以香港邮政署长
根据电子交易条例作为认可核证机关

之

香港邮政
电子证书（个人）
电子证书（机构）
电子证书（保密）
电子证书（服务器）

核证作业准则

Linking people Delivering business
傳心意 遞商機

日期 :二零零四年八月二十日
对象识别码：1.3.6.1.4.1.16030.1.1.5

目录

(1.0.1)

©本文版权属香港邮政署长所有。未经香港邮政署长明确许可，不得复制本文之全部或部分。

前言

香港法例第 553 章电子交易条例（“条例”）列载公开密码匙基础建设（公匙基建）之法律架构。公匙基建利便电子交易作商业及其它用途。公匙基建由多个元素组成，包括法律责任、政策、硬件、软件、数据库、网络及保安程序。

公匙密码技术涉及运用一条私人密码匙及一条公开密码匙。公开密码匙及其配对私人密码匙在运算上有关连。电子交易运用公匙密码技术之主要原理为：经公开密码匙加密之信息只可用其配对私人密码匙解密；和经私人密码匙加密之信息亦只可用其配对公开密码匙解密。

设计公匙基建之目的，为支持以上述方式在香港特别行政区进行商业活动及其它交易。

根据条例所载规定，就条例及公匙基建而言，香港邮政署长为认可核证机关。根据条例，香港邮政署长可透过香港邮政署职员履行核证机关之职能并提供服务。香港邮政署长已决定履行其职能，而就此文件而言，其身分为**香港邮政**。

根据条例，香港邮政为认可核证机关，负责使用稳当系统发出、暂时吊销或撤销及利用公开储存库公布已认可及已接受之数码证书作为在网上进行稳妥的身分辨识。根据本核证作业准则发出的电子证书（个人）、电子证书（机构）、电子证书（保密）及电子证书（服务器），在本核证作业准则内称为“证书”或“电子证书”。

香港邮政发出可加载智能身份证内的个人电子证书。另外，在香港邮政及登记人的同意下，个人电子证书亦可加载其它存储介质，如软磁盘、智能卡等。

根据条例，香港邮政可以采取任何合宜举措以履行核证机关职能及提供核证机关服务。而根据政府信息科技总监颁布之认可核证机关作业守则，香港邮政可以指定代理人或分包商进行其若干或所有作业。

香港邮政可合宜地指定若干机构为代理人，履行香港邮政作为认可核证机关之若干职能。在本核证作业准则中，该等机构称为核证登记机关，核证登记机关的职能已列载于本核证作业准则中。**附录 E** 列载核证登记机关之清单。香港邮政对其代理人即核证登记机关履行香港邮政作为认可核证机关有关签发及撤销电子证书之职能或提供服务的行为负责。

本核证作业准则之结构如下：

第 1 条载有概述及联络资料
第 2 条列载各方责任及义务
第 3 条列载申请及身分确认程序
第 4 条载述运作要求
第 5 条介绍保安监控措施
第 6 条列载如何产生及监管公开/私人配对密码匙
第 7 条简介技术要求
第 8 条叙述如何管理本核证作业准则

1. 引言

1.1 概述

本核证作业准则（“准则”）由香港邮政公布，使公众有所了解，并规定香港邮政在发出、暂时吊销或撤销及公布电子证书时采用之做法及标准。

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.5」为本准则的对象识别码 (Object Identifier, OID) （见**附录 B** 内关于核证政策(Certificate Policies)的说明）。

本准则列载参与香港邮政所用系统之人士之角色、职能、义务及潜在责任。本准则列出核实证书（即根据本作业准则发出的证书）申请人身分的程序，并介绍香港邮政之运作、程序及保安要求。

香港邮政根据本准则发出之证书将得到倚据证书人士之倚据并用来核实数码签署。利用由香港邮政发出之证书之各倚据证书人士须独立确认基于公匙基建之数码签署乃属适当及充分可信，可用来认证各倚据证书人士之特定公匙基建应用程序上之参与者之身分。

根据条例，香港邮政为认可核证机关。而根据本核证作业准则而发出的电子证书（个人）、电子证书（机构）、电子证书（保密）及电子证书（服务器），香港邮政已指明为认可证书。对登记人及倚据证书人士而言，根据该条例香港邮政在法律上有义务使用稳当系统，发出、暂时吊销或撤销及在可供公众使用之储存库公布获接受之认可证书。认可证书的内容不但准确，并根据条例载有法例界定之事实陈述，包括陈述此等证书为按照本准则发出者（下文详述其定义）。香港邮政已指定核证登记机关为其代理人之事实并无减轻香港邮政使用稳当系统之义务，亦无变更电子证书作为获认可证书具有之特性。

附录 D 载有根据本准则发出之电子证书特点摘要。

1.2 社区及适用性

1.2.1 核证机关

根据本准则，香港邮政履行核证机关之职能并承担其义务。香港邮政乃唯一根据本准则授权发出证书之核证机关（见第 2.1.1 条）。

1.2.1.1 香港邮政所作之陈述

根据本准则而发出之证书，香港邮政向根据本准则第 2.1.5 条及其它有关章条之倚据证书人士表明，香港邮政已根据本准则发出证书。透过公布本准则所述之证书，香港邮政即向根据本准则第 2.1.5 条及其它有关章条之倚据证书人士表明，香港邮政已根据本准则发出证书予其中已辨识之登记人。

1.2.1.2 生效

经香港邮政签署之证书一经发出并由登记人接受，香港邮政将迅速于储存库公布已发出之证书。（见第 2.5 条）

1.2.1.3 香港邮政进行分包合约之权利

只要分包商同意与香港邮政签订合约承担有关职务，香港邮政可把履行本准则及登记人协议之部分或全部工作之义务，批予分包商执行。无论有关职务是否批出由分包商执行，香港邮政仍会负责履行本准则及登记人协议。

1.2.2 最终实体

根据本核证作业准则，存在两类最终实体，包括登记人及倚据证书人士。登记人指于附录 A 内所指的”登记人”或”登记人机构”。倚据证书人士乃倚据香港邮政发出之任何类别或种类证书（包括但不限于电子证书）以用于交易之实体。特此澄清，**倚据证书人士不应倚据核证登记机关。香港邮政透过其代理人核证登记机关发出电子证书，而核证登记机关对倚据证书人士并无任何谨慎职责，亦不需对倚据证书人士就发出电子证书而负责**（见第 2.1.2 条）。于交易中依据其它登记人之电子证书之申请人及登记人乃为有关此证书之倚据证书人士。**请倚据证书人士留意，香港邮政电子证书系统并无年龄限制，未成年人仕可申请并领取电子证书。**

1.2.2.1 登记人之保证及陈述

各申请人（如申请电子证书（机构）、电子证书（保密）及电子证书（服务器），获授权代表会代表申请人）须签署或确定接受一份协议（按本准则规定之条款），其中载有一条款，申请人据此条款同意，申请人一经接受根据本准则发出之证书，即表示其向香港邮政保证（承诺）并向所有其它有关人士（尤其是倚据证书人士）作出陈述，在证书之有效期间，以下事实乃属真实并将保持真实：

a) 除电子证书（个人）及电子证书（服务器）登记人、电子证书（机构）的获授权用户及电子证书（保密）的获授权单位外，并无其它人士曾取用登记人之私人密码匙；
b) 使用与登记人电子证书所载之公开密码匙相关之登记人私人密码匙所产生之每一数码签署实属登记人之数码签署。
c) 电子证书（保密）将只会用于第 1.2.3.4 条指明的用途。
d) 证书所载之所有资料及由登记人作出之陈述均属真实。
e) 证书将只会用于符合准则之认可及合法用途。
f) 在证书申请过程中所提供之所有资料，均并无侵犯或违反任何第三方之商标、服务标记、品牌、公司名称或任何知识产权。

1.2.3 登记人之类别

根据本准则香港邮政仅发出证书予其申请已获香港邮政批准并已以适当形式签署或确定接受登记人协议之申请人士。四类电子证书会根据本准则而发出：

1.2.3.1 电子证书（个人）

根据本准则和登记人协议，电子证书（个人）会发出予持有香港身份证人仕。此等证书可用来从事商业经营。电子证书（个人）可发出予持有香港身份证之十八岁以下人士（另见第 3.1.1.2 条）。

1.2.3.2 电子证书（机构）

电子证书（机构）发给香港特别行政区政府各政策局及部门、获香港特别行政区政府签发有效商业登记证之机构以及获香港法例认可存在之本港法定团体（即「登记人机构」），并识别已获该登记人机构授权使用该电子证书（机构）私人密码匙的成员或雇员（即「获授权用户」）。此等证书与电子证书（个人）之用途大致相同。

1.2.3.3 电子证书（服务器）

电子证书（服务器）发给香港特别行政区政府各政策局及部门、获香港特别行政区政府签发有效商业登记证之机构以及获香港法例认可存在之本港法定团体（即「登记人机构」），并拟持有以该机构所拥有服务器名称发出之证书。

1.2.3.4 电子证书（保密）

电子证书（保密）发给香港特别行政区政府各政策局及部门、获香港特别行政区政府签发有效商业登记证之机构以及获香港法例认可存在之本港法定团体（即「登记人机构」），并拟供已获登记人机构授权使用电子证书（保密）私人密码匙之机构单位（"获授权单位"）使用。

此类证书只可用作：

i) 传送加密之电子信息予登记人机构；

ii) 容许登记人机构为信息解密；及

iii) 容许登记人机构发出认收信息并附加其数码签署以证实其登记人机构收件身分，藉此确认已收讫送出之加密信息。

登记人机构向香港邮政承诺，不会授权予获授权单位使用此类证书之数码签署作其它用途。由此，利用此类证书私人密码匙产生之数码签署如作为上文所述认收信息以外的用途，必须视为未经授权许可产生之签署，此签署亦必须视作未经授权之签署。

此外，此类证书产生之数码签署只可用作认收电子信息，并只可用于与联机付款或联机投资无关或不相连或不会联机为任何人士或实体带来任何性质之财务利益之交易。不论任何情况，此等证书产生之数码签署均不得用作认收与洽商或订定合约或任何具法律效力之协议有关而传送之电子信息。

1.2.4 证书之期限

根据本核证作业准则发出予新申请人之证书，其有效期如下：

证书类别	在证书内指明的有效期
电子证书（个人）	三年
电子证书（机构）	一年或二年（申请人可于申请时选择）
电子证书（服务器）	
电子证书（保密）	

根据本核证作业准则之证书续期程序而发出之证书有效期可超过上述之有效期(见第 3.2.2 及 3.3 条)。电子证书内会注明其有效期。根据本准则发出之证书格式列于附录 B。

1.2.5 在香港邮政处所进行申请

所有首次申请及证书撤销或到期后之申请，申请人须依据第 3 及 4 条指明的程序递交申请。

1.3 联络资料

登记人可经由以下途径作出查询、建议或投诉：

邮寄地址：东九龙邮政信箱 68777 号香港邮政核证机关
电话 ： 2921 6633　　传真 ： 2775 9130
电邮地址 ： enquiry@hongkongpost.gov.hk

1.4 处理投诉程序

香港邮政会尽快处理所有以书面及口头作出的投诉，并在十天内给予详细的答复。若十天内不能给予详细的答复，香港邮政会向投诉人作出简覆。在可行范围内，香港邮政人员会于收到投诉后尽快以电话、电邮或信件与投诉人联络确认收到有关投诉及作出回复。

2. 一般规定

2.1 义务

香港邮政对登记人之义务乃由本准则及与登记人以登记人协议形式达成之合约之条款进行定义及限制。无论登记人是否亦为有关其它登记人证书之倚据证书人士，均须如此。关于非登记人倚据证书人士，本准则知会该等人士，香港邮政仅承诺采取合理技术及谨慎以避免在根据条例及准则发出、暂时吊销或撤销、及公布证书时对倚据证书人士造成若干类型之损失及损害，并就下文及所发出之证书所载之责任限定币值。

2.1.1 核证机关之义务

根据条例，香港邮政为认可核证机关，负责使用稳当系统发出、暂时吊销或撤销、及利用公开储存库公布已获登记人接受之认可证书。根据本准则，香港邮政有下述义务：

a) 依时发出及公布证书（见第 2.5 条），
b) 通知申请人有关已批准或被拒绝的申请（见第 4.1、4.2、4.3 及 4.4 条），
c) 暂时吊销或撤销证书及依时公布证书撤销清单（见第 4.5 条），
d) 通知登记人有关已暂时吊销或撤销的证书（见第 4.5.1., 4.5.2. 及 4.5.3 条），

2.1.2 核证登记机关之义务及责任

核证登记机关仅遵照与香港邮政就获其指定为代理人，代表其履行本准则详述之若干义务而订立之合约(代理人合约)之条款对香港邮政负责。核证登记机关代表香港邮政收集及保留根据本准则及登记人协议之条款所提供之文件及资料。香港邮政须由始至终对其核证登记机关所执行或其本意是执行香港邮政的功能、权力、权利和职责负责。

核证登记机关不为任何登记人协议之签约方，亦不就发出、暂时吊销或撤销或公布电子证书，或就收集及保留文件或资料对登记人或倚据证书人士承担任何谨慎职责。核证登记机关之行为仅为代表香港邮政履行香港邮政于此等事项之义务及责任。核证登记机关有权代表香港邮政实施登记人协议之条款（除非及直至该机关被撤销及登记人正式获通知任何该等撤销）。在任何情况下，核证登记机关不须就登记人协议或核证登记机关代表香港邮政作为认可核证机关发出之证书对登记人或倚据证书人士承担任何责任。

2.1.3 登记人之义务

登记人负责：

a) 同意香港邮政，在其处所内使用稳当的系统，在安全的环境下代表登记人制作配对密码匙。
b) 适当完成申请程序并在适当表格内签署或确定接受登记人协议（如申请电子证书（机构）、电子证书（保密）及电子证书（服务器），则由获授权代表完成）；履行该协议规定其应承担之义务及确保在申请证书时所作的陈述准确无误。
c) 准确地按照本准则所载关于完成证书之程序。
d) 承认承诺使用合理预防措施来保护其证书私人密码匙之机密性（即对其保密）及完整性以防丢失、泄露或未经授权使用之义务。
e) 发现其证书的私人密码匙之任何丢失或外泄时，立即呈报丢失或外泄（外泄乃属违反保安，使资料遭受未经授权之进入，从而导致未经授权即对资料进行披露、更改或使用）。
f) 不时将登记人提供之证书资料之任何变动立即通知予香港邮政。
g) 将可能致使香港邮政根据下文第 4 条所载之理由行使权利，撤销由该登记人负责之证书之任何事项立即通知予香港邮政。

h) 同意其透过获发出或接受证书向香港邮政保证（承诺）并向所有倚据证书人士表明，在证书之有效期间，以上第 1.2.2.1 条载明之事实乃属真实并将一直保持真实。
i) 在登记人明知香港邮政根据准则条款可能据以暂时吊销或撤销证书之任何事项之情况下，或登记人已作出撤销申请或经香港邮政知会，香港邮政拟根据本准则之条款暂时吊销或撤销证书后，均不得在交易中使用证书。
j) 在明知香港邮政可能据以暂时吊销或撤销证书之任何事项之情况下，或登记人作出撤销申请或经香港邮政知会拟暂时吊销或撤销证书时，须立即通知从事当时仍有待完成之任何交易之倚据证书人士，用于该交易之证书须予暂时吊销或撤销(由香港邮政或经登记人申请)，并明确说明，因情形乃属如此，故倚据证书人士不得就交易而倚据证书。

