E-CERT CONTROL MANAGER

for e-Cert on Smart ID Card

USER GUIDE

Version 1.4

CONTENTS

Introduction

Using e-Cert Control Manager

Using the Certificate Stores

Securing E-Mail with e-Cert Control Manager

Using e-Cert Control Manager with Secure Web Sites

Requirements for Secure Operation

Troubleshooting

CHAPTER 1

INTRODUCTION

What are smart cards, and what can they do?

In this User Guide, "smart card" refers to the "Smart ID Card" issued to each Hong Kong citizen.

Smart cards are becoming increasingly common, and many people are familiar with the small gold plate that identifies a smart card. This gold plate is the *contact plate*—the interface to the tiny microchip embedded in the card itself, and makes contact with connectors that transfer data (via electrical signals) to and from the microchip.

There are two distinct types of smart card:

- **Memory cards** only store data on their chip, like a small floppy disk.
- **Processor cards** can store data as well as *run programs*, like a small computer. Your **Smart ID Card** is a processor card.

The capacity of a smart card chip is quite small, so the amount of data and the size of the applications they run is limited, but still large enough to be quite functional. Because smart cards are highly portable and their chips store and manipulate computer data, they are ideally suited to applications that require mobile data, such as:

- Stored value (such as phone cards)
- Parking and toll collection (account information)
- Access control identification (through secure doorways)
- Digital signatures and decryption

It is for this last purpose—digital signatures and decryption—that e-Cert Control Manager uses the e-Cert on your smart ID card.

Because many of the above uses of smart cards necessitate some form of protection (you wouldn't want just anybody to be able to read the information stored in the chip), smart cards have some built-in security features: the chips are tamper-resistant, information on the card can be PIN-protected, and the chip can store data that only it can read (i.e. cannot be transferred from the chip).

Using smart cards to manage a 'digital identity'

e-Cert Control Manager treats smart cards like a set of keys that unlock the private key and e-Cert as a *digital identity* that can be used for signing transactions and e-mail, and reading secure messages meant for your eyes only. With the onset of the Internet, and the pervasiveness of digital communication, people frequently communicate over this vast, loosely connected public network without any guarantee that their message is not intercepted (and potentially *changed*) or that forged messages are not sent in their name.

This poses two problems: how can you ensure your messages are not read without your knowledge, and how can you make certain the messages you receive are genuinely from the sender? Fortunately, in 1976 Whitfield Diffie and Martin Hellman published a seminal paper "New Directions in Cryptography" that began the development of a collection of technologies that address exactly these problems: *Public Key Infrastructure*.

An introduction to Public Key Infrastructure

At the heart of Public Key Infrastructure (PKI) is a special *encryption* technique. Encryption, which has existed since ancient times, is the process of transforming a message, making it unintelligible without the knowledge of some secret information, commonly called a *key*. One of the problems that have plagued cryptography is that the same key is required to both encrypt and decrypt a message. This means that the sender of the encrypted message also needs to secretly communicate the key to the recipient so the message can be decrypted. The need to find alternative methods to securely communicate the key has proven a weakness of traditional encryption systems.

The revolution that Diffie and Hellman proposed in 1976 is to have *two* keys that are uniquely related to each other—one for encrypting and one for decrypting. Because of the special mathematical relationship the two keys have, the encrypting key can be freely distributed to the public, while the key owner should closely guard the decrypting key. The mathematical relationship ensures that it is not feasible to calculate one key from the other. Thus the encrypting key is called the *public key*, and the decrypting key is called the *private key*. To send a message to a recipient, you obtain the recipient's public key (which can be freely distributed) and encrypt the message. The recipient then uses the private key to recover the original message.

While this new technique—called *public key encryption*—addresses the need to secretly communicate a decrypting key to the message recipient, it introduces a new problem: how can you be sure the public key you use to encrypt a

message actually belongs to the intended recipient? If you meet the recipient face-to-face and you are given the public key directly, this is not an issue. But if you cannot meet the recipient in person, and must obtain the public key from somewhere else, you need to be sure the public key has not been tampered with, or substituted with another public key that allows someone other than the intended recipient to decrypt the message.

Certificates

A solution to the problem of identifying the owner of a public key is the *digital certificate*.

The concept of digital certificates was created solely to bring a level of trust to public keys. This is achieved through the use of a trusted third party: a *Certificate Authority*. Certificate Authorities are entrusted to impose a set of requirements for clearly identifying an individual (such as the presentation of a passport). Once the individual is unambiguously identified, the CA digitally signs the individual's *distinguished name* and public key—this signed information forms a digital certificate.

Hongkong Post is the first recognized Certification Authority in Hong Kong issuing recognized digital certificates ("**e-Cert**") that complies with the Electronic Transactions Ordinance (Cap. 553).

The certificate shows that a public key owner has met the identification requirements of a Certificate Authority. If you *trust* the Certificate Authority, then by extension you trust certificates signed by the Certificate Authority. In this way you can obtain a high level of trust that a public key is genuine—if a Certificate Authority you trust has signed it.

How do you trust a Certificate Authority? If you are confident a Certificate Authority is rigorous in its identification process, you can make a declaration that you trust the public key of the Certificate Authority, and thereby trust all certificates it produces.

A digital identity is made up of a *key pair* (a public key and its associated private key), and a certificate (the public key and the distinguished name of the key owner signed by a Certificate Authority). e-Cert Control Manager uses the built-in security features of smart cards to protect your private key, and runs programs on the card to sign and decrypt messages. In this way, your private key is protected by the card's PIN, and never leaves the card itself.

Digital signatures

An important function of a digital identity is the generation of digital signatures. Using a signature to endorse a document has been a convention in commerce for centuries, as it is accepted that a signature is unique to an individual and difficult to forge. Digital signatures based on public key cryptography work in the same way by assuming that each individual has a unique private key that no one else can access.

Under the Electronic Transactions Ordinance (Cap. 553), a digital signature supported by a Hongkong Post e-Cert has the same legal status as a paper-based signature.

Before messages are digitally signed, they are usually reduced to a fixed-length amount of data called a *hash*. Hashes are unique representations of messages—messages that differ by only one letter do not produce the same hash. Because digitally signing a message (particularly a lengthy one) is time-consuming, it is more expedient to produce a hash of a message and sign that. A signed message consists of the plain message, the signed hash of the message, and the certificate of the author for verifying the signature.

Recipients use the author's certificate to verify the public key and recover the original hash produced by the author. The recipient constructs another hash of the message, and if it matches the signed hash, the recipient can be sure the message has not been altered and has been produced by the certificate owner.

Digitally signed hashes are an excellent way to check that electronic messages are not tampered with in transit. However, they highlight the dependence public key cryptography has on authentic public keys. If the recipient of a signed message uses a forged digital certificate (which is thought to be genuine) to recover the hash and verify the message, the recipient can be led to believe messages sent by the forger are authentic. The best solution for this problem in use today is based on the notion of trust in a Certificate Authority.

Deeper into PKI

This section delves further into topics discussed previously and is not required reading for you to start using e-Cert Control Manager, but explains more fully the concepts behind PKI and some of the *caveats* PKI users should consider.

Encryption algorithms

One of the most popular public key encryption algorithms is RSA, named for its creators: Rivest, Shamin and Adleman. However the RSA algorithm can be quite time-consuming when encrypting and decrypting large messages and, to improve the performance of the whole process, faster alternatives have been developed.

One alternative to using RSA is to encrypt the message with a *symmetric* algorithm (where the same key is used to both encrypt and decrypt the message), which is much faster than RSA. The *symmetric key*, which is usually much shorter than the message, is then encrypted with the recipient's public key, and the entire package—encrypted message and RSA-encrypted symmetric key—is sent to the recipient.

When the recipient receives the package, the symmetric key is decrypted with a private key, and then the symmetric key is used to decrypt the message. This method takes advantage of the speed of symmetric algorithms, as well as the fact that the symmetric key can be changed for each message because it is sent along with the message. However, using this method requires careful choice of the symmetric algorithm. If the symmetric algorithm can be easily

reversed, the original message can be recovered without the need to decrypt the symmetric key. The strength of the symmetric algorithm should match the requirements for data confidentiality.

Signature algorithms

As has been mentioned, the popular method to improve performance when signing a large message is to use a hash. Hashes are also known as *cryptographic one-way digests* because it is infeasible to recover the input from the output, and the output is shorter than the input. It is an essential property of one-way digests that it is *mathematically difficult* to reverse the process, in much the same way that it is hard to reverse the process of grating cheese. Another essential property of cryptographic one-way digests is that it is *mathematically difficult* to find two messages that produce the exact same hash.

When signing large messages, it is faster to produce a hash of the message (the output from a one-way digest), and then apply a digital signature to the hash, which is much shorter. The signed hash is then packaged up with the original message and sent to the recipient. To verify the message, the recipient recovers the hash with the sender's public key, then produces another hash of the message (using the same one-way function) and compares it with the sender's hash. If they match, the recipient knows the message has not been tampered with.

The most common one-way digest functions in use are: SHA-1 (Secure Hash Algorithm version 1), SHA-256 (Secure Hash Algorithm 256 bits) and MD5 (Message Digest version 5). e-Cert Control Manager can use all of these one-way digest functions.

