Fusion Token Creation Using Windows Native Tools

1.0 Purpose:

The purpose of this SOP is to document the enrollment of Fusion tokens for use with PKI certificates using MS Windows native tools.

1.1 Server/Machine affected:

- Windows Server

1.2 Materials Required:

- Latest Safenet Authentication Client
- Thales eToken or smart card that supports PKI x.509 certificates

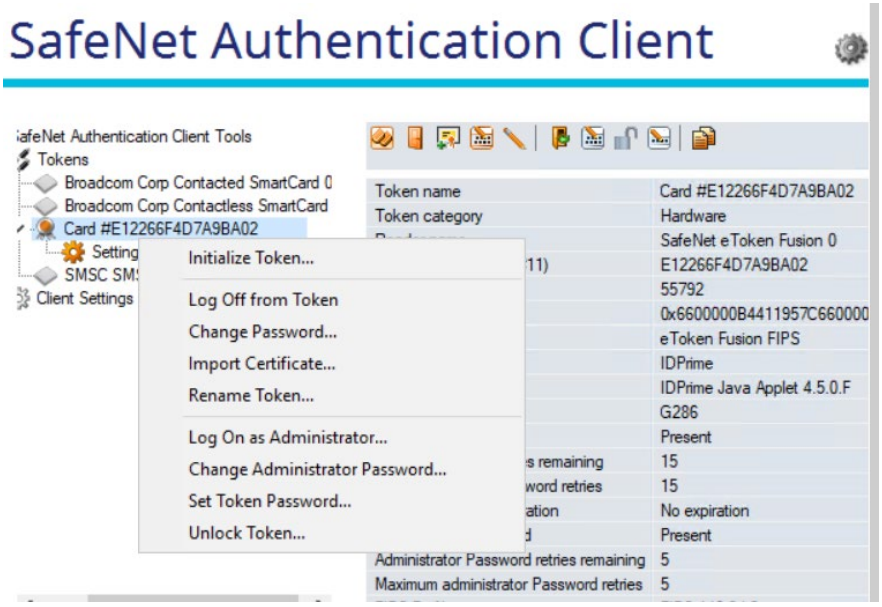
1.3 Prerequisites:

- Existing Active Directory and Public Key Infrastructure

2.0 SOP Tasks:

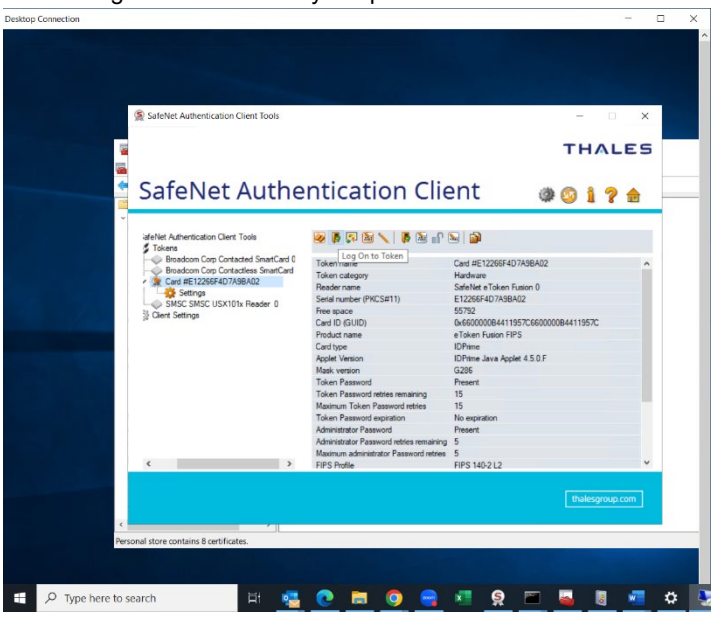
Step 1. Initialize the token and set the token password

1. Launch the Safenet Authentication Client Tools
2. Right click on the token and choose initialize.



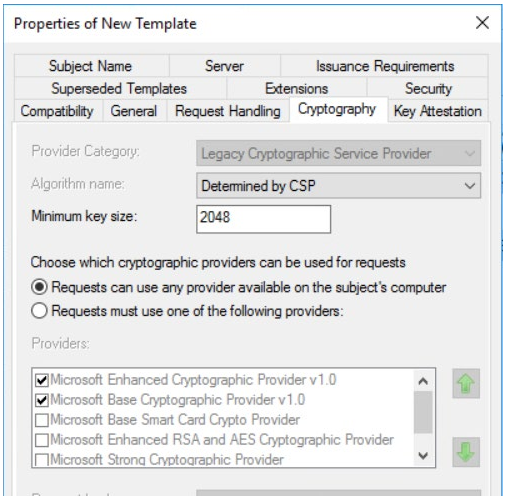
3. Choose preserve the token settings and policies.
4. Check use factory default administrator password and select next.

