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（伺服器）

核证作业准则

日期：二零一七年七月二十日
物件识别码：1.3.6.1.4.1.16030.1.1.34

目录

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他用途。公匙基建由多个元素组成，包括法律责任、政策、硬体、软件、资料库、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，为支援以上述方式在香港特别行政区进行商业活动及其他交易。

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**。

自 2007 年 4 月 1 日起，香港邮政核证机关的营运已外判给私营机构承办。目前，香港邮政已批出合约予翘晋电子商务有限公司（“合约”），根据本作业准则营运和维持香港邮政核证机关的系统和服务，合约期由 2012 年 4 月 1 日至 2018 年 3 月 31 日止。

根据合约，在得到香港邮政的书面同意后，翘晋电子商务有限公司可以委任合约分判商执行合约中的部份工作。**附录 F** 列载翘晋电子商务有限公司的合约分判商之名单（若有的话）。在本核证作业准则内，“承办商” 是指翘晋电子商务有限公司及其合约分判商（若有的话）。

香港邮政依然为条例第 34 条下之认可核证机关而承办商则为香港邮政根据政府资讯科技总监在条例第 33 条下颁布之认可核证机关业务守则第 3.2 段所委任之代理人。

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（伺服器）均为条例下的认可证书，在本核证作业准则内称为“证书”或“电子证书”。

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。而根据政府资讯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核证登记机关为代理人，履行香港邮政作为认可核证机关于本作业准则所列举之若干职能。**附录 E** 列载核证登记机关之清单（若有的话）。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。

本核证作业准则列载电子证书的实务守则，其结构如下：

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 条简介证书，证书撤销清单及线上证书状态应答结构
第 8 条叙述如何管理本核证作业准则

附录 A 词汇表
附录 B 香港邮政电子证书格式
附录 C 香港邮政电子证书撤销清单，香港邮政授权撤销清单(ARL)以及线上证书状态应答格式
附录 D 香港邮政电子证书特点摘要
附录 E 香港邮政电子证书核证登记机关名单（若有的话）
附录 F 香港邮政电子证书服务 - 翘晋电子商务有限公司之合约分判商名单（若有的话）
附录 G 核证机关根源证书的有效期
附录 H 香港邮政电子证书特定应用名单及相对应之特定应用编码
附录 I RFC3647 与本核证作业准则之比较表

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。

香港邮政将维护本准则，以符合香港《电子交易条例》（第 553 章）及《认可核证机关业务守则》(“业务守则”) 相关规例和符合《粤港两地电子签名证书互认办法》下的《粤港电子签名证书互认证书策略》(“互认证书策略”) 相关规例。

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.1.34」为本准则的物件识别码 (Object Identifier, OID) （见**附录 B** 内关于核证政策(Certificate Policies)的说明）。此外，香港邮政亦会在电子证书（个人）“互认版 " 和 电子证书（机构）“互认版 " 的核证政策内加入政府资讯科技总监办公室指派给互认证书策略的物件识别码(Object Identifier, OID) 「2.16.344.8.2.2008.810.2.2012.1.0」。

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（伺服器），香港邮政已指明为认可证书。其中，电子证书（个人）和电子证书（机构）分别可选包含符合互认证书策略的“互认版 " 功能，均是条例下的认可证书。**对登记人及倚据人士而言，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 2.1.6 条及其他有关章条之倚据人士表明，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 2.1.6

条及其他有关章条之倚据人士表明，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
香港邮政将于储存库公布经由登记人接受并已发出之认可证书。（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，包括但不限于用于交易之电子证书。特此澄清，倚据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或承办商发出电子证书，而核证登记机关及承办商对倚据人士并无任何谨慎职责，亦不需对倚据人士就发出电子证书而负责（见第 2.1.2 条）。于交易中依据其他登记人之电子证书之登记人乃为有关此证书之倚据人士。**请倚据人士留意，除特别声明外，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（伺服器）及电子证书（保密），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）并向所有其他有关人士（尤其是倚据人士）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（伺服器）登记人、电子证书（机构）的授权用户及电子证书（保密）的授权单位外，并无其他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（伺服器）将只会用于第 1.2.3.3 条指明的用途。
d) 电子证书（保密）将只会用于第 1.2.3.4 条指明的用途。
e) 证书所载之所有资料及由登记人作出之陈述均属真实。
f) 证书将只会用于符合本核证作业准则之认可及合法用途。
g) 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。而电子证书（个人）“互认版 " 同时适用于《粤港两地电子签名证书互认办法》下的适用范围。

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），而电子证书（个人）“互认版 " 则只会发出予十八岁或以上人士。

1.2.3.2 电子证书（机构）

电子证书（机构）发给 (i) 香港特别行政区政府各政策局及部门、(ii) 获香港特别行政区政府签发有效商业登记证或获税务局根据《税务条例》(第 112 章)发出的有效证明文件的登记人，以及 (iii) 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「授权用户」）。此等证书与电子证书（个人）之用途大致相同。而电子证书（机构）“互认版 " 同时适用于《粤港两地电子签名证书互认办法》下的适用范围。电子证书（机构）“互认版 " 不可发出予十八岁以下人士。

登记人机构作为《税务条例》(第 112 章)所指获香港特别行政区政府税务局签发有效证明文件的申报财务机构，向香港邮政承诺，除了按**附錄 H** 内所指的特定应用作加密与解密电子信息及數码签署以外，不会授权予授权用户使用电子证书（机构）于任何其他用途。

1.2.3.3 电子证书（伺服器）

电子证书（伺服器）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之一个或多个伺服器名称发出之证书。因应香港邮政的酌情权，伺服器名称的完整格式网域名称的最左边部份可为通配符（即星号“*”）。

此类证书只可用于加密电子通讯以及伺服器验证。如证书内之数码签署密码匙使用方法（于**附录 B** 内指明）有被启用，此类证书之数码签署亦只可用于伺服器验证以及与伺服器建立安全通讯通道。不论任何情况，此等证书产生之数码签署均不得用作洽商或订定合约或任何具法律效力之协议或任何金钱交易。

登记人机构向香港邮政承诺，不会授权予任何人使用此类证书之数码签署作伺服器验证或与伺服器建立安全通讯通道以外之用途。由此，任何人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。

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（“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，不会授权予授权单位使用此类证书之数码签署作其他用途。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

证书的有效期由产生自香港邮政系统当日起即日生效。

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（个人）“互认版 "	一年、二年或三年（申请人可于申请时选择）
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（机构）“互认版 "	一年、二年或三年（申请人可于申请时选择）
电子证书（保密）	一年、二年、三年或四年（申请人可于申请时选择）
电子证书（伺服器）	一年或二年（申请人可于申请时选择）
电子证书（伺服器）“通用版 " 或“多域版 "	一年、二年或三年（申请人可于申请时选择）

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 3.3 及 3.4 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 在香港邮政指定之处所进行申请

所有首次申请及证书撤销或到期后之申请，申请人须依据本核证作业准则第 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，并在收到投诉后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他登记人证书之倚据人士，均须如此。关于非登记人倚据人士，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本准则发出、暂时吊销、撤销、及公布证书时对倚据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、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 至 4.4 条），
c) 暂时吊销或撤销证书并依时公布证书撤销清单以及线上证书状态应答（见第 4.6 条），及
d) 通知登记人有关已暂时吊销或撤销的证书（见第 4.6.1., 4.6.2. 及 4.6.3 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人士承担任何责任。**

2.1.3 承办商之义务

承办商祇会依据香港邮政及承办商之合约条款，包括承办商作为香港邮政所委任之代理人而须依据本作业守则建立、修改、提供、供应、交付、营运、管理、推广及维持香港邮政核证机关之系统及服务，而对香港邮政负责。香港邮政会依然对承办商在其执行或将会执行香港邮政之功能权力，权利及职能之行为负责。

2.1.4 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（就申请电子证书（个人）、电子证书（机构）或电子证书（保密）而言）。
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（伺服器），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证书之程序直至证书过期。
d) 承认会履行义务，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、泄露或未经授权之使用，且须对在任何情况下外泄私人密码匙而引致的后果负责。

e) 发现其证书的私人密码匙之任何丢失或外泄时，立即向香港邮政呈报丢失或外泄（外泄乃属违反保安，使资料遭受未经授权之进入，从而导致资料有可能在未经授权下被披露、更改或使用）。
f) 不时将登记人提供之证书资料或授权用户之任何变动立即通知香港邮政。
g) 不时把电子证书(机构)、电子证书(保密)及电子证书(伺服器)的获授权代表的委任及资料的变动立即通知香港邮政。
h) 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。
i) 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。
j) 在登记人明确知晓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。
k) 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，故倚据人士不得就交易而倚据证书。
l) 承认知悉一经递交电子证书申请表，即授权向其他人或在香港邮政储存库公布其电子证书。
m) 用于身份鉴别的证书，其私人密码匙只可以在证书有效期内使用。

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他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他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 4.6.2 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（伺服器）登记人亦负责确保此类证书只可用于加密电子通讯以及伺服器验证。如证书内之数码签署密码匙使用方法（于**附录 B** 内指明）有被启用，不会试图使用该电子证书（伺服器）的私人密码匙以产生数码签署并用作伺服器验证或与伺服器建立安全通讯通道以外之用途。

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，不得作其他用途；
- 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。

2.1.5 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/或其他人士(包括倚据人士)就可能因此产生之责任或损失及损害赔偿损失。

2.1.6 倚据人士之义务

倚据电子证书之倚据人士负责：

a) 倚据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，确定证书之使用及其证明的任何数码签署乃适合本准则规定之用途，而承办商或核证登记机关（若有的话）(见**附录 E**)并不对倚据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或者相关的线上证书状态应答（如适用）。
d) 如属电子证书（个人）“互认版 " 及 电子证书（机构）“互认版”，于倚据证书前请参阅广东省经济和信息化委员会发布的官方信任列表，以确定证书类别是否具互认资格及其有效期。政府资讯科技总监办公室亦会在其信任列表备存有关资料的副本，以供参考(见第 2.2.12 条)。
e) 执行所有适当证书路径认可程序。
f) 于证书有效期届满后，仅公开密码匙还可以在签名验证时继续使用。

2.2 其他规定

香港邮政对登记人及倚据人士之义务

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、承办商及代表香港邮政之核证登记机关向各登记人及倚据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人士承担任何绝对义务。**香港邮政不保证香港邮政、承办商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、承办商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人士、或非登记人的倚据人士，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，各登记人及各倚据人士同意香港邮政、邮政署、及承办商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、承办商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，若登记人或倚据人士因倚据另一登记人由香港邮政所发出之认可证书支援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、承办商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、承办商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，若登记人或倚据人士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、承办商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他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、罢工或暴乱或其他登记人或其他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，登记人仅有权申请发出证书及根据该登记人协议之条款倚据此证书及其他登记人之证书。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他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人士接达之公开储存库内

提供之证书，并非作为对倚据人士供应任何商品；亦不会作为对倚据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；亦不会作为向倚据人士作出供应商品的陈述或保证。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 2.2.3-2.2.4 条所述责任。另外，由香港邮政转让的物品可内载其他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人士、或其他人、或以其他任何方式，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，而登记人或倚据人士（无论作为根据准则或以其他任何方式定义之登记人或倚据人士）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他补救措施：**

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) **本登记人协议及核证作业准则条文；或**
b) **任何谨慎职责－尤其当登记人或倚据人士、或其他人士、或以其他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，而登记人或倚据人士蒙受损失及损害（无论作为根据准则或以其他任何方式定义之登记人或倚据人士），对于任何登记人、或任何倚据人士（无论作为根据准则或以其他任何方式定义之登记人或倚据人士或以任何其他身分），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（伺服器）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、承办商、核证登记机关及各自之人员

无论香港邮政署、承办商或任何核证登记机关或其各自之任何职员、雇员或其他代理人均非登记人协议之签约人，登记人及倚据人士必须向香港邮政承认，就登记人及倚据人士所知，香港邮政署、承办商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、或倚据人士担负任何个人责任或谨慎职责；每一位登记人及倚据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他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：

"香港邮政署职员及承办商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，根据香港法例第 553 章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 www.hongkongpost.gov.hk）。香港特别行政区法律适用于本证书，倚据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、承办商，其各自职员、雇员及代理人）发出本证书，但无须对倚据人士承担任何责任或谨慎职责（准则中列明者除外）。

倚据人士倚据本证书前负责：

a. *只有当倚据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，确定证书之使用及其证明的任何数码签署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或者相关的线上证书状态应答（如适用）；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、承办商、其各自职员、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、香港邮政署承办商、其各自职员、雇员或代理人对倚据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、承办商、其各自职员、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、承办商、其各自职员、雇员或代理人概不对倚据人士就本证书承担任何谨慎职责。

索赔时限
任何倚据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、承办商、其各自职员、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 香港邮政对已获接收但有缺陷之电子证书所承担之责任

尽管上文已列明香港邮政承担责任之限制，若登记人接收证书后发现，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，以便撤销证书及（如愿意接受）重新发出。或倘此通知已于接收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。倘登记人于接收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、承办商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他规则、指引或合约有冲突，登记人、倚据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、承办商或代表香港邮政之任何核证登记机关并非登记人或倚据人士之代理人、受信人、受托人或其他代表。登记人及倚据人士无权以合约或其他方式约束香港邮政、承办商或代表香港邮政之任何核证登记机关承担登记人或倚据人士之代理人、受信人、受托人或其他代表之责任。

2.2.11 相互核证
香港邮政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（伺服器），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。

香港邮政根据本核证作业准则并符合互认证书策略而发出的电子证书（个人）“互认版 " 及 电子证书（机构）“互认版”，则可放弃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 互认证书的互认信任列表
香港邮政已指定电子证书（个人）“互认版 " 及电子证书（机构）“互认版 " 参与 《粤港两地电子签名证书互认办法》下的证书互认计划。有关具互认资格的特定证书类别及这些证书类别的互认识别方法，请参阅广东省经济和信息化委员会发布的官方信任列表，以确定证书类别是否具互认资格及其有效期。政府资讯科技总监办公室亦会在其信任列表备存有关资料的副本，以供参考。

