



E-CERT CONTROL MANAGER

for e-Cert on Smart ID Card

INSTALLATION GUIDE

Version v1.3



Copyright ©2003 Hongkong
Post

CONTENTS

Introduction

About e-Cert Control Manager	3
Features	3
System requirements	4
Supported Smart Card	4
Supported applications	4
Installation overview	4
Obtaining support	5
Preparing for secure installation.....	5
Integrity of the installation environment	5

Installing e-Cert Control Manager

Connecting the smart card reader	6
Installing the e-Cert Control Manager software.....	6
Registering your certificate.....	7
Registering the Hongkong Post CA Root and Signer Certificates	7

Setting Up Your E-mail Application

Setting up Microsoft Outlook Express / Windows Mail.....	10
Setting up Netscape Messenger	11
Registering the Hongkong Post CA Root and Signer Certificates with Netscape	14

Troubleshooting

e-Cert Control Manager errors.....	19
Microsoft Management Console errors	19

INTRODUCTION

About e-Cert Control Manager

E-Cert Control Manager is designed to manage a *digital identity* and secure it on a smart card. e-Cert Control Manager protects private keys—the crucial element of a digital identity—on the smart card, provides decryption and digital signing functions, and integrates with Microsoft Windows to provide cryptographic security services to e-mail clients, web browsers, and other applications.

When an application, such as an e-mail program, needs to use cryptographic services (to sign an e-mail for example), e-Cert Control Manager automatically recognises and processes the request, using the smart card for signing and/or decrypting as required.

In this way, e-Cert Control Manager transparently secures your business operations, while at the same time securing your private key—the crucial element of your digital identity—on a tamper-proof, lockable smart card.



Note More information about e-Cert Control Manager and the concepts used in its underlying technology—Public Key Infrastructure—can be found in Chapter 1 of the *e-Cert Control Manager User Guide*.

Features

The e-Cert Control Manager software and the e-Cert application on the smart card provide the following features.

Cryptographic functions:

- 1024-bit on-card RSA digital signing.
- 1024-bit on-card RSA key generation.
- MD5 and SHA-1 cryptographic hashes in-software.
- Strong random number generation for transport and encryption keys.

Key management:

- Secure password-protected smart card access.
- Support for separate signing and encryption keys.
- PKCS #12 keystore loading support.

- Auto-detection of smart card and reader types.
- Certificate registration to Microsoft Certificate Store.

Interface standards:

- Netscape PKCS #11 and Microsoft CryptoAPI support.
- X.509 and PKCS #12 certificate services support.

Smart cards and readers:

- Support for multiple smart card types.
- PC/SC smart card reader support.

System requirements

- Intel Pentium 166 processor
- 32mb RAM
- 10mb unused hard disk space
- An available serial, PCMCIA or USB port for smart card reader installation
- A PC/SC smart card reader, such as:
 - Gemplus GemPC 400, GemPC 410 or GemPC 430
 - Smart Silicon Systems CardPro
 - Omnikey CardMan
 - KeyCorp Smart Mouse
- Smart card reader PC/SC drivers

Supported Smart Card

- Smart ID Card issued by the Immigration Department of the Hongkong Special Administrative Region

Supported applications

Operating systems:

- Microsoft Windows 98 SE
- Microsoft Windows ME
- Microsoft Windows NT with Service Pack 6A
- Microsoft Windows 2000 with Service Pack 1
- Microsoft Windows XP
- Microsoft Windows Vista

Web browsers:

- Microsoft Internet Explorer 5.5, 6.0 and 7.0
- Netscape Navigator 4.51, 4.80, 7.02 and 8.1 (support of Netscape auto-detect has ceased from Version 9)

E-mail applications:

- Microsoft Outlook Express 5.5 and 6.0 / Windows Mail 6.0
- Netscape Messenger 4.51, 4.80 and 7.02

Installation overview

Setting up e-Cert Control Manager is performed in these key steps:

1. Connecting the smart card reader to your PC
2. Installing the reader drivers.
3. Installing the e-Cert Control Manager software.
4. Configuring your e-mail applications to use your smart card.