如电子证书（个人）登记人的智能身份证已遗失、损毁、污损或损坏，或已向入境事务处或其它执法机关退回其智能身份证，或其智能身份证已被入境事务处或其它执法机关根据香港特别行政区法例终止有效或扣押，登记人亦负责同意放弃使用任何载于该智能身份证内的私人密码匙。登记人亦同意香港邮政，及香港特别行政区政府，在此等事宜上对申请人或登记人并不负有任何责任。申请人/登记人可根据第 4.5.2 条说明的程序，要求香港邮政撤销载于智能身份证内的电子证书

电子证书（保密）登记人亦负责确保：

- 获授权使用者只获登记人机构授权使用证书以及有关之数码签署，以解密并认收对方送来加密之电子信息，不得作其它用途；
- 此等证书只可用以(i)向登记人传送加密电子信息，(ii)容许登记人机构为信息解密，以及(iii)容许登记人机构发出认收信息并附加其数码签署以证实其登记人机构收件身分，藉此确认送出之加密信息已经收讫；
- 不会试图使用电子证书（保密）的私人密码匙以产生数码签署并用作认收信息以外用途；及
- 获授权使用者采取合理预防措施以维护私人密码匙之安全。

2.1.4 登记人之责任

各登记人承认，若上述义务未得以履行，则根据登记人协议及/或法例，各登记人有或可能有责任向香港邮政及/或其它人士(包括倚据证书人士)就可能因此产生之责任或损失及损害赔偿损失。

2.1.5 倚据证书人士之义务

倚据香港邮政电子证书之倚据证书人士负责：

a) 倚据证书人士于依赖证书时如考虑过所有因素后确信倚据证书实属合理，方可依赖该等证书。
b) 于倚据该等证书前，确定使用证书乃适合本准则规定之用途，而核证登记机关(见**附录 E**)并不对倚据证书人士承担任何谨慎职责。
c) 于倚据证书前查核证书撤销清单上之证书状态。
d) 执行所有适当证书路径认可程序。

2.2 其它规定

香港邮政对登记人及倚据证书人士之义务

2.2.1 合理技术及谨慎

香港邮政谨此与各登记人协议，根据本准则香港邮政或代表香港邮政之核证登记机关向各登记人及倚据证书人士履行及行使作为核证机关所具之义务和权利时，采取合理程度之技术及谨慎。香港邮政不向登记人或倚据证书人士承担任何绝对义务。**香港邮政不保证香港邮政或代表香港邮政之核证登记机关根据本准则提供之服务不中断或无错误或比香港邮政、其职员、雇员或代理人行使合理程度之技术及谨慎执行本准则时应当取得之标准更高或不同。**

换言之，尽管香港邮政或代表香港邮政之核证登记机关于执行本合约及其根据准则行使应有之权利及义务时采取合理程度之技术及谨慎，若登记人作为准则定义下之登记人或倚据证书人士而遭受出自准则中描述之公开密码匙基础建设或与之相关任何性质之债务、损失或损害，包括随后对另外一登记人证书之合理倚据而产生之损失或损害，各登记人同意香港邮政及任何核证登记机关无需承担任何责任、损失或损害。

即如香港邮政或代表香港邮政之核证登记机关已采取合理程度之技术及谨慎之前提下，若登记人因倚据另一登记人由香港邮政所发出之认可证书支持之虚假或伪造之数码签署而蒙受损失或损害，香港邮政、邮政署或代表香港邮政之核证登记机关概不负责。

亦即如在香港邮政（邮政署或代表香港邮政之核证登记机关）已采取合理程度之技术或谨慎以避免及/或减轻无法控制事件后果之前提下，若登记人因香港邮政不能控制之情况遭受不良影响，香港邮政、邮政署或任何核证登记机关概不负责。香港邮政控制以外之情况包括但不限于互联网或电讯或其它基础建设系统之可供使用情况，或天灾、战争、军事行动、国家紧急状态、疫症、火灾、水灾、地震、罢工或暴乱或其它登记人或其它第三者之疏忽或蓄意不当行为。

2.2.2 非商品供应

特此澄清，登记人协议并非任何性质商品之供应合约。任何及所有据此发出之证书持续为香港邮政之财产及为其拥有且受其控制，证书中之权利、所有权或利益不得转让于登记人，登记人仅有权根据该登记人协议之条款倚据此证书及其它登记人之证书。因此，该登记人协议不包括（或不会包括）明示或暗示关于证书为某一特定目的之可商售性或适用性或其它适合于商品供应合约之条款或保证。同样地，香港邮政在可供倚据证书人士接达之公开储存库内提供之证书，并非作为对倚据证书人士供应任何商品；亦不会作为对倚据证书人士关于证书为某一特定目的之可商售性或适用性的保证；亦不会作为向倚据证书人士作出供货商品的陈述或保证。香港邮政虽同意将上述物品转让予申请人或登记人作本准则指定用途；但亦合理谨慎确保此等物品适合作本准则所述完成及接受证书之用途。若未能履行承诺，香港邮政须承担下文第 2.2.3 及 2.2.4 条所述责任。另外，由香港邮政转让的物品可内载其它与完成及接受电子证书无关之资料。若确实如此，与此等资料有关之法律观点并非由核证作业准则或登记人协议规管，而须由电物品内另行载述之条文决定。

2.2.3 法律责任限制

2.2.3.1 限制之合理性

各登记人或倚据证书人士必须同意，香港邮政按本登记人协议及准则所列条件限制其法律责任实属合理。

2.2.3.2 可追讨损失种类之限制

在香港邮政违反：

a) 本登记人协议；或
b) 任何谨慎职责－尤其当登记人或倚据证书人士、或其它人、或以其它任何方式，倚据或使用香港邮政根据公开密码匙基础建设而发出之任何证书时－应根据登记人协议，为登记人或倚据证书人士，而采取合理技巧及谨慎及/或职责

的情况下，而登记人或倚据证书人士（无论作为根据准则或以其它任何方式定义之登记人或倚据证书人士）蒙受损失及损害，**香港邮政概不负责关乎下述原因之赔偿或其它补救措施：**

a) 任何直接或间接利润或收入损失、信誉或商誉损失或伤害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；或

b) 任何间接、相应而生或附带引起之损失或损害，而且即使在后者情况下，香港邮政已获提前通知此类损失或损害之可能性。

2.2.3.3 限额 -- 20 万港元

除下文所述例外情况外，在香港邮政违反：

a) 本登记人协议；或
b) 任何谨慎职责－尤其当登记人或倚据证书人士、或其它人士、或以其它任何方式倚据或使用香港邮政根据公开密码匙基础建设而发出之任何证书时－应根据登记人协议、本准则、或法例，为登记人或倚据证书人士，采取合理技巧或谨慎及/或职责

之情况下，而登记人或倚据证书人士蒙受损失及损害（无论作为根据准则或以其它任何方式定义之登记人或倚据证书人士），对于任何登记人、或任何倚据证书人士（无论作为根据准则或以其它任何方式定义之登记人或倚据证书人士或以任何其它身分），香港邮政所负法律责任限制于且任何情况下每份电子证书（个人）、电子证书（机构）、电子证书（服务器）或电子证书（保密）不得超过 20 万港元、或每份发出予未满 18 岁人仕的电子证书（个人）0（零）港元。

2.2.3.4 提出索偿之时限

任何登记人或倚据证书人士如欲向香港邮政提出索偿，且该索偿源起于或以任何方式与发出、暂时吊销、撤销或公布任何证书相关，则应在登记人或倚据证书人士察觉其有权提出此等索偿的事实之日起一年内、或透过行使合理努力其有可能清楚此等事实之日起一年内（若更早）提出。特此澄清，不知晓此等事实之法律重要性乃无关重要。一年期限届满时，此等索偿必须放弃且绝对禁止。

2.2.3.5 香港邮政署、核证登记机关及各自之人员

无论香港邮政署或任何核证登记机关或其各自之任何职员、雇员或其它代理人均非登记人协议之签约人，登记人及倚据证书人士必须向香港邮政承认，就登记人及倚据证书人士所知，香港邮政署或任何核证登记机关之任何职员、雇员或代理人（就任何出于真诚、并与香港邮政履行本登记人协议或由香港邮政作为核证机关发出之任何证书相关，而作出的行动或遗漏事项）均不会自愿接受或均不会接受向登记人、或倚据证书人士担负任

何个人责任或谨慎职责；每一位登记人及倚据证书人士接受并将继续接受此点，并向香港邮政保证不起诉或透过任何其它法律途径对前述任何关于该人出于真诚（不论是否出于疏忽）、并与香港邮政履行本登记人协议或由香港邮政作为核证机关发出之任何证书相关，而作出的行动或遗漏事项寻求任何形式之追讨或纠正，并承认香港邮政享有充分法律及经济利益以保护香港邮政署及上述机构及个人免受此等法律行动。

2.2.3.6 蓄意之不当行为或个人伤亡之责任

任何因欺诈或蓄意之不当行为或个人伤亡之责任均不在本准则、登记人协议或香港邮政发出之证书之任何限制或除外规定范围内，亦不受任何此等规定之限制或被任何此等规定免除。

2.2.3.7 证书通知、限制及倚据限额

香港邮政发出之证书须被认作已包括下列倚据限额及／或法律责任限制通知：

> *“香港邮政署职员按香港邮政署长之核证作业准则所载条款及条件适用于本证书之情况下，根据电子交易条例作为认可核证机关发出本证书。*
>
> *因此，任何人士倚据本证书前均应阅读适用于电子证书的准则（可浏览 http://www.hongkongpost.gov.hk）。香港特别行政区法律适用于本证书，倚据证书人士须提交因倚据本证书而引致之任何争议或问题予香港特别行政区法庭之非专有司法管辖权。*
>
> *倘阁下为倚据证书人士而不接受本证书据以发出之条款及条件，则不应倚据本证书。*
>
> *香港邮政署长（经香港邮政署，其职员、雇员及代理人）发出本证书，但无须对倚据证书人士承担任何责任或谨慎职责（准则中列明者除外）。*
>
> *倚据证书人士倚据本证书前负责：*
>
> a. *只有当倚据证书人士于倚据时所知之所有情况证明倚据行为乃属合理及本着真诚时，方可倚据本证书；*
> b. *倚据本证书前，确定证书之使用就准则规定之用途而言乃属适当；*
> c. *倚据本证书前，根据证书撤销清单检查本证书之状态；及*
> d. *履行所有适当证书路径认可程序。*
>
> *若尽管香港邮政署长及香港邮政署、其职员、雇员或代理人已采取合理技术及谨慎，本证书仍在任何方面不准确或误导，则香港邮政署长、香港邮政署、其职员、雇员或代理人对倚据证书人士之任何损失或损害概不承担任何责任，在该等情况下根据条例适用于本证书之倚据限额为 0 港元。*
>
> *若本证书在任何方面不准确或误导，而该等不准确或误导乃因香港邮政署长、香港邮政署、其职员、雇员或代理人之疏忽所导致，则香港邮政署长将就因合理倚据本证书中之该等不准确或误导事项而造成之经证实损失向每名倚据证书人士支付最多 20 万港元、或支付最多 0（零）港元（如该证书为发出予未满 18 岁人仕的电子证书（个人）），惟该等损失不属于及不包括（1）任何直接或间接利润或收入损失、信誉或商誉损失或伤害、任何商机或契机、失去工程或失去或无法使用任何数据、设备或软件或（2）任何间接、相应而生或附带引起之损失或损*

害，而且即使在后者情况下，香港邮政已被提前通知此类损失或损害之可能性。在该等情况下根据条例适用于本证书之倚据限额为 20 万港元、或 0（零）港元（如该证书为发出予未满 18 岁人仕的电子证书（个人）），而在所有情形下就第（1）及（2）类损失而言倚据限额则为 0 港元。

在任何情况下，香港邮政署、其职员、雇员或代理人概不对倚据证书人士就本证书承担任何谨慎职责。

索赔时限
任何倚据证书人士如拟向香港邮政署长索赔，且该索偿源起于或以任何方式与发出、暂时吊销、撤销或公布任何证书相关，则应在倚据证书人士知悉存在任何有权提出此等索偿事实之日起一年内或透过行使合理努力彼等有可能知悉此等事实之日起一年内（若更早）提出。特此澄清，不知晓此等事实之法律重要性乃无关重要。一年期限届满时，此等索偿必须放弃且绝对禁止。

倘本证书包含任何由香港邮政署长、香港邮政署、其职员、雇员或代理人作出之故意或罔顾后果之失实陈述，则本证书并不就彼等对因合理倚据本证书中之失实陈述而遭受损失之倚据证书人士所应承担之法律责任作出任何限制。

本文所载之法律责任限制不适用于个人伤害或死亡之(不大可能发生之)情形。”

2.2.4 香港邮政对已获接受但有缺陷之电子证书所承担之责任

2.2.4.1 尽管上文已列明香港邮政承担责任之限制，若登记人接受证书后发现，因证书内之私人密码匙或公开密码匙出现差错，导致基于公匙基建预期之交易无法适当完成或根本无法完成，则登记人须将此情况立即通知香港邮政，以便撤销证书（如愿意接受）重新发出。或倘此通知已于接受证书后三个月内发出且登记人不再需要证书，则香港邮政若同意确有此差错将进行退款。倘登记人于接受证书三个月过后方将此类差错通知香港邮政，则费用不会自动退还，而需由香港邮政酌情退回。

2.2.5 登记人的转让
登记人不可转让登记人协议或证书赋予之权利。拟转让之行为均属无效。

2.2.6 陈述权限
除非获得香港邮政授权，香港邮政署或任何核证登记机关之代理人或雇员无权代表香港邮政对本准则之意义或解释作任何陈述。

2.2.7 更改
香港邮政有权更改本准则，而无须发出预先通知(见第 8 条)。登记人协议不得作出更改、修改或变更，除非符合本准则中之更改或变更规定，或获得香港邮政署长之明确书面同意。