2.2.13 互认证书的免责条款

在遵守本地法律监管要求和互认证书策略的基础上，任何由于香港邮政或电子证书（个人）“互认版 " 或 电子证书（机构）“互认版”的不足或疏忽所引起的责任和索偿，香港邮政、登记人和倚据人士对粤港两地政府和电子认证服务主管部门免责。

2.2.14 有关本核证作业准则与 RFC3647 标准制定电子认证业务规则的内容比较
本核证作业准则与互认证书策略分别根据 RFC2527 和 RFC3647 标准而建构，考虑到登记人、倚据人士和其他相关人士已采用当前格式的核证作业准则了一段长时间，如为按照互认证书策略第四（一）(3) 段中对签发参与《粤港两地电子签名证书互认办法》互认证书计划的电子证书（个人）“互认版 " 和 电子证书（机构）“互认版 " 的要求，而对目前应用的准则格式作出重大修订，可能会令登记人、倚据人士和其他相关人士对本核证作业准则的内容产生混淆。有鉴于此，目前决定提供依据本核证作业准则和 RFC3647 核证作业准则概要的比较表于**附录 I** 以符合相同目的。

2.2.15 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 可分割性、保留、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他条款之可执行性。

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，以英文本为准。唯本准则之任何条文如适用于电子证书（个人）“互认版"或电子证书（机构）“互认版"，其中英文本措词诠释若有歧异，则以繁体中文本为准。

2.4 登记费用

除获得香港邮政豁免，否则一切登记及行政费用须于每一登记使用期(见第 3.2 条)开始前由电子证书登记人付清。如在证书指定有效期内中止登记，香港邮政可暂时吊销或撤销证书（见第 4.6.1.4(f) 条）。香港邮政保留绝对权力， 不时检讨及订定登记及行政费用，并经其网址 http://www.hongkongpost.gov.hk 通知登记人及公众。根据香港邮政及翘晋电子商务有限公司之合约条款，翘晋电子商务有限公司可收取电子证书之登记年费、续期费用及行政费。

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。

每份电子证书（个人）“互认版”的收费如下：

电子证书（个人）“互认版”收费	一年有效期的电子证书	二年有效期的电子证书	三年有效期的电子证书
首次及续期申请	每份电子证书港币 50 元	每份电子证书港币 100 元	每份电子证书港币 150 元
存储介质	每份电子证书可免费载入智能身份证内或付费存放于指定之存储介质中，最新的存储介质价格会在香港邮政网页 http://www.hongkongpost.gov.hk 公布。		

2.4.2 电子证书（机构）

<table>
<tr><th colspan="2">电子证书（机构）收费</th><th>一年有效期的电子证书</th><th>二年有效期的电子证书</th><th>三年有效期的电子证书</th></tr>
<tr><td rowspan="4">不属于
“互认版 "</td><td>首次申请</td><td>每份电子证书
港币 50 元</td><td>每份电子证书
港币 200 元</td><td rowspan="4">不适用</td></tr>
<tr><td>非首次申请或续期</td><td>每份电子证书
港币 150 元</td><td>每份电子证书
港币 300 元</td></tr>
<tr><td></td><td colspan="2">承办商就电子证书（机构）登记费用提供推广折扣优惠，详情请参阅香港邮政网址 http://www.hongkongpost.gov.hk 或经由第 1.3 条所列之途径向香港邮政核证机关作出查询。</td></tr>
<tr><td>行政费
（不论授权用户数目多少）</td><td>每份申请港币 150 元</td><td>每份申请港币 300 元</td></tr>
<tr><td colspan="4">如申请表内包括多个年份的有效期的电子证书申请，行政费是跟据申请中最长年份有效期的电子证书作计算。</td></tr>
<tr><td rowspan="4">“互认版 "</td><td>新申请或续期</td><td>每份电子证书
港币 150 元</td><td>每份电子证书
港币 300 元</td><td>每份电子证书
港币 450 元</td></tr>
<tr><td>行政费
（不论授权用户数目多少）</td><td>每份申请港币 150 元</td><td>每份申请港币 300 元</td><td>每份申请港币 450 元</td></tr>
<tr><td colspan="3">如申请表内包括多个年份的有效期的电子证书申请，行政费是跟据申请中最长年份有效期的电子证书作计算。</td></tr>
<tr><td>存储介质</td><td colspan="3">每份电子证书必须独立存放于指定之存储介质，最新的存储介质价格会在香港邮政网页 http://www.hongkongpost.gov.hk 公布。</td></tr>
</table>

2.4.3 电子证书（伺服器）

<table>
<tr><th>电子证书（伺服器）收费</th><th>一年有效期的电子证书</th><th>二年有效期的电子证书</th><th>三年有效期的电子证书</th></tr>
<tr><td rowspan="2">不属于“通用版 " 或“多域版 " 之新申请或续期</td><td>每份电子证书
港币 2,500 元</td><td>每份电子证书
港币 5,000 元</td><td rowspan="2">不适用</td></tr>
<tr><td colspan="2">承办商就电子证书(伺服器)登记费用提供推广折扣优惠，详情请参阅香港邮政网址 http://www.hongkongpost.gov.hk 或经由第 1.3 条所列之途径向香港邮政核证机关作出查询。</td></tr>
<tr><td rowspan="2">“通用版 " 之新申请或续期</td><td>每份电子证书港币 8,700 元
+ 每个附加伺服器
港币 500 元</td><td>每份电子证书港币 17,400 元
+ 每个附加伺服器
港币 1,000 元</td><td>每份电子证书港币 26,100 元
+ 每个附加伺服器
港币 1,500 元</td></tr>
<tr><td colspan="3">电子证书（伺服器）“通用版”的证书预设在一台伺服器上使用。如需在多台伺服器上使用，必须缴交相关登记费，无论证书于何时在附加伺服器上使用，每个附加伺服器的登记费必须覆盖其电子证书整个有效期。</td></tr>
<tr><td rowspan="2">“多域版 " 之新申请或续期</td><td>每份电子证书港币 3,000 元
+ 每个额外伺服器名称
港币 2,500 元</td><td>每份电子证书港币 6,000 元 +
每个额外伺服器名称
港币 5,000 元</td><td>每份电子证书港币 9,000 元 +
每个额外伺服器名称
港币 7,500 元</td></tr>
<tr><td colspan="3">电子证书（伺服器）“多域版”的证书预设识别一个伺服器名称。如电子证书用于识别多于一个但不多于 50 个伺服器名称，必须缴交相关登记费。</td></tr>
</table>

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	三年有效期的电子证书	四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	每份电子证书 港币 450 元	每份电子证书 港币 600 元
	承办商就电子证书（保密）登记费用提供推广折扣优惠，详情请参阅香港邮政网址 http://www.hongkongpost.gov.hk 或经由第 1.3 条所列之途径向香港邮政核证机关作出查询。			
行政费 （不论授权单位数目多少）	每份申请 港币 150 元	每份申请 港币 300 元	每份申请 港币 450 元	每份申请 港币 600 元
	如申请表内包括多个年份的有效期的电子证书申请，行政费是跟据申请中最长年份有效期的电子证书作计算。			

2.5 公布资料及储存库

根据条例之规定，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、最新的线上证书状态应答，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他资料，包括电子证书申请表及其中包含的《登记人条款及条件》。本准则以及最新版本的《登记人条款及条件》将构成公开的登记人协议以及倚据人士协议。香港邮政会及时发布及更新储存库中有关披露文档和文档以往发布、修订信息的披露记录。除平均每周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。香港邮政会把经由登记人接受并按本准则确认接受的电子证书，尽快在储存库作出公布。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

经授权之香港邮政人士方可进入储存库更新及修改内容。在运行及管理储存库时，香港邮政不会进行任何对倚据储存库（包括证书和其他信息）的人士造成不合理风险的活动。

2.5.3 证书储存库更新周期

每份证书一经登记人接受及发出后，以及如更新证书撤销清单和线上证书状态应答等其他相关情况时，储存库会尽快作出更新。

2.5.4 核准使用证书储存库内的资料

证书储存库内的资料，包括个人资料，会按照条例之规定且在符合方便进行合法电子交易或通讯之目的下作出公布。

2.6 遵守规定之评估

须根据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，检视香港邮政发出、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、资讯、文件或其他物料之香港邮政、承办商、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、不得允许或容受向他人披露载于该等纪录、书刊、纪录册、登记册、通讯、资讯、文件或物料内与另一人有关的任何资料。香港邮政会确保香港邮政、承办商、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资料，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他香港邮政指定之机构处所，并面对面出示第 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）作为身分证明。

电子证书（机构）、电子证书（伺服器）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他香港邮政指定之机构处所，并面对面出示第 3.1.8 条所述身分证明。在电子证书(机构)上列明之授权用户，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并经签署之申请表。电子证书（机构）、电子证书（伺服器）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，说明如何发出证书。

3.1.1 名称类型

3.1.1.1 电子证书（个人）

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)

如不属于电子证书（个人）“互认版 "，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) 登记人机构在有关登记机关之登记名称或香港特别行政区政府各政策局或部门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各政策局或部门，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各政策局或部门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，或该机构之税务局参考编号。

3.1.1.4 电子证书（伺服器）

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

a) 登记人机构在有关登记机关或香港特别行政区政府各政策局或部门之登记名称，又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) 登记人机构所拥有伺服器（包括伺服器的网域名称）之名称。因应香港邮政的酌情权，伺服器名称的完整格式网域名称的最左边部份可为通配符（即星号“*”），亦即证书可用于登记人机构所拥有的同一域名或子域名的所有伺服器名称。

如登记人机构申请电子证书（伺服器）“通用版 " 或“多域版 " ，电子证书（伺服器）将包含主体别名 (Subject Alternative Name)（于**附录 B** 内指明），其中包括于主体名称所指由登记人机构拥有的伺服器名称（包括伺服器的网域名称）。电子证书（伺服器）“通用版 " 之主体别名亦包含一个由登记人机构拥有而不带有通配符部分的伺服器名称。至于电子证书（伺服器）“多域版 " 之主体别名，则可包含额外的伺服器名称，而每个额外伺服器名称必须由该登记人机构拥有。带有通配符（即星号“*”）的额外伺服器名称将不会被接受。

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（保密）登记人机构之身分，该名称由以下资料组成：

a) 登记人机构在有关登记机关之登记名称或香港特别行政区政府各政策局或部门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各政策局或部门，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各政策局或部门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) 登记人机构内授权单位之名称。

3.1.1.6 获授权代表

登记人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（伺服器）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（个人）、电子证书（保密）及电子证书（伺服器）一律只用英文发出。如电子证书（保密）或电子证书（伺服器）之登记人机构仅有中文名称或仅提供其中文名称，该电子证书将不会显示其机构名称。

电子证书（机构）用英文发出，但如登记人机构在申请表格上提供了中文名称，该电子证书将会包含其机构及分行中文名称。如电子证书（机构）之登记人机构仅有中文名称，其机构英文名称将被预设为「***CHINESE NAME ONLY***」。

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载入之登记人名称(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
香港邮政可酌情处理有关名称争议之事宜并享有最终决定权。

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将储存在电子证书储存媒体上，并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（伺服器）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他香港邮政指定之机构处所以面对面的审核方式递交，获授权代表亦须出示其香港身份证或护照。香港邮政可酌情容许申请人提交申请表连获授权代表签署的香港身份证或护照副本，代替获授权代表亲身办理手续，惟须符合 (a) 登记机构在过去提交的申请中已认证该获授权代表的身分，以及该获授权代表曾于该次申请时亲身到指定的香港邮政处所或其他香港邮政指定之机构处所核实身分；及(b)有合理理据再次确认获授权代表的身分，例如经电话与他核实身分或核对他在过去提交的申请表上的签署。香港邮政在有怀疑的情况下，可拒绝有关申请。

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）上的授权用户；
b) 所有按此方式识别身分之授权用户之香港身份证或护照副本。如授权用户并非香港公民，亦可接受其提交有效旅游证件的副本；
c) 由有关香港登记机关发出证明此机构确实存在之文件。有关文件的有效期由提交申请时起计，必须超过一个月。

3.1.8.3 每份电子证书（伺服器）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伺服器证书内的主体名称及主体别名（如有）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。有关文件的有效期由提交申请时起计，必须超过一个月。

3.1.8.4 每份电子证书（保密）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；
b) 由有关香港登记机关发出证明此机构确实存在之文件。有关文件的有效期由提交申请时起计，必须超过一个月。

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或上级人员签署。

3.1.8.6　获发出多于一年有效期电子证书（机构）、电子证书（伺服器）及电子证书（保密）之登记人机构，香港邮政会约于电子证书有效期内每个周年日，再核对登记人机构的存在；及伺服器证书所载网域名称拥有权（就电子证书（伺服器）而言）。如登记人机构的存在或网域名称拥有权（就电子证书（伺服器）而言）未能核实，香港邮政可根据本准则第 4.6 条（暂时吊销及撤销证书）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他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。该前述处所人员将以面对面的审核方式，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。并无持有有效电子证书(个人)之申请人应按上文(a)的程序核实身分。
c) 香港邮政在有怀疑的情况下，可拒绝有关申请。

3.2 电子证书（个人）的登记使用期

3.2.1.　如不属于电子证书（个人）“互认版 "，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。如属于电子证书（个人）“互认版 "，发出的证书有效期为一年、二年或三年（见第 1.2.4 条），登记使用期与其有效期一致，有关延长登记使用期的安排不适用。

3.2.2　如不属于电子证书（个人）“互认版 "，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（见第 4.1 条），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　如不属于电子证书（个人）“互认版 "，为证书延长登记使用期可不须进行身分认证（递交新证书申请时，须对申请人进行身分认证）。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 电子证书（个人）续期

3.3.1 香港邮政会于证书的有效期届满前，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的实际有效期会超过于第 1.2.4 条指明的证书有效期：

如不属于电子证书（个人）“互认版 "

