

PKIUSER MANUAL

JANUARY 2, 2013

Document Classification:

Confidential

VERSION 2.0

Copyright © 2013 National Center for Digital Certification, Kingdom of Saudi Arabia. This document is intended for use only by the National Center for Digital Certification and authorized Saudi National PKI participants. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes without prior consent.

NCDC – Brief Introduction

1. About NCDC

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has created a National Public key Infrastructure. Named the National Centre for Digital Certification (NCDC), the NCDC is created by an act of law and its mandate is stipulated in the Saudi e-transaction law.

NCDC provides trust services to secure the exchange of information between key stakeholders. Participants include:

- Government employees
- Citizens
- Businesses

2. Government Certification Authority

Government Certification Authority (Government-CA) is owned by the Ministry of Communication and Information Technology (MCIT). Government-CA is the Certification Authority under the NCDC-Root-CA. NCDC-Root-CA has issued a digitally signed CA Certificate to the Government-CA. The Government-CA is responsible for issuing and managing Digital Certificates to Government employees, entities, non-human subscribers (like Servers and Network Devices) within the Government domain, through Certificate Service Providers (henceforth referred as CSPs) within the framework.

3. NCDC ESP Kit

Every user participating in the PKI usage will be provided with an NCDC ESP Kit, which will contain the following

- 1. Digital Certificate
- 2. Entrust Entelligence Security Provider (ESP) for Windows
- 3. Entrust Entelligence Security Provider (ESP) for Outlook
- 4. SafeNet USB token Drivers

4. Digital Certificates

The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called a "digital ID," "digital identity certificate," "identity certificate" and "public key certificate," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as NCDC Government Certification Authority

Every subscriber participating in the PKI usage will obtain a Digital Signature Certificate (DSC) issued by Government CA. Before issuance of the Digital Certificate, the subscriber has to fill a request form and get the required approvals from the Authorizing Person.

Subscriber's identity then verified by the Registration office and a Digital Certificate is issued. The Subscriber can perform the followings using the issued Digital Certificate

- 1. Digital Signing and Verification of an Email
- 2. Encrypting and Decrypting an Email

- 3. Digital Signing and Verification of a Document
- 4. Encrypting and Decrypting a Document

5. Entrust Entelligence Security Provider (ESP)

Entrust Entelligence Security Provider (ESP) is a desktop security solution and is an enterprisewide security platform for Windows desktops, domain controllers, and authentication servers that allows organizations to deploy the digital identities that enable the strong authentication, encryption and digital signature capabilities within a number of authentication applications and other applications such as data encryption and secure email.

6. Secure Storage Device – Safenet ikey USB tokens

SafeNet USB token offers a compact hardware solution for authentication and digital identity management. SafeNet USB token offers onboard key generation, key storage, encryption, and digital signing capabilities add high-assurance security to user login, digitally sign emails, holding master keys for disk encryption, VPN authentication, and other secure client applications.

7. Pre-Requisites

The following pre-requisites are needed before installation of ESP and SafeNet USB token Drivers

- 1. End user Operating System Windows XP or Vista
- 2. Microsoft Outlook installed for the Entelligence Security Provider for Outlook

8. Help Desk Contacts

For any assistance or technical support please contact NCDC operations centre by sending an email to <u>helpdesk@ncdc.gov.sa</u> or via helpdesk Telephone numbers: (01)452 2086 / (01)452 2037 / (01) 452 2196

Installation of ESP and USB Token Drivers

Every subscriber will be provided with a PKI CD which will have the software's for ESP and SafeNet USB token or the subscriber can download the NCDC Clients Packager from NCDC Web Repository (<u>http://web.ncdc.gov.sa</u>)

- a. To run the Installation from CD
 - Insert the PKI CD into the CD Drive
 - You will find the NCDC Clients Packager, to install the packager Right Click and select **Open**
- b. If you have downloaded the NCDC Clients Packager from NCDC Web Repository (<u>http://web.ncdc.gov.sa</u>), save the Packager on desktop and to install the packager Right Click and select **Open**



• Click "**Run**" on the Open File Security Warning window to proceed the installation

Do you	u want to run this file?
	Name:MCIT\Desktop\PKI CD\NCDC_Clients_v1.0-32.ex Publisher: National Center for Digital Certification
	Type: Application
	From: C:\Users\pshankara.MCIT\Desktop\PKI CD\NCDC
V Alwa	Run Cancel
٢	While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you to st. What's the risk?

