDP only a simple web server is needed.

****Test if MS SCL fetches all the CRLs or only the first.. if so: recommend to use the CA URL as the last one for better reliability without overloading the CA****

1.2 Define a certificate that fulfills all the MS DC requirements (This step can be omitted if the profiles were imported.)

1.2.1 Create Certificate Profile "DomainController"

1. Check "Use CRL Distribution Point"
2. Select "Key Usage" "Digital Signatures" and "Key encipherment"



Use CRL Distribution Point	<input checked="" type="checkbox"/>
CRL Distribution Point Critical	<input type="checkbox"/>
Use CA defined CRL Dist. Point	<input checked="" type="checkbox"/>
CRL Distribution Point URI	<input type="text"/>

3. Check "Use Extended Key Usage"

4. Select "Extended Key Usage" "Server Authentication" and "Client Authentication"

5. Check "MS Template Value"

Key usage	<ul style="list-style-type: none"> Digital Signature Non-repudiation Key encipherment Data encipherment Key agreement Key certificate sign CRL sign Encipher only Decipher only
Allow Key Usage Override	<input checked="" type="checkbox"/>

Use Extended Key Usage	<input checked="" type="checkbox"/>
Extended Key Usage Critical	<input type="checkbox"/>

Extended Key Usage	<ul style="list-style-type: none"> Any Extended Key Usage Server Authentication Client Authentication Code Signing Email Protection IPSec End System IPSec Tunnel IPSec User Time Stamping MS Smart Card Logon OCSPSigner
--------------------	--

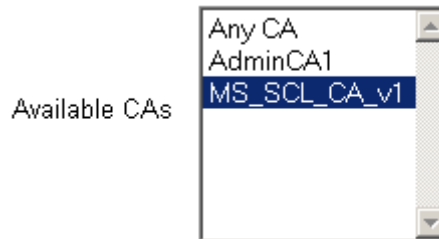
Use MS Template Value	<input checked="" type="checkbox"/>
-----------------------	-------------------------------------

Microsoft Template Value (Only the value not the actual template)	DomainController
--	------------------

6. Check "Use a Subset of Subject Alt. Name"

7. Select "Subset of Subject Alt. Name" "Global Unique Id" "DNS"

8. Select "Available CAs" "MS_SCL_CA_v1"



The rest should use the default values

1.2.2 Create End Entity Profile "DomainController"

1. Use required CN

CN, Common Name

Required Modifyable

2. Add required Subject Altname GUID

3. Add required Subject Altname DNS

DNS Name

Required Modifyable

Globally Unique Id

Required Modifyable

4. Uncheck use email

Email Domain

(Use only the domain part of address, without '@' char) Use Required Modifyable

5. "Default Certificate Profile" "DomainController"

6. Select "Available Certificate Profiles" "DomainController"

7. "Default CA" "MS_SCL_CA_v1"

8. Select "Available CAs" "MS_SCL_CA_v1"



Default Certificate Profile	DomainController
Available Certificate Profiles	DomainController ENDUSER OCSPSIGNER
Default CA	MS_SCL_CA_v1
Available CAs	AdminCA1 MS_SCL_CA_v1
Default Token	User Generated
Available Tokens	User Generated P12 file JKS file PEM file

The rest can use default option.

1.3 Create profiles for end users

(This step can be omitted if the profiles were imported.)