2.2.8 保留所有权
根据本准则发出之证书上所有资料之实质权利、版权及知识产权现属香港邮政所有，日后亦然。

2.2.9 条款冲突
倘本准则与登记人协议或其它规则、指引或合约有冲突，登记人、倚据证书人士及香港邮政须受本准则条款约束，除非该等条款受法律禁止。

2.2.10 受信关系
香港邮政或代表香港邮政之任何核证登记机关并非登记人或倚据证书人士之代理人、受信人、受托人或其它代表。登记人及倚据证书人士无权以合约或其它方式约束香港邮政或代表香港邮政之任何核证登记机关承担登记人或倚据证书人士之代理人、受信人、受托人或其它代表之责任。

2.2.11 相互核证
香港邮政在所有情形下均保留与另一家核证机关定义及确定适当理由进行相互核证之权利。

2.2.12 财务责任
保单已经备妥，有关证书之潜在或实质责任以及对倚据限额之索偿均获承保。

2.3 解释及执行（管辖法律）

2.3.1 管辖法律
本准则受香港特别行政区法律规管。登记人及倚据证书人士同意受香港特别行政区法庭之非专有司法管辖权囿制。

2.3.2 可中止性、尚存、合并及通知
若本准则之任何条款被宣布或认为非法、不可执行或无效，则应删除其中任何冒犯性词语，直至该等条款成为合法及可执行为止，同时应保留该等条款之本意。本准则之任何条款之不可执行性将不损害任何其它条款之可执行性。

2.3.3 争议解决程序
香港邮政关于本准则范围内之事宜之决定为最终决定。如有索偿，请送交下列地址：

东九龙邮政信箱 68777 号香港邮政核证机关
电邮地址 ： enquiry@hongkongpost.gov.hk

2.3.4 诠释
本准则中英文本措词诠释若有歧异，则以英文本为准。

2.4 登记费用

2.4.1 电子证书（个人）
每份电子证书（个人）（包括首次及续期申请）年费为 50 港元。

2.4.2 电子证书（机构）

电子证书（机构）收费	一年有效期的电子证书	二年有效期的电子证书

首次申请	每份电子证书港币 50 元	每份电子证书港币 200 元
非首次申请或续期	每份电子证书港币 150 元	每份电子证书港币 300 元
行政费 （不论获授权用户数目多少）	每份申请港币 150 元	每份申请港币 300 元
	如申请表内包括一年及二年有效期电子证书的申请，行政费为每份申请港币 300 元。	

2.4.3 电子证书（服务器）

电子证书（服务器）收费	一年有效期的电子证书	二年有效期的电子证书
新申请或续期	每份电子证书港币 2,500 元	每份电子证书港币 5,000 元

2.4.4 电子证书（保密）

电子证书（保密）收费	一年有效期的电子证书	二年有效期的电子证书
新申请或续期	每份电子证书港币 150 元	每份电子证书港币 300 元
行政费 （不论获授权单位数目多少）	每份申请港币 150 元	每份申请港币 300 元
	如申请表内包括一年及二年有效期电子证书的申请，行政费为每份申请港币 300 元。	

除非获得香港邮政豁免，否则登记人需在每一有效登记时段开始前，缴付登记费及行政费。香港邮政保留经常检讨及决定登记费及行政费的绝对权利，及会利用其网页（http://www.hongkongpost.gov.hk）通知登记人及公众。

2.5 公布资料及储存库

香港邮政维持一储存库，内有根据本核证作业准则签发并已经由登记人接受的证书清单、最新证书撤销清单、香港邮政公开密码匙、本准则文本一份以及与本准则电子证书有关之其它资料。除每周最多两小时之定期维修及紧急维修外，储存库基本保持每日 24 小时、每周 7 日开放。香港邮政在收到登记人确认接受电子证书后，会尽快在储存库公布该证书。香港邮政储存库可透过下述 URL 接达：

http://www.hongkongpost.gov.hk
ldap://ldap1.hongkongpost.gov.hk

2.5.1 证书储存库控制

储存库所在位置可供在线浏览，并可防止擅进。

2.5.2 证书储存库进入要求

经授权之香港邮政雇员方可进入储存库更新及修改内容。

2.5.3 证书储存库更新周期

每份证书一经登记人接受或例如撤销证书或其它核证机关披露记录情况一旦发生，储存库均会实时更新。

2.6 遵守规定之评估

须根据香港法例第 553 章电子交易条例以及认可核证机关守则之规定，至少每 12 个月进行一次遵守规定之评估，查清香港邮政发出、暂时吊销或撤销及公布证书之系统是否妥善遵守本准则。

2.7 机密性

在履行与香港邮政发出、暂时吊销、撤销及公布证书之有关任务时可取阅任何纪录、书刊、纪录册、登记册、通讯、信息、文件或其它物料之香港邮政、核证登记机关及任何香港邮政分包商之人员，不得向他人披露该等纪录、书刊、纪录册、登记册、通讯、信息、文件或物料，也不得允许或容受向他人披露该等纪录、书刊、纪录册、登记册、通讯、信息、文件或物料。香港邮政会确保香港邮政、核证登记机关及任何香港邮政分包商之人员均会依循此条限制事项。作为根据本准则申请电子证书之组成部分而提交之登记人资料，只会用于收集资料之目的并以机密方式保存；香港邮政需根据本准则履行其责任之情况除外。除非经法庭发出之传召或命令要求，或香港法例另有规定，否则未经登记人事先同意，不得将该等资料对外发布。除非法庭发出传票或命令，或香港法例另有规定，香港邮政尤其不得发表登记人清单或其数据，惟无法追溯个别人登记人之综合资料除外。

3. 鉴别及认证

3.1 首次申请

电子 证书（个人）之申请人（除非申请人为有效电子证书（个人）之持有人）须亲身到指定之香港邮政处所或其它香港邮政指定之机构处所，并出示第 3.1.9 条所述身分证明。如申请人为电子 证书（个人）之持有人，则无须亲身呈递， 但须提交申请人的数码签署（须由申请人的电子证书（个人）证明）作为身份证明。

电子证书（机构）、电子证书（服务器）及电子证书（保密）之申请人，其获授权代表须亲身到指定之香港邮政处所或其它香港邮政指定之机构处所，并出示第 3.1.8 条所述身分证明。在电子证书(机构)上列明之获授权用户，则无须亲身递交申请。

所有证书申请人须向香港邮政呈交一份填妥之申请表。电子证书（机构）、电子证书（服务器）及电子证书（保密）之申请须由申请机构之获授权代表填妥及签署，而申请机构亦会成为登记人。申请获批准后，香港邮政即准备证书并向申请人发出通知，说明如何发出及接受证书。

3.1.1 名称类型

3.1.1.1 电子证书（个人）

a) 透过证书上的主体名称（于**附录 B** 内指明），包括登记人香港身份证上显示之姓名，可识别电子证书（个人）登记人之身分。登记人香港身份证号码则以杂凑数值形式储存于证书内(见**附录 B**)。

3.1.1.2 向十八岁以下登记人签发电子证书(个人)

透过第 3.1.1.1 条内说明之证书上的主体名称及”e-Cert (Personal/Minor)”字样（见附录 B），可识别登记人之身分，及显示登记人获发出证书时未满 18 岁。

3.1.1.3 电子证书（机构）

透过证书上的主体名称（于**附录 B** 内指明）可识别电子证书（机构）登记人机构之身分，该名称由以下资料组成：

a) 授权用户香港身份证/护照上显示之姓名；

b) 登记人机构在有关香港政府部门或登记机关之登记名称或获香港法例认可之本港法定团体名称；如登记人机构为香港特别行政区政府部门或政策局，则为该部门或政策局之正式名称；及

c) 若登记人机构并非香港特别行政区政府部门或政策局或香港法例认可存在之法定团体，则包括该机构之香港公司注册/商业登记号码。

3.1.1.4 电子证书（服务器）

透过证书上的主体名称（于**附录 B** 内指明）可识别电子证书（服务器）登记人机构之身分，该名称由以下资料组成：

a) 登记人机构在有关香港政府部门或登记机关之登记名称或获香港法例认可之本港法定团体名称；如登记人机构为香港特别行政区政府部门或政策局，则为该部门或政策局之正式名称；

b) 若登记人机构并非香港特别行政区政府部门或政策局或香港法例认可存在之法定团体，则包括该机构之香港公司注册/商业登记号码；及

c) 登记人机构所拥有服务器（包括网域名称）之名称。

3.1.1.5 电子证书（保密）

透过证书上的主体名称（于**附录 B** 内指明）可识别电子证书（服务器）登记人机构之身分，该名称由以下资料组成：

a) 登记人机构在有关香港政府部门或登记机关之登记名称或获香港法例认可之本港法定团体名称；如登记人机构为香港特别行政区政府部门或政策局，则为该部门或政策局之正式名称；

b) 若登记人机构并非香港特别行政区政府部门或政策局或香港法例认可存在之法定团体，则包括该机构之香港公司注册/商业登记号码；及

c) 登记人机构内获授权单位之名称。

3.1.1.6 获授权代表

机构获授权代表虽替登记人机构办理电子证书（机构）、电子证书（服务器）或电子证书（保密）之申请手续，然而该证书并不会辨识此获授权代表身分。

3.1.1.7 机构中文名称

电子证书一律只用英文发出。只有中文名称或只提供中文名称作登记之机构，其名称不会显示在证书上。虽然如此，登记人仍可按网页 http://www.hongkongpost.gov.hk 之指示搜寻机构之中文名称。

3.1.2 名称需有意义

所采用名称之语义必须为一般人所能理解，方便辨识登记人身分。

3.1.3 诠释各个名称规则

香港邮政电子证书会加载之登记人名称(主体名称)类型见第 3.1.1 条。有关香港邮政电子证书主体名称之诠释应参照附录 B。

3.1.4 名称独特性

对登记人而言，主体名称 （于**附录 B** 内指明）应无歧义而具独特性。然而，此准则并不要求名称某一特别部分或成分本身具独特性或无歧义。

3.1.5 名称申索争议决议程序

香港邮政对有关名称争议之事宜的决定为酌情性及最终决定。

3.1.6 侵犯及违反商标注册

申请人及登记人向香港邮政保证（承诺）并向倚据证书人士申述，申请证书过程提供之资料概无以任何方式侵犯或违反第三者之商标权、服务商标、商用名称、公司名称或知识产权。

3.1.7 证明拥有私人密码匙之方法

香港邮政为登记人提供代制密码匙服务。香港邮政在其处所内使用稳当的系统，在安全

的环境下替登记人制作证书，以保证私人密码匙不受干扰。私人密码匙连同证书以本核证作业准则第 4.1、4.2、4.3 及 4.4 条中指明的安全方式交付予登记人。

3.1.8 机构申请人身分认证

3.1.8.1 电子证书（机构）、电子证书（服务器）及电子证书（保密）之申请，应由申请人之获授权代表亲身到指定之香港邮政处所或其它香港邮政指定之机构处所递交，获授权代表亦须出示其香港特区身份证或护照。

3.1.8.2 每份电子证书（机构）之申请须附有以下文件：

a) 盖上申请机构 “For and on behalf of “（代表机构签署）印章及附有该机构的获授权签署 之授权书。授权书注明该机构已授权有关人士 (即「获授权代表」)代表该机构提交申请及识别列于电子证书（机构）上的获授权用户；
b) 所有按此方式识别身分之获授权用户之香港身份证或护照副本；及
c) 由有关香港登记机关发出证明此机构确实存在之文件。

3.1.8.3 每份电子证书（服务器）之申请须附有以下文件：

a) 盖上申请机构 “For and on behalf of “（代表机构签署）印章及附有该机构的获授权签署 之授权书。授权书注明该机构已授权有关人士 (即「获授权代表」)代表该机构提交申请并证明服务器证书所载网域名称拥有权；
b) 由有关香港登记机关发出证明此机构确实存在之文件。

3.1.8.4 每份电子证书（保密）之申请须附有以下文件：

c) 盖上申请机构 “For and on behalf of “（代表机构签署）印章及附有该机构的获授权签署 之授权书。授权书注明该机构已授权有关人士 (即「获授权代表」)代表该机构提交申请；
d) 由有关香港登记机关发出证明此机构确实存在之文件。

3.1.8.5 香港特别行政区政府各政策局或部门之申请须附有盖上该政策局或部门印鉴之便笺、信函或有关申请表格，指定获授权代表以代表该政策局或部门签署与申请、撤销及续发香港邮政电子证书有关之所有文件。该便笺、信函或有关申请表格须由部门主任秘书或同级人员签署。

3.1.8.6 获发出二年有效期电子证书（机构）、电子证书（服务器）及电子证书（保密）之登记人机构，香港邮政会约于首年有效期届满时，再核对登记人机构的存在；及服务器证书所载网域名称拥有权（就电子证书（服务器）而言）。如登记人机构的存在或网域名称拥有权（就电子证书（服务器）而言）未能核实，香港邮政可根据本准则第 4.5 条的条款暂时吊销或撤销发出予该登记人机构的证书。

3.1.9 个人申请人身分认证

各电子证书（个人）申请人身分之确认将透过如下运作完成：

a) 各证书申请人可亲身到指定之香港邮政处所或其它已获香港邮政指定之机构处所，出示填妥并已签署之申请表及登记人协议以及申请人香港身份证。该前述处所人员将复核并认证所有申请文件，随后将申请递转交香港邮政核证机关处理。
b) 各证书申请人可出示由其电子证书（个人）证明的数码签署。

3.2 电子证书（个人）的登记使用期

3.2.1. 发出的电子证书（个人）有效期为三年，而登记使用期为一年。香港邮政会于证书的登记使用期届满前前一个月内以电子邮件或信件向登记人发出登记使用期届满通知。登记使用期可因应登记人的要求、香港邮政的酌情权或香港邮政的推广活动，在证书的登记使用期届满前得到延长。香港邮政不会为过期或已撤销的证书延长登记使用期。

3.2.2 在证书的三年有效期内延长登记使用期，登记人不会获发出另一电子证书。如登记人未能在证书的登记使用期届满前因应需要缴付费用，其证书可被撤销；如该证书存于智能身份证内，该证书可继续存于智能身份证内。登记人亦可前往指定邮政局要求移除智能身份证内的电子证书。