Key lengths

The *key length* (the number of binary codes that make up the key) of a particular algorithm often determines its *strength* (resistance to successful attack). The reason for this is that shorter keys can be *exhaustively searched*—a computer program can try every possible combination until it finds the right key. While it is a good rule of thumb to assume that the longer the key, the more secure it is, it is important to remember that there is more than one way to reverse an encryption algorithm.

The RSA algorithm, for example, uses the product of large prime numbers (in the order of 310 digits) as its keys. Large RSA keys are considered safe because, using current technology, it is *computationally infeasible* to try to discover the keys. In order to do this, you would need to rapidly factor the product of large prime numbers, and factorisation is considered a *mathematically difficult* problem. Hongkong Post e-Cert uses1024/2048-bit RSA keys.

'Mathematical difficulty' and 'computational infeasibility'

When using Public Key Infrastructure for security, it is important to be aware that, with today's rapid advances in computing technology, there are no mathematical absolutes. The strength of PKI lies in the fact that the mathematics involved makes it *extremely* difficult (the task is considered impossible) to reverse encryption. Every year since its creation, the most

talented mathematicians in the world have attempted to reverse the RSA algorithm in a competition sponsored by RSA Data Security Inc, but the algorithm is yet to be 'cracked'. However, by thinking in terms of *infeasibility* and *difficulty*, you accept that at some stage it may be possible and are not holding any false assumptions that PKI will be forever invincible against attack.

How e-Cert Control Manager uses PKI

The e-Cert Control Manager, which is made up of two distinct components: the e-Cert Application on the smart ID card, and the interface software on the PC[1] specially made for managing the Hongkong Post e-Cert and private keys on the Smart ID Card. The e-Cert application manages your private keys on the smart card, and provides the decryption and signing algorithms. e-Cert Control Manager software integrates with the operating system to provide system-level cryptographic services. When other applications, such as an e-mail program, need to use cryptographic services (to sign an e-mail for example), e-Cert Control Manager software automatically recognises this and signs the message using your private key, then returns the signed message to the e-mail application.

In this way, e-Cert Control Manager provides end-to-end signing and decryption services while securing your private key on a tamper-proof, lockable smart card.

[1] Based on the TrustedNet Connect products developed by SecureNet Limited

CHAPTER 2

USING E-CERT CONTROL MANAGER

Overview

e-Cert Control Manager is designed to integrate with Windows applications to provide services that are not a standard part of the Windows operating system. In this way, e-Cert Control Manager acts as a *subsystem*—it is not a 'standalone' application, but instead facilitates access to smart cards and the information they contain. Whenever a Windows application such as an e-mail client or a web browser needs to use digital identities from a smart card, e-Cert Control Manager automatically responds to the request and provides a bridge between the application and the information on the smart card.

Using the e-Cert Control Manager

The e-Cert Control Manager is an administrative tool for viewing the e-Cert on your smart card, registering your e-Cert with Internet Explorer and changing your PIN. The e-Cert Control Manager also provides an advanced mode for managing smart cards, readers, and e-Cert key pairs.

To launch the e-Cert Control Manager:

- Double click the e-Cert Control Manager icon in the system tray.

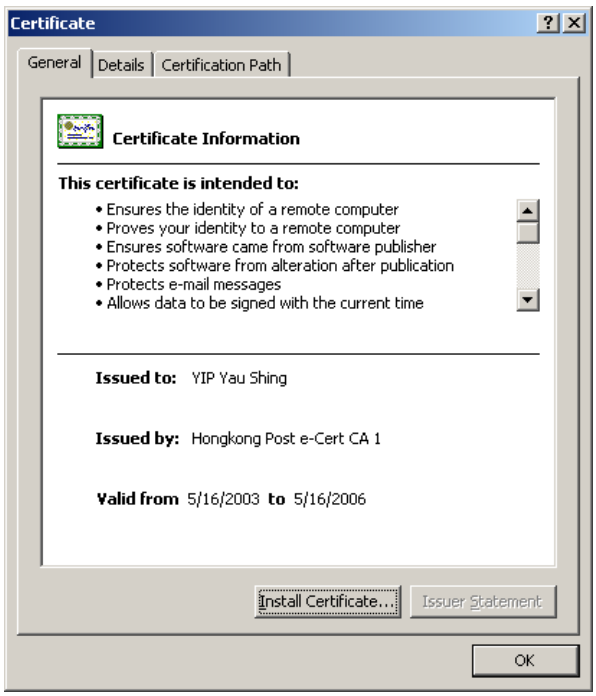
The e-Cert Control Manager

Viewing your e-Cert on Smart Card

You can get more information about your certificate on the smart card, such as the name of the issuing Certificate Authority and its period of validity, by viewing the certificate with the e-Cert Control Manager.

To view a certificate:

- Click the **View e-Cert on Smart Card** button on the e-Cert Control Manager.



Viewing a certificate

The certificate window has three tabs:

- The **General** tab describes the uses of the certificate, the certificate owner, who issued it, and what period it is valid for.
- The **Details** tab provides complete information on all the fields in the certificate including what signature algorithm was used, the public key, and the distinguished name (**Subject**).
- The **Certification Path** traces the route from this certificate back to the root Certification Authority, showing any *Intermediate CAs* that make up the certificate's authentication path.

You can copy the certificate to Internet Explorer by clicking **Install Certificate** on the **General** tab, which is the same as clicking the **Copy certificate to IE certificate store** button on the e-Cert Control Manager.

Your e-Cert PIN

The information on your smart card is protected by an unlocking number, or PIN. You need to enter the e-Cert PIN every time you access sensitive objects,

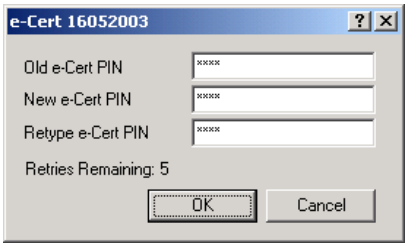
such as key pairs and certificates. This is known as *logging on* to the smart card.

Logging in to a smart card

Every time you incorrectly enter your PIN, the number of **Retries Remaining** decreases. If this number reaches zero, your smart card is *blocked* and cannot be used until you contact Hongkong Post to unblock it.

Tip: To immediately lock all key pairs, remove your smart card from the reader. Even if the smart card is re-inserted all key pairs remain locked. You can also right-click the system tray icon and select Lock Passwords from the shortcut menu.

You can change the PIN you use to log in to your smart card, by clicking the **Change e-Cert PIN on smart card** button on the e-Cert Control Manager. Enter your existing PIN, then select a new PIN and type it twice to confirm.



Changing the e-Cert PIN

Copying your e-Cert to Internet Explorer

Before you can use your certificate to sign e-mails, or authenticate your identity in a web browser, your certificate needs to be registered with the Microsoft Internet Explorer Certificate Store.

Note: More information about using the Microsoft Internet Explorer Certificate Store is available in Chapter 3.

To register your certificate with the IE Certificate Store:

- Click the **Copy e-Cert to IE certificate store** button on the e-Cert Control Manager.

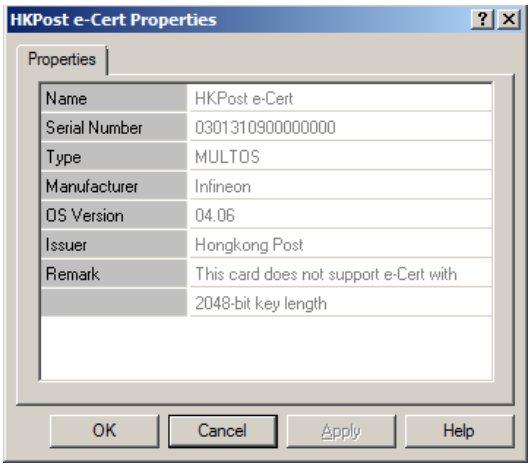
Your certificate is automatically copied to the IE Certificate Store and is immediately available for use.

Checking the version of Smart ID Card to support 2048-bits e-Cert

With the e-Cert Control Manager, you can check if the version of your smart ID card supports 2048-bits RSA key length of e-Cert.

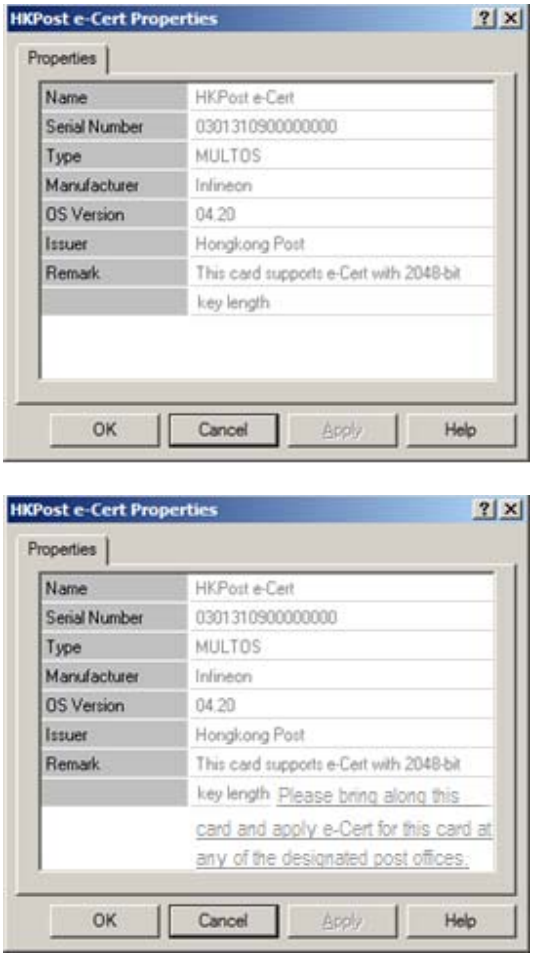
To check the smart card version:

1. From the console tree view pane, select the **Smart Cards** folder.
2. Right-click the smart card icon and select **Properties**.