5. Type in a new token password (twice). Uncheck the token password must be changed on first logon.
6. Set and record an administrator password or check keep the current administrator password (default is 48 zeros). PLEASE NOTE: If you change the administrator PIN/password on the token and you misplace/forget/mistype the PIN/password you will brick the token and it will be unusable and you will not be able to reinitialize it. The PIN/password, without a CMS, is only stored on the token/smart card itself, thus the recommendation for the CMS to manage the token/smart card PINs.
7. Choose finish and choose OK.
8. Choose logon to token and try the password.



Step 2. Modify certificate templates on ADCS to allow for enrollment

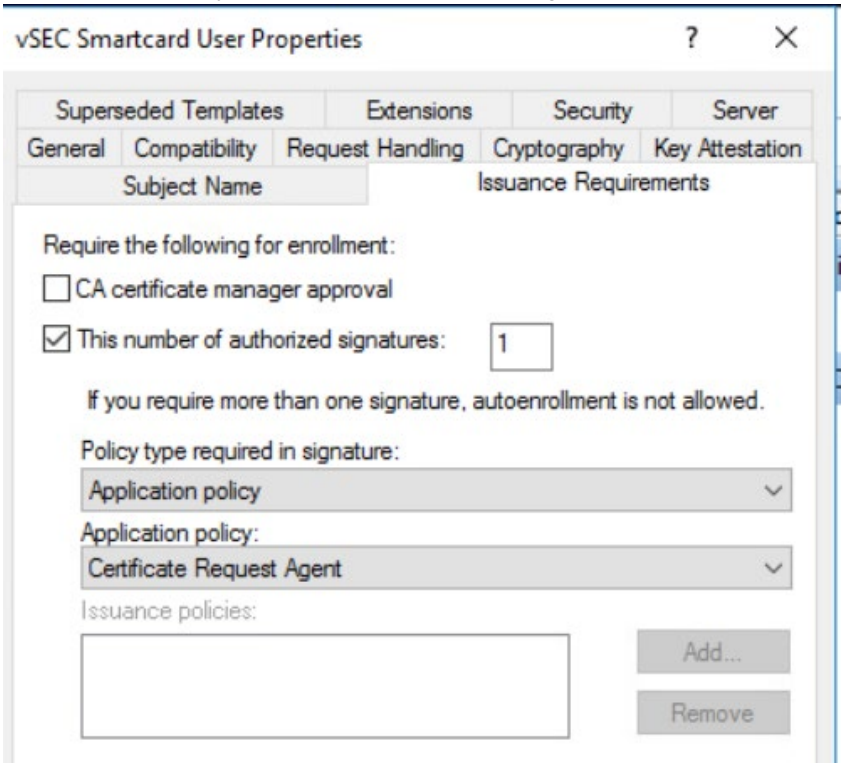
1. Launch the Certification Authority MMC console.
2. Expand your CA.
3. Right click on the Certificate Templates folder and choose manage.
4. Double click on your enrollment agent template.
5. Choose the Cryptography tab.
6. Choose “Requests can use any provider available on the subject’s computer” for the Choose which cryptographic providers can be used for requests options. (Note: This allows for the use of the Thales eToken Fusion minidriver on your enrollment station or CMS server. The Thales driver needs to be chosen when executing the certificate enrollment process. Using the default Microsoft smartcard driver will result in an error.)



7. Click Ok.
8. Double click your smart card certificate template.
9. Choose the Cryptography tab.
10. Choose “Requests can use any provider available on the subject’s computer” for the Choose which cryptographic providers can be used for requests options. (Note: This allows for the use of the Thales eToken Fusion minidriver on your enrollment

station or CMS server. The Thales driver needs to be chosen when executing the certificate enrollment process. Using the default Microsoft smartcard driver will result in an error.)