Obtaining support

If you encounter problems requiring support, check the *Troubleshooting* section at the end of this guide or contact HKPost CA at :-

Email : enquiry@hongkongpost.gov.hk

Tel. : 2921 6633

Preparing for secure installation

There are a few guidelines that can help ensure the environment into which you are installing e-Cert Control Manager is not hostile or potentially degrading to e-Cert Control Manager's security measures.

Integrity of the installation environment

To ensure the installation environment does not counter the data security mechanisms of e-Cert Control Manager, you should only install smart card readers that you trust do not interfere with communications between the smart card and your computer. Further, e-Cert Control Manager should be installed only on a securely managed computer, with up-to-date security patches. This means:

- Access to the computer from public networks (such as the Internet) must be protected with a properly configured and trusted firewall.
- Active content (such as ActiveX and Java) should be controlled so that only trustworthy code is allowed to access e-Cert Control Manager (see your web browser's on-line help for information about protecting your system from active content).
- The computer must have active protection from viruses, with up-to-date virus definition files.
- Only trusted services are running on the computer.
- The user profiles must be insulated so that other users cannot change paths to executable files and configuration data.

Failure to protect your computer from malicious software could result in the bypassing or deactivation of the security features of e-Cert Control Manager.



Once installed, you can check the version of e-Cert Control Manager by right clicking the e-Cert Control Manager icon in the system tray and selecting **Manager**. You can check the version numbers of applications on your smart card by viewing the properties of the application in the e-Cert Control Manager (for more information, see the *e-Cert Control Manager User Guide*).

INSTALLING E-CERT CONTROL MANAGER

This chapter describes the process for installing e-Cert Control Manager and registering the certificate on your smart card with your computer.

The installation process has these key steps:

1. Install e-Cert Control Manager which can be downloaded from the Hongkong Post CA Website (www.hongkongpost.gov.hk).
2. Run e-Cert Control Manager and set it up to work with your smart card reader.
3. Insert your smart card and register your certificate with the Microsoft Certificate Store.

Connecting the smart card reader

Different smart card readers have different installation procedures, and you should use the instructions provided by the reader manufacturer for connecting your particular reader.

Typically, installing a new smart card reader requires physically connecting the reader cables to your PC, and ensuring the correct drivers are loaded so that Windows can recognise and use your reader. Most modern smart card readers support the PC/SC interface, and Microsoft Windows is shipped with PC/SC drivers, so separate driver installation is usually not required. However, you should confirm this with the documentation provided by the smart card reader manufacturer.

Installing the e-Cert Control Manager software

To install e-Cert Control Manager:

1. Download e-Cert Control Manager from the Hongkong Post CA Website (if you have not done so).
2. Run e-Cert Control Manager set up program
3. Follow the setup instructions
4. Click **Finish** to complete the installation.
5. Restart your PC when the installation is finished.

If you intend using the e-Cert Control Manager for advanced functions, you will need the Microsoft Management Console to be installed on your PC. This is preinstalled on Windows 2000 and Windows XP but may need to be

installed on other operating systems. Refer to the troubleshooting section of this document for information on where to get the Microsoft Management Console software.

When you have restarted your PC, you need to register the certificate on your smart card with the Microsoft Certificate Store. The Certificate Store is a common access point for applications that require certificates, such as e-mail programs and web browsers.

Registering your certificate

To enable your e-mail application or web browser to use your certificate, you need to register it with the Microsoft Certificate Store.



Note More information about the Microsoft Certificate Store can be found in the *e-Cert Control Manager User Guide*.

Registering your certificates ensures that your certificate is available to the applications that want to use it.

You can register the certificate on your smart card using the e-Cert control manager by clicking the Copy e-Cert to the IE certificate store button. You may be prompted to enter your PIN. When you have supplied the correct PIN, a confirmation message is shown.



To register your certificate using the advanced mode:

1. Right-click the e-Cert Control Manager icon in the system tray and select **Manager** from the context menu to open the e-Cert Control Manager.
2. Select the certificate to register.
3. From the Action menu, select **Copy e-Cert to IE**.
4. Your certificate is registered.

Your smart card is now ready for use.

You may need to install the Hongkong Post CA Root Certificates if they are not already installed in the Microsoft Certificate Store. Please download and install the Hongkong Post CA certificates from our web site at www.hongkongpost.gov.hk.