1.3.1 Create new certificate profile "MSSmartCardLogon"

1. Check "Use CRL Distribution Point"

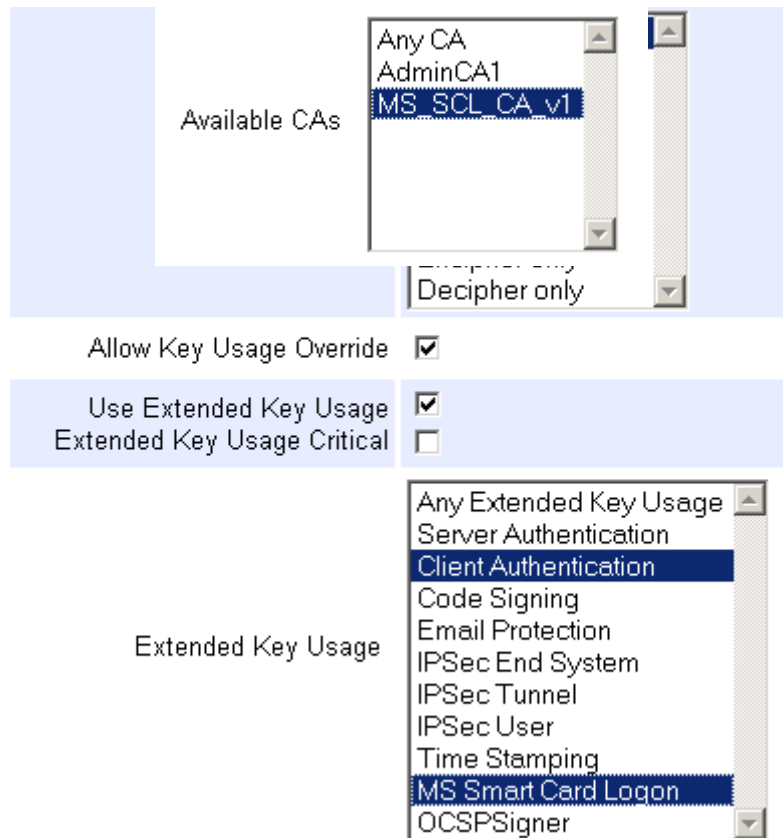
Use CRL Distribution Point	<input checked="" type="checkbox"/>
CRL Distribution Point Critical	<input type="checkbox"/>
Use CA defined CRL Dist. Point	<input checked="" type="checkbox"/>
CRL Distribution Point URI	

2. Select "Key Usage" "Digital Signatures"

3. Check "Use Extended Key Usage"

4. Select "Extended Key Usage" "Client Authentication" and "MS Smart Card Logon"

5. Select "Available CAs" "MS SCL CA v1"



The rest should use the default values

1.3.2 Create new end entity profile "MSSmartCardLogon"

1. Use required CN

CN, Common Name
Required Modifyable

2. Uncheck use email

Email Domain
(Use only the domain part of address, without '@' char) Use Required Modifyable

3. Add required UPN=testing.primekey.se (if username@testing.primekey.se is the identifier)

UPN (domain part only)
Required Modifyable

4. "Default Certificate Profile" "MS SmartCardLogon"

5. "Available Certificate Profiles" "MS SmartCardLogon"

6. "Default CA" "MS SCL CA v1"

7. "Available CAs" "MS SCL CA v1"



Default Certificate Profile

Available Certificate Profiles

- DomainController
- ENDUSER
- MSSmartCardLogon**
- OCSPSIGNER

Default CA

Available CAs

- AdminCA1
- MS_SCL_CA_v1**

The rest should use the default values

1.4 Issue Domain Controller Certificate s for all DCs

In our example there is only one. Repeat this for each DC.

1.4.1 Add end entity "DomainController-001"

1. Set "Username" to "DomainController-001"
2. Set "Password" to "foo123"
3. Set required CN=<<name of domain controller>>
4. Set DNS=<<from "DomainControllerInfo-<hostname>.txt">>
5. Set GUID=<<from "DomainControllerInfo-<hostname>.txt">>



End Entity Profile	DomainController	Required
Username	DomainController-001	<input checked="" type="checkbox"/>
Password	XXXXXXXXXX	<input checked="" type="checkbox"/>
Confirm Password	XXXXXXXXXX	
Subject DN Fields		
CN, Common Name	milton	<input checked="" type="checkbox"/>
Subject Alternative Name Fields		
DNS Name	milton.testing.primekey.se	<input checked="" type="checkbox"/>
Globally Unique Id	8ff85d36b034f9488726cd5011e47377	<input checked="" type="checkbox"/>
Certificate Profile	DomainController	<input checked="" type="checkbox"/>
CA	MS_SCL_CA_v1	<input checked="" type="checkbox"/>
Token	User Generated	<input checked="" type="checkbox"/>
<input type="button" value="Add End Entity"/>		<input type="button" value="Reset"/>