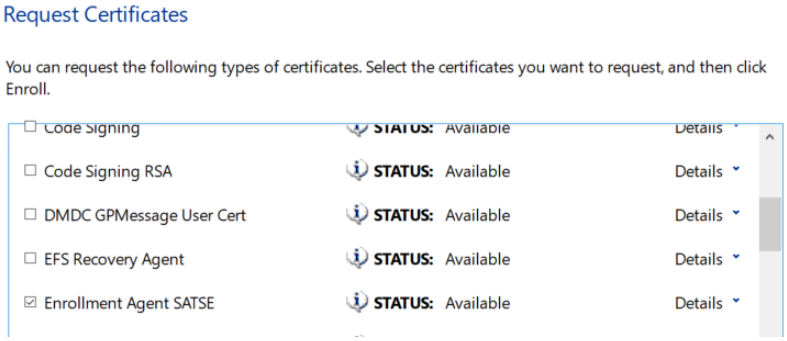
11. Choose the issuance requirements tab.
12. Check the “This number of authorized signatures” option and set the value to 1.
13. For policy type required in signature choose Application Policy.
14. For application policy choose Certificate Request Agent.



15. Select OK.
16. Publish the enrollment agent and smart card certificates.

Step 3. Request an enrollment agent certificate

1. Launch certificates.msc console.
2. Right click on the personal folder.
3. Choose All Tasks -> Request new certificate.
4. Choose Next at the “Before you Begin” window.
5. Choose Next at the Enrollment Policy window.
6. Select the enrollment agent certificate.

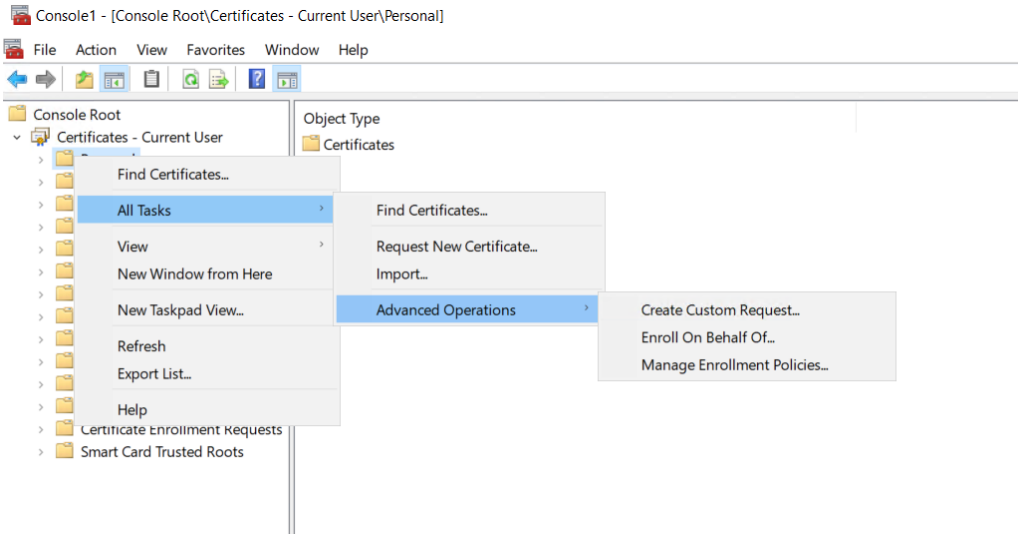


7. Choose enroll.
8. Ensure the process completes successfully and close the window.

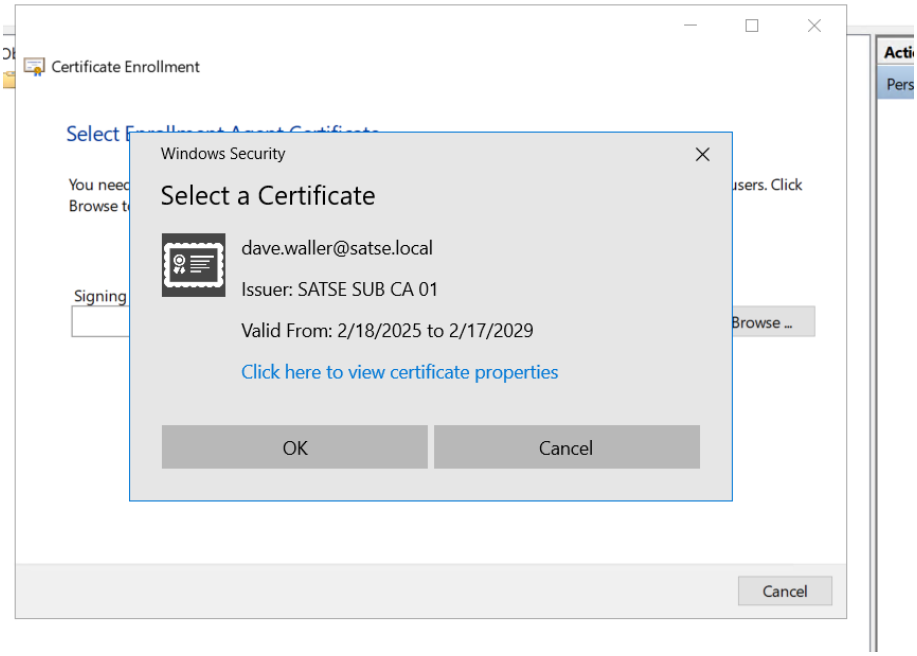
Step 4. Request certificate on behalf of user

