Guide to setting up Windows Smart Card Logon using EJBCA

PKI Configuration Guide

Table of contents

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.

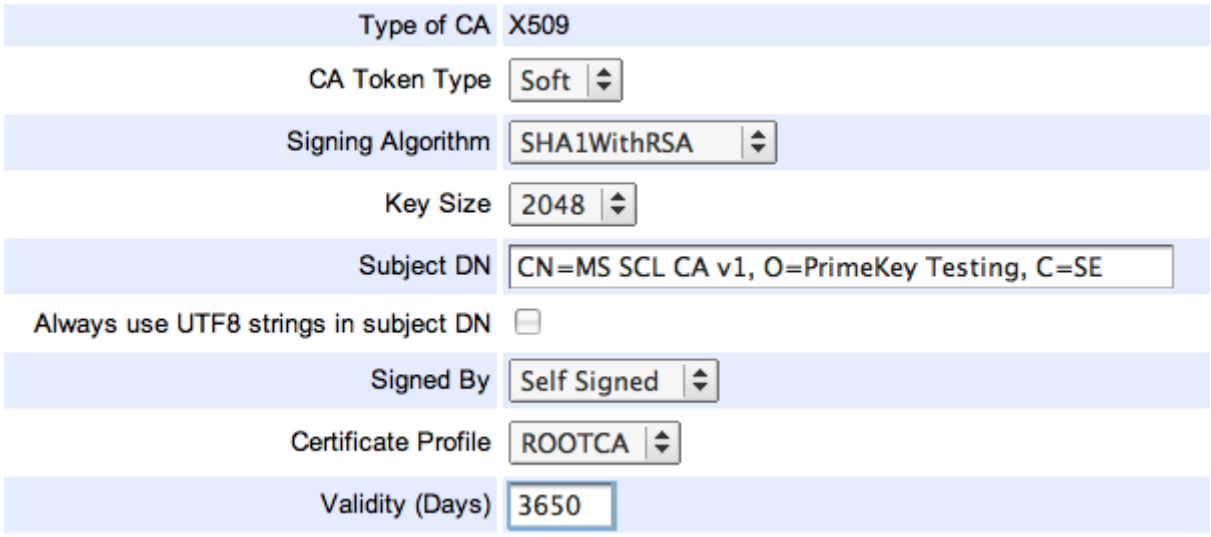
Configuring the PKI involves a few steps:

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

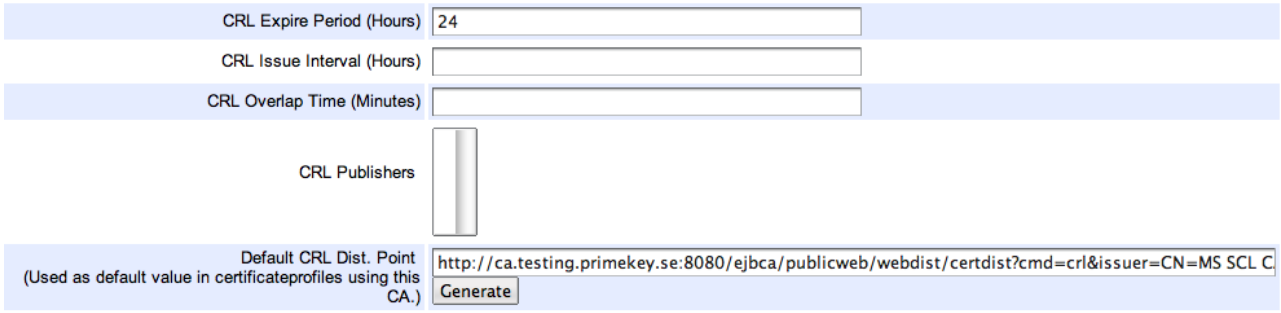
All of these steps are done in the EJBCA Administration GUI at "https://ca-machine:8443/ejbca/adminweb/" if nothing else is stated.

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:



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.