1.4.2 Fetch certificate

1. Go to EJBCA's Public Web Pages
2. Click "Manually or for a server"
3. Enter username "DomainController-001"
4. Enter password "foo123"
5. Paste the content of "DomainControllerCertRequest-<hostname>.req" that was generated on the Domain Controller.
6. Choose PKCS7

New EJBCA Public Web Pages → Fetch CA & OCSP Certificates → For Internet Explorer
 “CN=MS SCL CA v1,O=PrimeKey Testing,C=SE” → Save as “MS_SCL_CA_v1.cer”

Installing this certificate is described “EJBCA-SmartCardLogon-Guide-Windows”.

1.6 Create an end user

1.6.1 Add a “MS SmartCardLogon” end entity

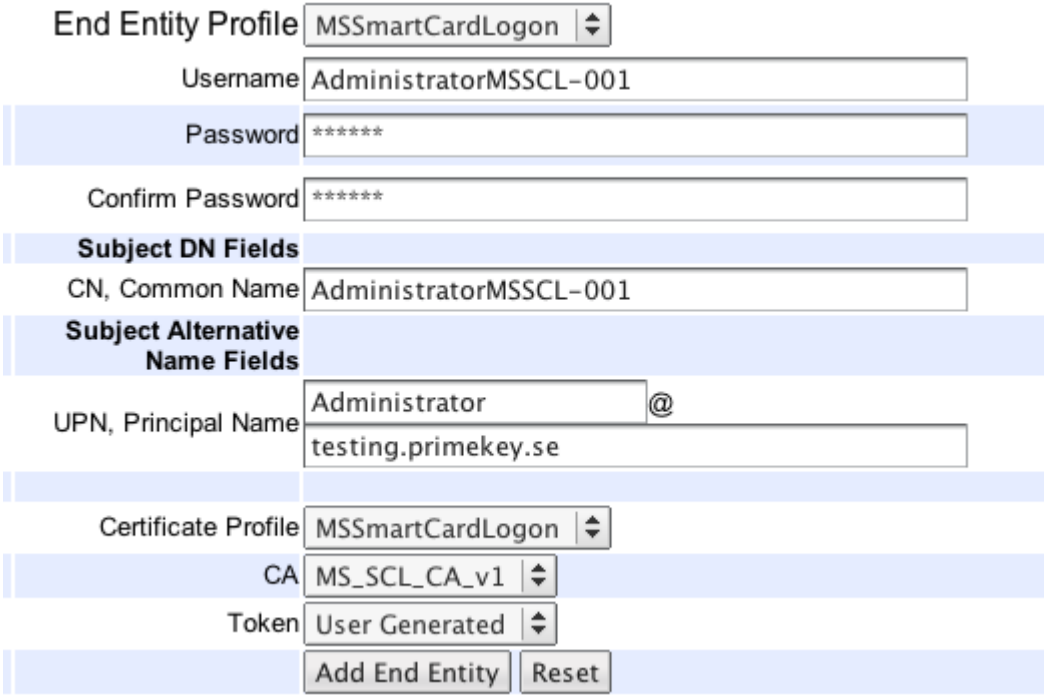
We start by creating an “Administrator” token, since we know this user exists and can logon by default.

Username AdministratorMSSCL-001 (Can be any unique value.)

Password foo123 (Can be any unique value.)

CN=AdministratorMSSCL-001 (Can be any unique value.)

UPN=Administrator@testing.primekey.se



End Entity Profile

Username

Password

Confirm Password

Subject DN Fields

CN, Common Name

Subject Alternative Name Fields

UPN, Principal Name

Certificate Profile

CA

Token

Make sure to give the Username and Password to the person that does the enrollment.