新证书有效期[1]	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
三年	新证书产生日期	原有证书(即须续期的证书）到期日之后三年	新的电子证书的有效期可超过三年,但不会超过三年另一个月

如属于电子证书（个人）“互认版 "

新证书有效期 1	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
三年	新证书产生日期	原有证书(即须续期的证书）到期日之后三年	新的电子证书的有效期可超过三年,但不会超过三年另一个月

3.3.2 透过上文 3.1.9(b)提及的有效数码签署为电子证书(个人)续期，可无需如首次申请般进行认证登记人身分的程序。登记人亦可填妥并签署证书续期申请表送交香港邮政申请续期。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（伺服器）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，向电子证书（机构)、电子证书（伺服器）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 1	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
三年[2]	新证书产生日期	原有证书(即须续期的证书）到期日之后三年	新的电子证书的有效期可超过三年,但不会超过三年另一个月

[1] 见第 1.2.4 条

四年[3]	新证书产生日期	原有证书(即须续期的证书）到期日之后四年	新的电子证书的有效期可超过四年,但不会超过四年另一个月

3.4.2 电子证书（机构)、电子证书（伺服器）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 3.1.8.1 条所述“机构申请人身分认证”之过程进行认证。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他文件以及续期费用，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。

[2] 只适用于电子证书（机构）“互认版 "，电子证书（伺服器）“通用版 " 或“多域版 "，及电子证书（保密）

[3] 只适用于电子证书（保密）

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 根据本核证作业准则发出之电子证书的申请人可于指定香港邮政处所或香港邮政指定的其他机构的处所用香港邮政指定的表格递交申请并完成申请程序。

4.1.1.1.2 如不属于电子证书（个人）“互认版 "，在申请电子证书时，申请人可选择将电子证书及私人密码匙储存在指定的电子证书储存媒体上，除此之外，申请人亦可于指定香港邮政处所同时申请将电子证书及私人密码匙载入智能身份证内。

如属于电子证书（个人）“互认版 "，在申请电子证书时，申请人只可选择将电子证书及私人密码匙储存在指定的 PKCS#11 兼容的电子证书储存媒体上，或是选择于指定香港邮政处所申请将电子证书及私人密码匙载入智能身份证内。

4.1.1.1.3 如不属于电子证书（个人）“互认版 "，申请人可于递交电子证书申请表时，要求额外一份电子证书及私人密码匙的副本，此副本可被逐一储存于由申请人所提供的替代储存媒体上。如香港邮政认为该要求可以接受，则此电子证书及私人密码匙副本会被逐一储存于替代储存媒体上。第 4.1.2 条所述程序适用于此电子证书及私人密码匙副本，尤其是此电子证书及私人密码匙副本会受电子证书个人密码所保护，并以安全方式交付予申请人。

4.1.1.1.4 香港邮政对所有用于存储私人密码匙的存储介质的预备、启动、使用、分派及终止使用均制定有内部程序及控制措施，并定期经独立第三方审核。

4.1.1.1.5 电子证书申请表一经递交，申请人即批准香港邮政向其他人士或在香港邮政储存库公布其电子证书，并接受香港邮政将发给申请人的电子证书。

4.1.1.2 核对身分

4.1.1.2.1 正如第 3.1.9(a)条所述，申请人须于指定香港邮政处所或香港邮政指定的其他机构的处所，向香港邮政职员或其代理人出示其香港身份证，以核对身分。完成核对身分手续后，申请人会收到一个电子证书「个人密码信封」。

4.1.1.2.2 每份载入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。

4.1.2 发出及公布电子证书（个人）

4.1.2.1 在指定香港邮政处所发出电子证书（个人）并载入智能身份证内

4.1.2.1.1 申请人若持有可载入 2048 位元 RSA 密码匙长度的电子证书的智能身份证，并选择将

电子证书及私人密码匙载入其智能身份证内（见第 4.1.1.1.2 条），可于指定香港邮政处所（位置刊登于香港邮政网址 http://www.hongkongpost.gov.hk），经以下程序办理申请电子证书及将一份证书及私人密码匙载入其智能身份证内：

a) 申请人根据第 4.1.1.1 及 4.1.1.2 条所述程序递交申请表、完成核对身分及领取密码信封；

b) 香港邮政职员或其代理人会使用电脑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) 拟产生的电子证书内容会在显示屏上展示，以便申请人核实；

d) 如申请人确认将载入电子证书内其个人资料的准确度，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载入智能身份证内。载入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。如申请人拒绝确认将载入电子证书内的个人资料，其智能身份证将不会载入电子证书及私人密码匙；

e) 当上述程序完成后，该智能身份证会即时交回申请人；

f) 如不属于电子证书（个人）“互认版 "，私人密码匙及证书将随后被存储在申请人所选择的电子证书储存媒体及替代储存媒体（若有的话）上。每份载入电子证书储存媒体及替代储存媒体（若有的话）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。电子证书储存媒体及替代储存媒体（若有的话）会密封于一可防止改动的封套或其他容器内；并以安全方式交付予申请人，例如挂号邮件；

g) 已获接受并已发出的电子证书会在香港邮政储存库内公布。

4.1.2.2 发出电子证书并载入电子证书储存媒体及替代储存媒体内

4.1.2.2.1 申请人可于指定香港邮政处所或其他已获香港邮政指定之机构处所，经以下程序办理申请电子证书后，经邮递方式领取存储在电子证书储存媒体及替代储存媒体（若有的话）内的电子证书：

a) 申请人于指定香港邮政处所或其他已获香港邮政指定之机构处所，如第 3.1.9(a)条所述，向香港邮政职员或其代理人出示其香港身份证，以核对身分。完成核对身分手续后，申请人会收到一个电子证书「个人密码信封」；

b) 在核对身分手续后，香港邮政会在其处所内之稳当系统及环境下产生申请人之电子证书（包括配对密码匙），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申请人所选择的电子证书储存媒体及替代储存媒体（若有的话）上。每份载入电子证书储存媒体及替代储存媒体（若有的话）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。电子证书储存媒体及替代储存媒体（若有的话）会密封于一可防止改动的封套或其他容器内；并以安全方式交付予申请人，例如挂号邮件；

d) 已获接受并已发出的电子证书会在香港邮政储存库内公布。

4.1.2.3 私人密码匙

4.1.2.3.1 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，申请人应该保存电子证书储存媒体及替代储存媒体（若有的话）内的电子证书及私人密码匙作为备份。

4.1.2.3.2 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。

4.1.2.4 核实证书资料

申请人可浏览证书档案或经香港邮政储存库核实证书资料。申请人亦可使用适当的智能卡阅读器核实存于智能身份证内的电子证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

4.2 电子证书（机构）

4.2.1 证书申请

4.2.1.1 处理申请

4.2.1.1.1 电子证书（机构）之申请人须到指定之香港邮政处所或其他香港邮政指定之机构处所递交申请表格，包括按香港邮政要求之附加申请表格，连同申请书内列明的其他文件以及登记费用，一并交回。

4.2.1.1.2 如不属于电子证书（机构）“互认版 "，在申请电子证书时，申请人可选择将电子证书及私人密码匙储存在指定的电子证书储存媒体上。申请人可于递交电子证书申请表时，要求额外一份电子证书及私人密码匙的副本，此副本可被逐一储存于由申请人所提供的替代储存媒体上。如香港邮政认为该要求可以接受，则此电子证书及私人密码匙副本会被逐一储存于替代储存媒体上。第 4.2.2 条所述程序适用于此电子证书及私人密码匙副本，尤其是此电子证书及私人密码匙副本会受电子证书个人密码所保护，并以安全方式交付予申请人。

但如属于电子证书（机构）“互认版 "，在申请电子证书时，申请人只可选择将电子证书及私人密码匙储存在指定的 PKCS#11 兼容的电子证书储存媒体上。

4.2.1.1.3 香港邮政对所有用于存储私人密码匙的存储介质的预备、启动、使用、分派及终止使用均制定有内部程序及控制措施，并定期经独立第三方审核。

4.2.1.1.4 电子证书申请表一经递交，申请人即批准香港邮政向其他人士或在香港邮政储存库公布其电子证书，并接受香港邮政将发给申请人的电子证书。

4.2.1.2 核对身分

用以证明登记人机构、获授权代表及授权用户身分之文件，于本准则第 3.1.8 条说明。电子证书「密码信封」将于获授权代表在指定之香港邮政处所提交申请表时当面接收， 或于完成核对身分手续后，以安全方式交付予获授权代表，例如挂号邮件。

4.2.2 发出证书

4.2.2.1 在核对身分手续后，香港邮政会在其处所内之稳当系统及环境下产生申请人之电子证书（包括配对密码匙），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申请人所选择的电子证书储存媒体及替代储存媒体（若有的话）上。电子证书储存媒体及替代储存媒体（若有的话）会密封于一可防止改动的封套或其他容器内；并以安全方式交付予申请人，例如挂号邮件。

4.2.2.3 登记人机构同意，他们一旦接获电子证书储存媒体及替代储存媒体（若有的话），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 公布电子证书

根据《电子交易条例》的规定，香港邮政会尽快在储存库公布已获接受并已发出的电子证书（见第 2.5 条）。申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

4.3 电子证书（保密）

4.3.1 证书申请

4.3.1.1 处理申请

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

4.3.1.1.2 在申请电子证书时，申请人可选择将电子证书及私人密码匙储存在指定的电子证书储存媒体上。申请人可于递交电子证书申请表时，要求额外一份电子证书及私人密码匙的副本，此副本可被逐一储存于由申请人所提供的替代储存媒体上。如香港邮政认为该要求可以接受，则此电子证书及私人密码匙副本会被逐一储存于替代储存媒体上。第 4.3.2 条所述程序适用于此电子证书及私人密码匙副本，尤其是此电子证书及私人密码匙副本会受电子证书个人密码所保护，并以安全方式交付予申请人。

4.3.1.1.3 电子证书申请表一经递交，申请人即批准香港邮政向其他人士或在香港邮政储存库公布其电子证书，并接受香港邮政将发给申请人的电子证书。

4.3.1.2 核对身分

用以证明登记人机构、获授权代表及授权用户身分之文件，于本准则第 3.1.8 条说明。电子证书「密码信封」将于获授权代表在指定之香港邮政处所提交申请表时当面接收， 或于完成核对身分手续后，以安全方式交付予获授权代表，例如挂号邮件。

4.3.2 发出证书

4.3.2.1 在核对身分手续后，香港邮政会在其处所内之稳当系统及环境下产生申请人之电子证书（包括配对密码匙），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申请人所选择的电子证书储存媒体及替代储存媒体（若有的话）上。电子证书储存媒体及替代储存媒体（若有的话）会密封于一可防止改动的封套或其他容器内；并以安全方式交付予登记人，例如挂号邮件。

4.3.2.3 登记人机构同意，他们一旦接获电子证书储存媒体及替代储存媒体（若有的话），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 公布电子证书

根据《电子交易条例》的规定，香港邮政会尽快在储存库公布已获接受并已发出的电子证书（见第 2.5 条）。申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

4.4 电子证书（伺服器）

4.4.1 证书申请

4.4.1.1 处理申请

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

4.4.1.1.2 电子证书申请表一经递交，申请人即批准香港邮政向其他人士或在香港邮政储存库公布其电子证书，并接受香港邮政将发给申请人的电子证书。

4.4.1.2 核对身分

用以证明登记人机构、获授权代表及授权用户身分之文件，于本准则第 3.1.8 条说明。香港邮政不会复核证书内用于识别其域名的核证机关授权记录。电子证书「密码信封」将于获授权代表在指定之香港邮政处所提交申请表时当面接收， 或于完成核对身分手续后，以安全方式交付予获授权代表，例如挂号邮件。

4.4.1.3　网域授权或控制的确认

为依循核证机关 / 浏览器论坛基线要求 (CA / Browser Forum Baseline Requirements, (BR)) 对确认网域授权的责任要求，香港邮政确定在发出电子证书 (伺服器)当日使用以下一个或多个程序以确认申请人对每个列于电子证书 (伺服器)的网域名称(Fully-Qualified Domain Name (“FQDN”))之拥有权或控制权:

a) 按域名注册机构提供的邮寄地址、电邮地址或电话号码直接与域名登记人联络，以获取确认申请人申请电子证书之答复，来进行 FQDN 之核证 (即 BR 3.2.2.4.2 及 BR 3.2.2.4.3 预留部分) ;
b) 直接以新组合的电邮地址与域名登记人联络以进行核证，新组合电邮地址的区域部份以 ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’ 或 ‘postmaster’ 为开始，跟着是 “@” 符号，随后为删除了零字符或其他字符的申请网域名称；(即 BR 3.2.2.4.4 预留部分); 或
c) 依据域名注册机构的公开记录，例如 WHOIS 或其他 DNS 的记录资料 (即 BR 3.2.2.4.5)。

4.4.2 发出及公布证书

4.4.2.1　在核对身分手续后，香港邮政会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」经由香港邮政位于 http://www.hongkongpost.gov.hk 的指定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) 申请人于香港邮政位于 http://www.hongkongpost.gov.hk 的指定网页核对和确认电子证书的内容是否准确。如申请人拒绝接受电子证书，香港邮政会撤销该电子证书。已获接受并已发出的电子证书将传送给申请人，并根据《电子交易条例》的规定在香港邮政储存库公布。
f) 申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

4.5 证书申请的处理期限

香港邮政将作出合理努力，确保在合理的时间内完成证书申请。在登记人提交的证书申请资料齐全并且符合要求的情况下，香港邮政承诺完成证书申请时间如下：

证书类别	完成证书申请时间
电子证书（个人）	三个工作天
电子证书（个人）“互认版 "	
电子证书（机构）	

证书类别	完成证书申请时间
电子证书（机构）“互认版 "	十个工作天
电子证书（保密）	
电子证书（伺服器）	
电子证书（伺服器）“通用版 " 或“多域版 "	