Smart card properties

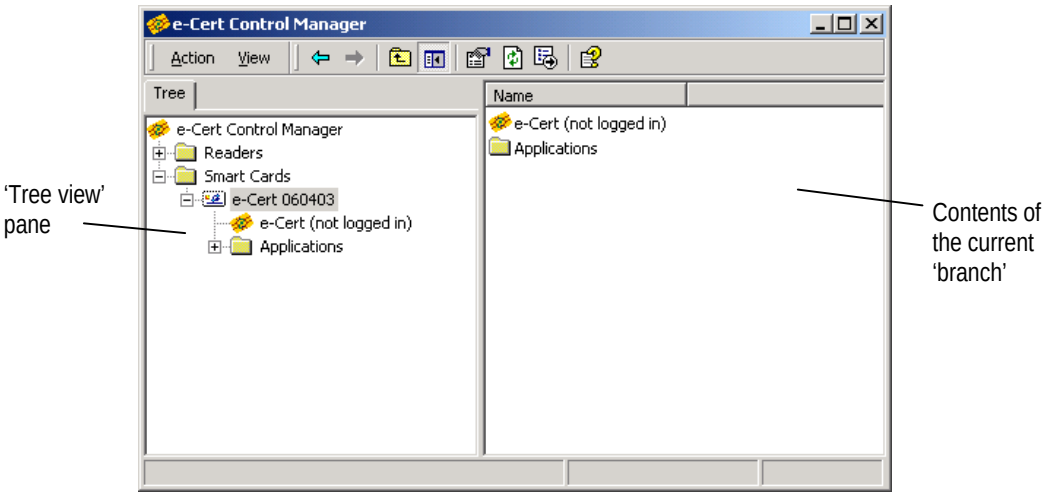
If "04.06" is shown in the field "OS Version", the Smart ID card does not support e-Cert with 2048-bit RSA key length. However, if "04.20" or above is shown in the field "OS Version" (see below), the Smart ID card supports e-Cert with 2048-bit RSA key length. Additional information will be provided in the "Remark" to remind you that you need to bring along this card and apply e-Cert for this card at any of the designated post offices.



Smart card properties

Advanced mode

In the Advanced Mode, the e-Cert Control Manager provides a hierarchical 'tree view' of the smart card readers, smart cards and the items on the cards.



The e-Cert Control Manager Advanced Mode

Beneath the e-Cert Control Manager branch of the tree, all the smart card readers attached to the computer are listed, along with all the smart cards currently inserted into the readers. The e-Cert Control Manager automatically detects when a smart card is inserted or removed from a reader and updates the view.

The Microsoft Management Console

To use the e-Cert Control Manager's Advanced Mode, you need the Microsoft Management Console. The Management Console is usually installed with Windows, but if it is not installed, it is freely available from the Microsoft Windows Update web site:
`http://windowsupdate.microsoft.com`

You do not need to install the Management Console if you do not use the e-Cert Control Manager's Advanced Mode.

Starting and stopping the server

When the e-Cert Control Manager icon is in the system tray, the e-Cert Control Manager server is running in the background, waiting for the operating system to request cryptographic functions.

To stop the server:

- Right-click the icon in the system tray and click **Shut down** from the shortcut menu. You can also right-click the e-Cert Control Manager icon in the Manager and select **Stop server** from the shortcut menu.

If the server is stopped, and the operating system requests a cryptographic function from e-Cert Control Manager (such as signing an e-mail), the server is automatically started by the operating system, and the request is passed to it.

To start the server:

- Right-click the e-Cert Control Manager icon in the Manager and select **Start server** from the shortcut menu.

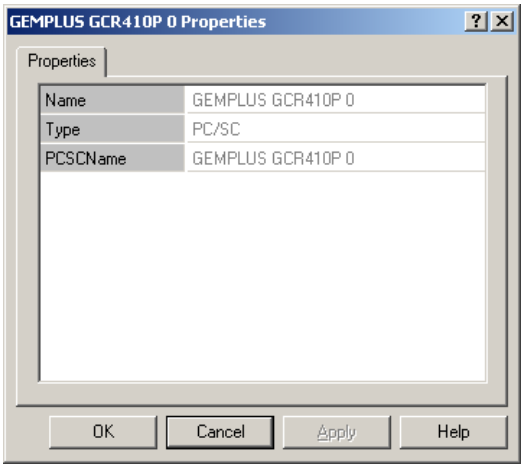
Smart card readers

In the advanced mode, the e-Cert Control Manager shows all the smart card readers connected to your computer. In order to use e-Cert Control Manager, you should have at least one smart card reader installed.

To view or change the smart card reader properties:

1. Click the **Readers** folder in the tree view pane of the e-Cert Control Manager.

2. Right-click the smart card reader icon and select **Properties** from the shortcut menu.



Smart card reader properties

Smart card readers have the following properties:

- **Name**. This is the display name for the smart card reader.
- **Type**. This is the *interface* used to connect the smart card reader to the computer. Types include PC/SC only.
- **PCSCName**. This is the name of the reader automatically registered with Windows by the PC/SC-compliant reader.

Setting up a new smart card reader

The e-Cert Control Manager automatically recognises PC/SC-compliant smart card readers when they are connected to your computer, and no configuration is necessary.

Smart cards

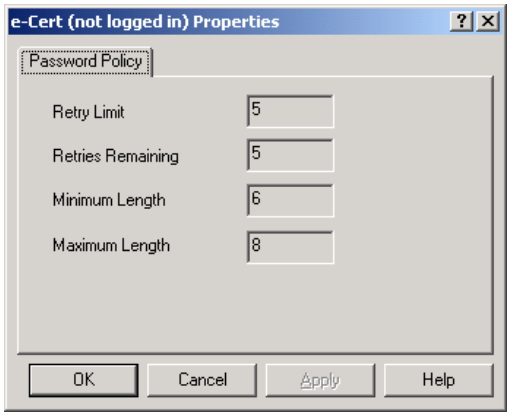
The e-Cert Control Manager identifies smart cards (your Smart ID Card) by their serial number. When a smart card is inserted into a reader, the e-Cert Control Manager is automatically updated to show the contents of the smart card.

Information on smart cards is divided into three categories:

- **Certificates**. Certificates are *public keys* signed by a *Hongkong Post Certificate Authority*
- **Key pairs**. These are the *public* and *private keys* used to sign and encrypt information.
- **Applications**. Applications are the actual programs on the smart card that process information. Smart ID cards used with e-Cert Control Manager have at least the **e-Cert application**.

PIN policy

The PIN that protects access to your smart card can only be used according to the e-Cert *Password Policy*. To view the policy, right-click the e-Cert icon and select **Properties** from the shortcut menu.



The e-Cert Password Policy

PINs have the following policy options:

- **Retry Limit**. The total number of incorrect PIN entry attempts before the card becomes *blocked*.
- **Retries Remaining**. If the smart card is not *blocked*, this is the remaining number of incorrect PIN entry attempts that are allowed. If the smart card is blocked, this is the number of unblock attempts that are allowed.
- **Minimum Length**. The minimum number of digits that make up the PIN.
- **Maximum Length**. The maximum number of digits that make up the PIN.

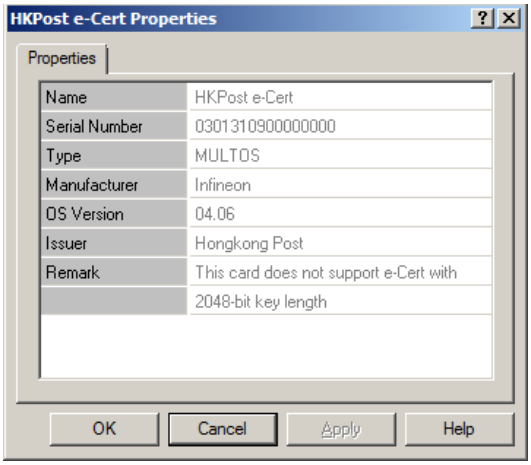
Warning: If you exceed the Retry Limit when attempting to unlock your smart card, your smart card becomes blocked and cannot be used. When the smart card is blocked, the key pair status is shown as Blocked and you cannot Login to your smart card. In this case, the Retries Remaining is the number of times the smart card can be unblocked. You must contact Hongkong Post for unblocking.

Smart card properties

With the e-Cert Control Manager, you can view the particular properties given to your smart card when it was created.

To view the smart card properties:

3. From the console tree view pane, select the **Smart Cards** folder.
4. Right-click the smart card icon and select **Properties**.



Smart card properties

Smart cards can have the following properties:

- **Name** is the human-readable name given to the smart card.
- **Serial number** is the smart card's serial number.
- **Type** is the type of smart card.
- **Manufacturer** is the name of the smart card manufacturer.
- **OS Version** is the version number of the operating system used by the smart card to run applications.
- **Issuer** is the name of the organisation that issued the smart card.
- **Remark** is the additional information provided on the 2048-bits key length support of the smart card.