3.2.3 为电子证书（个人）延长登记使用期可不须进行身份认证（递交新证书申请时，须对申请人进行身份认证）。要求延长登记使用期时，登记人须以香港邮政随时规定的方式付款。香港邮政可行使酌情权延长登记人的登记使用期而无需登记人提出延长登记使用期的要求。延长登记使用期以后，登记人的电子证书及私人密码匙会继续有效，而不须为登记人制作新的配对密码匙。延长登记使用期以后，只要登记人协议原有之条款及条件与延长登记使用期当日有效的核证作业准则条款并无抵触，则原订的条文仍适用于该证书。如两者有所抵触，则以延长登记使用期当日之核证作业准则内的条款为准。申请人应细阅当日有效的核证作业准则，方可延长登记使用期。

3.3 证书续期

3.3.1 香港邮政会于证书的有效期届满前，以电子邮件或信件向电子证书（个人）登记人发出续期通知。证书可因应登记人的要求及香港邮政的酌情权，在证书的有效期届满前获得续期。香港邮政不会为过期、已暂时吊销或已撤销的证书续期。因应香港邮政的酌情权，发出给登记人的新证书可由新证书产生日期起有效，而有效期会于原有证书（即须续期的证书）到期日的三年后届满。由此，新的电子证书（个人）的有效期可超过三年，但不会超过三年另一个月。

3.3.2 每一电子证书(个人)续期可无须如首次申请时般进行认证登记人身分的程序申请续期时，登记人须填妥并签署证书续期申请表向香港邮政递交申请。续期申请的详情可向邮政局查询或参阅香港邮政网址 http://www.hongkongpost.gov.hk。证书一经续期，登记人的新配对密码匙会透过香港邮政的代制密码匙服务来产生。证书续期以后，只要登记人协议原有之条款及条件与续期当日有效的核证作业准则条款并无抵触，则原订的条文仍适用于新续期之证书。如两者有所抵触，则以续期当日之核证作业准则内的条款为准。申请人应细阅续期当日有效的核证作业准则，方可递交续期申请表。

3.4 电子证书（机构）、电子证书（服务器）及电子证书（保密）续期

3.4.1 香港邮政会于证书的有效期届满前，以电子邮件或信件向电子证书（机构）、电子证书（服务器）及电子证书（保密）登记人发出续期通知。证书可因应登记人的要

求及香港邮政的酌情权，在证书的有效期届满前获得续期。香港邮政不会为过期、已暂时吊销或已撤销的证书续期。因应香港邮政的酌情权，发出给登记人的新证书的实际有效期会超过于第 1.2.4 条指明的证书有效期：

新证书有效期	新证书内指明的有效期开始日	新证书内指明的有效期届满日	备注
一年	新证书产生日期	原有证书（即须续期的证书）到期日之后一年	新的电子证书的有效期可超过一年，但不会超过一年另一个月
二年	新证书产生日期	原有证书（即须续期的证书）到期日之后二年	新的电子证书的有效期可超过二年，但不会超过二年另一个月

3.4.2 电子证书（机构）、电子证书（服务器）及电子证书（保密）不会自动续期。若香港邮政接收到续期申请，即会根据 3.1.8 条所述“机构申请人身分认证”之过程重新进行认证。机构的获授权代表须填妥证书续期申请表(可于香港邮政网址 http://www.hongkongpost.gov.hk 下载)，并连同申请书内列明的其它文件以及续期费用，一并交回。如获授权代表人选有变，新的获授权代表亦须填妥申请表，一并交回香港邮政。

3.4.3 续期以后，只要登记人协议原有之条款及条件与续期当日有效之核证作业准则条款并无抵触，则原订的条文仍适用于新续期的证书。如两者有所抵触，则以续期当日之核证作业准则内的条款为准。申请人应细阅续期当日有效的核证作业准则，方可递交续期申请表。

4. 运作要求

4.1 电子证书（个人）

4.1.1 证书申请

4.1.1.1 处理申请

4.1.1.1.1 未获发给智能身份证的市民可经以下途径申请将电子证书（个人）加载智能身份证内（见第 4.1.2 条）：

a) 在前往入境事务处的智能身份证中心办理更换身份证手续前，亲自到香港邮政服务柜位、以邮递、传真或经互联网预先递交电子证书申请表；或
b) 在入境事务处的智能身份证中心办理更换身份证手续时，于设于智能身份证中心内的香港邮政服务柜位递交电子证书申请表。

4.1.1.1.2 已获发给智能身份证但未申请在智能身份证加载电子证书的市民可于指定香港邮政服务柜位申请将电子证书加载智能身份证内（见第 4.1.3 条）。

4.1.1.1.3 市民可于指定香港邮政服务柜位申请电子证书，并将电子证书存储在软磁盘或替代存储介质上（智能身份证以外的存储介质）（见第 4.1.3.2 条）。

4.1.1.2 电子证书及私人密码匙备份

4.1.1.2.1 如智能身份证已遗失或损坏，该智能身份证内的电子证书（包括其私人密码匙）将不能复原。就此，申请人可选择付费获取其在智能身份证内的电子证书及其私人密码匙的备份。该备份会存储于软磁盘或替代存储介质上。申请人可于递交电子证书申请表时，选取备份电子证书及私人密码匙的选项。

4.1.1.2.2 如申请人已选择电子证书备份，以申请人的个人密码保护的私人密码匙及证书将随后被存储在软磁盘或替代存储介质上。软磁盘或替代存储介质会密封于一可防止改动的封套或其它容器内；并以申请表中指明的方式交付予登记人。

4.1.1.2.3 申请人同意，他们一旦接获磁盘或替代存储介质，即须完全为私人密码匙的安全保管负责，并且同意，他们将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。

4.1.1.2.4 所有存于香港邮政系统内的私人密码匙均经加密。香港邮政会以恰当的保安措施防范私人密码匙在未经授权下被接达或披露。在完成送递电子证书及私人密码匙给申请人后，申请人的私人密码匙会从香港邮政系统中删除。

4.1.1.3 核对身份

4.1.1.3.1 申请人须于香港邮政服务柜位，向香港邮政职员出示其香港身份证，以核对身份。完成核对身份手续后，申请人会收到一个电子证书「个人密码信封」。

4.1.1.3.2 每份加载智能身份证内的电子证书及私人密码匙均由个别的「电子证书个人

密码」保护。「电子证书个人密码」会另外以密码信封形式分发给电子证书申请人。在随后使用电子证书及私人密码匙时，均需要该「电子证书个人密码」以防范电子证书及私人密码匙在未经准许情况下被接达。

4.1.1.3.3 香港邮政会以电子邮件或邮寄信件通知申请人申请已获批核。若香港邮政未能根据本准则列明的要求成功核实有关申请，香港邮政会拒绝有关申请并通知申请人。

4.1.2 发出电子证书及经入境事务处将电子证书（个人）加载智能身份证内

4.1.2.1 在第 4.1.1.1.1 条指明的地点递交的申请，香港邮政会透过在本 4.1.2 条列明的程序发出可加载申请人智能身份证内的电子证书；以便申请人可于入境事务处领取已载有电子证书的智能身份证。

4.1.2.2 确定资料

4.1.2.2.1 入境事务处与香港邮政双方的计算机系统会每天进行下述的确定资料的程序：

a) 已申请电子证书市民的资料会稳妥地存储于由香港邮政开发及管理的数据库内；

b) 经预先设定，香港邮政的系统会每天整理一份「申请人名单」；列出属于当日更换身份证组别（于宪报刊登）的的电子证书申请人的身份证号码及英文姓名；

c) 香港邮政的系统会每天将「申请人名单」，经由设有终端加密的稳妥通讯线路，传送到入境事务处的系统，以进行确定资料的程序；

d) 入境事务处的系统会根据「申请人名单」内各申请人的身份证号码，确定各申请人是否已登记更换身份证。入境事务处的系统并会将一份列有申请人状况（”已确定” 或 “未能确定”）的「确定结果名单」传回香港邮政的系统。入境事务处不会保留「申请人名单」或「确定结果名单」的副本；及

e) 入境事务处系统与香港邮政系统之间的数据传送，均经由设有终端加密的稳妥通讯线路传输。

4.1.2.2.2 上述确定资料的程序不会构成在个人资料（私隐）条例（香港法例第 486 章）内指明的「核对程序[1]」。进行上述确定资料程序的目的，是要确定有关的电子证书申请人已登记更换身份证，以便香港邮政可制作申请人的电子证书，并将电子证书传送至入境事务处及加载申请人的智能身份证内。上述确定资料的程序并非以引致香港邮政对电子证书申请人（作为 “资料当事人”）作出「不利行动[2]」为目的。上述确定资料的程

[1] 根據個人資料（私隱）條例，“核對程序”(matching procedure) 指將爲 1 個或 1 個以上的目的而取自 10 個或 10 個以上的資料當事人的個人資料與爲其他目的而自該等資料當事人收集的個人資料比較的程序(用人手方法的除外)，而—
(a) 所作比較(不論是全部的還是部分的)是爲了產生和核實某些可(即時或於其後任何時間)用作對任何該等資料當事人採取不利行動的資料的；或
(b) 所作比較產生和核實某些資料，而就該等資料而言可合理地相信將該等資料(即時或於其後任何時間)用作對任何該等資料當事人採取不利行動是切實可行的。

[2] 根據個人資料（私隱）條例，”不利行動”(adverse action)，就個人而言，指可對該人的權利、利益、特權、責任或權益(包括合法期望)有不利影響的任何行動。

序不会剥夺市民享有一年免费使用载于智能身份证内电子证书的机会。香港邮政会跟进在确定资料程序中 ” 未能确定” 的申请人资料，使他们可将电子证书及私人密码匙加载智能身份证内。

4.1.2.3 制作及将电子证书加载智能身份证内

4.1.2.3.1 经过确定资料程序后，香港邮政会为 “ 已确定” 的申请人制作电子证书（包括配对密码匙）；并将电子证书及私人密码匙传送至入境事务处及加载申请人的智能身份证内。香港邮政代表申请人产生配对密码匙，并由香港邮政制作证书。在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰。

4.1.2.3.2 将电子证书及私人密码匙加载智能身份证内的流程如下：

a) 香港邮政会将电子证书及私人密码匙（由「电子证书个人密码」保护（见第 4.1.1.3.2 条）及已加密）经由设有终端加密的稳妥通讯线路传输至入境事务处。已加密的电子证书及私人密码匙会存于入境事务处的稳妥系统内以便加载智能身份证内;
b) 入境事务处的系统会将个别已加密的电子证书及私人密码匙加载配对的智能身份证内;及
c) 入境事务处的系统会将已加密的电子证书及私人密码匙从其数据库中删除。

4.1.2.4 接受电子证书

4.1.2.4.1 香港邮政会为智能身份证持有人提供合理机会，从入境事务处领取智能身份证后，确认接受其电子证书。申请人同意，他们一旦接获智能身份证，即须完全为载于智能身份证内的私人密码匙的安全保管负责，并且同意，他们将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。接受电子证书可经由第 4.1.2.4.2 条（经由香港邮政网页）或 4.1.2.4.3 条（经由香港邮政服务柜位）说明的步骤完成。

4.1.2.4.2 申请人可经互联网在指定的香港邮政网页上完成以下步骤确认接受其电子证书：

a) 申请人在网页输入其个人资料；
b) 如申请人所输入资料与香港邮政系统所存有的资料吻合，申请人的电子证书内容会展示，以申请人便核实；
c) 申请人可确认接受电子证书（见第 4.1.2.4.4 条）；
d) 申请人确认接受电子证书的资料会传回香港邮政系统。

4.1.2.4.3 申请人可于指定香港邮政服务柜位完成以下步骤确认接受其电子证书：

a) 将智能身份证插入安装于服务柜位上计算机的智能卡阅读器内；
b) 展示智能身份证内的电子证书内容，以便智能身份证持有人核实；
c) 智能身份证持有人确认接受电子证书（见第 4.1.2.4.4 条）；
d) 申请人确认接受电子证书的资料会传回香港邮政系统。

4.1.2.4.4 在上述第 4.1.2.4.2(c)条及第 4.1.2.4.3(c)条所述程序中，申请人亦可确认不接受其电子证书而香港邮政会撤销该电子证书。申请人可将 ” 不接受” 的电子证书继续存于智能身份证上、或到指定邮政局将电子证书移除。

4.1.2.5 公布电子证书

在登记人确认接受其电子证书后，香港邮政会根据电子交易条例的要求，于香港邮政的储存库公布已获接受的电子证书（见第 2.5 条）。未获接受的电子证书不会于香港邮政的储存库公布。

4.1.3 在香港邮政服务柜位发出电子证书（个人）

4.1.3.1 在香港邮政服务柜位发出电子证书（个人）并加载智能身份证内

4.1.3.1.1 就获发给智能身份证后才决定申请电子证书人仕、及” 未能确定资料” 人仕（见第 4.1.2.2 条），此等人仕可于指定香港邮政服务柜位办理申请电子证书及将证书加载其智能身份证内。指定香港邮政服务柜位的位置刊登于香港邮政网址 www.hongkongpost.gov.hk.

4.1.3.1.2 获发给智能身份证后才决定申请电子证书人仕，可于指定香港邮政服务柜位，经以下程序办理申请电子证书及将证书及私人密码匙加载其智能身份证内：

a) 申请人根据第 4.1.1.1.2、4.1.1.2 及 4.1.1.3 条所述程序递交申请表、完成核对身份及领取密码信封；
b) 香港邮政职员会使用计算机终端机输入申请人在申请表上提供的资料，以制作电子证书；
c) 已制作电子证书的内容会在显示屏上展示，以便申请人核实；
d) 申请人可确认接受电子证书（见第 4.1.2.4 条）；确认接受电子证书的资料会传回香港邮政系统；
e) 如申请人确认接受电子证书，申请人的智能身份证会放进智能卡阅读器内。申请人的电子证书及私人密码匙会经由稳妥的机制从后端的稳妥系统内提出并加载智能身份证内。加载的电子证书已由申请人密码信封内的电子证书个人密码保护。如申请人拒绝确认接受电子证书，其智能身份证将不会加载电子证书及私人密码匙；
f) 当上述程序完成后，该智能身份证会实时交回申请人；
g) 已获接受的电子证书会在储存库内公布。

4.1.3.1.3 在第 4.1.2.2 条内所指” 未能确定资料” 的申请人，可经以下程序办理申请电子证书及将证书及私人密码匙加载其智能身份证内：

a) 申请人向香港邮政职员出示智能身份证，以便香港邮政职员经由柜位计算机终端机核对其申请状况；
b) 根据香港邮政系统内的申请人纪录，如确定申请人已递交申请表、完成核对身份及领取密码信封，香港邮政职员会安排经由柜位计算机终端机制作申请人的电子证书；
c) 已制作电子证书的内容会在显示屏上展示，以便申请人核实；
d) 申请人可确认接受电子证书（见第 4.1.2.4 条）；确认接受电子证书的资料会传回香港邮政系统；
e) 如申请人确认接受电子证书，申请人的智能身份证会放进智能卡阅读器内。申请人的电子证书及私人密码匙会经由稳妥的机制从后端的稳妥系统内提出并加载智能身份证内。加载的电子证书及私人密码匙已由申请人密码信封内的电子证书个人密码保护。如申请人拒绝确认接受电子证书，其智能身份证

将不会加载电子证书及私人密码匙。

f) 当上述程序完成后，该智能身份证会实时交回申请人；

g) 已获接受的电子证书会在储存库内公布。

4.1.3.2 发出电子证书并加载软磁盘或替代存储介质内

4.1.3.2.1 欲申请存储在软磁盘或替代存储介质（智能身份证除外）上的电子证书的人仕，可于指定香港邮政服务柜位办理申请电子证书手续。指定香港邮政服务柜位的位置刊登于香港邮政网址 www.hongkongpost.gov.hk.