• Click "Next" to continue the installation.



- Accept the License Agreement when prompted and Click "Install"
- Wait for the Packager to install the components

ktract: NCDC-SafeNet-14MAY	12-x32-8.1-SP1.msi 100%	%
Output folder: C:\Program File Extract: NCDC-SafeNet-14MA	es NCDC Clients Package \SA Y12-x32-8.1-SP1.msi 100	AC 0%

• Upon successful installation, you will be prompted to restart the computer. Click **Yes** to reboot.

NODE Clients Packager 1.0 Setup	
Setup has completed successfully. A Do you wish to reboot now?	reboot is required to finish the installation.

c. Upon successful installation of Entrust Entelligence Security Provider (ESP) for Windows, the subscriber can view an Icon in the system tray.



d. Upon successful installation of Entrust Entelligence Security Provider (ESP) for outlook, the subscriber can view 2 new options added to the Outlook New Message Window



 To check that the SafeNet USB token driver has been successfully installed. Click on Start>Programs>SafeNet>SafeNet Authentication Client>SafeNet Authentication Client



To Digitally Sign an e-Mail Message

The following steps will be invoked to execute this procedure:

1. Ensure that Entrust Entelligence Security Provider (ESP) for Outlook and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure 2. Open a New Mail in Microsoft Outlook

	50	4 ¥)7	Un	titled - M	essage	(HTML)			-	= >	¢
	lessage	Insert	Options	Format	Text					(0
Paste	B 4	ZU L Basi	• 9 • • 注 • 詳 審 彊 ▶1 c Text	A * *	Names	1 0 · · · · · · · · · · · · · · · · · ·	Options	Spelling Proofing	Encrypt Securi	Sign	
Send .	<u>To₂</u> <u>C</u> c <u>B</u> cc Subject:										

3. Select the recipients to whom you like to send a Digitally Signed Mail. Click on Sign Button on the Tool Bar and Click "**Send**"



4. Entrust Entelligence Security Provider (ESP) for Outlook will Digitally Sign the email

Entrust	Entelligence Security Provider 🛛 🛛 🛛	
<u>*</u>	Signing S/MIME format message	
	Cancel	

5. The Wizard will prompt to provide the USB Token PIN; after Providing the PIN, Click "**OK**"

Enter the Token PIN. Foken Name: 90285743 Foken PIN: ••••••• Current Language: EN	SafeNet. SafeN	let Authentication Client
Foken Name: 90285743 Foken PIN: ••••••••• Current Language: EN	Enter the Token PIN.	
Token PIN: Current Language: EN	Token Name:	90285743
Current Language: EN	Token PIN:	•••••
		Current Language: EN
		OK Cance

6. The signed message is now sent to the recipient and the process is completed.

To Verify a Digitally Signed e-Mail Message

The following steps will be invoked to execute this procedure:

1. The recipient of the Digitally Signed Mail will receive the messages with a mail envelope with RED Seal Symbol

🤤 Inbox			Search Inbox			
Click here to enable Instant Se	earch					
🖬 : 近 🖸 🛛 From	Subject	Received	Size	Categories	8	
Date: Today						
Phani Shankar	à	Wed 8/26/2009	9:2 15 KB		V	

2. On clicking the Digitally Signed Mail, Entrust Entelligence Security Provider (ESP) will verify the sender's signature

Entrust E	ntelligence Security Provider	×
&	Verifying signer pshankara@ncdc.gov.sa's certificate	
		Cancel