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

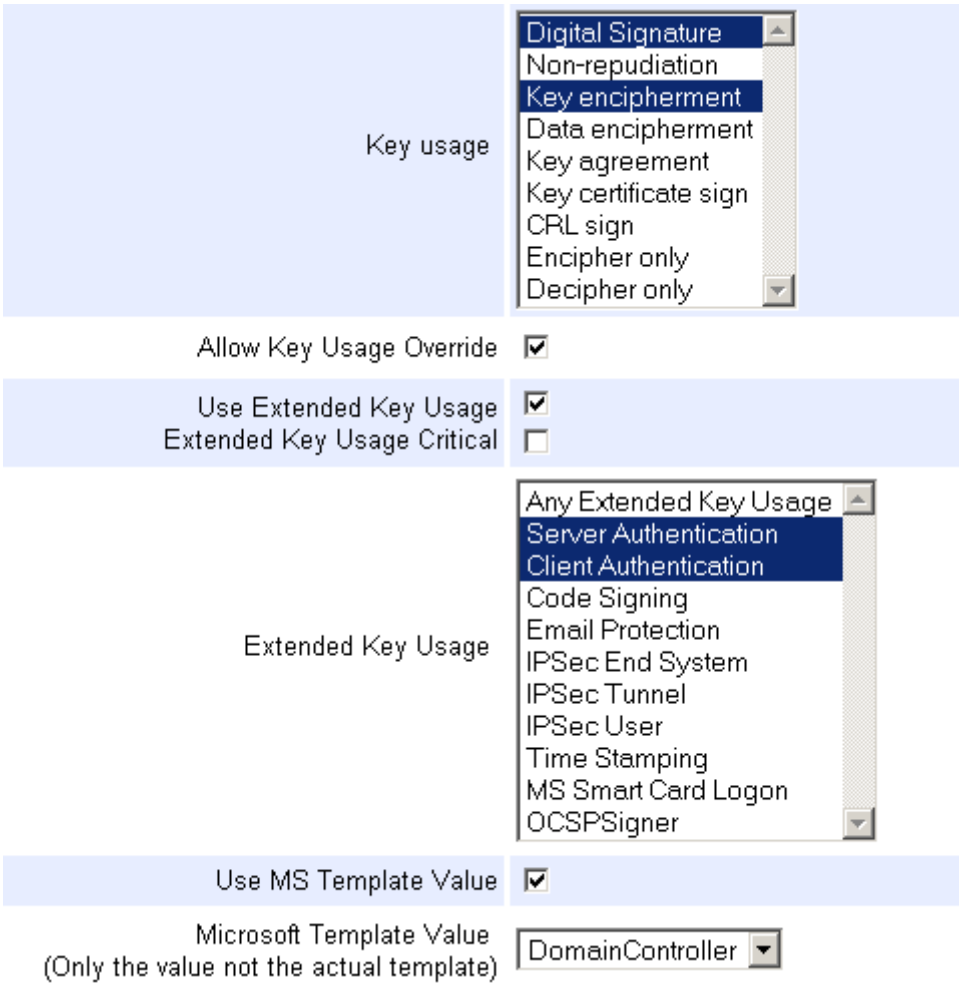
1.2 Define a certificate that fulfills all the MS DC requirements

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

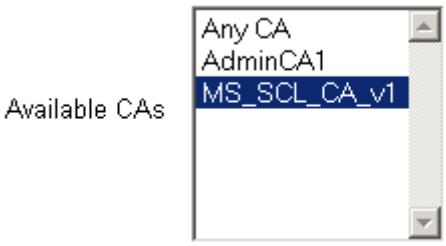
1.2.1 Create Certificate Profile "DomainController"

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

3. Check "Use Extended Key Usage"
4. Select "Extended Key Usage" "Server Authentication" and "Client Authentication"
5. Check "MS Template Value"



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"

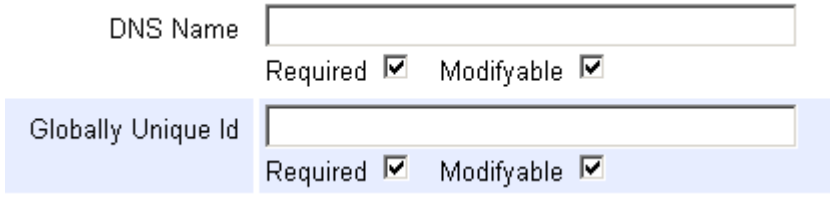


The rest should use the default values

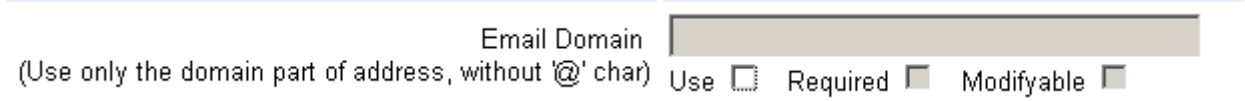
1.2.2 Create End Entity Profile "DomainController"