4.1.3.2.2 市民可于指定香港邮政服务柜位，经以下程序办理申请电子证书及领取存储在软磁盘或替代存储介质上的电子证书：

a) 申请人根据以下程序递交申请表、完成核对身份及领取密码信封：
   - 申请人于香港邮政服务柜位，向香港邮政职员出示其香港身份证，以核对身份。完成核对身份手续后，申请人会收到一个电子证书「个人密码信封」。
   - 每份加载软磁盘或替代存储介质内的电子证书及私人密码匙均由个别的「电子证书个人密码」保护。「电子证书个人密码」会另外以密码信封形式分发给电子证书申请人。在随后使用电子证书及私人密码匙时，均需要该「电子证书个人密码」以防范电子证书及私人密码匙在未经准许情况下被接达。

b) 香港邮政职员会使用计算机终端机输入申请人在申请表上提供的资料，以制作电子证书；在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰；

c) 已制作电子证书的内容会在显示屏上展示，以便申请人核实；

d) 申请人可确认接受电子证书（见第 4.1.2.4 条）；确认接受电子证书的资料会传回香港邮政系统；

e) 如申请人确认接受电子证书，申请人的电子证书及私人密码匙会经由稳妥的机制从后端的稳妥系统内提出并存储在软磁盘或替代存储介质上。加载的电子证书及私人密码匙已由申请人密码信封内的电子证书个人密码保护。如申请人拒绝确认接受电子证书，其电子证书及私人密码匙不会在香港邮政服务柜位存储到任何软磁盘或替代存储介质上；

f) 当上述程序完成后，软磁盘或替代存储介质会实时交给申请人；

g) 已获接受的电子证书会在储存库内公布。

4.1.3.2.3 市民可于指定香港邮政服务柜位，经以下程序办理申请电子证书后经邮递方式领取存储在软磁盘或替代存储介质上的电子证书：

a) 申请人于香港邮政服务柜位，向香港邮政职员出示其香港身份证，以核对身份。完成核对身份手续后，申请人会收到一个电子证书「个人密码信封」；

b) 在核对身份手续后，香港邮政会产生电子证书（包括配对密码匙）。在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰；

c) 私人密码匙及证书将随后被存储在软盘或替代存储介质上。每份加载软磁盘或替代存储介质内的电子证书及私人密码匙均由申请人「个人密码信封」内的「电子证书个人密码」保护。在随后使用电子证书及私人密码匙时，均需要该「电子证书个人密码」以防范电子证书及私人密码匙在未经准许情况下被接达。软盘或替代存储介质会密封于一可防止改动的封套或其它容器内；并以安全方式

交付予申请人；

d) 申请人可将填妥的接受证书表格以传真、信件或电邮，或经指定网页（www.hongkongpost.gov.hk）交回香港邮政，以确认接受电子证书。申请人亦可确认不接受其电子证书而香港邮政会撤销该电子证书；

e) 已获接受的电子证书会在储存库内公布。

4.2 电子证书（机构）

4.2.1 证书申请

4.2.1.1 处理申请

电子证书（机构）之申请人须到指定之香港邮政处所或其它香港邮政指定之机构处所递交申请。

4.2.1.2 核对身份

用以证明登记人机构、获授权代表及获授权用户身分之文件，于本准则第 3.1.8 条说明。完成核对身份手续后，各电子证书「个人密码信封」会以安全方式送递获授权代表。

4.2.2 发出证书

4.2.2.1 在核对身份手续后，香港邮政会产生电子证书（包括配对密码匙）。在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰。

4.2.2.2 以密码保护的私人密码匙及证书将随后被存储在软盘或替代存储介质上。软盘或替代存储介质会密封于一可防止改动的封套或其它容器内；并以安全方式交付予申请人。

4.2.2.3 登记人机构同意，他们一旦接获磁盘或替代存储介质，即须完全为私人密码匙的安全保管负责，并且同意，他们将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。

4.2.2.4 所有存于香港邮政系统内的私人密码匙均经加密。香港邮政会以恰当的保安措施防范私人密码匙在未经授权下被接达或披露。在完成送递电子证书及私人密码匙给申请人后，申请人的私人密码匙会从香港邮政系统中删除。

4.2.3 接受证书

4.2.3.1 香港邮政会为申请人提供合理机会，核对其电子证书的内容及确认接受其电子证书。申请人可将填妥的接受证书表格以传真、信件或电邮，或经指定网页（www.hongkongpost.gov.hk）交回香港邮政，以确认接受电子证书（机构）。

4.2.3.2 申请人亦可确认不接受其电子证书而香港邮政会撤销该电子证书。

4.2.4 公布电子证书

在登记人确认接受其电子证书后，香港邮政会根据电子交易条例的要求，于香港邮政的

储存库公布已获接受的电子证书（见第 2.5 条）。未获接受的电子证书不会于香港邮政的储存库公布。

4.3 电子证书（保密）

4.3.1 证书申请

4.3.1.1 处理申请

电子证书（保密）之申请人须到指定之香港邮政处所或其它香港邮政指定之机构处所递交申请。

4.3.1.2 核对身份

用以证明登记人机构、获授权代表及获授权用户身分之文件，于本准则第 3.1.8 条说明。完成核对身份手续后，各电子证书「个人密码信封」会以安全方式送递获授权代表。

4.3.2 发出证书

4.3.2.1 在核对身份手续后，香港邮政会产生电子证书（包括配对密码匙）。在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰。。

4.3.2.2 以密码保护的私人密码匙及证书将随后被存储在软盘或替代存储介质上。软盘或替代存储介质会密封于一可防止改动的封套或其它容器内；并以安全方式交付予登记人。

4.3.2.3 登记人机构同意，他们一旦接获磁盘或替代存储介质，即须完全为私人密码匙的安全保管负责，并且同意，他们将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。

4.3.2.4 所有存于香港邮政系统内的私人密码匙均经加密。香港邮政会以恰当的保安措施防范私人密码匙在未经授权下被接达或披露。在完成送递电子证书及私人密码匙给申请人后，申请人的私人密码匙会从香港邮政系统中删除。

4.3.3 接受证书

4.3.3.1 香港邮政会为申请人提供合理机会，核对其电子证书的内容及确认接受其电子证书。申请人可将填妥的接受证书表格以传真、信件或电邮，或经指定网页（www.hongkongpost.gov.hk）交回香港邮政，以确认接受电子证书（保密）。

4.3.3.2 申请人亦可确认不接受其电子证书而香港邮政会撤销该电子证书。

4.3.4 公布电子证书

在登记人确认接受其电子证书后，香港邮政会根据电子交易条例的要求，于香港邮政的储存库公布已获接受的电子证书（见第 2.5 条）。未获接受的电子证书纭不会于香港邮政的储存库公布。

4.4 电子证书（服务器）

4.4.1 证书申请

4.4.1.1 处理申请

电子证书（服务器）之申请人须到指定之香港邮政处所或其它香港邮政指定之机构处所递交申请。

4.4.1.2 核对身份

用以证明登记人机构、获授权代表及获授权用户身分之文件，于本准则第 3.1.8 条说明。完成核对身份手续后，各电子证书「个人密码信封」会以安全方式送递获授权代表。

4.4.2 发出、接受及公布证书

4.4.2.1 在核对身份手续后，香港邮政会以电邮或信件通知申请人其申请已被接纳。发出电子证书的过程如下：

a) 申请人在其装置上自行产生私人密码匙及公开密码匙。
b) 申请人在其装置上自行产生载有其公开密码匙的「签发证书要求」（Certificate Signing Request），及将「签发证书要求」经由指定的香港邮政网页传送给香港邮政。
c) 在收到「签发证书要求」后，香港邮政会查证载有公开密码匙资料的「签发证书要求」上的数码签署，以核对申请人是持有配对的私人密码匙。香港邮政并不会持有申请人的私人密码匙。
d) 在核对申请人是持有配对的私人密码匙后，香港邮政会产生载有申请人公开密码匙的电子证书。
e) 申请人可于指定的香港邮政网页核对电子证书的内容及确认接受该电子证书。
f) 在申请人确认接受电子证书后，香港邮政会将电子证书传送给申请人；并根据电子交易条例的要求，于香港邮政的储存库公布已获接受的电子证书。申请人亦可确认不接受其电子证书而香港邮政会撤销该电子证书。未获接受的电子证书不会于香港邮政的储存库公布。

4.5 撤销证书

4.5.1 撤销

若香港邮政私人密码匙资料外泄，会导致香港邮政迅速地撤销所有经由该私人密码匙发出的证书。在私人密码匙资料外泄的情况下，香港邮政会根据在业务持续运作计划内定明的程序迅速地撤销所有已发出的证书（见第 4.9.2 条）。

按照准则中列明之撤销程序，各登记人可于任何时间以任何理由要求撤销依据本登记人协议须由其承担责任之证书。

登记人之私人密码匙或内载与某电子证书公开密码匙相关私人密码匙之媒界，若已外泄或怀疑已外泄，各登记人必须立即按照本准则的撤销程序，向香港邮政申请撤销证书（见第 2.1.3(g) 条）。

不论何时，若有以下情况，香港邮政均可按准则中程序暂时吊销或撤销证书并会以书面(证书撤销通知书) 通知登记人：

a) 知道或有理由怀疑登记人之私人密码匙已外泄；
b) 知道或有理由怀疑证书之细节不真实或已变得不真实或证书不可靠；
c) 认为证书并非根据准则妥当发出；
d) 认为登记人未有履行本准则或登记人协议列明之责任；
e) 证书适用之规例或法例有此规定；
f) 认为登记人未曾缴付登记费；
g) 知道或有理由相信其资料出现在电子证书（个人）上之登记人：
   i) 死亡或已死亡；
   ii) 在拟撤销证书前五年内已达成香港法例第六章破产条例所指之债务重整协议或债务偿还安排或自愿安排；或
   iii) 因欺诈、舞弊或不诚实行为，或违反电子交易条例而在本港或海外被定罪；
h) 知道或有理由相信在电子证书（机构）上指明之获授权用户已非登记人机构之成员或雇员；或 i) 知道或有理由相信其资料出现在电子证书（机构）、电子证书（服务器）或电子证书（保密）上之登记人：
   i) 正被清盘或接到有司法管辖权之法庭所判清盘令；
   ii) 在拟撤销证书前五年内已达成香港法例第六章破产条例所指之债务重整协议或债务偿还安排或自愿安排；
   iii) 其董事、职员或雇员因欺诈、舞弊或不诚实行为，或违反电子交易条例被定罪；或
   iv) 在撤销证书前五年内登记人资产之任何部分托给接管人或管理人接管。

4.5.2 撤销程序请求

登记人，或登记人机构的获授权代表，可透过香港邮政位于http:www.hongkongpost.gov.hk的指定网页、传真、邮寄信件、电子邮件或亲身前往邮局，向香港邮政提出撤销证书要求。如登记人未能缴付登记费及拒绝接受香港邮政的推广活动以延长登记使用期，登记人须提出撤销证书的要求。香港邮政接到此要求后会暂时吊销证书。经登记人，或经初始接收撤销证书要求的核证登记机关，最后确认撤销证书后，该证书即会撤销且永久失效。撤销证书之最后确认程序包括收到由登记人以其私人密码匙进行数码签署之电子邮件、登记人亲笔签署之信件正本或登记人亲笔签署之撤销证书申请表格。如未有收到登记人的最后确认，证书会继续暂时失效，并列入证书撤销清单，直至证书有效期届满为止。撤销证书申请表格可从香港邮政网页 http://www.hongkongpost.gov..hk下载。香港邮政会考虑登记人的要求，把暂时吊销的证书回复为有效。但香港邮政只会在谨慎的情况下把暂时吊销的证书回复为有效。

所有被暂时吊销或撤销证书之有关资料（包括表明暂时吊销或撤销证书之原因代码）将刊载于撤销证书名单内。（见第 7.2 条）下次更新的证书撤销清单不会包括由"暂时吊销"状态回复有效的证书。

香港邮政处理撤销证书要求的办公时间如下：

星期一至星期五	：	上午九时至下午五时
星期六	：	上午九时至中午十二时
星期日及公众假期	：	上午九时至中午十二时

如悬挂八号或以上之热带气旋警告信号或黑色暴风雨警告信号，香港邮政将停止处理撤

销证书要求。如在该日早上六时或以前信号除下，香港邮政将如常办公；如信号在早上六时至十时之间或十时正除下，香港邮政将于该日（周六、周日或公众假期除外）下午二时如常办公。

4.5.3 服务承诺及证书撤销清单更新

a) 香港邮政将作出合理努力，确保在 (1) 香港邮政从登记人处收到撤销申请或 (2) 在无此申请之情况下，香港邮政决定暂时吊销或撤销证书，两个工作日内，将该暂时吊销或撤销证书数据于证书撤销清单公布。然而，证书撤销清单并不会于各证书暂时吊销或撤销后随即在公众目录中公布。祇有在下一份证书撤销清单更新时一并公布，证书撤销清单介时才会显示该证书已暂时吊销或撤销之状态。证书撤销清单每日公布，并存盘七年。

特此澄清，星期六、星期日、公众假期及悬挂热带风暴及暴雨警报信号之工作日，一律不视作工作日计算。

香港邮政会以合理的方式，尽量在收到撤销证书申请一星期内，透过电子邮件或以邮寄方式向有关登记人发出撤销证书通知书。

b) 在登记人明知香港邮政根据准则条款可能据以撤销证书之任何事项之情况下，或登记人已作出撤销申请或经知会香港邮政，香港邮政拟根据本准则条款暂时吊销或撤销证书后，登记人均不得在交易中使用证书。倘若或登记人无视本条所述的规定，仍确实在交易中使用证书，则香港邮政毋须就任何该等交易向登记人或倚据证书人士承担责任。

c) 此外，登记人明知香港邮政任何事项之情况下撤销证书，或登记人作出申请或经知会香港邮政拟撤销证书时，须立即通知从事当时仍有待完成之任何交易之倚据证书人士，用于该交易之证书须予撤销 (由香港邮政或经登记人申请) ，并明确说明，因情况乃属如此，故倚据证书人士不得就交易而倚据证书。若登记人未能通知倚据证书人士，则香港邮政无须就该等交易向登记人承担责任，并无须向虽已收到通知但仍完成交易之倚据证书人士承担责任。

