

Certificate Export/Import

[VERSION 1.0]





1 Digital Certificate

Certificates issued by Dohatec CA are in X.509 v3 format. In Microsoft windows machines, these are recognized by the extension '.cer'.

To view a certificate, simply double click the .cer file.

Certificate In	formation	
This certificate is int • All application po	tended for the following purpose(plicies	(5):
Issued to: Sum	non Md. Zahidul Islam	
Issued by: Test	t Dohatec CA	
Valid from 11/6	j/2012 to 11/5/2013	

> To view the details of a certificate, click the 'Details' tab.

Dohatec CA Certifying Authority

	<all></all>	•	
Field		Value	
Su	bject	Sumon Md. Zahidul Islam, PPN	
Pu	blic key	RSA (2048 Bits)	
Su	bject Key Identifier	41 67 69 57 ff e8 2a 59 3e e8	
TO AU	thority Key Identifier	KeyID=c4 51 c1 69 de 1e a0 5	
	L Distribution Points	[1]CRL Distribution Point: Distr	
Ke	y Usage	Digital Signature, Non-Repudia	
	umbprint algorithm	shal	_
N = S	iumon Md. Zahidul Islam NUMBER = PPNeb6279		D
ostal	lode = 1000 rsonal		

Certificate	? ×
General Details Certification Path	
Certification path Test Root CA Bangladesh Test Dohatec CA Sumon Md. Zahidul Islam	
View Certificate	
Certificate status:	
This certificate is OK.	
	ок

Certifying Authority

> The hierarchy of trust for a certificate can be seen by clicking the 'Certification Path' tab. In this example, the certificate is issued by Dohatec CA, whose certificate is issued by CCA Bangladesh.

2 PKCS #12 Files

PKCS stands for Public Key Cryptographic Standard. PKCS #12 is the standard for transporting the private key along with the certificate securely. It has both the private key and the certificate. The private key is encrypted.

When the Subscriber downloads the certificate into the IE browser, the certificate is stored in the key store where the private key is generated. To use the credentials in some other machine, the Subscriber has to export the private key and the certificate from the browser as a PKCS #12 file.

The extension for the PKCS #12 file is either '.p12' or '.pfx'

2.1 Exporting a PKCS#12 File from the Browser

- > Open an Internet browser window
- Click the Tools > Internet Options tab on the IE browser
- Click on the Content > Certificates tab on the dialog box shown.





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

rtificates			3	2
ntended purpose: <a>	·			-
Personal Other People Ir	ntermediate Certification	Authorities Tru	sted Root Certification	
Issued To	Issued By	Expiratio	Friendly Name	-
🖼 Ahmed Sharif	Test Dohatec CA	9/19/2013	<none></none>	
🔛 Akter Fahmida	Test Dohatec CA	3/18/2014	Akter Fahmida	
🔛 habib saki	Test Dohatec CA	9/10/2013	<none></none>	
🔛 Hasan Hasib Md	Test Dohatec CA	9/10/2013	<none></none>	
🖼 Rahaman Masudur	Test Dohatec CA	3/19/2014	Rahaman Masudur	
🔛 Rased Rased	Test Dohatec CA	9/10/2013	<none></none>	
🔛 Rehana Jinat	Test Dohatec CA	3/19/2014	Rehana Jinat	
🔤 Sumon Md. Zahidul	Test Dohatec CA	11/5/2013	<none></none>	
🔛 Sumon Zahidul Isla	Test Dohatec CA	9/10/2013	<none></none>	
,				
Import	Remove		Advanced.	
Certificate intended purpose	es			-
<all></all>			View	
			Close	

> Click Next to the dialog to continue.

Certificate Export Wizard		×
	Welcome to the Certificate Export WizardThis wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.To continue, click Next.	
	< <u>B</u> ack (<u>Next</u> > Cancel	

Certifying Authority

> To export the private key with the certificate, choose the option 'Yes' and click 'Next'

Certificate Export Wizard	×
Export Private Key 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	
No, do not export the private key	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	

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

the format you want to use:	
DER encoded binary X.509 (.C	ER)
Bage-64 encoded X.509 (.CER))
Gryptographic Message Syntax	Standard - PKCS #7 Certificates (.P7B)
\square Include all certificates in the	e certification path if possible
Personal Information Exchange	∋ - PKC5 #12 (.PFX)
Contractive all certificates in the	e certification path if possible
Enable strong protection (r	equires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if th	e export is successful



> Enter the password to protect the PKCS#12 file

Certificate Export Wizard	×
Password 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 > Can	:el

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	Next > Cancel

Certifying Authority

> Click Finish to export the private key and the certificates.

Certificate Export Wizard		×
	Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings: File Name Export Keys	Export
	Include all certificates in the certification path	Yes
	< <u>B</u> ack Finish	Cancel

> 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.



2.2 IMPORTING PKCS# 12 FILE INTO THE BROWSER

- Double-click on the '.p12' or '.pfx' file
- Click 'Next' on the dialog to continue.



> Check the File location and click 'Next'.

to Import		
Specify the file you want t	to import.	
Eile name:		
	Bro	wse
Note: More than one cert	ificate can be stored in a single file in the following	formats:
Personal Information E	xchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message	e Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Cer	rtificate Store (.SST)	

Enter the password, with which the private key is protected in the PKCS #12 file.

Certificate Import Wizard	×
Password To maintain security, the private key was protected with a password.	
	-
Type the password for the private key.	
Password:	
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
Mark the private key as exportable	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	



- Select the option 'Mark the private key as exportable', if you further want to export the private key from the browser. If it is not selected, then the private key cannot be exported from the browser again.
- Choose the option to automatically select the certificate store as shown and click 'Next'.

tificate Import Wizard		
Certificate Store		
Certificate stores are system areas where	certificates are kept.	
Windows can automatically select a certific	ate store, or you car	n specify a location for
Automatically select the certificate	tore based on the ty	/pe of certificate
C Place all certificates in the following	store	
Certificate store;		
		Browse
	< Back	Next > Cancel
	- Back	Cancer

➤ Click 'Finish' to import the PKCS #12 file.

Certificate Import Wizard		×		
	Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings:			
	Certificate Store Selected Content File Name	Automatically determined by t PFX		
	< <u>B</u> ack	Finish Cancel		



Click 'OK' to import the private key.

Importing a ne	w private exchange key!	×
	An application is creating a Protected item.	
近	Security level set to Medium Set Security Level OK Cancel Details	

> A message will be shown indicating the successful import of the private key.

Certificat	e Import Wizard	×
٩	The import was succe	ssful.
	ОК	