特此声明，星期六、星期日、公众假期及悬挂八号或以上之热带气旋警告信号或黑色暴雨警告信号之工作日，就此 4.5 条而言，一律不视作工作日计算。

4.6 暂时吊销及撤销证书

4.6.1 暂时吊销及撤销

4.6.1.1 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，香港邮政会根据在密码匙资料外泄计划内定明的程序迅速地撤销所有已发出的登记人证书（见第 4.11.2 条）。

4.6.1.2 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。

4.6.1.3 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储存媒体，若已外泄或怀疑已外泄，或电子证书上由登记人提供之资料有任何改变，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 2.1.4(h) 条）。

4.6.1.4 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电子邮件（证书撤销通知书（如有电子邮件地址））及透过更新证书撤销清单或线上证书状态应答（如适用）的方式通知登记人：

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）上指明之授权用户已非登记人机构之成员或雇员；
i) 知道或有理由相信由电子证书（伺服器）的主体名称或主体别名（如有）所识别的任何伺服器名称已非由登记人机构拥有；或
j) 知道或有理由相信其资料出现在电子证书（机构）、电子证书（伺服器）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；
(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；或
(v) 无法证明登记人之存在。

4.6.1.5 香港邮政将严格控制，作出合理努力避免由于证书制作过程中的失误（例如证书下载错误、密码匙不匹配）而导致证书吊销。

4.6.2 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验证该请求及其原因并在确认无误后暂时吊销证书。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，该证书即会被撤销且永久失效。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正本。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。如果证书支持线上证书状态通讯规约，该证书的线上证书状态应答也将保持撤销状态。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）将刊载于证书撤销清单内。（见第 7.2 条）。针对支持线上证书状态通讯规约的证书，其附有原因代码的证书状态将包括在个别证书的线上证书状态应答之中（见第 73 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，而且在相关证书的线上证书状态应答中的证书状态将会回复有效。

香港邮政核证机关处理以传真、邮寄信件、电子邮件或亲身递交的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	：	暂停服务

如悬挂八号或以上之热带气旋警告信号或黑色暴雨警告信号，将立即暂停处理撤销证书要求。如在该日早上六时或以前信号除下，处理撤销证书要求会于上述办公时间恢复；如信号在早上六时至十时正之间除下，处理撤销证书要求将于该日（周六、周日或公众假期除外）下午二时恢复。如信号在上午十时后除下，处理撤销证书要求将于下一个工作日的办公时间（周六、周日或公众假期除外）恢复。

4.6.3 服务承诺、证书撤销清单及线上证书状态应答的更新

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证书申请或撤销证书的

最后确认或 (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资料于证书撤销清单公布。就所有符合互认证书策略的“互认版 " 电子证书而言，处理时间会缩短为一个工作日。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。如果证书支持线上证书状态通讯规约，该证书的线上证书状态应答将于下一份证书撤销清单更新和公布同时被更新。证书撤销清单每日公布，并存档最少七年。

特此声明，星期六、星期日、公众假期及悬挂八号或以上之热带气旋警告信号或黑色暴雨警告信号之工作日，就此 4.6.3（a）条而言，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两个工作天内，透过电子邮件（如有电子邮件地址）及更新证书撤销清单和相关的线上证书状态应答的方式向有关登记人发出撤销证书通知。就所有符合互认证书策略的“互认版 " 电子证书而言，处理时间会缩短为一个工作天。

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人士承担责任。

c) 此外，登记人明知香港邮政根据准则可能据以撤销证书之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，故倚据人士不得就交易而倚据证书。若登记人未能通知倚据人士，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(根据申请或其他原因)之决定与此资讯出现于证书撤销清单之间，或者就作出暂时吊销或撤销证书之决定与更新相关的线上证书状态应答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他部分规限之范畴。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人士负责。

d) 当电子认证服务机构本身的证书被暂时吊销或撤销时，香港邮政将及时发布有关信息(包括证书撤销清单（如香港邮政授权撤销清单 ARL 及相关的线上证书状态应答（如适用））。

e) 证书撤销清单、香港邮政授权撤销清单 ARL 以及线上证书状态应答会依据在**附录 C** 内指明的时间表及格式更新及公布。补充证书撤销清单会在特殊的情况下于香港邮政网页 http://www.hongkongpost.gov.hk 公布。

f) 有关香港邮政对于倚据人士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 2.1.6 条(倚据人士之义务)及 2.2.1 条(合理技术及谨慎)。

4.6.4 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，而线上证书状态通讯

规约只是提供一个替代证书撤销清单的方法。如智能身份证已载入已暂时吊销或已撤销的电子证书(个人)，登记人可继续将该证书存于智能身份证内，或前往指定邮政局要求移除。

4.7 证书登记使用期的结束

以下三种情况将被视为证书登记使用期结束

a) 在证书有效期内，证书被香港邮政撤销；
b) 在证书到期前提出终止服务的申请，并获香港邮政接受；
c) 证书有效期满，没有进行证书更新或密码匙更新。

香港邮政已备有明确关于证书订购结束的规定，指导证书订购结束的具体实施流程，并妥善保存记录至第 4.9.2 条指定之最短之时限。

4.8 电脑保安审核程序

4.8.1 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资料
  - 签署线上证书状态应答
  - 核证机关密码匙转换
  - 档案备存
  - 紧急密码匙复原

4.8.2 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。

4.8.3 审核纪录之存留期间

存档审核纪录文档存留期为七年。

4.8.4 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。

4.8.5 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。

4.8.6 审核资料收集系统
香港邮政核证机关系统审核纪录及文档受自动审核收集系统控制，该收集系统不能为任何应用程式、程序或其他系统程式修改。任何对审核收集系统之修改本身即成为可审核事件。

4.8.7 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。

4.8.8 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。

4.9 纪录存档

4.9.1 存档纪录类型
香港邮政须确保存档纪录记下足够资料，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，及线上证书状态应答
- 定期事件纪录
- 其他需用以核实存档内容之数据
- 证书系统建设和升级文档；
- 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；
- 审计记录；
- 员工资料，包括但不限于背景调查、录用、培训等资料；
- 各类外部、内部评估文档。

4.9.2 存档保存期限
密码匙及证书资料以及 4.9.1 中提及之存档须妥为保存最少七年。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。

4.9.3 存档保护
香港邮政保存之存档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档媒体免受温度、湿度及磁场等环境侵害。

4.9.4 存档备份程序
在有需要时制作并保存存档之副本。归档时，须对归档记录的一致性进行验证。归档期间，须通过适当的技术或方法验证所有被访问的记录的一致性。

4.9.5 电子邮戳
存档资料均注明开设存档项目之时间及日期。香港邮政利用控制措施防止擅自调校自动系统时钟。

4.10 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有效期为不超过二十年（见**附录 G**）。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，相应之根源证书会在香港邮政网页 http://www.hongkongpost.gov.hk 公布供大众取用。原先之根源密码匙则保留至第 4.9.2 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。确保整个过渡过程安全、顺利，并力求减少对登记人和倚据人士的影响。

4.11 灾难复原及密码匙资料外泄之应变计划

4.11.1 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资讯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核证机关全面恢复提供服务，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要营运设施不少于十千米。业务持续运作计划每年均会检讨及进行演练，而有关主要人员均须参与，并对演练程序和结果进行记录。

如发生严重故障或灾难，香港邮政会即时知会政府资讯科技总监，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他临时设施内；及
c) 设施的出入通道会实施接达管制，以防范盗窃及被人擅自接达。

4.11.2 密码匙资料外泄之应变计划

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，香港邮政会即时知会政府资讯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，香港邮政会即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，并且在合理的时间内采用适当的方式及时通知登记人和倚据人士。

4.11.3 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资讯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。香港邮政核证机关根源证书的撤销请求，必须经过政府资讯科技总监确定后才可以进行。

4.11.4 计算机资源、软件和/或数据的损坏

业务持续运作计划内包含计算资源、软件和/或数据的损坏之正式程序。此等有关程序每年均会检讨及进行演练。

当发生计算机资源、软件和/或数据的损坏，香港邮政将评估事件的影响，调查原因，根据系统

内部备份的资料，执行系统恢复操作，使认证系统能够重新正常运行。倘若在计算机资源、软件和/或数据损坏的情况下，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资讯科技总监并作出公布。倘若在计算机资源、软件和/或数据损坏的情况下，香港邮政为登记人代制的私人密码匙资料外泄或遭破坏而无法复原，香港邮政会即时撤销有关证书，然后发出新证书取代，并且在合理的时间内采用适当的方式及时通知登记人和倚据人士。

4.12 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”所定程序知会政府资讯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档七年（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。

4.13 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 4.12 条）停止担任核证登记机关之职能，或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，分为不同的安全区域，并根据不同区域的物理安全要求，采取有效的物理安全控制措施以确保该区域的物理安全。同时，香港邮政对每一级物理安全层的访问都必须是可审计和可控的，从而保证每一级物理安全层的访问都只有获授权的人员才可以进行。

这些安全控制措施限制了进入就提供香港邮政核证机关服务而使用之硬件及软件（包括核证机关伺服器、工作站及任何外部加密硬件模组或受香港邮政控制之权标），而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用人手或电子方法监控，以防发生未经授权入侵。门禁系统设有进出时间记录和超时报警提示，并定期对记录进行整理归档，进出时间记录将被保留 6 个月。

5.1.3 机房环境控制

具备机房环境监控系统，对基础设施设备、机房环境状况、安防系统状况进行 每周 7 天和每天 24 小时的实时监测，监测记录将被保留 6 个月，以满足故障诊断、事后审计的需要。

5.1.4 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。

5.1.5 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。

5.1.6 防火及防水处理
核证机关设施备妥防火计划及灭火系统。火灾防护措施符合香港消防处的要求。机房设置火灾自动报警系统和自动灭火系统，设置两种火灾探测器以检测温度和烟雾，火灾报警系统与灭火系统联动。核证机关亦已制定相应的处理程序以防止水灾或漏水对系统造成损害及其它不利后果。

5.1.7 媒体存储
媒体存储及处置程序已经开发备妥。

5.1.8 场外备存
香港邮政已建立关键系统（包括香港邮政核证系统）和数据（包括审计数据在内的任何敏感信息）的备份制度及作场外储存，并获足够保护，以免被盗用、损毁及媒体衰变。（另见第 4.11.1 条）

5.1.9 保管印刷文件
印刷文件包括登记人协议及身分确认文件之影印本由香港邮政、承办商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。

5.1.10 废物处理
香港邮政将谨慎处理包含隐私或者敏感信息的任何废弃物，保证对此类废弃物进行彻底的物理销毁或信息清除，避免这类废物中包含的隐私或敏感信息被非授权使用、访问或披露。

5.2 程序控制

5.2.1 受信职责
可进入或控制密码技术或其他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资料库之受限制运作）之香港邮政、承办商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。根据工作性质和职位权限的情况，赋予在承担受信职责之人员在系统和物理环境中的权限，采用合适的访问控制技术，以完整地记录该人员所有敏感的操作行为。

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
- 采取职责分离措施

5.2.2 香港邮政、承办商与核证登记机关之间的文件及资料传递
香港邮政、承办商与核证登记机关之间的所有文件及资料的传递，均使用香港邮政所惯常规定在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程序控制之规定。（见第 2.6 条）

5.3 人员控制

5.3.1 背景及资格
香港邮政及承办商采用之人员及管理政策可合理确保香港邮政、承办商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当面调查（其受聘前及其后有需要时定期进行并要求被调查人提供有效身份证件），及 / 或香港邮政要求承办商及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。此外，在员工合同内已加入与安全相关的条款，在有关的人员在受聘前必须同意并签署。

5.3.3 培训要求
香港邮政及承办商及核证登记机关确保其所有人员（包括充当可信角色的人员）具备所需的技术资格和专业知识，以便能够有效地履行职责，同时须为其员工提供适当及足够的培训（核心岗位至少每年一次），以确保他们执行任务的能力和安全策略得以有效的推行和遵守。综合培训内容包括但不限于：

a) 适当的技术培训；
b) 规章制度和程序；
c) 处理安全事故及通知高层管理人员有关重大安全事故的程序。

5.3.4 在职人员的工作考察
香港邮政及承办商及核证登记机关确保制定适当的控制措施以考察人员的表现，例如：

a) 定期进行的工作绩效考核；
b) 正规的纪律程序（其中包括如何处置未获授权的行为）；
c) 正规的终止服务程序。

5.3.5 向人员提供之文件
香港邮政及承办商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他软件功能。

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（伺服器）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 位元 RSA。登记人配对密码匙为 2048 位元 RSA。

6.1.5 加密模组标准

香港邮政进行之产生签署密码匙、存储及签署操作在硬件加密模组进行。

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）之密码匙可用于数码签署以及加密电子通讯。电子证书（伺服器）之密码匙只可用于加密电子通讯以及伺服器验证。如电子证书（伺服器）内之数码签署密码匙使用方法（于**附录 B** 内指明）有被启用，电子证书（伺服器）之数码签署只可用于伺服器验证以及与伺服器建立安全通讯通道。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、(b)证书撤销清单及(c)线上证书状态通讯规约签署人的证书。

6.2 私人密码匙保护

6.2.1 加密模组标准

香港邮政私人密码匙利用加密模组产生，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（3 选 2 多人控制）启动、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私人密码匙托管程序。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启动。其他私人密码匙均不设备存。所有私人密码匙不会存档。

6.2.5 私人密码匙于密码模组之间传递

当香港邮政私人密码匙从一个硬件加密模组传递到另一个硬件加密模组上时，该私人密码匙会以加密的形式在模组之间传递，并且在传递前要进行模组间的相互身份鉴别。另外香港邮政还有严格的管理流程对私人密码匙的传递进行控制，以确保有效防止了私人密码匙的丢失、被窃、修改、非授权的使用或泄露。

6.3 配对密码匙管理其他范畴

香港邮政之核证机关密码匙使用期不超过二十年（见第 4.10 条）。所有香港邮政密码匙之产生、销毁、储存以及证书、撤销清单签署运作程序以及线上证书状态通讯规约签署运作程序，均于硬件加密模组内进行。第 4.9 条详述香港邮政公开密码匙纪录存档之工作。