除非香港邮政未能行使合理技术及谨慎且登记人未能按此等规定之要求通知倚据证书人士，否则，香港邮政无须就香港邮政作出暂时吊销或撤销证书(根据申请或其它原因)之决定与此信息出现于证书撤销清单之间之时间内进行之交易承担责任。任何此等责任均仅限于本准则其它部分规限之范畴。在任何情况下，核证登记机关自身无须对倚据证书人士承担独立谨慎责任(核证登记机关只是履行香港邮政之谨慎责任)。因此，即使出现疏忽，核证登记机关亦无须对倚据证书人士负责。

d) 电子证书的证书撤销清单会依据在**附录 C** 内指明的时间表及格式更新。

e) 有关香港邮政对于倚据证书人仕暂时未能获取已暂时吊销或撤销的证书资料时的政策，已列于本准则第 2.1.5 条(倚据证书人士之义务)及 2.2.1 条(合理技术及谨慎)。

4.5.4 撤销效力

在香港邮政把暂时吊销 / 撤销状况刊登到证书撤销清单，即终止某一证书。

4.6 计算机保安审核程序

4.6.1 记录事件类型

香港邮政核证机关系统内之重要保安事件，均以人手或自动记录在受保护的审核追踪档案内。此等事件包括而不限于以下例子：

- 可疑网络活动
- 多次试图进入而未能接达
- 与安装设备或软件、修改及配置核证机关运作之有关事件
- 享有特权接达核证机关各组成部分的过程
- 定期管理证书之工作包括：
  - 处理撤销及暂时吊销证书之要求
  - 实际发出、撤销及暂时吊销证书
  - 证书续期
  - 更新储存库资料
  - 汇编撤销证书清单并刊登新数据
  - 核证机关密码匙转换
  - 档案备存
  - 紧急密码匙复原

4.6.2 处理纪录之次数

香港邮政每日均会处理及覆检审核运行纪录，用以审核追踪有关香港邮政核证机关的行动、交易及程序。

4.6.3 审核纪录之存留期间

存盘审核纪录文文件存留期为七年。

4.6.4 审核纪录之保护

香港邮政处理审核纪录时实施多人式控制，可提供足够保护，避免有关纪录意外受损或被人蓄意修改。

4.6.5 审核纪录备存程序

香港邮政每日均会按照预先界定程序(包括多人式控制)为审核纪录作适当备存。备存会另行离机储存，并获足够保护，以免被盗用、损毁及媒体衰变。备存入档前会保留至少一星期。

4.6.6 审核资料收集系统

香港邮政核证机关系统审核纪录及文文件受自动审核收集系统控制，该收集系统不能为任何应用程序、程序或其它系统程序修改。任何对审核收集系统之修改本身即成为可审核事件。

4.6.7 事件主体向香港邮政发出通知

香港邮政拥有自动处理系统，可向适当人士或系统报告重要审核事件。

4.6.8 脆弱性评估

脆弱性评估为香港邮政核证机关保安程序之一部份。

4.7 纪录存盘

4.7.1 存盘纪录类型

香港邮政须确保存盘纪录记下足够资料，可确定证书是否有效以及以往是否运作妥当。香港邮政(或由其代表)存有以下数据：

- 系统设备结构档案
- 评估结果及/或设备合格覆检(如曾进行)
- 核证作业准则及其修订本或最新版本
- 对香港邮政具约束力而构成合约之协议
- 所有发出或公布之证书及证书撤销清单
- 定期事件纪录
- 其它需用以核实存盘内容之数据

4.7.2 存盘保存期限

密码匙及证书数据须妥为保存七年。审核跟踪文档须以香港邮政视为适当之方式存放于系统内。

4.7.3 存盘保护

香港邮政保存之存盘媒体受各种实体或加密措施保护，可避免未经授权进入。保护措施用以保护存盘媒体免受温度、湿度及磁场等环境侵害。

4.7.4 存盘备份程序

在有需要时制作并保存存盘之副本。

4.7.5 电子邮戳

存盘资料均注明开设存盘项目之时间及日期。香港邮政利用控制措施防止擅自调校自动系统时钟。

4.8 密码匙变更

由香港邮政产生，并用以证明根据本准则发出的证书的核证机关根源密码匙及证书寿命为期不超过二十年。香港邮政核证机关密码匙及证书在期满前至少三个月会进行续期。续发新根源密码匙后，相连之根源证书即会公布供大众取用。原先之根源密码匙则保留至第 4.6.2 条指定之最短之时限，以供核对用原先密码匙进行产生之签署。

4.9 灾难复原及密码匙资料外泄计划

4.9.1 灾难复原计划

香港邮政已备有妥善管理之程序，包括每天为主要业务信息及核证系统的资料备存及适当地备存核证系统的软件，以维持主要业务持续运作，保障在严重故障或灾难影响下仍可继续业务。业务持续运作计划之目的在于促使香港邮政全面恢复提供服务，内容包括一个经测试的独立灾难复原基地，而该基地现时位于香港特别行政区内并距离核证机关主设施不少于十千米。业务持续运作计划每年均会检讨及执行。

如发生严重故障或灾难，香港邮政会实时知会政府信息科技总监，并公布运作由生产基地转至灾难复原基地。

在发生灾难后但稳妥可靠的环境尚未重新确立前：

a) 敏感性物料或仪器会安全地锁于设施内；
b) 若不能将敏感性物料或仪器安全地锁于设施内或该等物料或仪器有受损毁的风险，该等物料或仪器会移离设施并锁于其它临时设施内；及
c) 设施的出入信道会实施接达管制，以防范盗窃及被人擅自接达。

4.9.2 密码匙资料外泄计划

业务持续运作计划内载处理密码匙资料外泄之正式程序。此等有关程序每年均会检讨及执行。

如根据本准则签发电子证书的香港邮政私人密码匙资料外泄，香港邮政会实时知会政府信息科技总监并作出公布。香港邮政的私人密码匙资料一旦外泄，香港邮政会实时撤销根据有关私人密码匙发出之证书，然后发出新证书取代。

4.9.3 密码匙的替补

倘若在密码匙资料外泄或灾难情况下，香港邮政根据本准则签发电子证书的私人密码匙资料外泄或遭破坏而无法复原，香港邮政会尽快知会政府信息科技总监并作出公布。公布内容包括已撤销证书的名单、如何为登记人提供新的香港邮政公开密码匙及如何向登记人重新发出证书。

4.10 核证机关终止服务

如香港邮政停止担任核证机关之职能，即按“香港邮政终止服务计划”所定程序知会政府信息科技总监并作出公布。在终止服务后，香港邮政会将核证机关的纪录适当地存盘七年（由终止服务日起计）；该等纪录包括已发出的证书、根源证书、核证作业准则及证书撤销清单。

4.11 核证登记机关终止服务

如核证登记机关根据核证登记机关协议或因核证机关终止服务（第 4.10 条）停止担任核证登记机关之职能，且其代表香港邮政行使之授权已予以收回，经由该核证登记机关申请之证书仍会按其条款及有效期继续有效。

5. 实体、程序及人员保安控制

5.1 实体保安

5.1.1 选址及建造
香港邮政核证机关运作位于商业上具备合理实体保安条件之地点。在场地建造过程中，香港邮政已采取适当预防措施，为核证机关运作作好准备。

5.1.2 进入控制
香港邮政实施商业上具合理实体保安之控制，限制进入就提供香港邮政核证机关服务而使用之硬件及软件（包括核证机关服务器、工作站及任何外部加密硬件模块或受香港邮政控制之权标）。可使用该等硬件及软件之人员只限于本准则第 5.2.1 条所述之履行受信职责之人员。在任何时间都对该等进入进行控制及人手或电子监控，以防发生未经授权入侵。

5.1.3 电力及空调
核证机关设施可获得之电力和空调资源包括专用的空调系统，无中断电力供应系统及一台独立后备发电机，以备城市电力系统发生故障时供应电力。

5.1.4 自然灾害
核证机关设施在合理可能限度内受到保护，以免受自然灾害影响。

5.1.5 防火及保护
香港邮政已为核证机关设施备妥防火计划及灭火系统。

5.1.6 媒体存储
媒体存储及处置程序已经开发备妥。

5.1.7 场外备存
香港邮政核证系统数据的适当备存会作场外储存，并获足够保护，以免被盗用、损毁及媒体衰变。（另见第 4.8.1 条）

5.1.8 保管印刷文件
印刷文件包括登记人勃议及身分确认文件之影印本由香港邮政或其核证登记机关妥为保存。获授权人员方可以取阅该等纪录。

5.2 过程控制

5.2.1 受信职责
可进入或控制密码技术或其它运作程序并可能会对证书之发出、使用或撤销带来重大影响（包括进入香港邮政核证机关数据库之受限制运作）之香港邮政或代表香港邮政之核证登记机关雇员、承包商及顾问（统称“人员”），应视作承担受信职责。该等人员包括但不限于系统管理人员、操作员、工程人员及获委派监督香港邮政核证机关运作之行政人员。

香港邮政已为所有涉及香港邮政电子证书服务而承担受信职责之人员订立、汇编及推行

相关程序。执行下列工作，有关程序即可完整进行：

- 按角色及责任订定各级实体及系统接达控制
- 职责划分

5.2.2 香港邮政与核证登记机关之间的文件及资料传递

香港邮政与核证登记机关之间的所有文件及资料的传递，均在受控制及安全的方式进行。

5.2.3 年度评估

评估工作每年执行一次，以确保符合政策及工作过程控制之规定。（见第 2.6 条）

5.3 人员控制

5.3.1 背景及资格

香港邮政采用之人员及管理政策可合理确保香港邮政或代表香港邮政之核证登记机关的人员，包括雇员、承包商及顾问之可信程度及胜任程度，并确保他们以符合本准则之方式履行职责及表现令人满意。

5.3.2 背景调查

香港邮政对担任受信职责之人员进行调查（其受聘前及其后有需要时定期进行），及 / 或香港邮政要求核证登记机关进行调查，以根据本准则及香港邮政之人员政策要求核实雇员之可信程度及胜任程度。未能通过首次及定期调查之人员不得担任或继续担任受信职责。

5.3.3 培训要求

香港邮政及核证登记机关人员已接受履行其职责所需要之初步培训。有需要时香港邮政亦会提供持续培训，使人员能掌握所需最新工作技能。

5.3.4 向人员提供之文件

香港邮政及核证登记机关人员会收到综合用户手册，详细载明证书之制造、发出、更新、续期及撤销程序及与其职责有关之其它软件功能。

6. 技术保安控制

本条说明香港邮政特别为保障加密密码匙及相关数据所订之技术措施。控制香港邮政核证机关密码匙之工作透过实体保安及稳妥密码匙存储进行。产生、储存、使用及毁灭香港邮政核证机关密码匙只能在由多人式控制之可防止篡改硬件装置内进行。

6.1 密码匙之产生及安装

6.1.1 产生配对密码匙

除非程序被获授权使用者外泄，否则香港邮政及申请人/登记人配对密码匙之产生程序可使配对密码匙的获授权使用者以外人士无法取得私人密码匙。香港邮政产生配对根源密码匙，用以发出符合本准则之证书。倘若由香港邮政为申请人代制密码匙，在完成送递电子证书及私人密码匙给申请人后，申请人的私人密码匙会从香港邮政系统中删除。

6.1.2 登记人公开密码匙交付

香港邮政会代表申请人 / 登记人按照代制密码匙的要求产生电子证书（个人）、电子证书（机构）及电子证书（保密）的配对密码匙。电子证书（服务器）的公开密码匙将由申请人产生，并须以确保附合以下要求的方式交付香港邮政：

- 该公开密码匙在交付过程中不会被更改；及
- 交付者持有与该公开密码匙配对的私人密码匙。

6.1.3 公开密码匙交付予登记人

用于核证机关数码签署之各香港邮政配对密码匙之公开密码匙可从网页 http://www.hongkongpost.gov.hk 取得。香港邮政采取保护措施，以防该等密码匙被人更改。

6.1.4 密码匙大小

香港邮政之签署配对密码匙为 2048 位 RSA。登记人配对密码匙则为 1024 位 RSA。

6.1.5 加密模块标准

香港邮政进行之签署产生密码匙、存储及签署操作在硬件加密模块进行。

6.1.6 密码匙用途

香港邮政电子证书(个人)、电子证书（机构）及电子证书（保密）使用之密码匙可用于数码签署以及加密电子通讯。电子证书（服务器）使用之密码匙可用于加密电子通讯。香港邮政根源密码匙（用于制造或发出符合本准则证书之密码匙）只用于签署(a)证书及(b)证书撤销清单。

6.2 私人密码匙保护

6.2.1 加密模块标准

香港邮政私人密码匙利用加密模块产生，其级别至少达到 FIPS 140-1 第 3 级。

6.2.2 私人密码匙多人式控制

香港邮政私人密码匙储存在可防止篡改加密硬件装置内。香港邮政采用多人式控制激

活、使用、终止香港邮政私人密码匙。

6.2.3 私人密码匙托管

香港邮政使用之电子证书系统并无为香港邮政私人密码匙及登记人私人密码匙设计整体性密码匙托管程序。有关香港邮政私人密码匙的备存，见第 6.2.4 条。

6.2.4 香港邮政私人密码匙备存

香港邮政私人密码匙的备存，是使用达到 FIPS 140-1 第 2 级保安标准的装置加密及储存。香港邮政私人密码匙的备存程序须经超过一名人士参与完成。备存的私人密码匙亦须超过一名人士激活。其它私人密码匙均不设备存。所有私人密码匙不会存盘。

6.3 配对密码匙管理其它范畴

香港邮政之核证机关密码匙使用期不超过二十年（见第 4.8 条）。所有香港邮政密码匙之产生、销毁、储存以及证书及撤销清单签署运作程序，均于硬件加密模块内进行。第 4.7 条详述香港邮政公开密码匙纪录存盘之工作。