3. The Digitally signed mail will now open in reading pane mode and the recipient can verify that the mail that was Digitally Signed as shown below



4. The recipient can click on the Digitally Signed Icon and view the Message Security Properties

👫 Message Security Properties	<u>?</u> ×
No Message Subject Available	
Secure messages may contain encryption and digital signature layers. Each digital signature layer will contain one or more digital signatures.	Review the decryption and verification information shown below.
Layers:	Details:
 S/MIME Format Message: No Message Subject Availa Digital Signature Layer Signer: pshankara@ncdc.gov.sa Original Message: Sender: Phani Shankara e-mail Address: pshankara@ncdc.gov.sa 	Signature Status: OK
etails <<	⊻jew Certificate
Close <u>H</u> elp	

To Encrypt an Email

The following steps will be invoked to execute this procedure:

- 1. Ensure that ESP for Outlook and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure
- 2. Ensure that the Person to whom you are encrypting the mail is part of NCDC PKI Trust Network and his public key certificates available in the LDAP.
- 3. Open a New Mail in Microsoft Outlook

	5) (2	**);	Un	titled - M	essage	(HTML)			-	= x
M	essage	Insert	Options	Format 1	Text				_	0
Paste	B *2-	I <u>U</u> ▲ Basi	• 9 · · · · · · · · · · · · · · · · · ·	A A 律 11 学	Names	0 🕰 - 0 💭 - 0 🖉 - Inclu 🕫	Options	Spelling Proofing	Encrypt Securit	Sign
Send (To <u></u> <u>C</u> c <u>B</u> cc									

4. Select the recipients to whom you wish to send an Encrypted Mail and Click on Encrypt Button on the Tool Bar and Click "**Send**"

	1 (4 4) =	Untitled ·	Message	(HTML)				x
Mess	age Insert	Options For	nat Text					0
Paste	B I U ∷≣ ≝2 - A - ■ Basic	·9·A ·注·课课 著::■ /1 14	A Names		Options	Spelling Proofing	Encrypt Si Security	gn G
	og Patel Chira .c	<u>s</u>						

5. Entrust Entelligence Security Provider (ESP) for Outlook will obtain the recipients Public key and encrypt the mail

Entrust	Entelligence Security Provider	×
2	Obtaining and verifying certificates	
	Cancel	

6. The Encrypted e-Mail will be sent to the selected recipient and the process will be completed.

9. To Decrypt an Email

The following steps will be invoked to execute this procedure:

1. The recipient of the Encrypted Mail will receive the messages with a mail envelope with **BLUE** Lock Symbol

🕒 Inbox			Sear	ch Inbox		۰ م	*
Click here to enable Instant Se	arch						
🔤 ! 🏠 🗋 🖉 From	Subject	Received	*	Size	Categories	7	-
Date: Today							
Phani Shankara	1	Wed 8/26/	2009.9	3 9 KB		Ŷ	

2. On clicking the Encrypted Email, Entrust Entelligence Security Provider (ESP) will decode the message contents

Entrust E	ntelligence Security Provider	×
&	Decoding the S/MIME format message contents	
		Cancel

3. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "**OK**"

hentication Client
90285743

Current Language: EN
OK Cancel

4. The Encrypted mail will now open in reading pane mode and the recipient can verify that the mail was Encrypted as shown below

🖬 🖬 " U 🍝	🔹 🔻 Untitled -	Message (HTML)		
Message				(
Reply Reply Forward to All	Delete Move to Folder *	Block Sender	Categorize * Follow Up * Mark as Unread	Find Encrypted
Respond	Actions	Junk E-mail 🕞	Options 5	Security

5. The recipient can click on the Encrypted Icon and view the Message Security Properties



10. To Digitally Sign a Document

The following steps will be invoked to execute this procedure:

- 1. Ensure that ESP for Windows and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure
- 2. Select a file which you like to Digitally Sign