6.4 电脑保安控制

香港邮政实行多人控制措施，控制启动数据（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，确保电子认证服务机构软件和存储数据文件的系统是安全、可信赖的系统，不会受到未经授权的内部和外部访问。此等保安控制措施接受第 2.6 条遵守规定之评估。香港邮政实行严格的管理体系来控制和监视运行系统，以防止未授权的修改。在处理废旧设备时，香港邮政将尽合理努力，清除所有可能影响认证业务安全性的信息存储并加以确认。

6.5 生命周期技术保安控制

香港邮政制定控制程序，为香港邮政核证机关系统购置及发展软件及硬件。并已定下更改控制程序以控制并监察就有关系统部件所作的调整及改善。
这些程序及措施的内容包括但不限于：

a) 无论由电子认证服务机构人员或在特殊情况下由其它机构进行开发工作，均能使用一致和有效的内部标准；
b) 将生产及开发的环境分隔开的有效程序；
c) 将操作、运维、开发人员的职责得以区分的有效程序；
d) 对用于生产及开发的环境内的资料及系统进行有效访问的控制措施；
e) 对变更控制程序（包括但不限于系统和数据的正常和紧急变更）的有效控制措施（包括但不限于版本的控制、严格的测试验证等）；
f) 系统上线前进行安全性的检查和评估的程序，检查和评估内容包括有否安全漏洞和被入侵

的危险等；

g) 对采购设备及服务进行妥善管理的有效程序；

h) 硬件密码匙设备的生命周期（从设备开始运作到逻辑/物理销毁）过程中，对该设备的访问至少有 3 名可信人员共同参与。

6.6 网络保安控制

香港邮政核证机关系统采用多级防火墙、入侵检测、安全审计、病毒防范系统及其他接达控制机制来保护电子认证服务机构网络环境的安全，适时更新版本，定期针对网络环境进行风险评估和审计，以检测有否被入侵的危险，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，尽可能降低来自网络的风险。

6.7 加密模组工程控制

香港邮政使用之加密装置至少达到 FIPS140-1 第 2 级。

7. 证书、证书撤销清单及线上证书状态应答结构

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**）。

7.3 线上证书状态应答结构

香港邮政线上证书状态应答符合 RFC6960 和 RFC5019（见**附录 C**）。

8. 准则管理

本准则之更改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，更改即时生效，并对当时及之后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，香港邮政会在实际可行的情况下尽快通知政府资讯科技总监。申请人、登记人及倚据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资讯是准确的；
   (ii) (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) 以其他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资讯是准确的；
   (ii) 批准将该证书向他人公布或在某储存库内公布；或
   (iii) 以其他方式显示承认该证书；”；

“替代储存媒体” 指一种储存媒体，例如软磁碟、可录光碟、USB 记忆体及/或 PKCS#11 兼容装置，可储存一份额外的电子证书及私人密码匙。

“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。成员则指已经与该登记人机构以某种形式维持合法关系的人。

“授权撤销清单” 列举获根源证书在已授权的中继证书原定到期时间前宣布无效之公开密码匙中继证书之资料。

“核证机关/ 浏览器论坛基线要求”指核证机关/浏览器论坛(CA / Browser Forum)在 https://cabforum.org 中发布，有关发行和管理公开可信证书的基线要求。

“核证机关”指向他人(可以为另一核证机关)发出证书者。

“核证机关授权记录”指一种核证机关授权域名系统资源记录，使得域名拥有者可以指定认可的核证机关为该域名颁发证书。

“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他主要特征；
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) 经发出纪录的核证机关签署。

“核证作业准则”或**“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（或其他类别证书）之资料。

“合约”指香港邮政所批出之香港邮政核证机关的外判合约，以委任承办商于 2012 年 4 月 1 日至 2018 年 3 月 31 日期间根据本作业准则营运及维持香港邮政核证机关之服务及系统。

“承办商”指翘晋电子商务有限公司及其合约分判商（列载于**附录 F**，若有的话）。其为香港邮政根据认可核证机关业务守则第 3.2 段所委任之代理人，根据合约条款，为香港邮政营运及维持香港邮政核证机关之服务及系统。

“对应”就私人或公开密码匙而言，指属同一配对密码匙。

“业务守则”指由政府资讯科技总监在条例第 33 条下颁布之认可核证机关业务守则。

“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。

“域名登记人” 指对域名有控制使用权的个人或机构。

“域名注册机构” 指负责域名注册的个人或机构，支持或参与以下协定: (i) 网际网路名称与数字地址分配机构 (ICANN)，(ii) 国家域名管理/注册局，或 (iii) 网路资讯中心（包括其分支机构、 承办商、 代表、 继任者或委托人）。

“电子证书档案卡” 为一张智能卡，是储存电子证书的储存媒体。

“电子证书档案 USB” 为一种 USB 快闪记忆体，是储存电子证书的储存媒体。最新的电子证书档案 USB 价格会在香港邮政网页 http://www.hongkongpost.gov.hk 公布。

“电子证书储存媒体”指一种储存媒体，例如电子证书档案卡或电子证书档案 USB，用于储存电子证书及私人密码匙。

“电子纪录”指资讯系统产生之数码形式之纪录，而该纪录：
(a) 能在资讯系统内传送或由一个资讯系统传送至另一个资讯系统；并
(b) 能储存在资讯系统或其他媒介内。

“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、数目字或其他符号，而该等字母、字样、数目字或其他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。

“资讯”包括资料、文字、影像、声音编码、电脑程式、软件及资料库。

“资讯系统”指符合以下所有说明之系统：
(a) 处理资讯；
(b) 纪录资讯；
(c) 能用作使资讯纪录或储存在不论位于何处之资讯系统内，或能用作将资讯在该等系统内以其他方式处理；及
(d) 能用作检索资讯(不论该等资讯纪录或储存在该系统内或在不论位于何处之资讯系统内) 。

“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，或就该纪录提供其他附带服务者。

“税务局参考编号 " 指税务局根据《税务条例》(第 112 章)向申报财务机构提供的参考编号。税务局参考编号会于税务局向申报财务机构发出的证明文件内提供。

“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资讯，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资讯，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。

“互认证书策略” 指香港与广东省两地政府颁布的《粤港两地电子签名证书互认办法》下的《粤港电子签名证书互认证书策略》。

“多域版" 就一张电子证书（伺服器）而言，指在证书主体别名内列出额外伺服器名称，使证书可用于多个伺服器名称之特点。

“互认版" 就一张电子证书（个人）或电子证书（机构）而言，指该证书符合香港与广东省两地政府颁布的《粤港电子签名证书互认证书策略 》，使证书可用于粤港两地跨境应用。

“OCSP” 指线上证书状态通讯规约。

“线上证书状态通讯规约” 指一种线上证书核对规约，允许倚据人士查明电子证书的状态。

“条例” 指香港法例第 553 章《电子交易条例》。

“个人密码” 指用于保护授权用户的电子证书及其私人密码匙的密码。

“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。

“PKCS#11 兼容装置” 指一种装置（例如智能卡），除可储存电子证书及支援加密功能外，亦符合由 RSA 实验室公布的公开密码匙加密标准 (PKCS)中第 11 项有关加密装置介面标准的规格，而该装置应获得 FIPS 140-2 第二级或以上的认证。

“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） 根据电子交易条例第 22 条认可之证书；
（b） 属根据电子交易条例第 22 条认可之证书之类型、类别或种类之证书；或
（c） 电子交易条例第 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” 指根据电子交易条例第 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、储存或以其他方式固定之资讯，亦指储存在电子或其他媒界可藉理解形式还原之资讯。

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

“倚据人士”，即依赖方，指证书的接收者，依赖于该证书和（或）该证书所验证的电子签名。

“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他与证书有关资讯之资讯系统。

“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” 指可将电子证书载入其中的**身份证**。

“中继证书” 指由根源证书"Hongkong Post Root CA 1"所签发的中继核证机关证书，并用于签发香港邮政认可证书。

“合约分判商” 指受翘晋电子商务有限公司委任的机构，执行合约中的部份工作。

“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，该机构为合资格并获发出电子证书之机构。

“稳当系统”指符合以下所有条件之电脑硬体、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。

“通用版" 就一张电子证书（伺服器）而言，指在证书所载之伺服器名称的完整格式网域名称的最左边部份指定为通配符（即星号“*”），使证书可用于登记人机构所拥有的同一域名或子域名的所有伺服器名称。

“主体名称”指证书持有者名字的信息。

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

本附录详述由中继证书"Hongkong Post e-Cert CA 1 - 10"、"Hongkong Post e-Cert CA 1-14"及"Hongkong Post e-Cert CA 1-15"根据本核证作业准则签发的电子证书格式。如欲了解由香港邮政其他中继证书或根据其他核证作业准则签发的电子证书格式，请根据电子证书上的发出日期或「证书政策」内的物件识别码，查阅相关版本的核证作业准则。

1) 电子证书（个人）格式

栏位名称		栏位内容		
		电子证书（个人）	电子证书（个人）“互认版”	发出予未满18岁人仕的电子证书（个人）
标准栏 (Standard fields)				
版本 (Version)		X.509 V3		
序号 (Serial number)		[由香港邮政系统设置的三位元组十六进制数字]		
签署算式识别 (Signature algorithm ID)		sha1RSA		
发出人 (Issuer)		cn=Hongkong Post e-Cert CA 1 – 10 o=Hongkong Post c=HK		
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政系统设置的UTC 时间]		
	不迟于 (Not after)	[由香港邮政系统设置的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
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元		
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		
标准延伸栏位 (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]		
密码匙使用方法 (Key usage)		不可否认，数码签署，密码匙加密 **（此栏为“关键”栏位）**	不可否认，数码签署 **（此栏为“关键”栏位）**	不可否认，数码签署，密码匙加密 **（此栏为“关键”栏位）**

栏位名称		栏位内容		
		电子证书（个人）	电子证书（个人）“互认版”	发出予未满18岁人仕的电子证书（个人）
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 6） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]	Policy Identifier = [物件识别码]（附注 6） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL] Policy Identifier =2.16.344.8.2.2008.810.2.2012.1.0（附注 7） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL] Policy Identifier = 1.3.6.1.4.1.16030.1.4（附注 8） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]	Policy Identifier = [物件识别码]（附注 6） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]
主体别名 (Subject alternative name)	DNS	[经加密的香港身份证号码]（附注9）		
	rfc822	[证书持有人电子邮箱地址]（附注2）		
发出人别名 (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 constraint)	无		
延伸密码匙使用方法 (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10）		
Netscape 延伸栏位 (Netscape extension)（附注5）				
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME		
Netscape SSL伺服器名称 (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. 申请人所提供的电子邮箱地址（如没有电子邮箱地址，此栏将会留空），该电子邮箱地址未经核实。
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，所有标准延伸栏位及 Netscape 延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。

6. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅本准则第 1.1 条。

7. 本栏已增加一个互认证书策略的物件识别码，以识别符合互认证书策略而发出的证书。

8. 本栏已增加一个支持 Adobe PDF 签名的物件识别码。

9. 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：

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

*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 $\textit{SHA-1}\,(\,\textit{RSA}_{\text{privatekey, sha-1}}\,(\,\text{hkid\_number}\,)\,)$，该杂凑数值会输入证书内的指定延伸栏位。

10. 证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1_<xxxxx>.crl，由中继证书 "Hongkong Post e-Cert CA 1 - 10"所发出，其中 <xxxxx> 为 经香港邮政系统产生，包含 5 个数字或字符的字串。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资料，会在该证书 “证书撤销清单分发点” 栏位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

栏位名称		栏位内容	
		电子证书（机构）	电子证书（机构）“互认版 "
标准栏 (Standard fields)			
版本 (Version)		X.509 V3	
序号 (Serial number)		[由香港邮政系统设置的三位元组十六进制数字]	
签署算式识别 (Signature algorithm ID)		sha1RSA	
发出人 (Issuer)		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK	
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政系统设置的UTC 时间]	
	不迟于 (Not after)	[由香港邮政系统设置的UTC 时间]	
主体名称 (Subject name)		cn=[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=[(商业登记证书编号或税务局参考编号)+注册证书/登记证书编号+其他]（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]（附注5） o=Hongkong Post e-Cert (Organisational) c=HK	
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元	
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	
标准延伸栏位 (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]	
密码匙使用方法 (Key usage)		不可否认，数码签署，密码匙加密 **（此栏为“关键”栏位）**	不可否认，数码签署 **（此栏为“关键”栏位）**
证书政策 (Certificate policy)		Policy Identifier =[物件识别码]（附注 7） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]	Policy Identifier =[物件识别码]（附注 7） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL] Policy Identifier =2.16.344.8.2.2008.810.2.2012.1.0（附注 8） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL] Policy Identifier = 1.3.6.1.4.1.16030.1.4（附注 9） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]

栏位名称		栏位内容	
		电子证书（机构）	电子证书（机构）“互认版 "
主体别名 (Subject alternative name)	DNS	[0-10特定应用编码]（附注10）	
	第一目錄名称 (First Directory Name)	ou=[登记人机构中文名称]（附注5） ou=[登记人机构分行/部门中文名称]（附注5）	
	rfc822	[证书持有人电子邮箱地址]（附注2）	
发出人别名 (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 constraint)	无	
延伸密码匙使用方法 (Extended key usage)		SSL client, S/MIME	
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11）	
Netscape 延伸栏位 (Netscape extension)（附注6）			
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME	
Netscape SSL伺服器名称 (Netscape SSL server name)		未使用	
Netscape 备注 (Netscape comment)		未使用	