With a registered certificate, you need to configure your applications so they can use your certificate for digital signatures and encryption.

Registering the Hongkong Post CA Root and Signer Certificates

Registering the CA Root certificates ensures that you can verify the digital signatures of other people who use their e-Cert to sign messages.

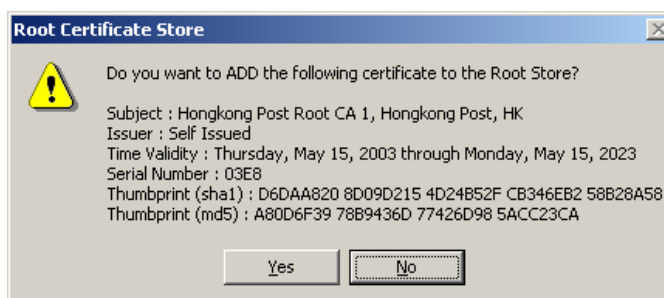
You only need to register the CA Root certificates once with your computer, however if you use Netscape Messenger, you need to register the certificates separately with Netscape. Information about this can be found in the section *Setting up Netscape Messenger* on page 11.

To register the CA Root certificate:

1. Download Hongkong Post CA Root Certificates from the Hongkong Post CA Website (if you have not done so).
2. Double-click the file smartid_rt.cer. You are shown the certificate information.
3. Click **Install Certificate** to start the Certificate Import Wizard.



4. Click **Next**.
5. Ensure that **Automatically select the certificate store based on the type of certificate** is selected and click **Next**.
6. Click **Finish**.



To register the CA Signer Certificate, You will need to repeat steps 2-6, using the file smartid_ca.cer (also available from the Hongkong Post CA Website).

The Hongkong Post CA Root and Signer Certificates are now registered with your computer. Netscape users should remember to register the certificates separately with Netscape (see page 11).

SETTING UP YOUR E-MAIL APPLICATION

This chapter describes the process for setting up an e-mail application to use the digital identity secured on your smart card to sign and decrypt messages. The following e-mail applications are discussed:

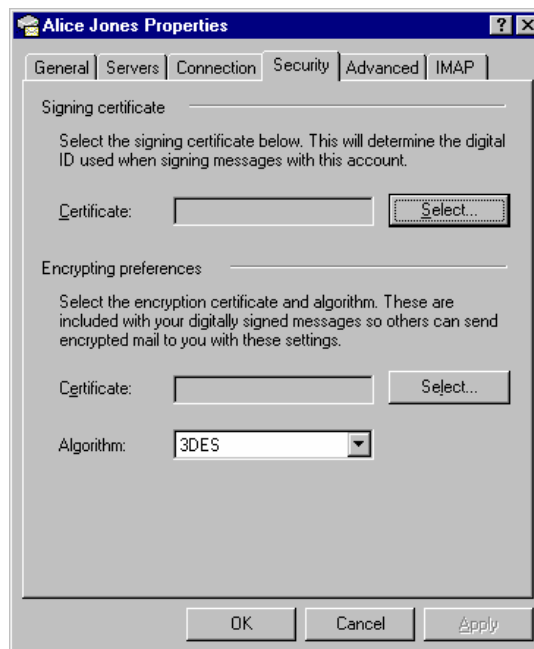
- Microsoft Outlook Express 5.5 and 6.0 / Windows Mail
- Netscape Messenger 4.51, 4.80 and 7.02

Setting up Microsoft Outlook Express / Windows Mail

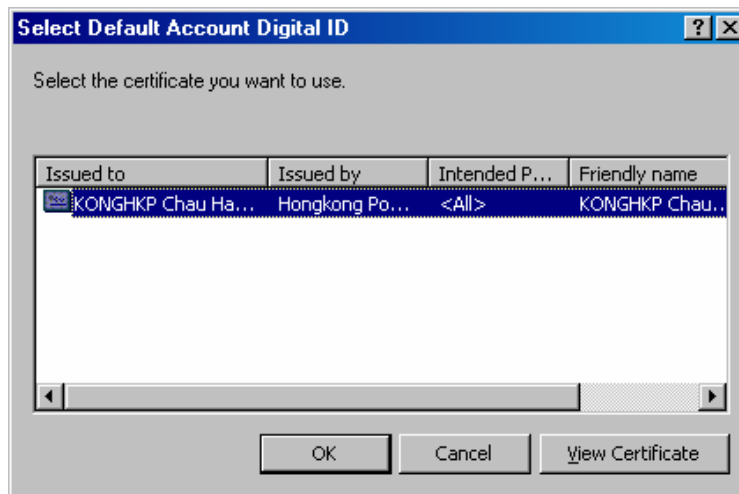
Outlook Express / Windows Mail stores your security policy as part of your e-mail account settings.