3. Right Click on the file and select the option of "Digitally Sign File"

🚞 ES	P								
File	Edit	View	Favorites	Tools	He	lp			2
		le to be icrosoft D KB	Signed.docx Office Word	Documer Open Edit New Print Encrypt Digitally Encrypt Scan wit Open W Send To Cut Copy Create S Delete Rename	File. Sign and h Of ith	 File Digitally Sign File ficeScan Client tcut	· · · · · · · · · · · · · · · · · · ·		

4. The Digitally Sign files Wizard would open which will guide you through the process of digitally signing of files, click "Next"

📑 Digitally Sign Files Wizard		×
F	Welcome to the Digitally Sign Files Wizard.	
	This wizard will guide you through the process of digitally signing files.	
	The files you are signing are:	
	🔁 File to be Signed.docx	
	To continue, click Next.	
	< Back. Next > Cancel	

5. The signing certificate and the Hash algorithm "SHA1" will appear, click "Next"

📑 Digitally Sign Files Wizard			×
Digital Signature Options Digitally signed files are sign	ned by yourself.		ß
Your Signing Certificate:	pshankara@ncdc.gov.sa	Key Usage: No	Choose
Hash Algorithm:	SHA1		
	< Back	Next >	Cancel

6. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "OK"

afeNet. SafeNo	et Authentication Client
Enterthe Token PIN.	
Token Name:	90285743
Token PIN:	•••••
	Current Language: EN

7. Click on "Finish" to complete the Digital Signing Process.

🛃 Digitally Sign Files Wizard		×
F	Completing the Digitally Sign Files Wizard.	
	You have successfully signed the following files:	
	File to be Signed.docx.p7m	
	Coursel	1
	K back Finish Lancel	

8. The output of the Digitally Signed file will be in a new format (.p7m)



To Verify a Digitally Signed Document

The following steps will be invoked to execute this procedure:

1. Select a Digitally Signed file to verify

🚞 ES	P					
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	1
P7M 1011 010 101		le to be ecure Fil 2 KB	Verified.doc: le	ĸ.p7m		

2. Right click on the Signed file and Select the "Decrypt and Verify"

🚞 ESI	Р				<u>- 🗆 ×</u>
File	Edit	View	Favorites	Tools Help	1
P7M		le to be	Verified.do	cx.p7m	
0101		ecure Fil 2 KB	e	Decrypt, Verify and Open	
				Decrypt and Verify	
				Scan with OfficeScan Client Open With	
				Send To	
				Cut	
			_	Сору	
				Create Shortcut	
				Delete	
			_	Rename	
				Properties	

3. Entrust Entelligence Security Provider (ESP) will start the verification process

Entrust E	ntelligence Security Provider						
P7N 1010 1010	Decrypting and Verifying File: C:\Documents and Settings\pshankara\Deskto\File to be Ve						
		Cancel					
	1 Seconds Remaining						

4. Once the process is completed, the original file can be obtained



To Encrypt a Document

The following steps will be invoked to execute this procedure:

- 1. Ensure that ESP for Windows and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure
- 2. Select a file which you wish to Encrypt



3. Right Click on the file and select the option of "Encrypt File"



4. The Encrypt files Wizard would open which will guide you through the process of Encrypting of files, click "**Next**"

🛃 Encrypt Files Wizard		×	
F	Welcome to the Encrypt Files Wizard.		
	This wizard will guide you through the process of encrypting files for yourself and others.	:	
	The files you are encrypting are:		
	Pile to be Encrypted.docx		
	To continue, click Next.		
	< Back Next > Cancel		

5. Your Encryption Certificate and Encryption Algorithm "3DES" will appear, then click "Next"

📑 Encrypt Files Wizard	×
Encryption Options Encrypted files are encrypted for yourself and optionally for other people.	ð
Files are always encrypted for yourself.	
Your Encryption Certificate: pshankara@ncdc.gov.sa Key Usage: Ke	Choose
Encryption Algorithm: 3DES	
Encrypt the files for other people in addition to myself	
< Back Next >	Cancel