附注：

1. 授权用户姓名格式: 英文格式 - 姓氏（大写）+ 名 （例如 CHAN Tai Man David）
2. 授权用户所提供的电子邮箱地址（如没有电子邮箱地址，此栏将会留空），该电子邮箱地址未经核实。
3. 登记人参考编号： 10 位数字
4. “商业登记证书编号”栏位 : 一串 16 位数字/字母【如无商业登记证书编号，栏位全部为零(“0”)】。如机构提交由税务局发出的证明文件副本，以代替商业登记证副本，则“商业登记证书编号”栏位会包括由证明文件提供的一串 8 位数字/字母之税务局参考编号连同后导的 8 个零("0")。“注册证书 / 登记证书”栏位 : 一串 8 位数字/字母【如注册证书 / 登记证书编号少于 8 位数字/字母，编号前导零(“0”)，如无注册证书 / 登记证书编号，栏位全部为零(“0”)】，“其他”栏位: 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”栏位全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入“其他” 栏位。
5. 只有中文名称作登记之机构，预设的名称「***CHINESE NAME ONLY***」将被设定为机构的英文名称。在任何情况下当登记人机构提供了中文名称并经香港邮政核实,其名称会于主体别名的第一目錄名称 (First Directory Name)栏位内显示（见本核证作业准则第 3.1.1.7 条）。机构中文名称须采用 ISO/IEC 10646 国际编码标准。
6. 除非另外注明，所有标准延伸栏位及 Netscape 延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。
7. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅本准则第 1.1 条。
8. 本栏已增加一个互认证书策略的物件识别码，以识别符合互认证书策略而发出的证书。
9. 本栏已增加一个支持 Adobe PDF 签名的物件识别码。
10. 特定应用中之特定应用编码会在此栏位进行定义。（见**附录 H**）
11. 证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl ，此为中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的「分割式证书撤销清单」。

3) 电子证书（保密）格式

栏位名称		栏位内容
标准栏 (Standard fields)		
版本 (Version)		X.509 V3
序号 (Serial number)		[由香港邮政系统设置的三位元组十六进制数字]
签署算式识别 (Signature algorithm ID)		sha1RSA
发出人 (Issuer)		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK
有效期 (Validity period)	**不早于 (Not before)**	[由香港邮政系统设置的UTC 时间]
	不迟于 (Not after)	[由香港邮政系统设置的UTC 时间]
主体名称 (Subject name)		cn=[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+其他]（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
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元
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
标准延伸栏位 (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]
密码匙使用方法 (Key usage)		数码签署，密码匙加密 **（此栏为“关键”栏位）**
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 7） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]
主体别名 (Subject alternative name)	**DNS**	未使用
	rfc822	[证书持有人电子邮箱地址]（附注2）
发出人别名 (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 constraint)	无

栏位名称		栏位内容
延伸密码匙使用方法 (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 延伸栏位 (Netscape extension)（附注6）		
Netscape 证书类型 (Netscape cert type)		SSL client, S/MIME
Netscape SSL伺服器名称 (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. 登记人机构之授权单位名称
2. 授权单位代表所提供的电子邮箱地址
3. 登记人参考编号： 10 位数字
4. “商业登记证书编号”栏位 : 一串 16 位数字/字母【如无商业登记证书编号，栏位全部为零(“0”)】，“注册证书 / 登记证书”栏位 : 一串 8 位数字/字母【如注册证书 / 登记证书编号少于 8 位数字/字母，编号前导零(“0”)，如无注册证书 / 登记证书编号，栏位全部为零(“0”)】，“其他”栏位: 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”栏位全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入“其他” 栏位。
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，所有标准延伸栏位及 Netscape 延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。
7. 本栏已包括本准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅本准则第 1.1 条。
8. 证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl，此为中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的「分割式证书撤销清单」。
9. 电子证书一律只用英文发出。以下为本栏位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（伺服器）格式

以下为适用于由中继证书"Hongkong Post e-Cert CA 1-10”以杂凑函數SHA-1发出的电子证书（伺服器）（不支持线上证书状态通讯规约）:-

栏位名称		栏位内容		
标准栏 (Standard fields)		电子证书（伺服器）	电子证书（伺服器）“通用版 "	电子证书（伺服器）“多域版 "
版本 (Version)		X.509 V3		
序号 (Serial number)		[由香港邮政系统设置的三位元组十六进制数字]		
签署算式识别 (Signature algorithm ID)		sha1RSA		
发出人 (Issuer)		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK		
有效期 (Validity period)	不早于 (Not before)	[由香港邮政系统设置的UTC 时间]		
	不迟于 (Not after)	[由香港邮政系统设置的UTC 时间]		
主体名称 (Subject name)		cn=[伺服器名称]（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+其他]（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		
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元		
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		
标准延伸栏位 (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]		
密码匙使用方法 (Key usage)		密码匙加密	数码签署，密码匙加密	
		（此栏为“关键”栏位）		
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 6） Policy Qualifier ID = CPS Qualifier = [核证作业准则的URL]		
主体别名 (Subject alternative name)	DNS	未使用	[主体名称内之伺服器名称] + [不带有通配符部分的伺服器名称]（附注7）	[主体名称内之伺服器名称] + [0 至 49] [额外伺服器名称]（附注8）
	rfc822	未使用		

栏位名称		栏位内容		
标准栏 (Standard fields)		电子证书（伺服器）	电子证书（伺服器） “通用版 "	电子证书（伺服器） “多域版 "
发出人别名 (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 constraint)	无		
延伸密码匙使用方法 (Extended key usage)		未使用	伺服器验证 用户端验证	
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9）		
Netscape 延伸栏位 (Netscape extension)（附注5）				
Netscape 证书类型 (Netscape cert type)		SSL Server	未使用	
Netscape SSL伺服器名称 (Netscape SSL server name)		未使用		
Netscape 备注 (Netscape comment)		未使用		

以下为适用于由中继证书"Hongkong Post e-Cert CA 1-14”以杂凑函數 SHA-256 发出的电子证书(伺服器）（不支持线上证书状态通讯规约）:-

栏位名称		栏位内容		
标准栏 (Standard fields)		电子证书（伺服器）	电子证书（伺服器） “通用版 "	电子证书（伺服器） “多域版 "
版本 (Version)		X.509 V3		
序号 (Serial number)		[由香港邮政系统设置的二十位元组十六进制数字]		
签署算式识别 (Signature algorithm ID)		sha256RSA		
发出人 (Issuer)		cn=Hongkong Post e-Cert CA 1 - 14 o=Hongkong Post c=HK		
有效期 (Validity period)	不早于 (Not before)	[由香港邮政系统设置的UTC 时间]		
	不迟于 (Not after)	[由香港邮政系统设置的UTC 时间]		
主体名称 (Subject name)		cn=[伺服器名称]（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+其他]（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		
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元		
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		
标准延伸栏位 (Standard extension)（附注5）				

栏位名称		栏位内容		
标准栏 (Standard fields)		电子证书（伺服器）	电子证书（伺服器）“通用版 "	电子证书（伺服器）“多域版 "
机构信息访问 (Authority Information Access)	核证机关发出人(Certification Authority Issuer)	[发出人的公开证书 URL]		
机关密码匙识别名称 (Authority key identifier)		[发出人证书的主体密码匙标识符]		
主体密码匙标识符 (Subject Key Identifier)		[主体的公开密码匙的杂凑值(Hash Value)]		
密码匙使用方法 (Key usage)		密码匙加密	数码签署，密码匙加密	
		（此栏为“关键”栏位）		
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 6） Policy Qualifier Id = CPS Qualifier = [核证作业准则的URL]		
主体别名 (Subject alternative name)	DNS	未使用	[主体名称内之伺服器名称] + [不带有通配符部分的伺服器名称]（附注7）	[主体名称内之伺服器名称] + [0 至 49] [额外伺服器名称]（附注8）
	rfc822	未使用		
发出人别名 (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 constraint)	无		
延伸密码匙使用方法 (Extended key usage)		未使用	伺服器验证 用户端验证	
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10）		
Netscape 延伸栏位 (Netscape extension)（附注5）				
Netscape 证书类型 (Netscape cert type)		SSL Server	未使用	
Netscape SSL伺服器名称 (Netscape SSL server name)		未使用		
Netscape 备注 (Netscape comment)		未使用		

以下为适用于由中继证书"Hongkong Post e-Cert CA 1-15”以杂凑函數 SHA-256 发出的电子证书（伺服器）（支持线上证书状态通讯规约）:-

栏位名称		栏位内容		
标准栏 (Standard fields)		香港邮政电子核证电子证书（伺服器）	香港邮政电子核证电子证书（伺服器）“通用版 "	香港邮政电子核证电子证书（伺服器）“多域版 "
版本 (Version)		X.509 V3		
序号 (Serial number)		[由香港邮政系统设置的二十位元组十六进制数字]		
签署算式识别 (Signature algorithm ID)		sha256RSA		

栏位名称		栏位内容		
标准栏 (Standard fields)		香港邮政电子核证电子证书（伺服器）	香港邮政电子核证电子证书（伺服器）“通用版 "	香港邮政电子核证电子证书（伺服器）“多域版 "
发出人 (Issuer name)		cn=Hongkong Post e-Cert CA 1 - 15 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK		
有效期 (Validity period)	不早于 (Not before)	[由香港邮政系统设置的UTC 时间]		
	不迟于（Not after）	[由香港邮政系统设置的UTC 时间]		
主体名称 (Subject name)		cn=[伺服器名称]（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+其他]（附注3） ou=Hongkong Post e-Cert (Server) ou=[登记人机构分行/部门名称] o=[登记人机构名称]（附注4） l=Hong Kong s=Hong Kong c=HK		
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元		
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		
标准延伸栏位 (Standard extension)（附注5）				
机构信息访问 (Authority Information Access)	核证机关发出人(Certification Authority Issuer)	[发出人的公开证书 URL]		
	线上证书状态通讯规约	[线上证书状态通讯规约应答伺服器的 URL]（附注 12）		
机关密码匙识别名称 (Authority key identifier)		[发出人证书的主体密码匙标识符]		
主体密码匙标识符 (Subject Key Identifier)		[主体公开密码匙的杂凑值(Hash Value)]		
密码匙使用方法 (Key usage)		数码签署，密码匙加密 **（此栏为“关键”栏位）**		
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 6） Policy Qualifier Id = CPS Qualifier = [核证作业准则的URL]		
主体别名 (Subject alternative name)	DNS	[主体名称内之伺服器名称]	[主体名称内之伺服器名称] + [不带有通配符部分的伺服器名称]（附注7）	[主体名称内之伺服器名称] + [0 至 49] [额外伺服器名称]（附注8）
	rfc822	未使用		
发出人别名 (Issuer alternative name)		未使用		
基本限制 (Basic constraints)	主体类型 (Subject type)	最终实体		

栏位名称		栏位内容		
标准栏 (Standard fields)		香港邮政电子核证电子证书（伺服器）	香港邮政电子核证电子证书（伺服器）“通用版 "	香港邮政电子核证电子证书（伺服器）“多域版 "
	路径长度限制 (Path length constraint)	无		
延伸密码匙使用方法 (Extended key usage)		伺服器验证 用户端验证		
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11）		
Netscape 延伸栏位 (Netscape extension)（附注5）				
Netscape 证书类型 (Netscape cert type)		未使用		
Netscape SSL伺服器名称 (Netscape SSL server name)		未使用		
Netscape 备注 (Netscape comment)		未使用		

附注：

1. 登记人机构拥有之伺服器名称（包括伺服器的网域名称(Domain Name)）。电子证书（伺服器）“通用版 " 的伺服器名称的完整格式网域名称的最左边部份必须为通配符（即星号“*”，称为通配符部份），亦即证书可用于登记人机构所拥有的同一域名或子域名的所有伺服器名称，例如：*.hongkongpost.gov.hk, *.subdomain.hongkongpost.gov.hk。
2. 登记人参考编号：10 位数字
3. “商业登记证书编号”栏位 : 一串 16 位数字/字母【如无商业登记证书编号，栏位全部为零(“0”)】，“注册证书 / 登记证书”栏位 : 一串 8 位数字/字母【如注册证书 / 登记证书编号少于 8 位数字/字母，编号前导零(“0”)，如无注册证书 / 登记证书编号，栏位全部为零(“0”)】，“其他”栏位: 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”栏位全部为零(“0”)，部门简称 (例如 HKPO 代表香港邮政)会放入“其他” 栏位。
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，所有标准延伸栏位及 Netscape 延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。
6. 本栏已包括本准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅第 1.1 条。
7. 电子证书（伺服器）“通用版 " 的主体别名包含二个伺服器名称，一个为显示在主体名称内之伺服器名称，其完整格式网域名称的最左边部份带有通配符（即星号“*”，称为通配符部份），另一个为不带通配符部份的伺服器名称（例如：*.hongkongpost.gov.hk 及 hongkongpost.gov.hk）。
8. 电子证书（伺服器）“多域版 " 之主体别名可包含多至 50 个伺服器名称，第一个是显示在主体名称内的伺服器名称，及可包含 0 至 49 个额外伺服器名称。任何带有通配符（即星号“*”）之伺服器名称将不会被接受。
9. 对于由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的证书，证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1.crl，此乃中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的「整体证书撤销清单」。
10. 对于由中继证书"Hongkong Post e-Cert CA 1 - 14"所发出的证书，证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-14CRL1.crl，此乃中继证书"Hongkong Post e-Cert CA 1 - 14"所发出的「整体证书撤销清单」。
11. 对于由中继证书"Hongkong Post e-Cert CA 1 - 15"所发出的证书，证书撤销清单分发点 URL 为 http://crl1.hongkongpost.gov.hk/crl/eCertCA1-15CRL1.crl，此乃中继证书"Hongkong Post e-Cert CA 1 - 15"所发出的「整体证书撤销清单」。
12. 线上证书状态通讯规约应答伺服器的 URL 为 http://ocsp1.hongkongpost.gov.hk

附录 C - 香港邮政证书撤销清单(CRL)、香港邮政授权撤销清单(ARL)以及线上证书状态应答(OCSP Response)格式

本附录 C 详述有关由中继证书"Hongkong Post e-Cert CA 1 - 10"、"Hongkong Post e-Cert CA 1 - 14"和"Hongkong Post e-Cert CA 1 - 15"所发出的证书撤销清单以及香港邮政授权撤销清单的更新及公布安排和其格式，以及由“Hongkong Post Root CA 1”所发出的授权撤销清单(ARL) 的更新及公布安排和其格式。