6.4 计算机保安控制

香港邮政实行多人控制措施，控制激活数据（如个人辨识密码及接达核证机关系统密码的生命周期）。香港邮政已制定保安程序，防止及侦测未获授权进入核证机关系统、更改系统及系统资料外泄等情况。此等保安控制措施接受第 2.6 条遵守规定之评估。

6.5 生命周期技术保安控制

香港邮政控制为香港邮政系统购置及发展软件及硬件之程序。现已定下更改控制程序以控制并监察就香港邮政系统部件所作的调整及改善。

6.6 网络保安控制

香港邮政系统有防火墙以及其它接达控制机制保护，其配置只允许已获授权使用本准则所载核证机关服务者接达。

6.7 加密模块工程控制

香港邮政使用之加密装置至少达到 FIPS140-1 第 2 级。

7. 证书及证书撤销清单结构

7.1 证书结构

本准则提及之证书内有用于确认电子讯息发送人身分及核实该等讯息是否完整之公开密码匙（即用于核实数码签署之公开密码匙）。本准则提及之证书一律以 X.509 第三版本之格式发出。（见附录 B）。**附录 D** 载有各类香港邮政电子证书之特点摘要。

7.2 证书撤销清单结构

香港邮政证书撤销清单之格式为 X.509 第二版本（见**附录 C**）。

8. 准则管理

更改本准则一律须经香港邮政核准及公布。有关准则一经香港邮政在网页http://www.hongkongpost.gov.hk或香港邮政储存库公布，更改实时生效，并对获发证书的申请人以及登记人均具约束力。就任何对本准则作出的更改，香港邮政会实际可行地尽快通知政府信息科技总监。申请人、登记人及倚据证书人士可从香港邮政网页http://www.hongkongpost.gov.hk或香港邮政储存库浏览此份准则以及其旧有版本。

附录 A - 词汇

除非文意另有所指，否则下列文词在本准则中释义如下：

“接受”就某证书而言—

（a） 在某人在该证书内指名或识别为获发给该证书的人的情况下，指—

(i) 确认该证书包含的关于该人的信息是准确的；

(ii) 批准将该证书向他人公布或在某储存库内公布；

（iii）使用该证书；或

（iv）以其它方式显示承认该证书；或

（b） 在某人将会在该证书内指名或识别为获发给该证书的人的情况下，指—

（i）确认该证书将会包含的关于该人的信息是准确的；

（ii）批准将该证书向他人公布或在某储存库内公布；或

（iii）以其它方式显示承认该证书；”；

“申请人”指自然人或法人并已申请电子证书。

“非对称密码系统”指能产生安全配对密码匙之系统。安全配对密码匙由用作产生数码签署之私人密码匙及用作核实数码签署之公开密码匙组成。

“获授权代表”指登记人机构之授权代表。

“授权单位”指登记人机构属下的单位；而登记人机构已授权该单位使用发出予该登记人机构的电子证书（保密）的私人密码匙。

“授权用户” 指登记人机构之成员或雇员；而登记人机构已授权该成员或雇员使用发出予该登记人机构的电子证书（机构）的私人密码匙。

“证书”或**“电子证书”**指符合以下所有说明之纪录：

a) 由核证机关为证明数码签署之目的而发出而该数码签署用意为确认持有某特定配对密码匙者身分或其它主要特征；

b) 识别发出纪录之核证机关；

c) 指名或识别获发给纪录者；

d) 包含该获发给纪录者之公开密码匙；并

e) 经发出纪录核证机关之负责人员签署。

“核证机关”指向他人(可以为另一核证机关)发出证书者。

“核证作业准则（准则）”指核证机关发出以指明其在发出证书时使用之作业实务及标准之准则。

“证书撤销清单”列举证书发出人在证书原定到期时间前宣布无效之公开密码匙证书（或其它类别证书）之资料。

“对应”就私人或公开密码匙而言，指属同一配对密码匙。

“数码签署”就电子纪录而言，指签署人之电子签署，该签署用非对称密码系统及杂凑函数将该电子纪录作数据变换产生，使持有原本未经数据变换之电子纪录及签署人之公开密码匙者能据此确定：

(a) 该数据变换是否用与签署人之公开密码匙对应之私人密码匙产生；以及

(b) 产生数据变换后，原本之电子纪录是否未经变更。

“电子纪录”指信息系统产生之数码形式之纪录，而该纪录：

(a) 能在信息系统内传送或由一个信息系统传送至另一个信息系统；并

(b) 能储存在信息系统或其它媒介内。

“电子签署”指与电子纪录相连或在逻辑上相联之数码形式之字母、字样、数目字或其它符号，而该等字母、字样、数目字或其它符号为认证或承认该纪录之目的定立或采用者。

“身份证” 指由香港特别行政区政府入境事务处发出的香港身份证，包括智能身份证。

“信息”包括资料、文字、影像、声音编码、计算机程序、软件及数据库。

“信息系统”指符合以下所有说明之系统：
(a) 处理信息；
(b) 纪录信息；
(c) 能用作使信息纪录或储存在不论位于何处之信息系统内，或能用作将信息在该等系统内以其它方式处理；及
(d) 能用作检索信息(不论该等信息纪录或储存在该系统内或在不论位于何处之信息系统内) 。

“中介人”就某特定电子纪录而言，指代他人发出、接收或储存该纪录，或就该纪录提供其它附带服务者。

“发出”就证书而言，指
（a） 制造该证书，然后将该证书包含的关于在该证书内指名或识别为获发给该证书的人的信息，通知该人；或
（b） 将该证书将会包含的关于在该证书内指名或识别为获发给该证书的人的信息，通知该人，然后制造该证书，
然后提供该证书予该人使用；

“配对密码匙”在非对称密码系统中，指私人密码匙及其在数学上相关之公开密码匙，而该公开密码匙可核实该私人密码匙所产生之数码签署。

“条例”指香港法例第 553 章电子交易条例。

“发讯者”就某电子纪录而言，指发出或产生该纪录者，或由他人代为发出或产生该纪录者，惟不包括中介人。

“香港邮政署长”指香港法例第 98 章《邮政署条例》所指署长。

“私人密码匙”指配对密码匙中用作产生数码签署之密码匙。

“公开密码匙”指配对密码匙中用作核实数码签署之密码匙。

“认可证书”指：
(a) 根据第 22 条认可之证书；
(b) 属根据第 22 条认可之证书之类型、类别或种类之证书；或
(c) 第 34 条所述核证机关所发出指明为认可证书之证书。

“认可核证机关”指根据第 21 条认可之核证机关或第 34 条所述核证机关。

“纪录”指在有形媒界上注记、储存或以其它方式固定之信息，亦指储存在电子或其它媒界可藉理解形式还原之信息。

“核证登记机关” 指由香港邮政指定，代表香港邮政行使一定职能，并提供香港邮政之若干服务之机构。

“倚据限额”指就认可证书倚据而指明之金钱限额。

“储存库”指用作储存并检索证书以及其它与证书有关信息之信息系统。

“负责人员”就某核证机关而言，指在该机关与本条例有关活动中居要职者。

“签”及**“签署”**包括由意图认证或承认纪录者签订或采用之任何符号，或该人使用或采用之任何方法或程序。

“智能身份证” 指可将电子证书加载其中的**身份证**。

“登记人”指符合以下所有说明的人：

(i) 在某证书内指名或识别为获发给证书；

(ii) 已接受该证书；及
(iii) 持有与列于该证书内的公开密码匙对应之私人密码匙；

“**登记人协议**” 指由登记人及香港邮政订立的协议，包含在申请表上列明的登记人条款及条件及本核证作业准则的条款。

“**登记人机构**” 指作为登记人的机构；而其获授权代表已签署登记人协议及根据此核证作业准则该机构为合资格获发出电子证书之机构。

“稳当系统”指符合以下所有条件之计算机硬件、软件及程序：
(a) 合理地安全可免遭受入侵及不当使用；
(b) 在可供使用情况、可靠性及操作方式能于合理期内维持正确等方面达到合理水平；
(c) 合理地适合执行其原定功能；及
(d) 依循广为接受之安全原则。

为执行电子交易条例，如某数码签署可参照列于某证书内之公开密码匙得以核实，而该证书之登记人为签署人，则该数码签署即可视作获该证书证明。

附录 B - 香港邮政电子证书格式

1) 电子证书（个人）格式

字段名称		字段内容	
		电子证书（个人）	发出予未满18岁人仕的 电子证书（个人）
标准栏 (Standard field)			
版本 (Version)		X.509 V3	
序号 (Serial number)		[由香港邮政系统设置]	
签署算式识别 (Signature algorithm ID)		sha1RSA	
发行者 (Issuer)		cn=Hongkong Post e-Cert CA 1 o=Hongkong Post c=HK	
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政设置的UTC 时间]	
	不迟于 (Not after)	[由香港邮政设置的UTC 时间]	
主体名称 (Subject name)		cn=[香港身份证姓名]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人参考编号]（附注3） o=Hongkong Post e-Cert (Personal) c=HK	cn=[香港身份证姓名]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人参考编号]（附注3） o=Hongkong Post e-Cert (Personal/Minor)（附注4） c=HK
主体公开密码匙数据 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为1024-bit	
发出人识别名称 (Issuer unique identifier)		未使用	
登记人识别名称 (Subject unique identifier)		未使用	
标准延伸字段 (Standard extension)（附注5）			
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK	
	序号 (Serial number)	[从发出人处获取]	
密码匙的使用 (Key usage)		不可否认，数码签署，密码匙加密 **（此栏为”关键”字段）**	
证书政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.5（附注 6） PolicyQualifierID = CPS Qualifier = [核证作业准则的URL]	
主体其它名称 (Subject alternative name)	**DNS**	[经加密的香港身份证号码]（附注7）	
	rfc822	[证书持有人电子邮箱地址]（附注2）	
发行者其它名称 (Issuer alternative name)		未使用	
基本限制 (Basic	**主体类型**	最终实体	

字段名称		字段内容	
		电子证书（个人）	发出予未满18岁人仕的电子证书（个人）
constraints)	(Subject type)		
	路径长度限制 (Path length constraints)	无	
延伸密码匙的使用 (Extended key usage)		未使用	
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL] （附注8）	
Netscape 延伸字段 (Netscape extension)（附注5）			
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME	
Netscape SSL服务器名称 (Netscape SSL server name)		未使用	
Netscape 备注 (Netscape comment)		未使用	

附注：

1. 申请人姓名格式: 英文格式 - 姓氏（大写）+ 名 （例如 CHAN Tai Man David）
2. 申请人电子邮箱地址（选项）
3. 登记人参考编号： 10 位数字
4. “e-Cert (Personal/Minor)” 表示 申请人于获发出证书时未满 18 岁（见本核证作业准则第 3.1.1.2 条）.
5. 除非另外注明，所有标准延伸字段及 Netscape 延伸字段均为 “非关键” (Non-Critical) 延伸字段。
6. 香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.5」为本准则的对象识别码 (Object Identifier, OID)。
7. 申请人的香港身份证号码(包括括号内的数字)(以 hkid_number 表示)将会经申请人的私人密码匙签署并转化为一杂凑数值(以 cert_hkid_hash 表示)后，存入证书：

$$cert\_hkid\_hash = SHA\text{-}1\,(\,RSA_{privatekey,\ sha\text{-}1}\,(\,hkid\_number\,)\,)$$

*SHA-1*为一杂凑函数而*RSA*则为签署函数

在代制密码匙的过程中，hkid_number则会在香港邮政处所内代制密码时签署，并产生已签署的香港身份证号码的杂凑数值$SHA\text{-}1\,(\,RSA_{privatekey,\ sha\text{-}1}\,(\,hkid_number\,)\,)$。该杂凑数值会输入证书内的指定延伸字段。

8. 证书撤销清单分发点URL为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl, 其中 <xxxxx> 为 经香港邮政系统产生，包含 5 个数字或字符的字符串。香港邮政会公布各「分割式证书撤销清单」。已暂时吊销或撤销证书的数据，会在 该证书” 证书撤销清单分发点” 字段内注明的已分割证书撤销清单内公布。

2) 电子证书（机构）格式

字段名称		字段内容
标准栏 (Standard field)		
版本 (Version)		X.509 V3
序号 (Serial number)		[由香港邮政系统设置]
签署算式识别 (Signature algorithm ID)		sha1RSA
发行者 (Issuer)		cn=Hongkong Post e-Cert CA 1 o=Hongkong Post c=HK
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政设置的UTC 时间]
	不迟于 (Not after)	[由香港邮政设置的UTC 时间]
主体名称 (Subject name)		cn=[获授权用户姓名]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人参考编号]（附注3） ou=[商业登记证书编号+注册证书/登记证书编号+其它]（附注4） ou=[登记人机构名称]（附注5） ou=[登记人机构分行/部门名称] o=Hongkong Post e-Cert (Organisational) c=HK
主体公开密码匙数据 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为1024-bit
发出人识别名称 (Issuer unique identifier)		未使用
登记人识别名称 (Subject unique identifier)		未使用
标准延伸字段 (Standard extension)（附注6）		
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK
	序号 (Serial number)	[从发出人处获取]
密码匙的使用 (Key usage)		不可否认，数码签署，密码匙加密 **（此栏为”关键”字段）**
证书政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.5（附注 7） PolicyQualifierID = CPS Qualifier = [核证作业准则的URL]
主体其它名称 (Subject alternative name)	**DNS**	未使用
	rfc822	[证书持有人电子邮箱地址]（附注2）
发行者其它名称 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主体类型 (Subject type)**	最终实体
	路径长度限制 (Path length constraints)	无

字段名称		字段内容
延伸密码匙的使用 (Extended key usage)		未使用
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL] （附注8）
Netscape 延伸字段 (Netscape extension)（附注6）		
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME
Netscape SSL服务器名称 (Netscape SSL server name)		未使用
Netscape 备注 (Netscape comment)		未使用

附注：

1. 获授权用户姓名格式: 英文格式 - 姓氏（大写）+ 名 （例如 CHAN Tai Man David）
2. 获授权用户电子邮箱地址（选项）
3. 登记人参考编号： 10 位数字
4. “商业登记证书编号”字段 : 一串 16 位数字/字母（首 11 位数字/字母代表商业登记编号）【如无商业登记证书编号，字段全部为零(“0”)】，“注册证书 / 登记证书编号”字段 : 一串 8 位数字/字母【如无注册证书 / 登记证书编号，字段全部为零(“0”)】，“其它”字段: 一串最多 30 位数字/字母 (如有)。香港特别行政区政府部门之”商业登记编号”及”注册证书 / 登记证书”字段全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入”其它” 字段。
5. 只有中文名称或只提供中文名称作登记之机构，其名称不会在此栏内显示（见本核证作业准则第 3.1.1.7 条）。
6. 除非另外注明，所有标准延伸字段及 Netscape 延伸字段均为 “非关键” (Non-Critical) 延伸字段。
7. 香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.5」为本准则的对象识别码 (Object Identifier, OID)。
8. 证书撤销清单分发点URL为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl

3) 电子证书（保密）格式

字段名称		字段内容
标准栏 (Standard field)		
版本 (Version)		X.509 V3
序号 (Serial number)		[由香港邮政系统设置]
签署算式识别 (Signature algorithm ID)		sha1RSA
发行者 (Issuer)		cn=Hongkong Post e-Cert CA 1 o=Hongkong Post c=HK
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政设置的UTC 时间]
	不迟于 (Not after)	[由香港邮政设置的UTC 时间]
主体名称 (Subject name)		cn=[获授权单位名称]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人参考编号]（附注3） ou=[商业登记证书编号+注册证书/登记证书编号+其它]（附注4） ou=[登记人机构名称]（附注5） ou=[登记人机构分行/部门名称] o=Hongkong Post e-Cert (Encipherment) c=HK
主体公开密码匙数据 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为1024-bit
发出人识别名称 (Issuer unique identifier)		未使用
登记人识别名称 (Subject unique identifier)		未使用
标准延伸字段 (Standard extension)（附注6）		
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK
	序号 (Serial number)	[从发出人处获取]
密码匙的使用 (Key usage)		数码签署，密码匙加密 **（此栏为”关键”字段）**
证书政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.5（附注 7） PolicyQualifierID = CPS Qualifier = [核证作业准则的URL]
主体其它名称 (Subject alternative name)	**DNS**	未使用
	rfc822	[证书持有人电子邮箱地址]（附注2）
发行者其它名称 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主体类型 (Subject type)**	最终实体
	路径长度限制 (Path length constraints)	无

字段名称		字段内容
延伸密码匙的使用 (Extended key usage)		未使用
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL] （附注8）
Netscape 延伸字段 (Netscape extension)（附注6）		
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME
Netscape SSL服务器名称 (Netscape SSL server name)		未使用
Netscape 备注 (Netscape comment) （附注9）		This e-Cert is used ONLY (i) to send encrypted electronic messages to the Subscriber Organisation; (ii) to permit the Subscriber Organisation to decrypt messages; and (iii) to permit the Subscriber Organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving Subscriber Organisation. For terms and conditions governing the use of this e-Cert, please see the e-Cert CPS which can be viewed at http://www.hongkongpost.gov.hk.

附注：

1. 登记人机构之获授权单位名称
2. 获授权单位电子邮箱地址（选项）
3. 登记人参考编号： 10 位数字
4. “商业登记证书编号”字段 : 一串 16 位数字/字母（首 11 位数字代表商业登记编号）【如无商业登记证书编号，字段全部为零(“0”)】, “注册证书 / 登记证书编号”字段 : 一串 8 位数字/字母【如无注册证书 / 登记证书编号，字段全部为零(“0”)】, “其它”字段: 一串最多 30 位数字/字母 (如有)。香港特别行政区政府部门之”商业登记编号”及”注册证书 / 登记证书”字段全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入”其它” 字段。
5. 只有中文名称或只提供中文名称作登记之机构，其名称不会在此栏内显示（见本核证作业准则第 3.1.1.7 条）。
6. 除非另外注明，所有标准延伸字段及 Netscape 延伸字段均为 “非关键” (Non-Critical) 延伸字段。
7. 香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.5」为本准则的对象识别码 (Object Identifier, OID)。
8. 证书撤销清单分发点URL为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl
9. 电子证书一律只用英文发出。以下为本字段内容的中文本以供参考，中英文本措词诠释若有歧异，则以英文本为准：

> 此类证书只可用作(i) 传送加密之电子信息予登记人机构；(ii) 容许登记人机构为信息解密；及(iii) 容许登记人机构发出认收信息并附加其数码签署以证实其收件登记人机构身分；以及藉此确认已收讫送出之加密信息。有关规管使用此证书之条文条款，请参阅可从 http://www.hongkongpost.gov.hk 网页浏览的电子证书核证作业准则。

4) 电子证书（服务器）格式

字段名称		字段内容
标准栏 (Standard field)		
版本 (Version)		X.509 V3
序号 (Serial number)		[由香港邮政系统设置]
签署算式识别 (Signature algorithm ID)		sha1RSA
发行者 (Issuer)		cn=Hongkong Post e-Cert CA 1 o=Hongkong Post c=HK
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政设置的UTC 时间]
	不迟于 (Not after)	[由香港邮政设置的UTC 时间]
主体名称 (Subject name)		cn=[服务器名称]（附注1） ou=[登记人参考编号]（附注2） ou=[商业登记证书编号+注册证书/登记证书编号+其它]（附注3） ou=[登记人机构名称]（附注4） ou=[登记人机构分行/部门名称] o=Hongkong Post e-Cert (Server) c=HK
主体公开密码匙数据 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为1024-bit
发出人识别名称 (Issuer unique identifier)		未使用
登记人识别名称 (Subject unique identifier)		未使用
标准延伸字段 (Standard extension)（附注6）		
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK
	序号 (Serial number)	[从发出人处获取]
密码匙的使用 (Key usage)		密码匙加密 **（此栏为”关键”字段）**
证书政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.5 （附注 6） PolicyQualifierID = CPS Qualifier = [核证作业准则的URL]
主体其它名称 (Subject alternative name)	DNS	未使用
	rfc822	未使用
发行者其它名称 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主体类型 (Subject type)**	最终实体
	路径长度限制 (Path length constraints)	无
延伸密码匙的使用 (Extended key usage)		未使用

字段名称		字段内容
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL] （附注7）
Netscape 延伸字段 (Netscape extension)（附注6）		
Netscape 证书类型 (Netscape cert type)		SSL Server
Netscape SSL服务器名称 (Netscape SSL server name)		未使用
Netscape 备注 (Netscape comment)		未使用

附注：

1. 登记人机构拥有之服务器名称（包括服务器的区位名址(Domain Name)）
2. 登记人参考编号： 10 位数字
3. “商业登记证书编号”字段 : 一串 16 位数字/字母（首 11 位数字代表商业登记编号）【如无商业登记证书编号，字段全部为零(“0”)】，“注册证书 / 登记证书编号”字段 : 一串 8 位数字/字母【如无注册证书 / 登记证书编号，字段全部为零(“0”)】，“其它”字段: 一串最多 30 位数字/字母 (如有)。香港特别行政区政府部门之”商业登记编号”及”注册证书 / 登记证书”字段全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入”其它” 字段。
4. 只有中文名称或只提供中文名称作登记之机构，其名称不会在此栏内显示（见本核证作业准则第 3.1.1.7 条）。
5. 除非另外注明，所有标准延伸字段及 Netscape 延伸字段均为 “非关键” (Non-Critical) 延伸字段。
6. 香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.5」为本准则的对象识别码 (Object Identifier, OID)。
7. 证书撤销清单分发点URL为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl

附录 C - 香港邮政证书撤销清单(CRL)格式

香港邮政每天三次更新及公布下述的证书撤销清单（更新时间为香港时间 09:15、14:15 及 19:00（即格林尼治平时[GMT] 时间 01:15、06:15 及 11:00））；证书撤销清单载有根据本核证作业准则而暂时吊销或撤销的电子证书的信息：

a) **「分割式证书撤销清单」 (Partitioned CRL)**包含分组的已暂时吊销或已撤销证书的资料。公众可于在证书的「证书撤销清单分发点 (CRL distribution point) 」字段内注明的 URL 获取相关的「分割式证书撤销清单」。

b) **「整体证书撤销清单」 (Full CRL)** 包含所有已暂时吊销或已撤销证书的资料。公众可于以下 URL 获取「整体证书撤销清单」：

http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl;或
ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 CRL1, o=Hongkong Post, c=HK)。

在正常情况下，香港邮政会于更新时间后，尽快将最新的证书撤销清单公布（见本准则第 2.5 条）。在不能预见及有需要的情况下，香港邮政可不作事前通知而更改上述证书撤销清单的更新及公布的时序。

分割式及整体证书撤销清单格式:-

标准字段 (Standard field)	子字段 (Sub-field)	分割式证书撤销清单字段内容	整体证书撤销清单字段内容	备注
版本 (Version)		v2		此栏显示证书撤销清单格式的版本为 X.509 第二版
签署算式识别 (Signature algorithm ID)		sha1RSA		此栏显示用以签署证书撤销清单的算法的识别码
发出人 (Issuer name)		CN=Hongkong Post e-Cert CA 1 O=Hongkong Post C-HK		此栏显示签署及发出证书撤销清单的机构
此次更新 (This update)		[UTC 时间]		此栏显示本证书撤销清单的发出日期 (是次更新)
下次更新 (Next update)		[UTC 时间]		表示下次证书撤销清单将于显示的日期或之前发出 (下次更新)，而不会于显示的日期之后发出。根据核证作业准则的规定，证书撤销清单是每天更新及发出
撤销证书 (Revoked certificates)	用户证书 (User certificate)	[证书序号]		此栏列出已撤销的证书并以证书序号排列次序
	撤销日期 (Revocation date)	[UTC 时间]		此栏显示撤销证书的日期
	输入证书撤销清单资料申延字段 (CRL entry extensions)			
	原因代码 (Reason code)	[撤销理由识别码]		（附注 1）
标准延伸字段 (Standard extension) （附注 2）				
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	CN=Hongkong Post Root CA 1 O=Hongkong Post		此栏提供有关数据以识别用作签署证书撤销清单的私人密码

标准字段 (Standard field)	子字段 (Sub-field)	分割式证书撤销清单字段内容	整体证书撤销清单字段内容	备注
		C=HK		匙的配对公开密码匙。
	序号 (Serial number)	[发出人证书的序号]		此栏显示发出人证书的序号
证书撤销清单号码 (CRL number)		[由核证彡 统产生]		此栏显示证书撤销清单的编号，该编号以顺序形式产生。
发出人分发点 (Issuer distribution point)		[以 DER 方式编码的证书撤销清单分发点 (Encoded CRL Distribution Point)] **（此栏为”关键”字段）**	[未使用]	本字段祇为分割式证书撤销清单使用。

附注：

1. 以下为可于撤销证书字段下列出的理由识别码：

   0 = 未注明；1 = 密码数据外泄；2 = 核证机关资料外泄；3 = 联号变更；
   4 = 证书被取代；5 = 核证机关终止运作；6 = 证书被暂时吊销

   由于登记人无须提供撤销证书的原因，所以「原因代码」会以「0」表示（即「未注明」）。

2. 除非另外注明，所有标准延伸字段均为 “非关键” (Non-Critical) 延伸字段。

附录 D

附录 D - 香港邮政电子证书 – 服务摘要

1) 电子证书（个人）

要点	*电子证书(个人)*	*发出予未满 18 岁人仕的电子证书(个人)*
登记人	持有有效香港身份证及年满 18 岁人仕	持有有效香港身份证及未满 18 岁人仕
依据限额	HK$200,000	HK$0
认可证书	是	
配对密码匙长度	1024-bit RSA	
产生配对密码匙	由香港邮政代制产生	
核对身份	当面核对申请人的身份，或由申请人提供可经其有效电子证书（个人）证明的数码签署	
证书用途	数码签署及数据加密	
证书内包含登记人的资料	香港身份证上列出的英文姓名； 香港身份证号码的杂凑数值 (hash value)； 电邮地址；及 登记人参考编号（由香港邮政系统产生）	
登记费用（见本准则第 2.4 条）	每份证书（包括首次及续期申请）每年 50 港元	
证书有效期	三年 （附注 1）	

附注

1. 根据证书续期程序而发出之证书有效期可超过三年，但不会超过三年另一个月（见本核证作业准则第 1.2.4 及 3.2 条）

2) 电子证书（机构）、电子证书(保密) 及电子证书(服务器)

要点	***电子证书(机构)***	***电子证书(保密)***	***电子证书(服务器)***
登记人	获香港特别行政区政府签发有效商业登记证之机构、获香港法例认可之本港法定团体及香港特别行政区政府政策局、部门或机关		
证书持有人	登记人机构之成员或雇员并为获授权用户	登记人机构之获授权单位	即登记人
依据限额	HK$200,000		
认可证书	是		
配对密码匙长度	1024-bit RSA		
产生配对密码匙	由香港邮政代制产生		由登记人自行产生
核对身份	核对机构及其获授权代表的身份		核对区位名址(Domain Name)、机构及其获授权代表的身份
证书用途	数码签署及数据加密	只作数据加密之用	SSL 加密
证书内包含登记人的资料	▪ 登记人机构名称 ▪ 获授权用户英文姓名及其电邮地址 ▪ 登记人参考编号（由香港邮政系统产生） ▪ 登记人机构之公司 / 商业登记信息	▪ 登记人机构名称 ▪ 获授权单位英文名称及其电邮地址 ▪ 登记人参考编号（由香港邮政系统产生） ▪ 登记人机构之公司 / 商业登记信息	▪ 登记人机构名称 ▪ 登记人机构之服务器名称 ▪ 登记人参考编号（由香港邮政系统产生） ▪ 登记人机构之公司 / 商业登记信息
登记费用（见本准则第 2.4 条）	见本核证作业准则第 2.4 条		
证书有效期	一年或两年 （见本核证作业准则第 1.2.4 及 3.3.1 条）		

附录 E - 香港邮政电子证书核证登记机关名单

核证登记机关名称 / 网址	证书名称	证书有效期	未成年人可否登记	办公时间	批注
中国银行（香港）有限公司 http://www.bochk.com	香港邮政电子证书 (机构)	一年或两年	不适用	星期一至星期五：上午九时至下午五时 星期六： 上午九时至下午一时 星期日及公众假期：休息	中国银行（香港）有限公司收取及转递其帐户持有人提交之香港邮政电子证书(机构) 之申请，及核实在申请表上指明为申请机构之获授权代表的身份
南洋商业银行有限公司 http://www.ncb.com.hk	香港邮政电子证书 (机构)	一年或两年	不适用	星期一至星期五：上午九时至下午五时 星期六： 上午九时至下午一时 星期日及公众假期：休息	南洋商业银行有限公司收取及转递其帐户持有人提交之香港邮政电子证书(机构)申请，及核实在申请表上指明为申请机构之获授权代表的身份
集友银行有限公司 http://www.chiyubank.com	香港邮政电子证书 (机构)	一年或两年	不适用	星期一至星期五：上午九时至下午五时 星期六： 上午九时至下午一时 星期日及公众假期：休息	集友银行有限公司收取及转递其帐户持有人提交之香港邮政电子证书(机构)申请，及核实在申请表上指明为申请机构之获授权代表的身份