1. Use required CN

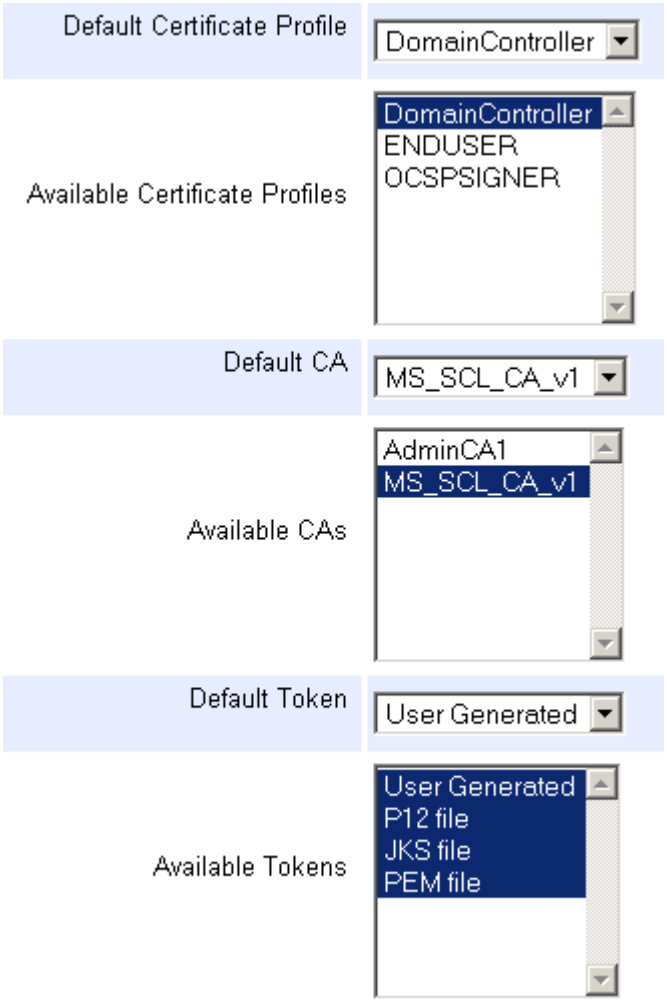
2. Add required Subject Altname GUID
3. Add required Subject Altname DNS



4. Uncheck use email



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"



The rest can use default option.

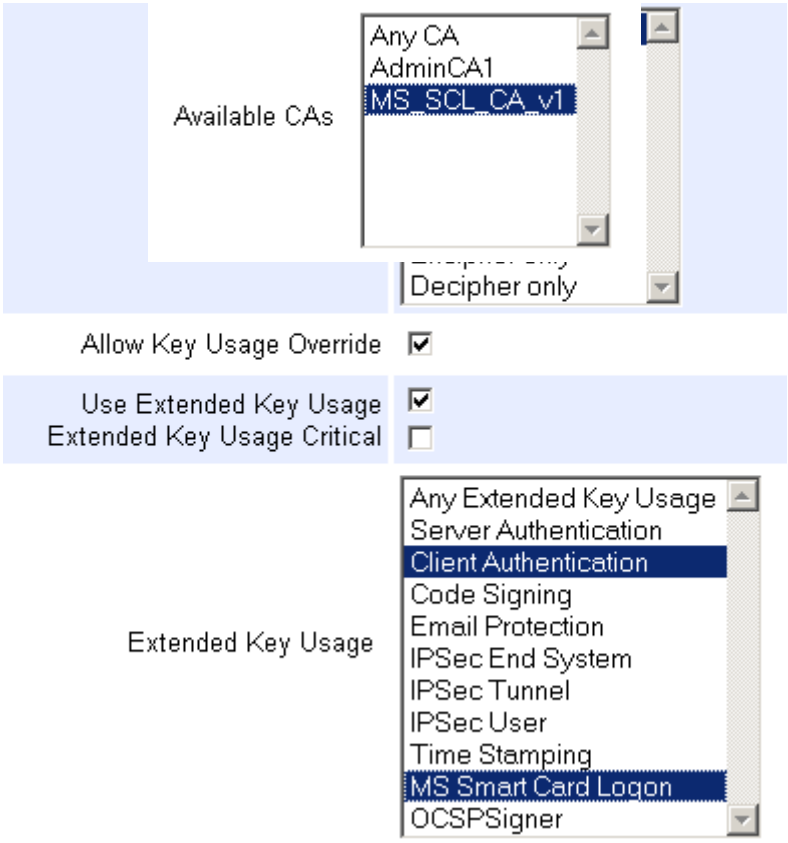
1.3 Create profiles for end users

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

1.3.1 Create new certificate profile "MSSmartCardLogon"

1. Check "Use CRL Distribution Point"

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"