To set up Outlook Express / Windows Mail to use your smart card:

1. Launch Outlook Express / Windows Mail.
2. From the **Tools** menu, select **Accounts**.
3. Click **Mail**.
4. Select your current e-mail account and click the **Properties** button.
5. Click **Security**.



6. In the **Signing Certificate** section, click **Select** to open the Certificate Store and select the signing certificate.



If your certificate is not listed, you need to register your certificate, see *Registering your certificate* on page 7 for more information.

7. In the **Encrypting Preferences** section, click **Select** to choose your certificate used for encryption – this may be the same as your signing certificate.
8. Select an available **Algorithm** from the list and click **OK**.



Note The *e-Cert Control Manager User Guide* contains information about how to digitally sign e-mail and obtain certificates for encryption. You can also find out more by looking up 'Sending Secure Messages' in the Outlook Express / Windows Mail help topics.

Setting up Netscape Messenger

The following instructions are for setting up Netscape Messenger versions 4 and 7. Messenger stores your cryptographic settings in the Communicator Security Information.

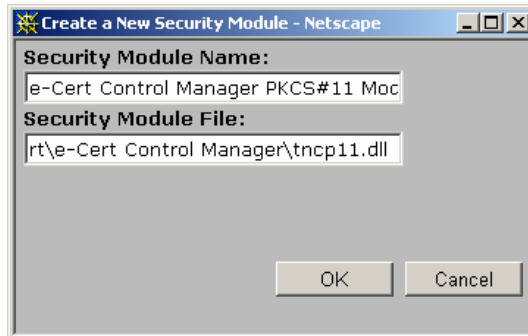


Note The e-Cert Control Manager attempts to automatically detect Netscape Messenger during installation. If your version of Netscape Messenger was detected, it is already set up to use your e-Cert, and you can skip these instructions.

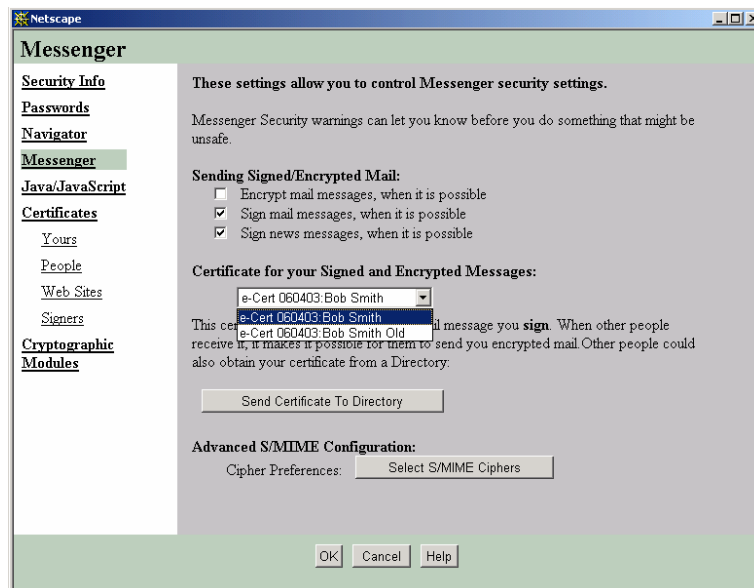
To set up Netscape Messenger version 4:

1. Insert your smart card into your reader.
2. From the **Communicator** menu, select **Tools** then **Security Info**.
3. From the Security Info dialog, select **Cryptographic Modules**.
4. Click **Add**.