Changing your smart card name

You can use the e-Cert Control Manager to name your smart card and make it more identifiable. The smart card's name is displayed in the Manager's tree view.

A named smart card

If a smart card has not been named, the e-Cert Control Manager uses the smart card serial number as its name.

To name a smart card:

1. Right-click the smart card in the e-Cert Control Manager and select **Rename** from the shortcut menu.
2. Type in a new name for the smart card. Preferably, smart card names should be descriptive and identify the smart card owner.

A smart card's name is stored locally on the card, and remains if you use the card at another computer.

Erasing all items on your smart card

You can easily erase all the keys and certificates on your smart card, as well as erase keys and certificates separately.

To erase *all* the items on your smart card:

1. Right-click the smart card in the e-Cert Control Manager and select **Erase Card** from the shortcut menu.
2. You are prompted for your e-Cert PIN. Enter your PIN to erase your smart card.

Certificates

Certificates are issued by Certificate Authorities after you make a *certificate request* and unambiguously identify yourself according to the CA policy. The policy and procedures adopted by Hongkong Post in issuing e-Certs can be found in Hongkong Post's Certification Practice Statement (CPS). The CPS can be viewed and downloaded at Hongkong Post CA's web site:
`http://www.hongkongpost.gov.hk`

When a certificate (e-Cert) is loaded onto your smart card, it is accessible under its associated key pair.

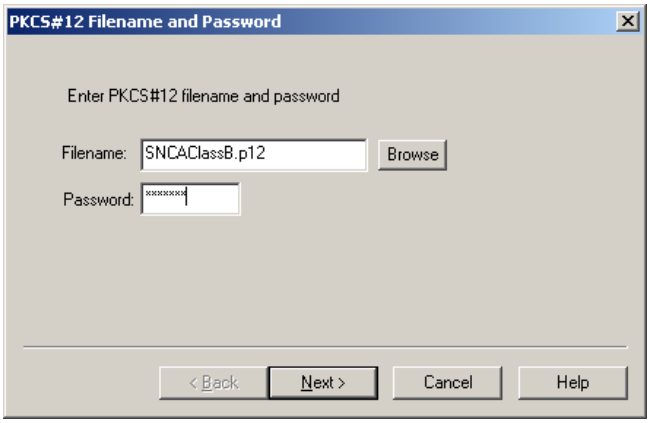
The certificate for Bob Smith's key

Loading certificates on your smart card

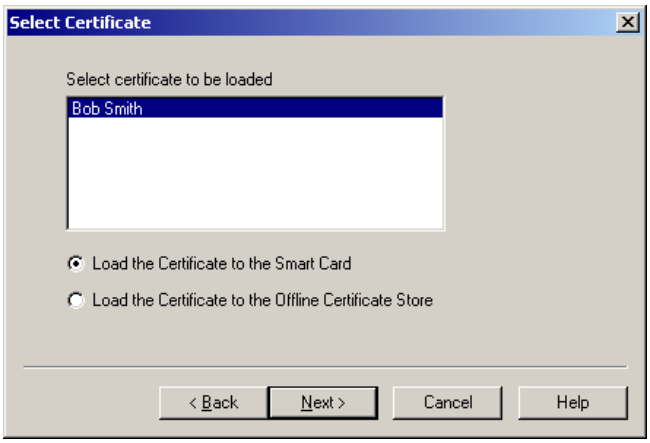
You can use the e-Cert Control Manager to load the certificate onto your smart card.

To load a certificate on your smart card:

1. Right-click the e-Cert icon in the e-Cert Control Manager and select **Load Certificates** from the shortcut menu.
2. Typically, certificates are issued in files, which may require a password to unlock. The password should be issued to you separately. Locate the certificate file by clicking **Browse**, type in the password if required, and click **Next**.



3. Select the certificate to load, and then choose the location for the certificate. You can load certificates to either the smart card or the offline certificate store. For more information about the offline certificate store see Chapter 3, "Using the Certificate Stores". Once you have chosen the certificate and loading location, click **Next.**



4. If the certificate is loaded to the smart card, the corresponding key becomes the *active key* and is used for all future digital signature and decryption functions.

When loading certificates, e-Cert Control Manager checks the certificate has a corresponding public key on the smart card, and the citizen name stored securely in the smart card matches the name in the certificate. If a public key that matches the certificate is not found, or the citizen name on the smart card is different, the certificate is not loaded and e-Cert Control Manager reports an error.

Tip: Key pairs (and their associated certificate) can also be loaded onto your smart card from files. This is handy if you have a key pair issued to you that is already certified. The same process above should be used to load a key pair from a file, as well as its certificate. Key pairs are loaded into the first available slot, or you are prompted to select a slot to overwrite. The certificate currently on the card is moved to the offline certificate store.

Exporting certificates to a file

Someone who wishes to send encrypted information to you, or verify your digital signature, requires your digital certificate. By exporting your certificate, you create a file that can be freely e-mailed or distributed.

To export a certificate:

1. Right click the certificate you want to export from e-Cert Control Manager, and select **Export Certificate** from the shortcut menu.
2. Type in a file name to save the certificate to a file.

Certificates are exported as X.509 DER-encoded files, and are compatible with the Microsoft Certificate store.

Deleting certificates

If your certificate expires, or you wish to replace an existing certificate on your smart card with a new one, you can delete the certificate from your smart card.

To delete a certificate:

1. From the tree view pane, right-click the certificate you wish to delete and select **Delete** from the shortcut menu.
2. Click **Yes** to confirm the operation.
3. Enter your e-Cert PIN to confirm you are authorised to delete the certificate from the smart card.

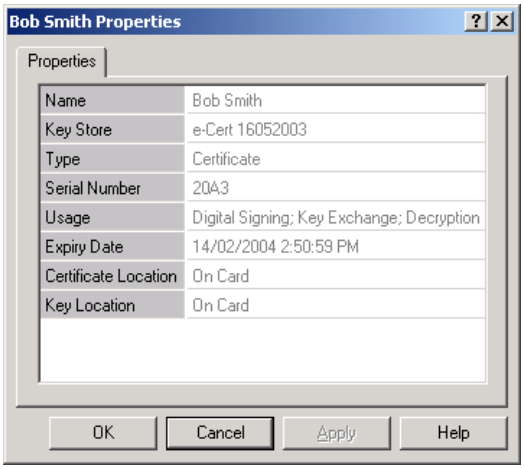
Unless a certificate has expired, you should export the certificate to a file to create a backup before permanently deleting it.

Certificate properties

Instead of viewing a certificate, you can quickly check your certificate properties from within the e-Cert Control Manager.

To view a certificate's properties:

1. From the tree view pane, select the certificate to view.
2. Right-click the certificate and select **Properties** from the shortcut menu.



Certificate properties

The e-Cert Control Manager reports the following properties for certificates:

- **Name**. The common name (as opposed to the distinguished name) of the certificate owner.
- **Key Store.** The name of the smart card that contains the certificate.
- **Type.** The type of smart card object.
- **Serial Number**. The unique certificate number.
- **Usage.** How the corresponding key pair can be used.
- **Expiry Date.** The date the certificate expires.
- **Certificate Location.** Whether the certificate is on the smart card or in the offline certificate store.
- **Key Location**. Whether the key pair is on the smart card.

Key pairs

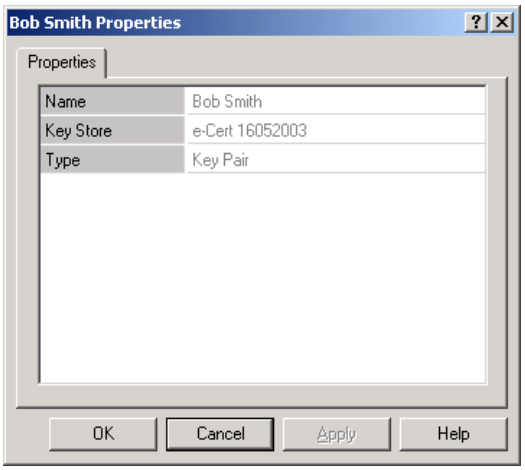
The heart of your digital identity is your key pair. As discussed in Chapter 1, your key pair consists of a *private key,* used to sign messages and decrypt messages sent to you, and a *public key*, which is used by others to verify your signature and encrypt messages to you.

Before you can use your e-Cert key pair, you need to log in to your e-Cert Smart ID Card. You log in and log out of your smart card by right-clicking the e-Cert icon in the tree view of the e-Cert Control Manager and selecting either **Login** or **Logout**.

Key pair properties

To view your key pair properties:

- Right-click the key pair in the tree view pane of the e-Cert Control Manager and select **Properties** from the shortcut menu.



Key pair properties

Key pairs have the following properties:

- **Name** is the name of the key pair, assigned when the key pair is created.
- **Key Store** is the name of the smart card hosting the private key for this key pair. If this is blank, the key is stored on the smart card, but the smart card has not yet been given a name (see *Changing your smart card name* on page 18 for more information).
- **Type** is the category of smart card object.

Deleting key pairs

If you no longer use a specific key pair, or the key pair has become compromised, you can delete the key pair from the smart card to recover the space and create a new key pair.

To delete a key pair:

1. From the tree view pane, right-click the key pair you wish to delete and select **Erase Key** from the shortcut menu.
2. Click **OK** to confirm the operation.
3. Enter your e-Cert PIN to erase the key pair.