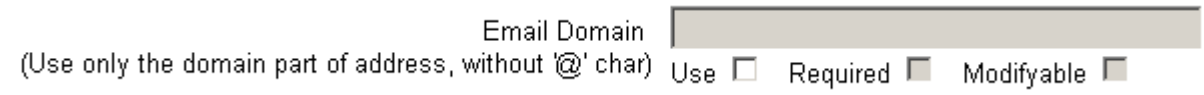


The rest should use the default values

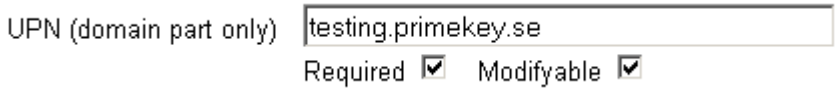
1.3.2 Create new end entity profile "MSSmartCardLogon"

1. Use required CN

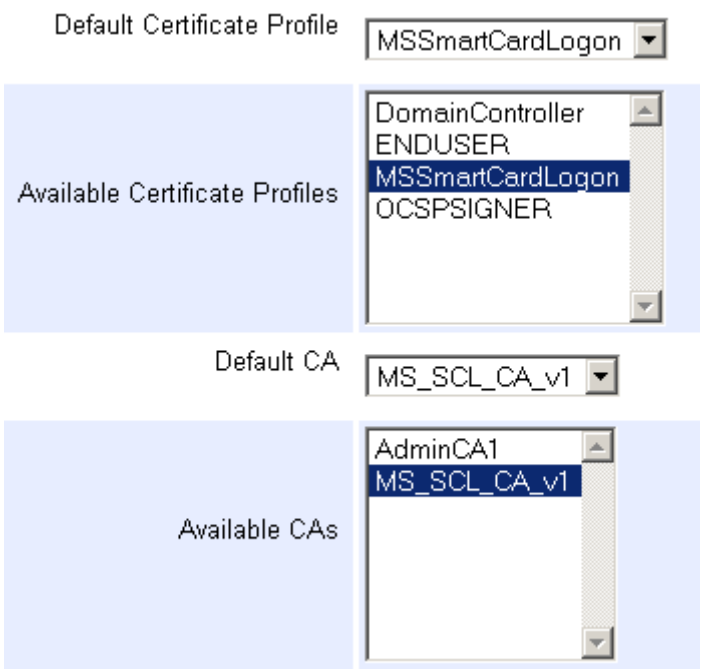
2. Uncheck use email



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



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"