- In the **Security Module Name** box, type e-Cert Control Manager PKCS#11 Module. In The **Security Module File** box, type the full path to the tncp11.dll file. The default installation location of this file is: C:\Program Files\Hongkong Post e-Cert\ e-Cert Control Manager\tncp11.dll



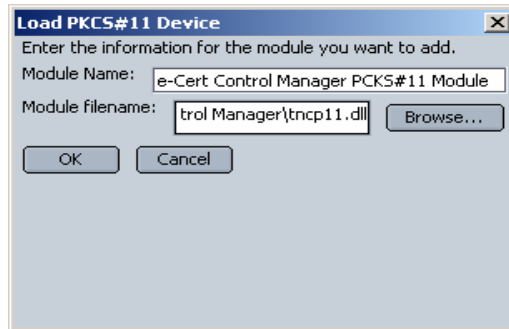
- Click **OK** to add the e-Cert Control Manager PKCS#11 Module to the list of cryptographic modules.
- From the Security Info dialog, select **Certificates** then **Yours**.
- Confirm that your certificate is listed there and click **OK**.
- You may have multiple e-Cert Certificates. To select which to use by default, go to the Security Info dialog, select **Messenger** and select the appropriate certificate from the drop-down list.



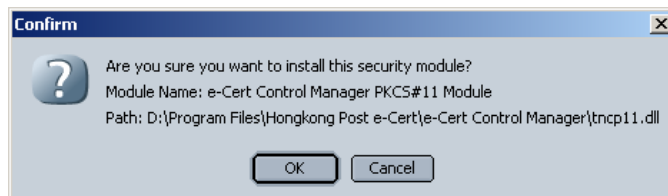
To set up Netscape Messenger version 7:

- Insert your smart card into your reader.
- From the **Edit** menu, select **Preferences**.
- From the list in the left side of the dialog box, select **Privacy & Security**, then **Certificates**.
- Click **Manage Security Devices** and then click the **Load** button.

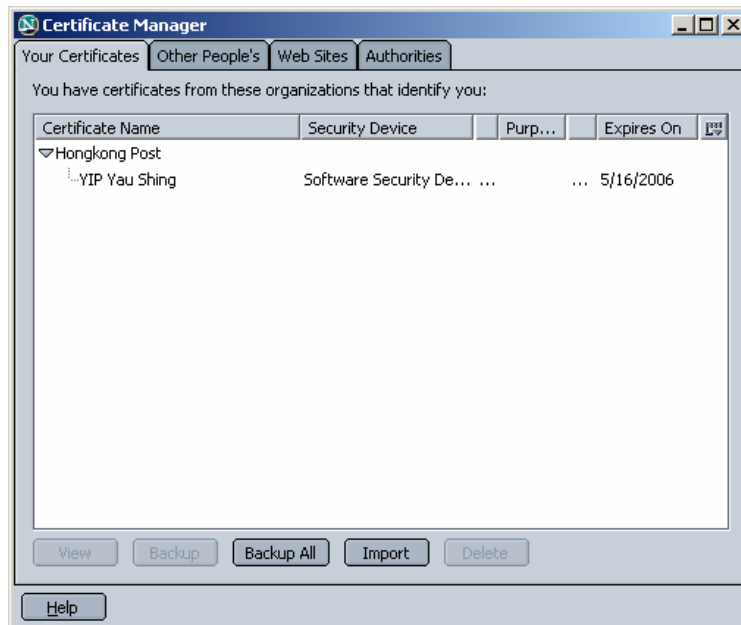
- In the **Module Name** box, type e-Cert Control Manager PKCS#11 Module. In the **Module filename** box, type the full path to the tncp11.dll file. The default installation location of this file is: C:\Program Files\Hongkong Post e-Cert\ e-Cert Control Manager\tncp11.dll



