

# Certificate Import to Aladdin eToken

# **CONTACT:**

CHARTERED INFORMATION SYSTEMS PVT. LTD. "Chartered House", West of Lata Mangeshkar Musical Park,

West of Lata Mangeshkar Musical Park, Bhandara Road, NAGPUR - 440 008 Tel: +91 (0712) 663 8888, 92252 45088 digitalsognature@charteredinfo.com www.charteredinfo.com

#### **GETTING STARTED**

To start the process, procure the Digital Signature Certificate Enrollment Kit from TCS-CA or its Registration Authorities. The kit contains:

- USB Token (Aladdin eToken)
- Installation CD. This contains:
  - USB Drivers
  - Mozilla Firefox
  - TCS FileSigner Plus Evaluation Copy

#### Note:

- Use the Installation CD to install the USB Token driver.
- Ensure the following before installing the USB token driver.
  - ✓ System Requirement:
    - Operating System: Windows 2000, XP
    - Browser: Internet Explorer 5.5 and above
    - ✓ You should have the Administrator privileges for installing the USB Token

### USING ALADDIN ETOKEN

#### To install the eToken:

- 1. Insert the CD into the CD drive of your computer.
- 2. To install eToken driver click on **etoken\_driver\_aladin.msi** Windows Installer Package. Accept the License Agreement and proceed with installation.
- 3. Insert the USB Token in the USB port of the computer, if prompted
- Restart the computer after the installation is complete. You can now see the eToken Properties from the Start Menu by selecting Programs> eToken> eToken Properties



Click "eToken Properties" and with your eToken inserted, the following screen is displayed:

	Advanced 🔃 Refres	n 🎦 Help	
	Change password	Rename eToken	
Local Machine	Name	eToken	
	Туре	PRO (Card OS/M4)	
	FW version	4.2.5.4 [0x8514]	
i	User	Present	
Talan TAVE IF	Administrator	Present	
Token [AKS IT	Token ID	40f7db14	
	Smartcard ID	21 5f c3 02 1d 20	
	Total Memory Capacity	32768 bytes	
	Largest free block	20809 bytes	
	Color	Blue	
	FIPS mode	Off	
	Reader name	AKS ifdh 0	

### CHANGING THE ETOKEN PASSWORD

All eTokens are configured at manufacture with the factory default password. This password is "1234567890". Click "Change password" on the eToken Properties screen and the following eToken Properties dialog is displayed:

Current Password:	Password quality
	00.0%
Confirm Password:	
A good password is at least 8 characte	rs long and a combination of various

Enter your current eToken password in the "Current Password" field and, the new password in the "New Password" field. Confirm new Password and click "OK" to set the new Password.

#### **RENAMING THE ETOKEN**

For additional convenience and ease of identification, the eToken name can also be personalized. Click "Rename eToken" on the eToken Properties screen. Since renaming the eToken requires the eToken password, the following dialog is displayed:

Give the Password for the eToken and click "OK"

eToken Pro	operties 👂
Enter eToke	en password
e <u>T</u> oken:	eToken [AKS ifdh 0]
Password	E.

Enter the new eToken name in the eToken Name field and click "OK" to set the eToken Name.

Enter eToken Nar	ne 🔀
eToken	
eToken Name:	Joe's eToken
You can use this frier	ndly name to identify your eToken
C	OK Cancel

Click "OK" and in the eToken Properties window the new eToken name is displayed.