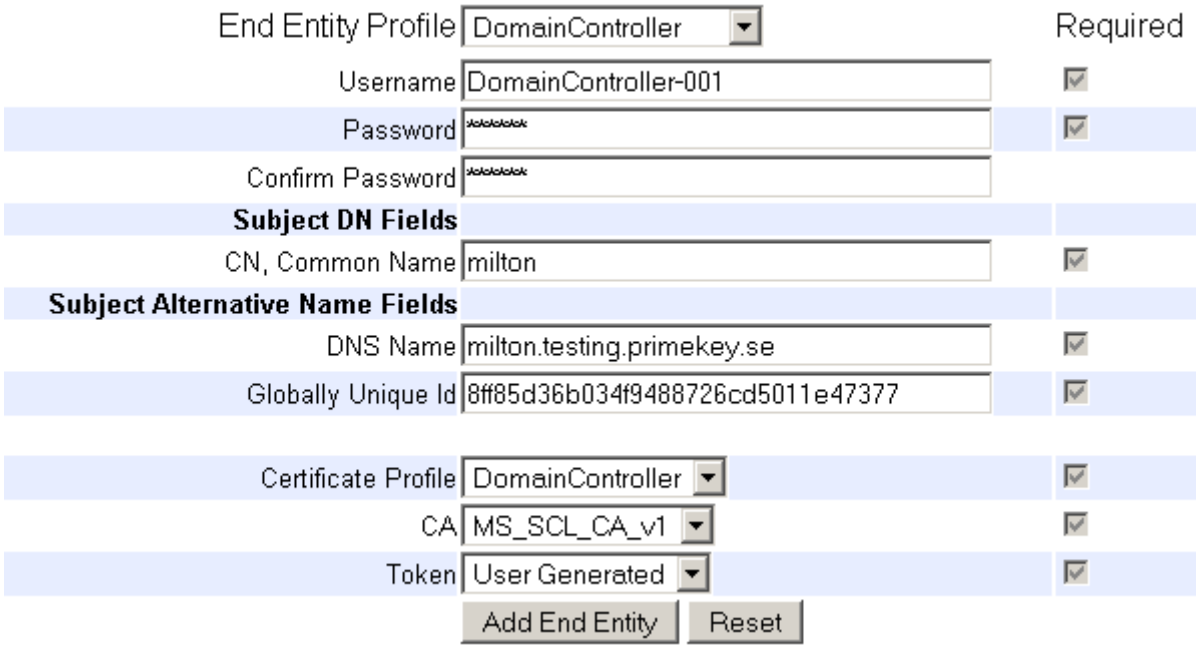
The rest should use the default values

1.4 Issue Domain Controller Certificate s for all DCs

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

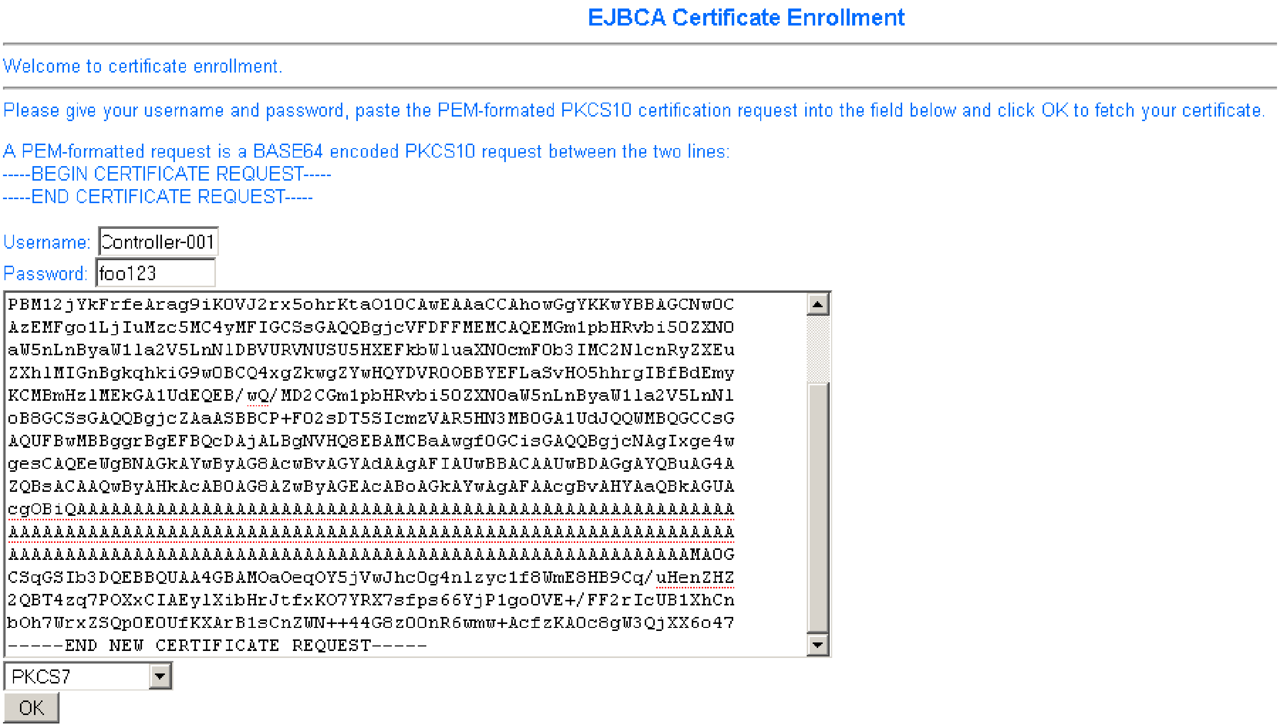
1.4.1 Add end entity "DomainController-001"

