

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.

SafeNe	et Authe	nticat	ion Clie	ent 🧔
afeNet Authentication 5 Tokens	n Client Tools	🥺 🔒 🗊 🙆	i 🔪 i 🖡 🔊 🔐 i	2 2
Broadcom Corp Contacted SmartCard 0		Token name		Card #E12266F4D7A9BA02
	Contactless SmartCard	Token category		Hardware
 Card #E12266 		D		SafeNet e Token Fusion 0
SMSC SM	Initialize Token		11)	E12266F4D7A9BA02
Client Settings	Lon Off from Token			55792
g client Settings	Log Off from Token			0x6600000B4411957C66000
	Change Password Import Certificate Rename Token			e Token Fusion FIPS
				IDPrime
				IDPrime Java Applet 4.5.0.F
				G286
	Log On as Administra	tor		Present
	Change Administrato	Password	s remaining	15
	-		word retries	15
	Set Token Password		ation	No expiration
	Unlock Token		đ	Present
		Administrator Pa	ssword retries remaining	5
		Maximum admin	istrator Password retries	5

- 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.

SafeNet Authentication Client Tools		-	
		тн	ALES
SafeNet Authe	ntication Clie	ent 🔹 💿 👔	? 🚖
afeNet Authentication Client Tools			
Tokens Broadcom Corp Contacted SmartCard 0	Log On to Token		
Broadcom Corp Contacted SmartCard U Broadcom Corp Contactless SmartCard	Tokenmarrie	Card #E12266F4D7A9BA02	
Card #E12266F4D7A9BA02	Token category	Hardware	
Settings	Reader name	SafeNet eToken Fusion 0	
SMSC SMSC USX101x Reader 0	Serial number (PKCS#11)	E12266F4D7A9BA02 55792	
Client Settings	Free space Card ID (GUID)	0x6600000B4411957C6600000B4411957C	
	Product name	e Token Fusion FIPS	
	Card type	IDPrime.	
	Applet Version	IDPrime Java Applet 4.5.0.F	
	Mask version	G286	
	Token Password	Present	
	Token Password retries remaining	15	
	Maximum Token Password retries	15	
	Token Password expiration	No expiration	
	Administrator Password	Present	
	Administrator Password retries remaining	5	
	Maximum administrator Password retries	5	
< >	FIPS Profile	FIPS 140-2 L2	

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.

Super	seded Template	s	Extensions		Security		Server
General	Compatibility	Request	Handling	Crypto	graphy	Key A	Attestation
	Subject Name			ssuanc	e Requir	ements	5
	the following for certificate mana number of auth	ger approv	val	1			
	ou require more cy type required			autoenro	ollment is	not all	owed.
Ap	plication policy						~
Арр	lication policy:						
Ce	rtificate Reques	t Agent					~
	uance policies:						
Issu	vanue policies.						
Issu	ance policies.				1	Ac	id

- 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.

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

V SIALUS: Available	Details
🗘 STATUS: Available	Details 👗
🗘 STATUS: Available	Details 👗
😲 STATUS: Available	Details *
🗘 STATUS: Available	Details *
	 STATUS: Available STATUS: Available STATUS: Available

- 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.

Console1 - [Console Root\Certificates - Current User\Personal]

Console Ro	Current lier	ect Type ertificates	
 > ><	All Tasks > View > New Window from Here	Find Certificates Request New Certificate Import	
> 11 > 11 > 11 > 11 > 11 > 11	New Taskpad View Refresh Export List	Advanced Operations	Create Custom Request Enroll On Behalf Of Manage Enrollment Policies
> 📫 > 📔 Cert	Help iticate Enrollment Requests irt Card Trusted Roots		

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

) IC	🛱 Certificate En	rollment	_			×	ers
	Select F	Windows Security		×			
	You need Browse to	Select a Certificate	ŕ		users. Clic	k	
	Signing	dave.waller@satse.local Issuer: SATSE SUB CA 01 Valid From: 2/18/2025 to 2/17/2029 Click here to view certificate proper			Browse		
		ОК	Cancel				
					Cano	cel	

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

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Next.

vSEC Smartcard User	i) STATUS: Available	Details ^	^
The following options de	escribe the uses and validity period that apply to th	is type of certificate:	
Key usage:	Digital signature		
	Key encipherment		
Application policies:	Smart Card Logon		
	Client Authentication		
	Secure Email		
Validity period (days	i): 1460		
		Properties	
			~

- 18. Click on the private key tab. Expand cryptographic service provider.
- 19. Uncheck "Microsoft Strong Cryptographic Provider" and check eToken Base Cryptographic provider. Certificate Properties ×

Next

Cancel

Private Key Certification Authority		
Cryptographic Service Provider	^	
A CSP is a program that generates a public and private key pair used in many certificate-related processes.		n clicl
Select cryptographic service provider (CSP):		^
Microsoft Strong Cryptographic Provider (Encryption)	^	
🖂 eToken Base Cryptographic Provider (Encryption)		
□ Microsoft Base Cryptographic Provider v1.0 (Encryption)		
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider (Encryption)		
Microsoft Base Smart Card Crypto Provider (Encryption)		
Microsoft DH SChannel Cryptographic Provider (Encryption)	~	
□ Show all CSPs		
		•
		Cano
		Carlo

- 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.

	ate Enrollment		_	×
The	SafeNet Authentication	n Client	THALE	s
	Enter the Token Password Token Name: Token Password:	Card #E12266F4D7A9BA02		
			OK Can	cel

26. Click OK.

27. Ensure the process completes successfully.

📮 Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Poli	cy	
vSEC Smartcard User	STATUS: Succeeded	Details 👻
	Ne	xt user Clos

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.



🏶 💁 🧎 🤶 🏚

SafeNet Authentication Client

					ction
eNet Authentication Client Tools Tokens Broadcom Corp Contacted SmartCard 0 Broadcom Corp Contactless SmartCard 0					
	Issued To	Issued By	Expiration D	Purposes	N
Card #E12266F4D7A9BA02 Card #E12266F4D7A9BA02 Settings Settings SMSC SMSC USX101x Reader 0 Client Settings	Administrator	SATSE SUB C	17-Feb-2029	Smartcard Logon, Client Authentication	

© SafeNet Assured Technologies, LLC Date Created: 6/14/2014

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com • thalestct.com