Changing the active key pair

The active key pair on your smart card is used for all digital signature and decryption functions, and has a certificate loaded for it. If you change the active key pair, you need to load the certificate for it from your offline certificate store.

To make another key pair the active key pair:

1. From the tree view pane, right-click the key pair you wish to make the active and click **Make Active** from the shortcut menu.
2. Enter your e-Cert PIN to import the certificate from your offline certificate store.

Applications

All smart cards used with e-Cert Control Manager contain the e-Cert Application.

The applications folder in the e-Cert Control Manager shows what applications are on the smart card. Applications are self-contained and do not require modification or configuration with the e-Cert Control Manager.

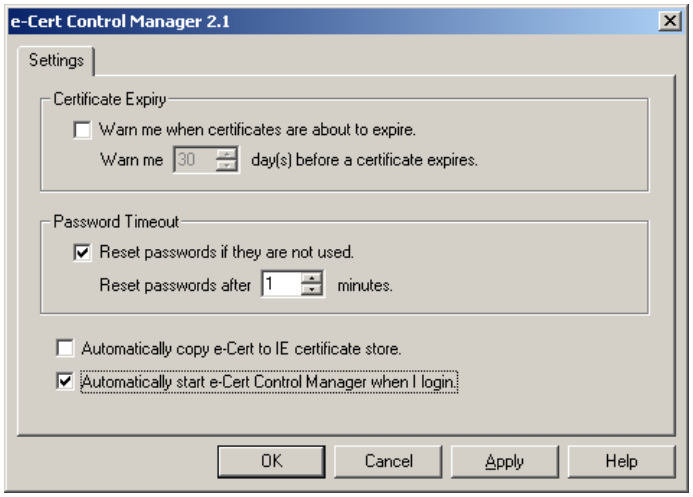
e-Cert Control Manager Settings

As well as the settings available with the e-Cert Control Manager in advanced mode, you can specify the following options:

- Certificate expiration warning.
- PIN timeout period.
- Automatic copying of certificates to the IE certificate store.
- Automatic start-up of e-Cert Control Manager.

To set these e-Cert Control Manager options:

- Select **Setting** from the Action menu.



Certificate expiration

Each certificate has a *validity period*, after which the certificate expires and you will need to re-apply to the Certificate Authority for a new certificate.

e-Cert Control Manager can remind you of imminent certificate expiration so you can contact your Certificate Authority and obtain a new certificate before your existing one expires. To enable expiration warning, check the **Certificate expiration** box and select the number of days warning you require.

PIN timeout

This is the amount of time that elapses before an unlocked key pair is automatically re-locked. When a key pair is re-locked, you need to present the e-Cert PIN to access the key pair again.

To immediately lock all key pairs, remove your smart card from the reader. Even if the smart card is re-inserted all key pairs remain locked. You can also lock all key pairs by right-clicking the system tray icon and selecting **Lock Passwords** from the shortcut menu.

Automatic options

The other options available are:

- **Copy e-Cert to IE**. When you insert a smart card into a reader, e-Cert Control Manager checks if the certificates on the card already exist in the Internet Explorer Certificate Store and, if not, copies them.
- **Automatic start**. When checked, this option automatically starts e-Cert Control Manager when you log in to your PC.

Note: If you set the Certificate Expiration warning and Automatic registration options, you are prompted for your PIN each time your smart card is inserted. If both of these options are unchecked, you are not prompted for your PIN.

CHAPTER 3

USING THE CERTIFICATE STORES

Overview

Managing certificates is an important part of maintaining and enforcing digital security with e-Cert Control Manager. In order to encrypt e-mail, or verify the authenticity of a digital signature, you need to know how to obtain, classify and view certificates.

The Microsoft Certificate Store is special software for managing certificates that can be used by applications. For example, whenever an e-mail program needs to verify a digital signature, it can retrieve a copy of the Certificate Authority's public key from the Certificate Store, provided it is registered.

Similarly, when you want to sign e-mail, the e-mail application needs to attach your certificate to the message so that the e-mail recipient can verify your signature. In this case, the e-mail program can retrieve your certificate from the Certificate Store.

The offline certificate store

e-Cert Control Manager can store up to four keys and one certificate on your smart card. The certificate on the smart card corresponds to the active key. Certificates corresponding to the non-active key are stored in the offline certificate store located under the installed directory of e-Cert Control Manager.

Note: On Windows Vista / 7, the offline certificate store is moved to the Windows all user directory as set by the environment variable ALLUSERPROFILE (in most cases are c:\ProgramData)

If you take your smart card to a different computer, you may not be able to access the certificates in your offline certificate store unless you transfer your offline certificate store to the new machine. To transfer your offline certificate store,

1. Copy the certificates under the directory folder of certificate store from the old machine to the certificate store of the new machine.
2. Restart the e-Cert Control Manager server (see Starting and stopping the server for more information).

When you insert your smart card, e-Cert Control Manager examines the offline certificate store and detects the certificates that correspond to keys on your card, making them available for use by applications.

The current active key pair depends on the certificate loaded on the smart card. To change the active key pair, load a certificate for the new key pair onto the smart card.

Note: To attach your certificates to e-mail and to create secure web sessions, your certificate needs to be either on your smart card or registered with the Microsoft Certificate Store. The offline certificate store simply archives the certificates for any keys on your smart card that are not currently the active key.

The remainder of this chapter discusses using the Microsoft Internet Explorer Certificate Store.

The IE Certificate Store

The Microsoft Certificate Store arranges certificates in four categories:

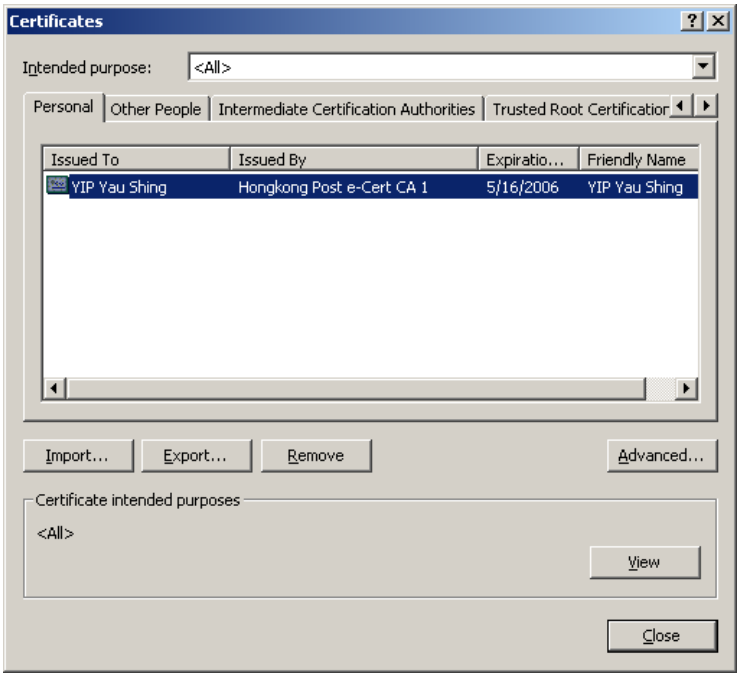
- **Personal**. These are the certificates that identify you, and contain your public key signed by a Certificate Authority.
- **Other People.** These are the certificates that identify other people, and can be used to encrypt messages.
- **Intermediate Certificate Authorities.** These are the certificates of Certificate Authorities that belong to a hierarchy, and are signed by Trusted Root Certificate Authorities.
- **Trusted Root Certificate Authorities.** These are self-signed certificates from Certificate Authorities you trust.

Opening the Certificate Store

The Certificate Store is installed as part of the Internet Options, available from the Control Panel.

To open the Certificate Store:

1. From the Start menu, select Settings, then Control Panel.
2. Double-click **Internet Options**.
3. Click **Content**.
4. Click the **Certificates** button.



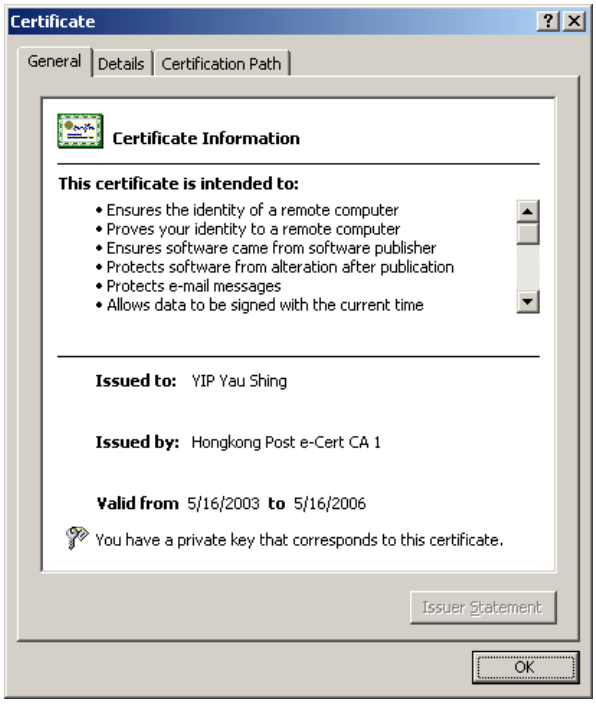
The Microsoft Certificate Store

Viewing certificates

All the certificates in the Certificate Store are arranged under their category.