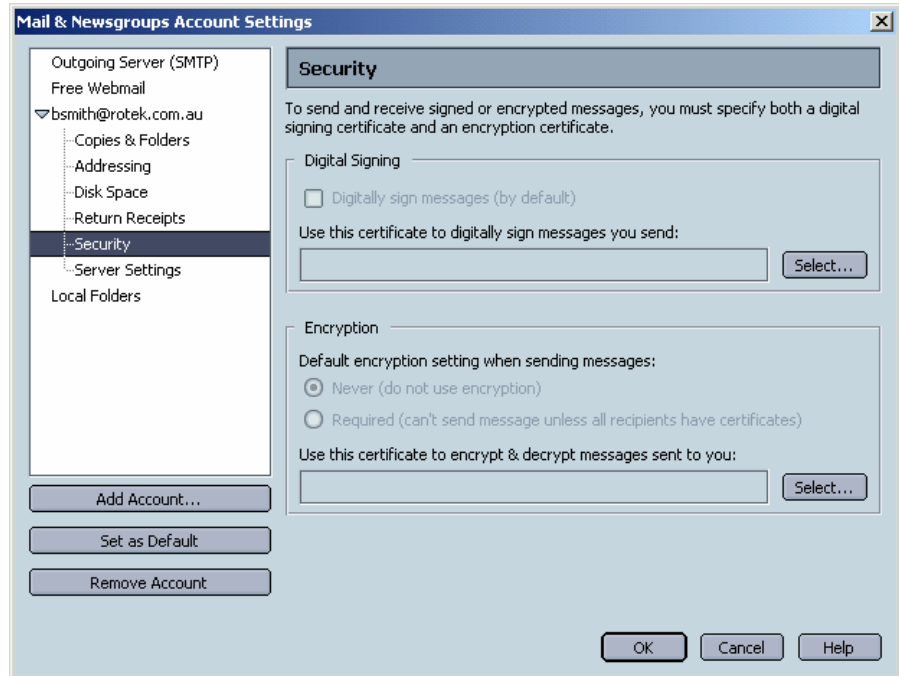
- Click **OK** to add the PKCS#11 module to the list of cryptographic modules. You are prompted to confirm this.



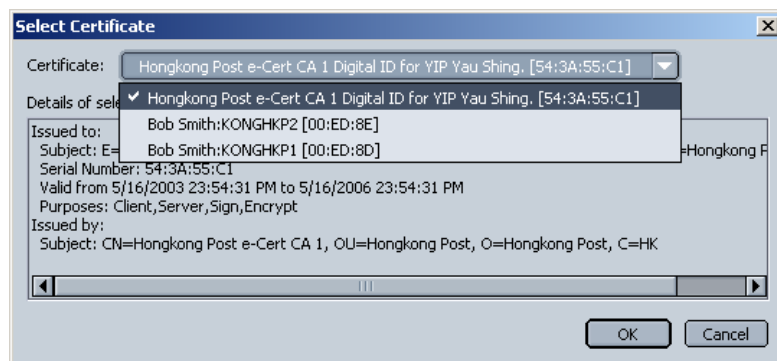
- Click **Manage Certificates** and confirm that your certificate is listed there and click **OK**.



- You may have multiple e-Cert Certificates. To select which to use by default, from the **Edit** menu, select **Mail & Newsgroups Account Settings**, then **Security**. Next to the **Use this certificate to digitally sign messages you send** option, click the **Select** button.



- At the next screen, select the certificate you wish to use for signing messages from the drop-down list. Click **OK**.



- If you intend to use encryption, you will need to repeat steps 8 and 9 to select the certificate people use when encrypting an email to you.

Registering the Hongkong Post CA Root and Signer Certificates with Netscape

The Hongkong Post CA Root certificate needs to be registered separately with Netscape. To register the certificate:

Netscape 4

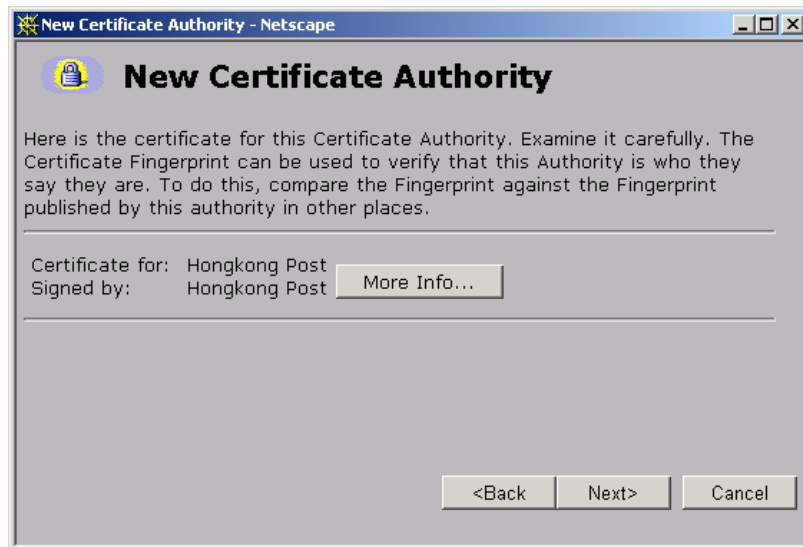
1. Launch Netscape Navigator.
2. From the **File** menu, select **Open**.
3. Download Hongkong Post CA Root Certificates from the Hongkong Post CA Website (if you have not done so).
4. Double-click the smartid_rt.cer file.