通过发布一个包含主题名为“Hongkong Post Root CA 1 OCSP Responder”的线上证书状态通讯规约签署人证书，香港邮政已授权一个线上证书状态通讯规约应答伺服器为根证书“Hongkong Post Root CA 1”进行线上证书状态通讯规约的签署。通过发布一个包含主题名为“Hongkong Post e-Cert CA 1 - 15 OCSP Responder”的线上证书状态通讯规约签署人证书，亦授权一个线上证书状态通讯规约应答伺服器为中继证书“Hongkong Post e-Cert CA 1 - 15”进行线上证书状态通讯规约的签署。除此以外，线上证书状态通讯规约应答伺服器获分配了一个唯一的物件识别码 OID **“1.3.6.1.4.1.16030.1.6”**，指定于线上证书状态通讯规约签署人证书的“证书政策” 栏位。在附录 C 的最后章节，还将提供线上证书状态应答的格式。

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 或 UTC] 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资讯：

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。公众可于下述位址(URL)获取相关的「分割式证书撤销清单」：

   i. 电子证书（个人）：
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1_<xxxxx>.crl
   由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出，其中 <xxxxx> 为包含 5 个数字或字符的字串。
   ii. 电子证书（机构）及电子证书（保密）：
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl
   由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出。
   iii. 电子证书（伺服器）：
   已暂时吊销或已撤销的电子证书（伺服器）资料只会在各自的中继证书的「整体证书撤销清单」(Full CRL)里公布。

b) **「整体证书撤销清单」(Full CRL)** 包含分别由中继证书"Hongkong Post e-Cert CA 1 - 10","Hongkong Post e-Cert CA 1 - 14"和"Hongkong Post e-Cert CA 1 - 15"所发出的所有已暂时吊销或已撤销证书的资料。公众可分别于下述位址(URL)获取「整体证书撤销清单」：

   i. 由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的证书：
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1.crl 或
   ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 10 CRL1, o=Hongkong Post, c=HK)

   ii. 由中继证书"Hongkong Post e-Cert CA 1 – 14"所发出的证书：
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-14CRL1.crl 或
   ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 14 CRL1, o=Hongkong Post, c=HK)

   iii. 由中继证书"Hongkong Post e-Cert CA 1 – 15"所发出的证书：
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-15CRL1.crl 或
   ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 15 CRL1, o=Hongkong Post, c=HK)

上述的证书撤销清单包含已暂时吊销或已撤销证书的资料，公众可于证书的「证书撤销清单分发点」(CRL distribution point) 栏位内注明的位址(URL)获取相关的证书撤销清单。

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。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。香港邮政也会在有需要及不作事前通知的情况下，于香港邮政网页 http://www.hongkongpost.gov.hk/ 公布补充证书撤销清单。

（I） 由中继证书"Hongkong Post e-Cert CA 1 - 10"根据本准则发出的分割式及整体证书撤销清单格式:-

标准栏位 (Standard Fields)	子栏位 (Sub-fields)	分割式证书撤销清单栏位内容	整体证书撤销清单栏位内容	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 - 10 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]		此栏列出已撤销证书的证书序号
	撤销日期 (Revocation date)	[UTC 时间]		此栏显示撤销证书的时间
	证书撤销清单资料延伸栏位 (CRL entry extensions)			
	原因代码 (Reason code)	[撤销理由识别码]		（附注 1）
标准延伸栏位 (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 c=HK		此栏提供有关资料以识别用作签署证书撤销清单的私人密码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)		[由核证系统产生]		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”栏位）**	[未使用]	本栏位祇为分割式证书撤销清单使用。

(II) 由中继证书"Hongkong Post e-Cert CA 1 - 14"根据本准则发出的整体证书撤销清单格式:-

标准栏位 (Standard fields)	子栏位 (Sub-fields)	整体证书撤销清单栏位内容	备注

标准栏位 (Standard fields)	子栏位 (Sub-fields)	整体证书撤销清单栏位内容	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)		sha256RSA	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 - 14 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]	此栏列出已撤销证书的证书序号
	撤销日期 (Revocation date)	[UTC 时间]	此栏显示撤销证书的时间
	证书撤销清单资料延伸栏位 (CRL entry extensions)		
	原因代码 (Reason code)	[撤销理由识别码]	（附注 1）
标准延伸栏位 (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 c=HK	此栏提供有关资料以识别用作签署证书撤销清单的私人密码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)		[由核证系统产生]	此栏显示证书撤销清单的编号，该编号以顺序形式产生。

(III) 由中继证书"Hongkong Post e-Cert CA 1 - 15"根据本准则发出的整体证书撤销清单格式:-

标准栏位 (Standard fields)	子栏位 (Sub-fields)	整体证书撤销清单栏位内容	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)		sha256RSA	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 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, 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]	此栏列出已撤销证书的证书序号
	撤销日期 (Revocation date)	[UTC 时间]	此栏显示撤销证书的时间
	证书撤销清单资料延伸栏位 (CRL entry extensions)		

标准栏位 (Standard fields)	子栏位 (Sub-fields)	整体证书撤销清单栏位内容	备注
	原因代码 (Reason code)	[撤销理由识别码]	（附注 1）
标准延伸栏位 (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 c=HK	此栏提供有关资料以识别用作签署证书撤销清单的私人密码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)		[由核证系统产生]	此栏显示证书撤销清单的编号，该编号以顺序形式产生。

香港邮政会更新及公布授权撤销清单，而清单内载有已暂时吊销或已撤销的中继证书的资料。香港邮政会每年在其下次更新日期前或在有需要时更新及公布。最新发出的授权撤销清单可于下述位置下载：

http://crl1.hongkongpost.gov.hk/crl/RootCA1ARL.crl 或
ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK)

(IV) 由根证书"Hongkong Post Root CA 1"根据本准则发出的授权撤销清单格式:-

标准栏位 (Standard fields)	子栏位 (Sub-fields)	授权撤销清单栏位内容	备注
版本 (Version)		v2	此栏显示授权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	此栏显示用以签署授权撤销清单的算法的识别码
发出人 (Issuer name)		cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK	此栏显示签署及发出授权撤销清单的机构
此次更新 (This update)		[UTC 时间]	此栏显示本授权撤销清单的发出日期 (是次更新)
下次更新 (Next update)		[UTC 时间]	表示下次授权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，授权撤销清单是每年更新及发出
撤销证书 (Revoked certificates)	用户证书 (User certificate)	[证书序号]	此栏列出已撤销证书的证书序号
	撤销日期 (Revocation date)	[UTC 时间]	此栏显示撤销证书的时间
	证书撤销清单资料延伸栏位 (CRL entry extensions)		
	原因代码 (Reason code)	[撤销理由识别码]	（附注 1）
标准延伸栏位 (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 c=HK	此栏提供有关资料以识别用作签署授权撤销清单的私人密码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)		[由核证系统产生]	此栏显示授权撤销清单的编号，该编号以顺序形式产生。
发出人分发点 (Issuer distribution point)		只存有用户证书 =否 只存有核证机关证书=是 间接的 CRL=否 **（此栏为“关键”栏位）**	

(V) 根据本准则的线上证书状态应答格式:-

香港邮政线上证书状态通讯规约应答伺服器只支持基本的线上证书状态应答类型。一个明确的线上证书状态应答数据由以下组成：

标准栏位 (**Standard Fields**)	子栏位 (**Sub-fields**)	子栏位 (**Sub-fields**)	栏位内容	备注
应答数据 (Response data)	版本(Version)		v1 (0x0)	
	应答伺服器识别 Responder ID	by key 凭密码匙	[应答伺服器的公匙 SHA-1 杂凑值]	
	Produced At 产生于		[Generalized 时间]	此应答签署的时间 (GMT+0).
	Sequence of Single Response 单一应答的序列			
	Single Response 单一应答	Certificate ID 证书识别	[要求的证书识别名称]	要求的证书识别名称包含： • 杂凑函數识别 • 发出人主题名称的杂凑值 • 发出人公匙的杂凑值 • 证书序号
		证书状态 (Certificate status)	[证书的状态]	有效、撤销（附有日期、时间(GMT+0)和撤销原因代码（附注 1)）或未知
		本次更新 This update	[Generalized 时间]	证书正确状态的最近日期和时间 (GMT+0).
		下次更新 Next update	[Generalized 时间]	更新证书状态的日期和时间 (GMT+0).
签署算式识别 (Signature algorithm ID)			sha256RSA	用于签署此应答的算法
签署(Signature)			[签署数据]	应答的签名
证书 (Certificate)			[应答伺服器签署人证书的数据]	应答伺服器的签署人证书

附注：

1. 以下为可于撤销证书栏位下列出的理由识别码：

   0 = 未注明；1 = 密码资料外泄；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，所有标准延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。

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)	电子证书（个人） “互认版 "	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	2048 位元 RSA		
产生配对密码匙	由香港邮政代制产生		
核对身分	当面核对申请人的身分，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	数码签署	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（由香港邮政核证机关系统产生）		
登记费用	每份证书（包括首次及续期申请）每年 50 港元（见本核证作业准则第 2.4 条）	见本核证作业准则第 2.4 条	每份证书（包括首次及续期申请）每年 50 港元（见本核证作业准则第 2.4 条）
证书有效期	三年	一年、二年或三年	三年
	（见本核证作业准则第 1.2.4，3.2 及 3.3.1 条）		

2) 电子证书（机构）、电子证书(保密) 及电子证书(伺服器)

要点	电子证书(机构)	电子证书(机构)“互认版”	电子证书(保密)	电子证书(伺服器)	电子证书（伺服器）“通用版”或“多域版 "
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[附注 1]、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授权用户		登记人机构之授权单位	即登记人	
依据限额	HK$200,000				
认可证书	是				
配对密码匙长度	2048 位元 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	
核对身分	核对机构及其获授权代表的身分			核对网域名称(Domain Name)、机构及其获授权代表的身分	
证书用途	数码签署及数据加密	数码签署	只作数据加密之用	数码签署[附注 2]及数据加密	数码签署及数据加密
证书内包含登记人的资料	▪ 登记人机构名称，包括其中文名称（如有提供） ▪ 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 / 商业登记资讯[附注 3]		▪ 登记人机构名称 ▪ 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 / 商业登记资讯	▪ 登记人机构名称 ▪ 登记人机构之伺服器名称 ▪ 登记人参考编号（由香港邮政系统产生） ▪ 登记人机构之公司 / 商业登记资讯	▪ 登记人机构名称 ▪ 登记人机构之伺服器名称及在主体别名内列出之额外伺服器名称 ▪ 登记人参考编号（由香港邮政系统产生） ▪ 登记人机构之公司 / 商业登记资讯
登记及行政费用	见本核证作业准则第 2.4 条				
证书有效期	一年或两年	一年、二年或三年	一年、两年、三年或四年	一年或两年	一年、两年或三年
	（见本核证作业准则第 1.2.4 及 3.4.1 条）				

附注：

1. 持有由香港特别行政区政府税务局根据《税务条例》(第 112 章)发出的有效证明文件的机构，亦可以成为电子证书（机构）的登记人（但非成为电子证书（机构）“互认版 " 的登记人）（见第 1.2.3.2 条）。
2. 数码签署的用途只适用于由中继证书"Hongkong Post e-Cert CA 1 – 15”发出的电子证书（服务器）。
3. 持有由香港特别行政区政府税务局根据《税务条例》(第 112 章) 发出的有效证明文件的机构，电子证书只会显示其税务局参考编号。

附录 E - 香港邮政电子证书核证登记机关名单（若有的话）

由本核证作业准则生效日期起，香港邮政电子证书并无指定之核证登记机关。

附录 F - 香港邮政电子证书服务 - 翘晋电子商务有限公司之合约分判商名单（若有的话）

由本核证作业准则生效日期起，就此核证作业准则而言，香港邮政电子证书服务并无指定之受翘晋电子商务有限公司委任的合约分判商。

附录 G - 核证机关根源证书的有效期

根源证书名称	有效期	备注
Hongkong Post Root CA 1	2003年5月15日 至 2023年5月15日	
Hongkong Post e-Cert CA 1	2003年5月15日 至 2013年5月15日	此中继证书由2010年2月26日起停止发出认可证书。
Hongkong Post e-Cert CA 1 - 10	2010年1月9日 至 2023年5月15日	此中继证书由2010年2月26日起开始发出认可证书给申请者。
Hongkong Post e-Cert CA 1 – 14	2014年11月30日 至 2023年5月15日	此中继证书由2015年1月1日起开始发出认可证书给申请者。
Hongkong Post e-Cert CA 1 – 15	2015年7月4日至 2023年5月15日	此中继证书由2015年9月1日起开始发出认可证书给申请者。

附录 H - 香港邮政电子证书特定应用名单及相对应之特定应用编码

特定倚据人士名称	特定应用	证书类别	界定 为证书主体别名 DNS 栏位的特定应用编码
香港特别行政区政府税务局	AEOI [附注 1]网站	电子证书（机构）（不包括电子证书（机构）“互认版＂）	“IRD_AEOI”

附注：

1. AEOI 代表 "自动交换资料"

附录 I - RFC3647 与本核证作业准则之比较表

免责声明：下方比较表旨在为本核证作业准则与 RFC3647 核证作业准则概要之间的相互参考提供便利，以及遵守互认证书策略第四（一）(3) 段中所述的要求。若本核证作业准则与 RFC3647 核证作业准则概要之间存在任何语义冲突，概以本核证作业准则的条文为准；如登记人或任何倚据人士因此等语义冲突或因其倚据下方的比较表而遭受任何损失及损害，香港邮政概不负责。