9. Launch certificates.msc console.
10. Right click on the personal folder.

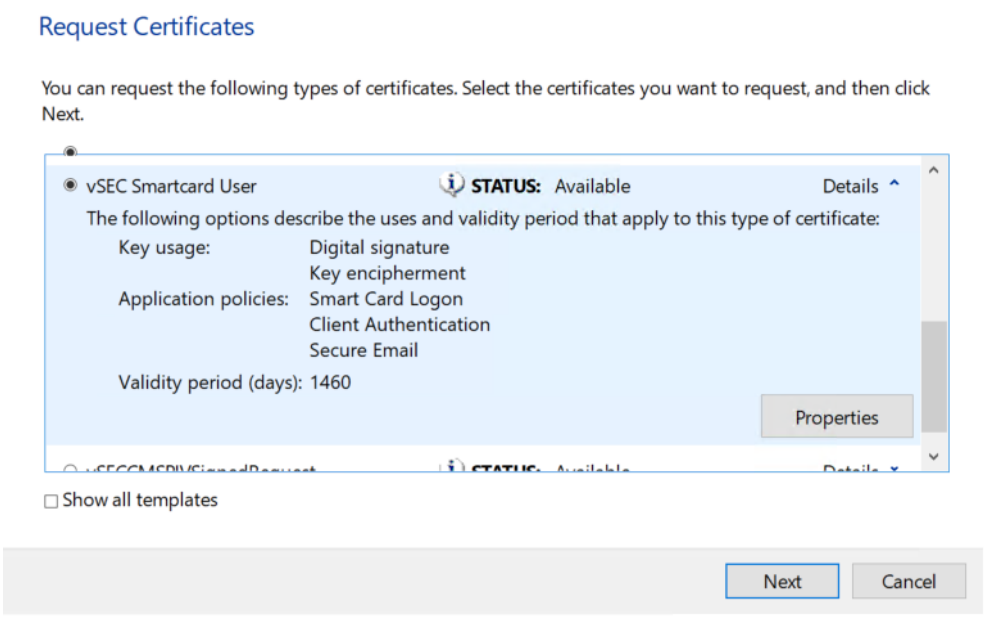
11. Choose all tasks -> Advanced Operations -> Enroll on behalf of.



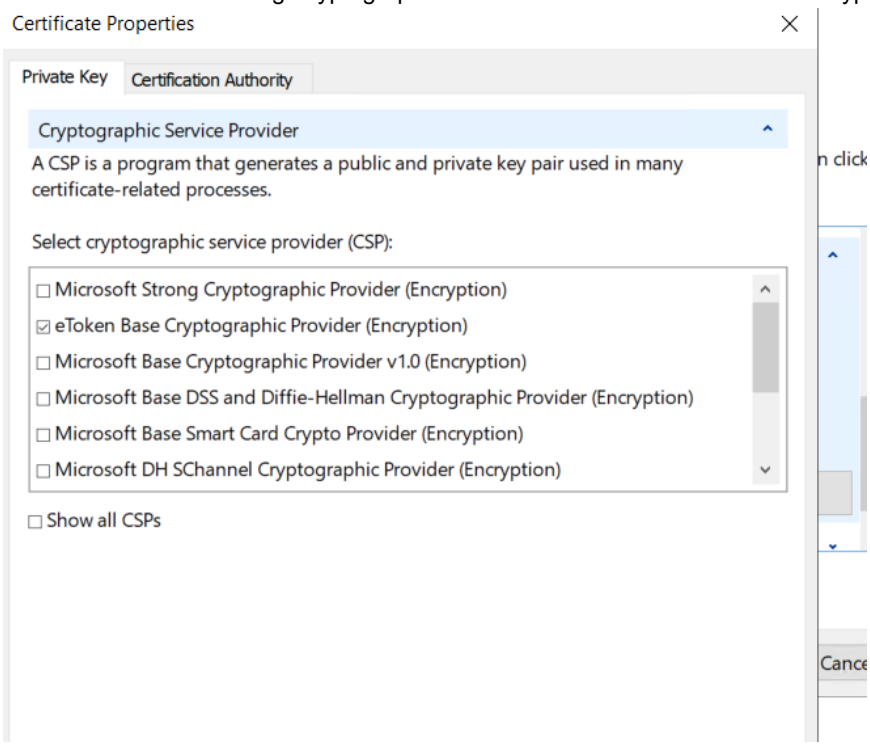
12. Choose next at certificate enrollment
13. Choose next.
14. Select the Enrollment Agent certificate.