6. Tick the box in case you intend to encrypt the file for other people in addition to yourself

📑 Encrypt Files Wizard	×
Encryption Options Encrypted files are encrypted for yours	and optionally for other people.
Files are always encrypted for yourself.	
Your Encryption Certificate: pshankar	Pinodoligovisa Key Usage: Kej <u>C</u> hoose
Encryption Algorithm: 3DES	•
Encrypt the files for other people in	Idition to myself
	< <u>B</u> ack <u>N</u> ext > Cancel

7. To encrypt files for other people you need their encryption certificate. Use the "Add" button to select the other people you wish to encrypt the file

📑 Encr	ypt Files Wizard		×			
Add	litional Recipients Select the other people these files will be en yourself will be able to decrypt the files.	crypted for. Only these peop	ole and			
	To encrypt files for other people you need their encryption certificates. Use the Add button to select the other people you wish to encrypt for.					
	Name	E-mail Address				
		Add <u>R</u> emove	⊻iew			
		< <u>B</u> ack <u>N</u> ext >	Cancel			

8. Type in name/email id of person to whom you wish to encrypt the file and use the "**search**" button to search the directory for their encryption certificates

🕌 Selec	t People	2		?×
<u> 8</u> ª	Please s encrypti	elect the other people you wish to encrypt for.Use the search button to se ion certificates.	earch the direct	tory for their
	<i>></i> [•	<u>S</u> earch 🝷
	Name	Email		
	S <u>h</u> ow:	All		⊻iew
		OK	Cancel	Help

9. Once the search results provides you with the details of the person to whom you wish to encrypt the file, select the persons certificate and click on "**OK**"

🐉 Selec	t People			<u>?×</u>			
<u>8</u> ª	Please select the other people you wish to encrypt for. Use the search button to search the directory for their encryption certificates.						
	🔎 pc			▼ Search ▼			
	Name	Email	Issued by	Expiration Date			
	NCDC CSP - Governme	nt CA					
	pchirag@ncdc.gov.sa	pchirag@ncdc.gov.sa	Government CA	7/21/2012			
				•			
	Show: Search Results	•		⊻iew			
			ок	Cancel Help			

10. Once the details of the person to whom you wish to encrypt the file are added to the Encrypt file wizard click "**Next**"

🛃 Encrypt Files Wizard						
Add	Additional Recipients Select the other people these files will be encrypted for. Only these people and yourself will be able to decrypt the files.					
	To encrypt files for other people you need their encryption certificates. Use the Add button to select the other people you wish to encrypt for.					
	Name	E-mail Address				
	pchirag@ncdc.gov.sa	pchirag@ncdc.gov.sa				
		<u>Add</u> <u>B</u> emove <u>⊻</u> iew				
		< <u>B</u> ack <u>N</u> ext > Cancel				

11. Click on "Finish" to complete the Encrypting process.



12. The output of the Encrypted file will be in a new format (.p7m). The encrypted file for other user may be sent using any medium such as flash memory, CD or by email.



To Decrypt an Encrypted Document

The following steps will be invoked to execute this procedure:

1. Select an Encrypted file to decrypt



2. Right click on the encrypted file and Select the "Decrypt and Verify"

3. Entrust Entelligence Security Provider (ESP) will start the verification process

Entrust Entelligence Security Provider					
Decrypting and Verifying File: C:\Documents and Settings\pshankara\Desk\File to be Decrypted.docx.p7r					

4. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "OK"

S Token Logon	×
GafeNet. SafeNet	et Authentication Client
Enter the Token PIN.	
Token Name:	90285743
Token PIN:	•••••
	Current Language: EN
	OK Cancel

5. The selected encrypted file will be decrypted and the output will be as follow

🚞 ES	Р						
<u>F</u> ile	<u>E</u> di	t <u>V</u> iew	F <u>a</u> vorites	<u>T</u> ools	<u>H</u> elp		2
P7M 1010 0101 1010		File to be Secure Fi 11,819 KI	Decrypted.d le B	locx.p7m		File to be Decrypted.docx Microsoft Office Word Document 11,818 KB	