To view a certificate:

- Locate the certificate from its category and double-click it.



A personal certificate

Certificate details

The certificate view provides:

- A general overview of the certificate and its intended purpose.
- A detailed summary of the fields that make up the certificate and their properties.
- The certificate's certification path.

General

The general view provides information about:

- The intended purpose of the certificate, such as e-mail protection, key exchange, and remote authentication.
- The name of the certificate's owner.
- The name of the Certificate Authority that issued the certificate.
- The validity period of the certificate.
- Whether you have a private key for the certificate, and can use the certificate to sign e-mail and decrypt messages encrypted with this certificate.

Details

The details view provides information on all the fields and their properties that make up the certificate. The fields of a certificate are:

- **Version.** The version number of the type of certificate.
- **Serial number**. The serial number applied to the certificate by the Certificate Authority.
- **Signature algorithm**. The algorithm used by the Certificate Authority to sign the certificate. An example is `md5RSA` which means that an RSA signature was applied to an MD5 digest of the certificate.
- **Issuer**. The Certificate Authority that signed the certificate.

- **Valid from**. The start of the validity period.
- **Valid to**. The end of the validity period.
- **Subject**. The distinguished name that uniquely identifies the owner of the certificate. Distinguished names are made up of fields that identify an individual by more than just a common name. In this way Certificate Authorities can distinguish between two people, both with the name 'Susan Smith'.
- **Public key**. The public key of the certificate owner.
- **Thumbprint algorithm**. The certificate contains a 'thumbprint' of the public key, to ensure it has not been modified. This is the algorithm used to generate the thumbprint.
- **Thumbprint**. The unique sequence of codes that verifies that the public key has not been modified.
- **Friendly name**. A short but meaningful display name for the certificate.

Certification path

The object of the certification path is to establish a line of trust between a Certificate Authority you trust and the certificate. The certificate path provides a status on the trustworthiness of the certificate by determining if you can trace the certificate to a trusted CA.

If the certificate cannot be traced to a trusted CA, you should be cautious about messages that use this certificate.

Importing and exporting certificate files

Certificate files come in three main formats:

- **DER encoded binary X.509**. This format is defined in the X.509 standard, and is encoded using the Direct Encoding Rules.
- **Base-64 encoded X.509**. This format also uses the X.509 standard, but is encoded in Base-64 (also called MIME).
- **PKCS #7 certificates**. This format is defined in Public Key Cryptography Standard number 7.

All of these file formats are recognised by the Certificate Store, so you can export and import certificates in any of these formats.

Importing a certificate file

There are two ways you can import a certificate to the Certificate Store:

- Double-click the certificate file and click **Install certificate** from the certificate view window.
- Launch the Certificate Store and click **Import**.

When you choose to import a certificate, the Certificate Store launches the Certificate Import Wizard. The Certificate Import Wizard has three stages to help you import the certificate:

1. The first stage describes the process of importing a certificate. Click **Next**.
2. The next stage determines in which store (Personal, Other People, Intermediate CA or Trusted Root CA) you want to place the certificate. The Certificate Import Wizard can attempt to determine which store

the certificate belongs to, or you can specify which store you want the certificate to go into.

3. The last step shows you a summary of your selection options for review. Click **Finish** to import the certificate.

Note: You only need to import certificates belonging to other people and Certificate Authorities directly into the IE Certificate Store. Your e-Cert is copied to the Microsoft Internet Explorer Certificate store from the e-Cert Control Manager. See page 12 for more information.

Importing Hongkong Post CA Root and Signer certificates

It is necessary for you to import the Hongkong Post CA Root and Signer certificates so that your web browser trusts all the certificates Hongkong Post issues. All the Hongkong Post CA Root and Signer certificates can be downloaded from http://www.hongkongpost.gov.hk.

By importing Hongkong Post CA Root and Signer certificates, you can establish a chain of trust to the Hongkong Post e-Certs given to you by other people.

You only need to import the Root and Signer certificates once with your computer, however if you use Mozilla Thunderbird or Mozilla Firefox, you need to register the certificates separately with them.

Detail information about how to import certificates can be found in the Installation Guide.

Exporting a certificate file

There are two common ways you can give your certificate to someone so that they can send you encrypted e-mail:

1. You can sign a message and e-mail it to them. This attaches your certificate to the message.
2. You can extract your certificate from the Certificate Store to a file and give them the file.

There are two ways you can export a certificate from the Certificate Store:

- Double-click the certificate and click **Copy to File** from the **Details** tab.
- Select the certificate from the Certificate Store and click **Export**.

When you choose to export a certificate, the Certificate Store launches the Certificate Export Wizard, which has three steps:

1. The first stage describes the process of importing a certificate. Click **Next**.
2. If you have the private key for this certificate (i.e. you are the certificate owner), you are prompted to export the private key along with the certificate. To protect the security of your private key, private keys protected on a smart card *cannot* be exported. Click **Next**.
3. You are prompted to select the format of the file. If you are exporting this certificate to send to someone who will then import it into the Certificate Store, you can use any of the available formats. For other recipients, check with them to see if they have any requirements for the certificate file format. Click **Next**.
4. You are prompted for the filename. Type in a file name and click **Next**.
5. The final stage shows you the details of the operation and asks for confirmation. Click **Finish** to export the certificate.

CHAPTER 4

SECURING E-MAIL WITH E-CERT CONTROL MANAGER

Overview

One of the most important jobs e-Cert Control Manager performs is the protection and authentication of sensitive e-mail. e-Cert Control Manager integrates with your e-mail application to provide encryption and digital signatures automatically to your outgoing e-mails.

This chapter describes how to set up and use e-Cert Control Manager's signing and encryption functions with these e-mail applications:

- Microsoft Outlook Express / Windows Mail / Windows Live Mail
- Mozilla Thunderbird

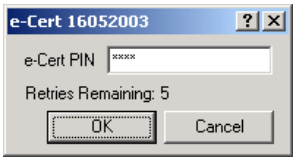
Tip: Information about setting up your e-mail application to use your e-Cert digital identity can be found in the Installation Guide.

Securing e-mail with Outlook Express / Windows Mail / Windows Live Mail

Signing e-mail

To digitally sign a message:

1. From the File menu, select **New Message**.
2. Compose your message.
3. From the Tools menu, select **Digitally Sign**. A certificate icon appears next to your e-mail address.
4. When you are ready to send your message, click **Send**. e-Cert Control Manager asks for your PIN to access the private key on your smart card and sign the message.



5. The message is signed and submitted for delivery.

Encrypting e-mail

Outlook Express / Windows Mail / Windows Live Mail requires that certificates used to encrypt messages are stored in your address book. You can create an address book entry containing a certificate in one of two ways:

- Automatically when you receive a signed e-mail message.
- Manually if you receive a certificate in a file, or as an attachment.

Obtaining a certificate

If you received the certificate attached to a signed e-mail message, you can automatically store the certificate in your Address Book:

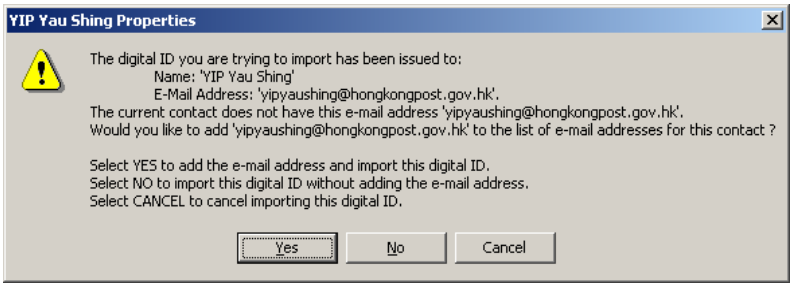
1. Open the message by double-clicking it.
2. Right-click the sender's e-mail address in the **From** field of the e-mail header and click **Add to Address Book** from the shortcut menu.
3. The certificate is inserted to the sender's entry in your Address Book.

If you received the certificate in a file, you need to create the Address Book entry and attach the certificate to the entry.

To attach a certificate to an Address Book entry:

1. Open the Address Book by selecting **Address Book** from the Tools menu.
2. If the certificate owner does not already have an entry in the Address Book, create a new entry by selecting **New** from the Entry menu.
3. Click **Digital IDs**.
4. From the **Select an E-mail Address** list, select the certificate owner's e-mail address.
5. Click **Import**.
6. Locate the certificate file and click **Open**.

The certificate is added to the Address Book entry. If the certificate owner's e-mail address you selected does not match the e-mail address in the certificate, you get the following message:



Adding a certificate

If you receive this error, do not import the certificate. If you click **No** and import the certificate, you are unable to use the certificate to encrypt e-mail. You should contact the certificate owner to obtain a correct certificate.

Encrypting e-mail

To encrypt e-mail to a recipient whose certificate you have set up in your Address Book:

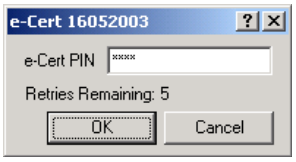
1. Compose your e-mail.
2. When you are ready to send, select **Encrypt** from the Tools menu. A padlock icon is shown next to the recipient's e-mail address, indicating this e-mail will be encrypted before it is sent.
3. Click **Send** to submit the encrypted e-mail for delivery. Because your digital identity is not required when encrypting e-mail to a recipient, you are not required to access your smart card.