Cotron		
oken		
	Madvanced 🔊 Refresh	2 Help
	<b>1</b> 2	
	Joe's eToken [PRO]	
The second	Change password	Rename eToken Unblock eToken
cal Machine		
27	Name	Joe's eToken
and the second second	Туре	eToken PRO 64K (4.20)
	Product ID	0x0600
	Firmware version	1.0 [0×0001]
	CARD/OS version	CardOS V4.2 (C) Siemens AG 1994-2003
s eroken []	User	Present
	Administrator	Not present
	eToken ID	0x00094170
	Smartcard ID	24 8c c8 0b 2b 09
	Total memory capacity	65536 bytes
	Largest free block	42597 bytes
	Color	Blue
	FIPS mode	Off
	1024-bit RSA keys count	7
	2048-bit RSA keys support	Off
	HMAC SHA-1 support	Off
	User login failures limit	15 times
	Reader name	AKS if db 0

### IMPORTING THE CERTIFICATE INTO ETOKEN

To import the Certificate, you first need to export the certificate from the IE Browser onto the Desktop and then import it into the eToken.

#### **EXPORTING THE CERTIFICATE**

Exporting the Digital Certificate from the browser and maintaining its backup as a `.pfx' file is essential since, at any point of time if your certificate gets deleted from the browser or token or if you format your system, you can always import it again.

For exporting your Certificate that has been downloaded in your browser, Open the IE Browser and follow the path

" Tools>Internet Options>Content>Certificate>Personal" tab.

Choose the certificate to be exported and click on the export tab.

Issued By	Expiratio	Friendly Name	
Safescrypt Class 1 Co	4/20/2003	<none></none>	
testCServer4	7/15/2003	<none></none>	
Tata Consultancy Ser	10/21/2003	<none></none>	
testCServer4	7/15/2003	<none></none>	
Tata Consultancy Ser	10/21/2003	<none></none>	
Tata Consultancy Ser	10/21/2003	<none></none>	
Tata Consultancy Ser	12/4/2003	<none></none>	-
testCServer4	3/16/2004	<none></none>	
testCServer4	7/15/2003	<none></none>	2
		A	dvanced
ises			
	Issued By Safescrypt Class 1 Co testCServer4 Tata Consultancy Ser testCServer4 Tata Consultancy Ser Tata Consultancy Ser testCServer4 testCServer4 testCServer4	Issued By  Expiratio    Safescrypt Class 1 Co  4/20/2003    testCServer4  7/15/2003    Tata Consultancy Ser  10/21/2003    testCServer4  7/15/2003    Tata Consultancy Ser  10/21/2003    Tata Consultancy Ser  10/21/2003    Tata Consultancy Ser  10/21/2003    Tata Consultancy Ser  10/21/2003    Tata Consultancy Ser  12/4/2003    testCServer4  3/16/2004    testCServer4  7/15/2003	Issued By  Expiratio  Friendly Name    Safescrypt Class 1 Co  4/20/2003 <none>    testCServer4  7/15/2003  <none>    Tata Consultancy Ser  10/21/2003  <none>    testCServer4  7/15/2003  <none>    Tata Consultancy Ser  10/21/2003  <none>    Tata Consultancy Ser  10/21/2003  <none>    Tata Consultancy Ser  10/21/2003  <none>    Tata Consultancy Ser  12/4/2003  <none>    Tata Consultancy Ser  12/4/2003  <none>    testCServer4  3/16/2004  <none>    testCServer4  7/15/2003  <none>    memove </none></none></none></none></none></none></none></none></none></none></none>

Click Next to the dialog to continue



choose the option `Yes', export the private key' and click `Next'

ertific	cate Export Wizard
Exp	<b>Dort Private Key</b> You can choose to export the private key with the certificate.
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
	Do you want to export the private key with the certificate?
	• Yes, export the private key
	O No, do not export the private key
	< <u>Back</u> <u>Next</u> > Cancel

Select the box indicated to include the CA certificate also with the Subscriber's certificate and Click 'Next'

Select th	e format you want to use:
C	ER encoded binary X.509 (.CER)
CE	age-64 encoded X,509 (,CER)
$\mathbf{C}$	ryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Г	Include all certificates in the certification path if possible
•	ersonal Information Exchange - PKC5 #12 (.PFX)
	Oclude all certificates in the certification path if possible
F	Z Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Г	Delete the private key if the export is successful

Enter the password to protect the PKCS#12 file. Ensure that you remember this password since you will be needing it while importing the certificate at a later point of time.