5. Click **Next**



6. Click Next



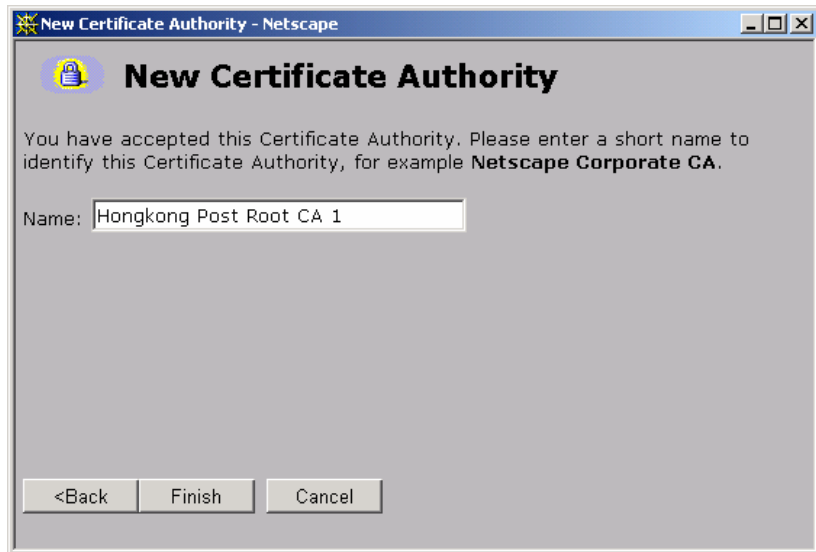
7. Click Next



8. You are prompted to accept the certificate authority. Ensure all boxes are checked and that you trust the CA to identify web sites, e-mail users, and software developers:

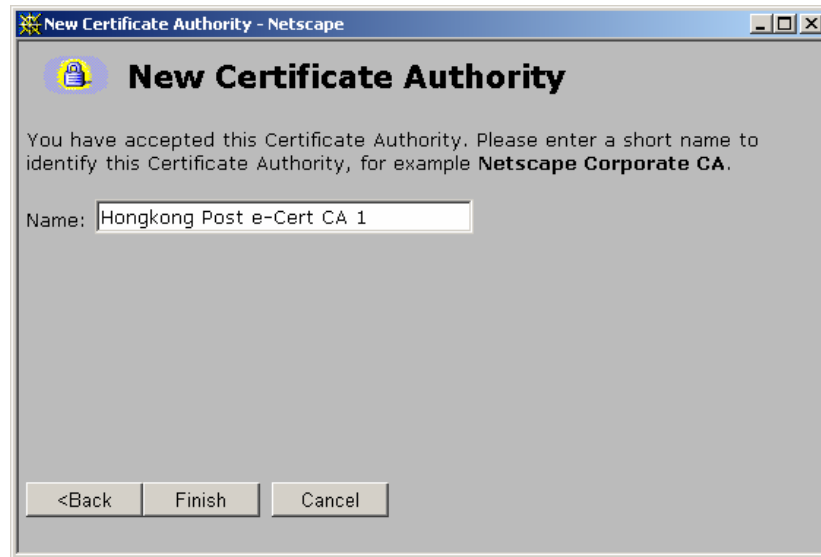


9. Click **Next**



10. Enter **Hongkong Post Root CA 1** as the name of the Certificate Authority.
11. Click **Finish** to register the certificate with Netscape 4.