Decrypting e-mail

When an encrypted e-mail arrives in your inbox, it appears with an icon containing a blue padlock.

To read the encrypted mail:

1. Double-click the e-mail item.
2. You are prompted for the e-Cert PIN to the private key that will decrypt the e-mail.



When you enter the correct e-Cert PIN, the e-mail is decrypted and displayed.

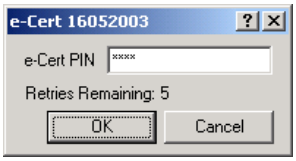
Securing e-mail with Mozilla Thunderbird

Mozilla Thunderbird version 3

Signing e-mail

To digitally sign a message:

1. Start Mozilla Thunderbird and click the **Write** button on the toolbar to compose a new message.
2. Type your message.
3. Click **Security** on the toolbar and select **Digitally Sign this Message**.
4. Click **Send** to submit the e-mail for delivery. To sign the message, e-Cert Control Manager requires access to your digital identity, and you are asked to enter the smart card PIN.



5. Enter your PIN to sign the message.

Verifying digital signatures

If you receive an e-mail message with an invalid signature, Mozilla Thunderbird displays an icon showing that the certificate cannot be trusted. Do not trust signed messages with an invalid signature.

More complete information about the security of a particular e-mail message is available by selecting **Message Security Info** from the **View** menu.

Encrypting e-mail

With Mozilla Thunderbird, you can only encrypt messages to people who have sent you their certificate in a signed message. You cannot import the certificate from a file.

When you receive a signed message (showing the signature icon), the certificate is automatically imported into the Security Manager. You can view the list of registered certificates by selecting through the Certificate Manager:

1. From the **Tools** menu, select **Options**.
2. Select **Advanced** from the navigation pane.
3. Select **Certificates**, and then click **View Certificates**.

All the certificates registered with Mozilla Thunderbird are displayed, click **People** to see the certificates of people you can send encrypted messages to (and verify their digital signature).

To send an encrypted e-mail to a recipient who has sent you a certificate:

1. Click the **Write** button to compose an e-mail.
2. Type in the recipient's e-mail address or locate it through the Address Book.

3. Click **Security** on the toolbar and select **Encrypt this Message**.
4. Click **Send** to encrypt the message and submit it for delivery.

Decrypting e-mail

When you click an encrypted e-mail in your Inbox, e-Cert Control Manager automatically requests your key pair e-Cert PIN to decrypt the message contents.

If you enter the correct PIN, and the private key can decrypt the message, the message is decrypted and displayed with an icon showing the message is encrypted, or signed, or both. Encrypted messages are not permanently decrypted—to view the encrypted message again later, you are required to re-enter the PIN (if the timeout period has expired) to decrypt and view the message.

CHAPTER 5

USING E-CERT CONTROL MANAGER WITH SECURE WEB SITES

Overview

In the same way that you can sign an e-mail message with your private key, and supply your certificate to a remote recipient as credentials for your digital identity, you can use your certificate and private key to authenticate your digital identity to a web site.

Authentication of your digital identity to a web site is performed through a special *protocol* called the Transport Layer Security, or TLS, and is also known as the Secure Sockets Layer (SSL). A protocol is a method computers use to communicate with each other, and the TLS protocol establishes an encrypted channel between your computer and a web site so that all the (potentially sensitive) information you submit to the web site is encrypted as it passes through the Internet.

How does TLS work?

Transport Layer Security is often called a *handshake protocol* because, at the beginning of a TLS session, the web server (simply called the 'server') and the computer accessing the server (the 'client') identify themselves to each other and come to an agreement on how the session is to be protected.

There are two types of TLS, each with their own security requirements:

- **Server-side authentication** means that the web server identifies itself to the client by sending its certificate. The client authenticates the certificate by checking that it is valid and is signed by a CA recognised by the client, and encrypts all data sent to the server with the server's public key. Hongkong Post also issues Server Certificates (i.e. e-Cert (Server)) to meet server-side authentication requirements.
- **Client-side authentication** goes a step further by authenticating the client. Once the server is authenticated according to server-side TLS, the client then sends its own certificate (e.g. e-Cert) to the server. The server then checks the validity and authenticity of the client's certificate and uses the client's public key to establish a secure communication channel.

A TLS session

A Transport Layer Security session handshake (the part of the session where the client and the server negotiate encryption) typically follows these steps:

1. The client requests a secure resource (such as a web page) from the server.
2. The server sends the client its certificate.
3. The client authenticates the server's certificate using a Trusted Root CA. If the certificate cannot be authenticated, the session stops here.
4. If the certificate is valid and authentic, the client and server negotiate the level of encryption that will apply to the TLS session.
5. The client creates a unique, one-off *session key* (a symmetric key that encrypts all traffic between the client and the server), encrypts the session key with the server's public key and sends the encrypted package to the server.
6. If the information on the server is restricted and requires client-side authentication, the server requests the client's certificate. The client signs a piece of data that is unique to this handshake, and sends the signed data and its certificate to the server with the session key.
7. The server decrypts the package and uses the session key to communicate with the client. If client-side authentication is used, the server checks the signed data and verifies the authenticity and validity of the client's certificate before communicating with the client.

Why use a session key?

If both the client and the server are exchanging certificates, why not use public key encryption to secure the entire session, instead of creating a symmetric session key? Because public key encryption is quite time-consuming, it is far more expedient to use a faster, symmetric algorithm to encrypt the communication channel, and use public-key encryption to transmit the key.

Some of the encryption algorithms used in TLS are: RC2, RC4, IDEA, DES and triple-DES. All of these algorithms have a significant speed advantage over public key encryption.

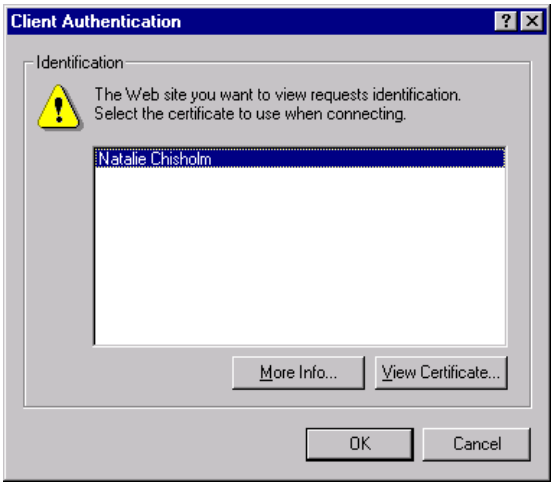
e-Cert Control Manager and TLS

With server-side TLS, you only need to verify the server's certificate with a recognised CA in your Certificate Store. Once the server's certificate is authenticated, you use the server's public key to securely transmit the session key. With server-side TLS, you do not need to digitally sign any messages, or transmit your own certificate, so you do not need to use e-Cert Control Manager.

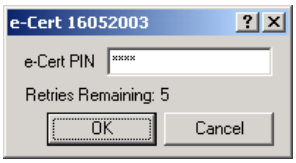
With client-side TLS, you need to sign a unique piece of data during the TLS handshake and submit a certificate. When the server requests your certificate, e-Cert Control Manager automatically prompts you to select a certificate to submit to the server, and requests the smart card e-Cert PIN to access the private key used to sign the data.

To authenticate your identity with client-side TLS:

1. Ensure your certificate has copied to Internet Explorer Certificate Store. See *Copying your e-Cert to Internet Explorer* on page 12 for more information.
2. Enter the URL of the web site in your browser.
3. When requested for a certificate, your browser prompts you to select a certificate from the Certificate Store:



4. Select the relevant certificate and click **OK**.
5. e-Cert Control Manager prompts you for your smart card e-Cert PIN to sign data to submit to the server:



6. If your authentication is approved, and you have the permissions to access the resource, you are granted access to the web site.

CHAPTER 6

REQUIREMENTS FOR SECURE OPERATION

e-Cert Control Manager is designed to provide high-strength security for your data, but this security can be undermined by improper use. The most important means of maintaining the security of e-Cert Control Manager is *vigilance*. Be wary of suspicious behaviour that may indicate an attack is being attempted.

This chapter describes how to detect attacks against the security of e-Cert Control Manager, and provides guidelines for using e-Cert Control Manager to ensure that it provides the maximum protection for your sensitive data.

Care for your smart card

Your smart card contains valuable information that allows you to sign and decrypt data. It is important that you take care of your card and keep it under your control at all times. Should an attacker manage to obtain both your smart card and the PIN that protects access to your private keys, the attacker could recover your data or impersonate you.

When you leave a computer running e-Cert Control Manager, be sure to take your card with you—especially when there is the possibility that someone else may access your computer while you're away. You should either remove the card from the reader, or lock the card to ensure that access to any sensitive data on the smart card requires a PIN.

Your smart card should be inserted only into a computer that is running e-Cert Control Manager, and then only into a smart card reader that is controlled by e-Cert Control Manager. If the e-Cert Control Manager does not show a particular card reader, the reader is not under the control of e-Cert Control Manager and must not be used for e-Cert Control Manager smart cards. Inserting the card into a reader under the control of an application other than e-Cert Control Manager, especially if the application is not trustworthy, allows that application to potentially destroy data on the card, or bypass security features of e-Cert Control Manager. Furthermore, e-Cert Control Manager must be installed according to the procedures detailed in the *e-Cert Control Manager Installation Guide*, and should make certain it is an authentic edition of the software with correct version. Failure to do so may leave e-Cert Control Manager vulnerable to viruses and illicit modification, or may allow unauthorised users on the network to access e-Cert Control Manager and sign or decrypt data.