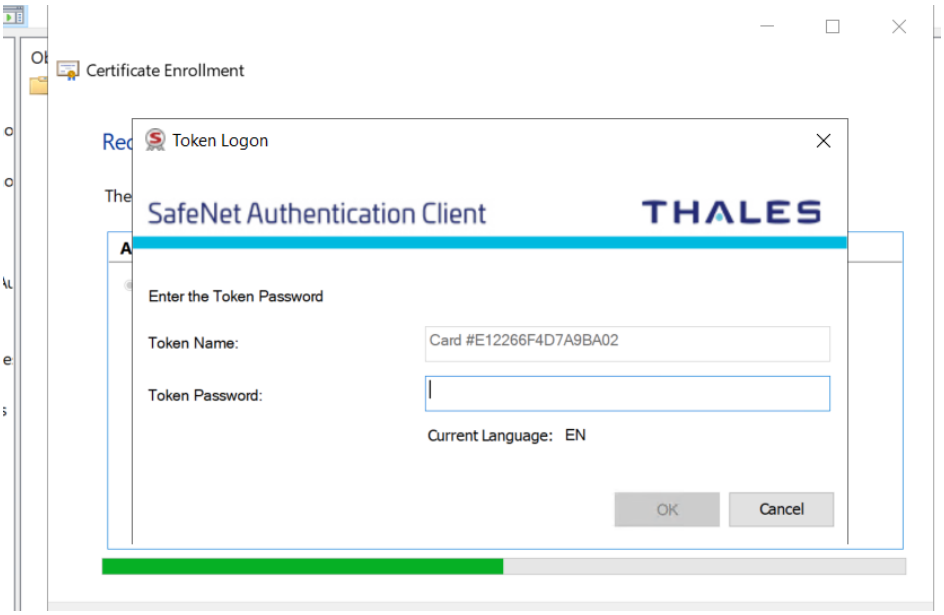
15. Choose next.
16. Select the certificate template to use. Expand the properties before choosing next.
17. Click on properties.



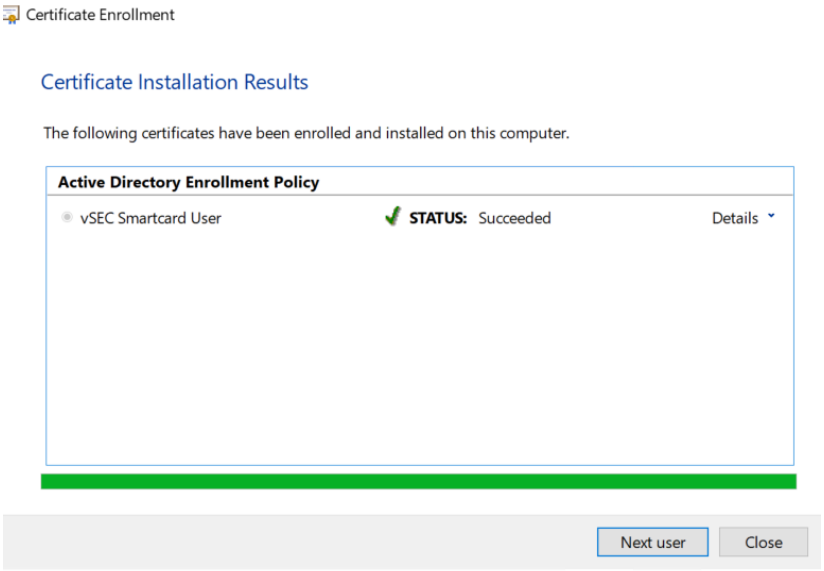
18. Click on the private key tab. Expand cryptographic service provider.
19. Uncheck “Microsoft Strong Cryptographic Provider” and check eToken Base Cryptographic provider.



20. Select OK.
21. Click on next.
22. Choose browse at the select a user window.
23. Select a user from your AD domain.
24. Select enroll
25. At the password prompt enter your token password.



26. Click OK.
27. Ensure the process completes successfully.



28. Select Close.

Verify the certificate is available on the token through the SAC tools console.

1. Launch the SAC tools console.
2. Navigate to the token.
3. Ensure the new certificate is available.