PKI SmartCardLogon Integration Guide

Introduction

PKI support the issuance of certificates for use with Microsoft Smart Card Logon platform implementation.

This requires three main steps:

- Trusting the CA certificate at domain level
- Enrolling the Domain Controllers
- Enrolling the Users

Trusting the CA certificate

Do the following steps:

1. Download the CA certificate (from "CA Management" section)
2. Execute, as administrator with "Enterprise Admins" rights:

```
certutil -dsPublish -f c:\path\to\ca.crt RootCA
certutil -dsPublish -f c:\path\to\ca.crt NTAuthCA
gpupdate /force
```

Enrolling Domain Controllers

Do the following steps:

1. Use ldp.exe to find the DC's objectGUID under CN=NTDS Settings, CN=<DCName>, CN=Servers, CN=<site-name>, CN=Sites, CN=Configuration, DC=<mydomain>, DC=<com>
2. Create a file named "Request.inf" with following content:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
KeySpec = 1
KeyLength = 2048
Exportable = FALSE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
```

```
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[Extensions]
2.5.29.17="{text}"
_continue_="guid=<objectGUID>&"
_continue_="dns=<DCName_as_FQDN>&"
```

Then:

1. Issue the following command, as administrator:
   ```
   certreq -new c:\path\to\Request.inf req.csr
   ```
2. Then, use the generated "req.csr" to request a certificate from the PKI with the following parameters:
   1. CN: <DCName_as_FQDN>
   2. Email: <your_email>
   3. Certificate Type: Microsoft Domain Controller (PKCS#10 checked)
   4. PKCS10: req.csr
3. Copy the generated certificate as "dccert.cer", and execute:
   ```
   certreq -accept c:\path\to\dccert.cer
   ```
4. Verify by launching:
   ```
   certutil -dcinfo -urlfetch verify
   ```

Enrolling Users

To enroll the users, you need to provide the following information for the certificate request:

- CN: User's first and last name
- Email: User's Microsoft UPN (User Principal Name)
- Certificate Type: Microsoft Smartcard Logon

You can find the user's Ms UPN at several places, e.g. the "Account" tab of the user in the "AD Users and Computers" administrative tool.
The Ms UPN is in the form of "<login>@<full_domain>".

Finally, when using the PKI through Internet Explorer (10+), you'll see a checkbox called "SmartCard" appear, in order to generate the private key directly into the Smart Card or Token, and import the certificate into the token as well.