You will need to repeat steps 2-11 to register the CA signer certificate, using the file smartid_ca.cer or ecert_ca_1-10.cer (also available from the Hongkong Post CA Website). In Step 10, enter **Hongkong Post e-Cert CA 1** or **Hongkong Post e-Cert CA 1 - 10** respectively as the name of the Certificate Authority.



Netscape 7

1. Launch Netscape Navigator.
2. From the **File** menu, select **Open**.
3. Download Hongkong Post CA Root Certificates from the Hongkong Post CA Website (if you have not done so).
4. You are prompted to import the certificate. Ensure all boxes are checked and that you trust the CA to identify web sites, e-mail users, and software developers:



5. Click **OK** to register the certificate with Netscape 7.

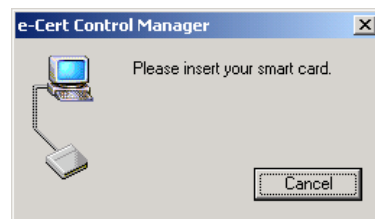
You will need to repeat steps 2-5 to register the CA signer certificates, using the file smartid_ca.cer or ecert_ca_1-10.cer (also available from the Hongkong Post CA Website).

TROUBLESHOOTING

This chapter describes the problems you might encounter when installing or using e-Cert Control Manager and provides information about overcoming the problems.

e-Cert Control Manager errors

Smart card is not found



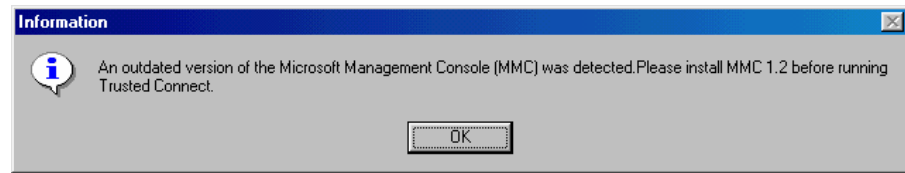
- Verify that the communication cable (and power cable, if present) from the reader is properly connected to your PC.
- Verify that the light on the card reader flashes and is continuously switched on when a smart card is inserted into the card reader. On systems not running PC/SC, the light initially flashes, changing to fully ON after e-Cert Control Manager accesses the smart card.
- Ensure that the smart card is inserted fully into the reader.
- Ensure the smart card is facing the right way and is not inserted upside-down or reversed.

P12 files cannot be loaded onto the smart card

- Ensure that the Microsoft Virtual Machine has been successfully installed on the computer. To obtain the latest Virtual Machine, visit the Microsoft Download Center:
<http://download.microsoft.com>
- Ensure that a valid P12 file is selected in 'Filename'.
- Enter correct P12 password and smart card password.

Microsoft Management Console errors

During installation, e-Cert Control Manager detects an outdated version of the Management Console

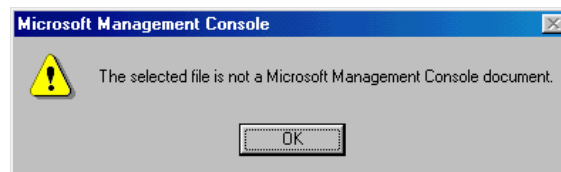


The e-Cert Control Manager requires the Microsoft Management Console version 1.1 or above. This is automatically installed in Microsoft Windows 2000 and Microsoft Windows XP operating systems, and may require separate installation on other systems. If you are running Windows NT/98/ME you will need to install MMC v1.1 for Chinese operating systems. If you are running an English operating system, download MMC v1.2.

The latest version of the Microsoft Management Console is freely available from the Microsoft Web Site, in the Windows Update section:

windowsupdate.microsoft.com

When starting the e-Cert Control Manager, the Manager reports that the selected file is not a Management Console document



Your version of the Microsoft Management Console is outdated – e-Cert Control Manager requires version 1.1 or above. The latest version of the Microsoft Management Console is freely available from the Microsoft Web Site, in the Windows Update section:

windowsupdate.microsoft.com

Please note: If you are running Windows NT/98/ME you will need to install MMC v1.1 for Chinese operating systems. If you are running an English operating system, download MMC v1.2.