Before using e-Cert Control Manager, you should check that there are no devices that intercept communication between the smart card and the computer.

Should you lose your card, or it is stolen, it is imperative that you contact your smart card issuer or certification authority as soon as possible to revoke all certificates associated with the smart card.

You must only allow programs that are trusted to perform requested actions to interface with e-Cert Control Manager. Failure to do so could allow a malicious program to delete your keys, or replace them without your consent. Never insert your card into a computer unless you are confident that the correct version of e-Cert Control Manager is properly installed.

Care for your e-Cert PIN

The primary protection mechanism for your smart card is the PIN that unlocks your private keys. You should select your own PIN so that no one else knows it. Pick PIN that is as random as possible. PIN must be chosen carefully to ensure that they are not easily guessed. In particular, PINs must not be prominent dates or phone numbers.

In some cases, your e-Cert issuer may need to personalise your card so that it only works with a PIN you know. You must take care of this PIN to ensure that no one else knows it. Once you receive your card, you should change the PIN as soon as possible to one that is difficult to guess, but you can easily remember.

It is extremely important you keep your PIN **secret**. PINs must be protected! If you must write down your PIN (which is not recommended), keep your PIN and your smart card separate at all times (**never** write your PIN on a smart card). Take care when entering your PIN to avoid the possibility someone might study the keys you type. Your PIN must be entered only into PIN prompt generated by e-Cert Control Manager.

If you entered your PIN into a program and then found that e-Cert Control Manager has not serviced the request or it started a PIN dialog box, the program may have compromised your PIN. Change your PIN immediately through the e-Cert Control Manager. Similarly, when e-Cert Control Manager is accessed through a program, and you enter your PIN in what appears to be a e-Cert Control Manager PIN dialog box, the request should be processed. If this doesn't happen, your PIN may have been compromised. Change your PIN immediately through the e-Cert Control Manager.

Each time e-Cert Control Manager displays a window for you to enter a PIN, the number of retries remaining is also displayed. It is important that this number accurately reflects the number of times you entered an incorrect PIN. Each time you enter a correct PIN, this value is reset to its maximum and each incorrect PIN decrements it. If this value is not consistent with your PIN attempts, then someone (or some application) is attempting to guess your PIN

over time. You should ensure that the smart card is not accessible by others and that there are no malicious applications running on your computer.

Over time, PINs 'age' and it becomes more and more likely that someone other than the PIN owner knows the PIN. PINs **must** be changed regularly—every three months at a minimum. Additionally, you must change your PIN any time you suspect that someone tried to guess your PIN (indicated if the displayed retry count is inconsistent).

Care for your sensitive data

e-Cert Control Manager must be installed on your machine in such a manner that other people cannot interfere with your use of the product, however no software is secure from tampering by users authorised to do so. The secure operation of e-Cert Control Manager requires that you can trust anyone with privileges to start processes on your machine, or with privileges to modify e-Cert Control Manager or security-critical operating system files.

When placed under its control, e-Cert Control Manager affords your data full protection. Protecting sensitive data requires the applications and computers that run e-Cert Control Manager provide your data the same level of security. Your computer must protect files decrypted with e-Cert Control Manager so that other people do not gain unauthorised access to them. This same care must be extended to any data that is to be encrypted, and any other data that you desire to be confidential.

The digital signature function of e-Cert Control Manager authenticates you to other parties. Your computer environment must be able to control communications with external parties so that it reflects your intentions. Digital signatures are used with Transport Layer Security (also known as the Secure Sockets Layer or SSL) to authenticate session keys so that the other party can be sure that only you can communicate with it. Your computer has to protect your confidential data, and prevent unauthorised messages being sent.

You must only use e-Cert Control Manager with applications that you trust so that the applications will not decrypt or sign data without your authorisation. When storing data that is encrypted with keys protected by e-Cert Control Manager, you need to consider the future availability of keys on your smart card. The loss of any keys results in encrypted data being rendered unrecoverable. Keys are lost if the card is lost, or the PIN that protects the keys is irrevocably blocked. If a secure storage medium exists, a copy of the unencrypted data can be archived, otherwise you may wish to consider key recovery tools that generate and backup cryptographic keys. Extreme care is required to ensure that keys are not compromised as they are transported from the key recovery tool to e-Cert Control Manager via a PKCS#12 file.

Disposing of your smart card

Before disposing of your smart card, you should delete all the keys on the card (see *Deleting key pairs* on page 23). This ensures that the cryptographic data is not available to anyone who gains possession of the card and attempts

to reverse engineer the card's protection mechanism. This is especially important as, in the future, it might be more likely that an attacker can recover data from smart cards than it is today.

If you cannot delete all your keys, you should contact Hongkong Post to delete the e-Cert application on your smart card.

CHAPTER 7

TROUBLESHOOTING

This chapter describes the errors that can occur when using e-Cert Control Manager, the possible causes, and the steps you can take to remedy the cause of the error.

Smart card reader errors

Reader timeout

Cause: The reader timeout error occurs when your smart card reader no longer responds to regular messages from e-Cert Control Manager. The error can occur as a result of a technical or hardware failure with the smart card reader, or an internal error with Windows.

Remedy: Restart Windows. If the timeout recurs, contact the supplier of your smart card reader.

Reader port error

Cause: A reader port error occurs when the port the smart card reader connected to is configured incorrectly. This may result from two smart card reader drivers attempting to access the same port.

Remedy: Remove or uninstall all the smart card reader driver software you have installed on your system, and install only the current driver for your smart card reader.

Reader read error

Cause: A reader read error occurs when the data received from the smart card reader is corrupt or incomplete. This error can occur as a result of a technical failure with the smart card reader, or a faulty connection between the computer and the smart card reader.

Remedy: Restart Windows and check the connection between the computer and the smart card reader. If the error recurs, contact the smart card reader supplier.

Reader write error

Cause: A reader write error has similar causes to a **reader read error** and usually occurs when data cannot be written to the smart card reader. This error can occur as a result of a technical failure with the smart card reader, the computer, or a faulty connection between the computer and the smart card reader.

Remedy: Restart Windows and check the connection between the computer and the smart card reader. If the error recurs, contact the smart card reader supplier.

Reader failure

Cause: A reader failure error indicates an unspecified problem with the smart card reader. This error occurs when e-Cert Control Manager encountered an error with the smart card reader but could not determine what the cause might be.

Remedy: The usual cause of a reader failure is the smart card reader hardware. Restart Windows and, if the error recurs, contact the smart card reader supplier.

Card security errors

PIN invalid

Cause: A PIN presented to unlock the card is not the correct PIN. This error decreases the *retry count*. If the PIN retry count reaches zero, the card is blocked.

Remedy: Double-check your PIN before attempting to unlock your smart card again.

PIN blocked

Cause: A smart card PIN is blocked when the wrong PIN is entered a certain number of times (the *retry* count). This could be a result of a brute-force attack on the PIN.

Remedy: The smart card can only be unblocked by contacting Hongkong Post.

PIN length

Cause: The length of the PIN provided is either longer than the maximum allowed, or shorter than the minimum allowed. PIN length is checked when you change PIN.

Remedy: Ensure the number of characters in the PIN falls within the allowed range.

PIN weak

Cause: A PIN is considered easily guessed. Weak PINs include sequential (e.g. '123456') or repeated numbers (e.g. '222222').

Remedy: Revise your PIN so it is stronger against a guessing attack.

Card application errors

Command not supported

Cause: The e-Cert Control Manager software is attempting to execute a function that is not supported by the smart card.

Remedy: Ensure you have the correct smart card inserted in the smart card reader. If you have the correct smart card inserted, the smart card has limited capabilities and cannot execute the function.

Command not permitted

Cause: The security permissions on the card do not permit the execution of the command you have requested.

Remedy: You cannot circumvent the security permissions on the smart card.

Card not present

Cause: A smart card is not present in the smart card reader, or the smart card was removed from the reader when an operation was in progress.

Remedy: Insert, or re-insert, a smart card.

Card full

Cause: There is insufficient free space on the card to permit the function you have requested.

Remedy: Deleting unused or unwanted items (such as certificates that are no longer needed) from the smart card will create more room.

Key store errors

Token exists

Cause: You are attempting to load a certificate or key pair onto a card, where one with the same identity already exists.

Remedy: Either cancel the operation (you already have the token on the card), or delete the existing token and re-load the certificate or key pair.

Token does not exist

Cause: You are attempting to access a certificate or key pair that does not exist on the smart card.

Remedy: Check the right smart card is in the reader, or remove and re-insert the smart card and try the operation again.

Token locked

Cause: You are attempting to access a certificate or key pair which is locked by a PIN.

Remedy: To access the token, present the e-Cert PIN.

Key pair does not exist

Cause: You are attempting to load a certificate onto the smart card for which a key pair does not already exist.

Remedy: Load the certificate's corresponding key pair before attempting to load the certificate.

Invalid file format

Cause: You are attempting to load a file to a smart card, such as a certificate or encrypted key pair, and the file format is not recognised. The file may be corrupted or an attempt made to tamper with the file.

Remedy: Double-check the file you are attempting to load and try the operation again. If the problem recurs, contact Hongkong Post.