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">>

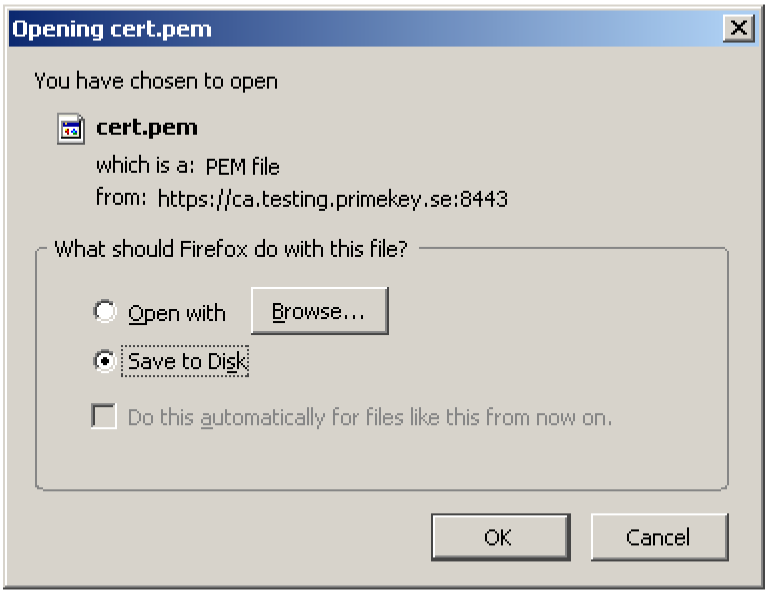


1.4.2 Fetch certificate

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



7. Save the certificate to disk an rename the to "DomainControllerCert-<hostname>.p7b"



Install each DC certificate as described in “EJBCA-SmartCardLogon-Guide-Windows”.

1.5 Fetch CA certificate

The CA certificate can be downloaded from the
Old EJBCA Public Web pages → View Certificates → Fetch CA and OCSP certificate(s) → For Internet Explorer “CN=MS SCL CA v1,O=PrimeKey Testing,C=SE” → Save as “MS_SCL_CA_v1.cer”

or

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"

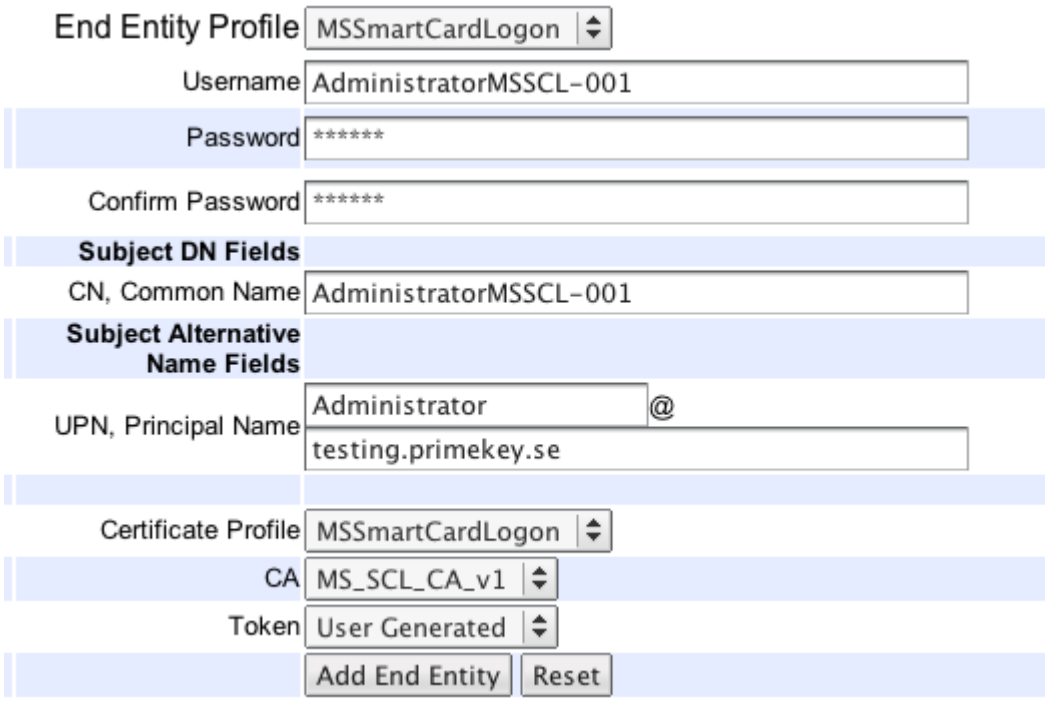
Installing this certificate is described "EJBCA-SmartCardLogon-Guide-Windows".

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



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