Certificate Export Wizard	×
<b>Password</b> To maintain security, you must protect the private key by using a password.	
Type and confirm a password.	
Password:	
Confirm password:	
	_
< <u>B</u> ack <u>N</u> ext > Cance	

Choose the file name and location to save the file. Give the extension of the file as `.p12' or `.pfx'

Certificate Export Wizard	×
File to Export Specify the name of the file you want to export	
Eile name:	Browse
< <u>B</u> ack <u>N</u> ext >	Cancel

Click Finish to export the private key and the certificates.



A dialog box will be shown for accessing the private key. Click 'OK' to continue



A message will be shown indicating the successful completion of the export.

Certificate Export Wizard	×
The export was successful.	
OK	

# IMPORTING THE CERTIFICATE INTO ETOKEN

From the Start Menu by selecting Programs> eToken> eToken Properties>Advanced>Certificate & Keys

The following Dialogue box appears. Click 'Import Certificate'

	rrties	
eloken		
	Advanced 🕢 Refresh 🔐 Help eToken [PRO]	
Local Machine	Details Settings Certificates & keys	
	🙀 Test User	Delete
1	Exchange key <fe60a79d-3042-4b1c-99a2-b0b< td=""><td>1 Import CA Chain</td></fe60a79d-3042-4b1c-99a2-b0b<>	1 Import CA Chain
eToken [AKS if	Exchange key <8089F048-4029-4DA8-971F39C	Set as Default
		Key Protection
	Version V3	
	Serial number 20 0c	
	Signature algorit RSA_SHA1RSA	
	Issuer IN, India PKI, TCS CA, Tata Const Valid from Friday, March 03, 2006 5:43:59 A	ultancy Services Certifyi — M
	Valid to Saturday, March 03, 2007 5:43:5 Subject Test User, TCS-CA - Registration	9 AM Authority, Individual
	Import Certificate	More Refresh

If the import is from a file, which has already been exported to a particular location on your computer, then select "Import certificate from the file" and click "OK".



Select the path of the ". pfx'' file and click "Open".

Open					? 🛛
Look in: 🙆	TCS-CA 🍟	0	ø	ø	<b></b>
i cab Para_backup Para_backup					
File name:				C	Open
Files of type:	PKCS #12 Files (*.pfx; *.p12)		*		Cancel

A prompt for Password for the private key appears. Give the password that you had set to protect the file, while exporting the file and click "OK"

Certificate Import	×						
To maintain security, the private key is protected with a password. Type the password for the private key.							
Password:							

A confirmation message is displayed if the import is successful.



## IMPORTING THE CA CHAIN

A certificate that is stored on the computer may be part of a hierarchical structure with more than one Certificate in the chain up to the Root CA. Importing a CA Chain takes the CA certificate and the complete CA Chain up to the root certificate that is stored on the computer and places it on the eToken.

When the "Import CA Chain" button is clicked, the CA Chain is imported onto the eToken and displayed in the certificate and key list window:

🚍 e Token Prop	erties					
eToken						
	💥 Advanced 🙋 Ref	fresh 🔚 Help				
Local Machine	eToken [PRO] Details Settings Cert	tificates & keys				
	Sss	Delete Import CA Chain Set as Default				
eToken [AKS if]	ा Tata Consultanc स्थि CCA India	Tata Consultancy Services Certifying Authority				
	Version	V3				
	Serial number	20 Oc				
	Signature algorit	RSA SHA1RSA				
	Issuer	IN, India PKI, TCS CA, Tata Consultancy Services Certifyi				
	Valid from	Friday, March 03, 2006 5:43:59 AM				
	Valid to	Saturday, March 03, 2007 5:43:59 AM				
	Subject	Test User, TCS-CA - Registration Authority, Individual 💌				
	Import Certificate		More Refresh			

A message confirming the import was successful is displayed