为免生疑问，如比较表中有注明“不适用”的，主要是因为香港邮政没有提供那些作业 / 服务或它们和香港邮政现有的作业 / 服务无关。

RFC3647 的章节	本准则的相关章节	说明
1. 概括性描述	1	
1.1 概述	1.1	
1.2 文档名称与标识	1.1	
1.3 电子认证活动参与者	1.2	
1.3.1 电子认证服务机构	1.2.1	
1.3.2 注册机构	2.1.2 及附录 E	
1.3.3 登记人	1.2.2 及 1.2.3	
1.3.4 倚据人士	1.2.2	
1.3.5 其他参与者	2.1.3 及附录 F	
1.4 证书应用	1.2.3	
1.4.1 适合的证书应用		
1.4.2 限制的证书应用		
1.5 策略管理	前言及 8	
1.5.1 策略文档管理机构	前言及 8	
1.5.2 联系人	1.3	
1.5.3 决定 CPS 符合策略的机构	前言及 8	
1.5.4 CPS 批准程式	8	
1.6 定义和缩写	附录 A	
2. 信息发布与信息管理	2.1.1 及 2.5	
2.1 核准使用证书储存库内的资料	2.5.4	
2.2 认证信息的发布	2.5	
2.3 发布的时间或频率	2.5	
2.4 信息库存取控制	2.5.1 及 2.5.2	
3. 身份标识与鉴别	3	
3.1 命名	3.1	
3.1.1 名称类型	3.1.1	
3.1.2 对名称意义化的要求	3.1.2	
3.1.3 登记人的匿名或伪名	不适用	本准则不接受登记人匿名或伪名
3.1.4 理解不同名称形式的规则	3.1.3	

RFC3647 的章节	本准则的相关章节	说明
3.1.5 名称的唯一性	3.1.4	
3.1.6 商标的识别、鉴别和角色	3.1.5 及 3.1.6	
3.2 初始身份确认	3.1	
3.2.1 证明拥有私人密码匙之方法	3.1.7	
3.2.2 组织机构身份的鉴别	3.1.8	
3.2.3 个人身份的鉴别	3.1.9	
3.2.4 没有验证的登记人资讯	不适用	本准则参照 RFC2527 制定，不披露此部分内容或仅在附录 B 中注明
3.2.5 授权确认	3.1.9	
3.2.6 互操作准则	1.1	
3.3 密码匙更新请求的标识与鉴别	3.3 至 3.4	证书密码匙将于证书续期过程中被更新
3.3.1 常规密码匙更新的标识与鉴别	3.3 至 3.4	
3.3.2 撤销后密码匙更新的标识与鉴别	3.3 至 3.4	
3.4 撤销请求的标识与鉴别	4.6.2	
4. 证书生命周期操作要求	4	
4.1 证书申请	4.1 至 4.4	
4.1.1 证书申请实体	4.1 至 4.4	
4.1.2 注册过程与责任	2.1 及 4.1 至 4.4	
4.2 证书申请处理	4.1 至 4.4	
4.2.1 执行识别与鉴别功能	3.1.8 及 3.1.9	
4.2.2 证书申请批准和拒绝	4.1 至 4.4	
4.2.3 处理证书申请的时间	4.5	
4.3 证书签发	4.1 至 4.4	
4.3.1 证书签发中注册机构和电子认证服务机构的行为	4.1 至 4.4	
4.3.2 电子认证服务机构和注册机构对登记人的通告	4.1 至 4.4	
4.4 证书接受	2.1.4 及 4.1 至 4.4	
4.4.1 构成接受证书的行为	4.1 至 4.4	
4.4.2 电子认证服务机构对证书的发布	2.5 及 4.1 至 4.4	
4.4.3 电子认证服务机构对其他实体的通告	2.5 及 4.1 至 4.4	
4.5 配对密码匙和证书的使用	2.1.4 及 2.1.6	
4.5.1 登记人私人密码匙和证书的使用	2.1.4	
4.5.2 倚据人士公开密码匙和证书的使用	2.1.6	
4.6 证书续期	3.2 至 3.4	
4.6.1 证书续期的情形	3.3 及 3.4	
4.6.2 请求证书续期的实体	3.3 及 3.4	
4.6.3 证书续期请求的处理	3.3 及 3.4	
4.6.4 颁发新证书时对登记人的通告	4.1 - 4.4	

RFC3647 的章节	本准则的相关章节	说明
4.6.5 构成接受续期证书的行为	4.1 - 4.4	
4.6.6 电子认证服务机构对续期证书的发布	2.5 及 4.1 至 4.4	
4.6.7 电子认证服务机构对其他实体的通告	2.5 及 4.1 至 4.4	
4.7 证书密码匙更新	3.2 至 3.4	
		证书密码匙将于证书续期过程中被更新
4.7.1 证书密码匙更新的情形	3.3 至 3.4	
4.7.2 请求证书密码匙更新的实体	3.3 至 3.4	
4.7.3 证书密码匙更新请求的处理	3.3 至 3.4	
4.7.4 颁发新证书时对登记人的通告	4.1 - 4.4	
4.7.5 构成接受密码匙更新证书的行为	4.1 - 4.4	
4.7.6 电子认证服务机构对密码匙更新证书的发布	2.5 及 4.1 至 4.4	
4.7.7 电子认证服务机构对其他实体的通告	2.5 及 4.1 至 4.4	
4.8 证书变更	不适用	本准则不接受变更已发出的证书
4.8.1 证书变更的情形		
4.8.2 请求证书变更的实体		
4.8.3 证书变更请求的处理		
4.8.4 颁发新证书时对登记人的通告		
4.8.5 构成接受变更证书的行为		
4.8.6 电子认证服务机构对变更证书的发布		
4.8.7 电子认证服务机构对其他实体的通告		
4.9 证书撤销和暂时吊销	4.6	
4.9.1 证书撤销的情形	2.1.4, 4.6.1 及 4.11.2	
4.9.2 请求证书撤销的实体	4.6.2	
4.9.3 撤销请求的流程	4.6.2	
4.9.4 撤销请求宽限期	4.6.2	
4.9.5 电子认证服务机构处理撤销请求的时限	4.6.3	
4.9.6 倚据人士检查证书撤销的要求	2.1.6 及 4.6.4	
4.9.7 CRL 发布频率	4.6.3 及 4.11.2	
4.9.8 CRL 发布的最大滞后时间	4.6.3	
4.9.9 在线状态查询的可用性	不适用	暂不提供在线状态查询服务
4.9.10 在线状态查询要求	不适用	暂不提供在线状态查询服务
4.9.11 撤销信息的其他发布形式	不适用	暂不提供其他发布形式
4.9.12 密码匙损害的特别要求	不适用	暂不提供此种服务
4.9.13 证书暂时吊销的情形	2.1.4 及 4.6.2	
4.9.14 请求暂时吊销证书的实体	4.6.2	
4.9.15 请求暂时吊销的流程	4.6.2	
4.9.16 暂时吊销的期限限制	4.6.2	
4.10 证书状态服务	4.6.3 及 4.6.4	

RFC3647 的章节	本准则的相关章节	说明
4.10.1 操作特征	4.6.3	
4.10.2 服务可用性	4.6.3	
4.10.3 可选特征	4.6.3	
4.11 登记使用期结束	4.7	
4.12 密码托管与恢复	6.2.3	
4.12.1 密码匙托管份与恢复的策略与行为	6.2.3	
4.12.2 工作阶段密码匙的封装与恢复的策略与行为	6.2.3	
5. 认证机构设施、管理和操作控制	2.1.4, 2.1.6, 4 及 5	
5.1 物理控制	5.1	
5.1.1 场地位置与建筑	5.1.1	
5.1.2 物理访问	5.1.2	
5.1.3 电力与空调	5.1.4	
5.1.4 水患防治	5.1.5	
5.1.5 火灾防护	5.1.6	
5.1.6 介质存储	5.1.7	
5.1.7 废物处理	5.1.10	
5.1.8 异地备份	5.1.8	
5.2 程式控制	5.2	
5.2.1 可信角色	5.2.1	
5.2.2 每项任务需要的人数	5.2.1	
5.2.3 每个角色的识别与鉴别	5.2.1	
5.2.4 需要职责分割的角色	5.2.1	
5.3 人员控制	5.3	
5.3.1 资格、经历和无过失要求	5.3.1	
5.3.2 背景审查程式	5.3.2	
5.3.3 培训要求	5.3.3	
5.3.4 再培训周期和要求	5.3.3	
5.3.5 工作岗位轮换周期和顺序	不予以披露	将遵守内部规定，本准则不予以披露
5.3.6 未授权行为的处罚	5.3.4	
5.3.7 独立合约人的要求	不予以披露	将遵守内部规定，本准则不予以披露
5.3.8 提供给员工的文档	5.3.5	
5.4 审计日志程式	4.8	
5.4.1 记录事件的类型	4.8.1	
5.4.2 处理日志的周期	4.8.2	
5.4.3 审计日志的保存期限	4.8.3	
5.4.4 审计日志的保护	4.8.4	
5.4.5 审计日志备份程式	4.8.5	

RFC3647 的章节	本准则的相关章节	说明
5.4.6 审计收集系统	4.8.6	
5.4.7 对导致事件实体的通告	4.8.7	
5.4.8 脆弱性评估	4.8.8	
5.5 记录归档	4.9	
5.5.1 归档记录的类型	4.9.1	
5.5.2 归档记录的保存期限	4.9.2	
5.5.3 归档文件的保护	4.9.3	
5.5.4 归档文件的备份程式	4.9.4	
5.5.5 记录时间戳要求	4.9.5	
5.5.6 归档收集系统	4.9.4	
5.5.7 获得和检验归档信息的程式	4.9.4	
5.6 电子认证服务机构密码匙更替	4.10	
5.7 损害与灾难恢复	4.11	
5.7.1 事故和损害处理程序	4.11	
5.7.2 计算资源、软件和/或数据的损坏	4.11.4	
5.7.3 实体私人密码匙损害处理常式	4.11.2	
5.7.4 灾难后的业务连续性能力	4.11.1	
5.8 电子认证服务机构或注册机构的终止	4.12 及 4.13	
6. 认证系统技术安全控制	6	
6.1 配对密码匙的生成和安装	6.1	
6.1.1 配对密码匙的生成	6.1.1 及 6.1.5	
6.1.2 私人密码匙传送给登记人	6.1.3	
6.1.3 公开密码匙传送给证书签发机构	6.1.2	
6.1.4 电子认证服务机构公开密码匙传送给倚据人士	4.1 - 4.4	
6.1.5 密码匙的长度	6.1.4	
6.1.6 公开密码匙参数的生成和品质检查	6.1.5	
6.1.7 密码匙使用目的	6.1.6	
6.2 私人密码匙保护和密码模组工程控制	6.2 及 6.7	
6.2.1 密码模组的标准和控制	6.2.1 及 6.7	
6.2.2 私人密码匙多人控制（m 选 n）	6.2.2	
6.2.3 私人密码匙托管	6.2.3	
6.2.4 私人密码匙备份	6.2.4	
6.2.5 私人密码匙归档	不予以披露	将遵守内部规定，本准则不予以披露
6.2.6 私人密码匙于密码模组之间传递	6.2.5	
6.2.7 私人密码匙在密码模组的存储	6.2.5	
6.2.8 启动私人密码匙的方法	6.2.4	
6.2.9 解除私人密码匙启动状态的方法	6.2.2	

RFC3647 的章节	本准则的相关章节	说明
6.2.10 销毁私人密码匙的方法	不予以披露	将遵守内部规定，本准则不予以披露
6.2.11 密码模组的评估	6.2.1 及 6.7	
6.3 配对密码匙管理的其他方面	6.3	
6.3.1 公开密码匙归档	6.3	
6.3.2 证书操作期和配对密码匙使用期限	6.3	
6.4 激活数据	6.1 及 6.2	
6.4.1 激活数据的产生和安装		
6.4.2 激活数据的保护		
6.4.3 激活数据的其他方面		
6.5 电脑安全控制	6.4	
6.5.1 特别的电脑安全技术要求	6.4	
6.5.2 电脑安全评估	6.4	
6.6 生命周期技术控制	6.5	
6.6.1 系统开发控制	6.5	
6.6.2 安全管理控制	6.5	
6.6.3 生命期的安全控制	6.5	
6.7 网络的安全控制	6.6	
6.8 时间戳	不适用	暂不提供
7. 证书、凭证撤销清单和线上证书状态通讯规约	7	
7.1 证书	7.1	
7.1.1 版本号	附录 B	
7.1.2 证书扩展项	附录 B	
7.1.3 演算法物件识别码	附录 B	
7.1.4 名称形式	附录 B	
7.1.5 名称限制	附录 B	
7.1.6 证书策略物件识别码	附录 B	
7.1.7 策略限制扩展项的用法	附录 B	
7.1.8 策略限定词的语法和语义	附录 B	
7.1.9 关键证书策略扩展项的处理规则	附录 B	
7.2 证书撤销清单	7.2	
7.2.1 版本号	附录 C	
7.2.2 CRL 和 CRL 条目扩展项	附录 C	
7.3 线上证书状态通讯规约	7.3	只适用于由中继证书 "Hongkong Post e-Cert CA 1-15" 发出的电子证书（伺服器）
7.3.1 版本号	附录 C	
7.3.2 OCSP 扩展项	附录 C	
8. 认证机构审计和其他评估	2.6	
8.1 评估的频率或情形	2.6	
8.2 评估者的资质	2.6	

RFC3647 的章节	本准则的相关章节	说明
8.3 评估者与被评估者之间的关系	2.6	
8.4 评估内容	2.6	
8.5 对问题与不足采取的措施	不予以披露	将遵守内部规定，本准则不予以披露
8.6 评估结果的传达与发布	不予以披露	将遵守内部规定，本准则不予以披露
9. 法律责任和其他业务条款	2	
9.1 费用	2.4	
9.1.1 证书签发和更新费用	2.4.1 - 2.4.4	
9.1.2 证书查询费用	2.4.1 - 2.4.4	
9.1.3 证书撤销或状态资讯的查询费用	2.4.1 - 2.4.4	
9.1.4 其他服务费用	2.4.1 - 2.4.4	
9.1.5 退款策略	2.4.1 - 2.4.4	
9.2 财务责任	2.2.15	
9.2.1 保险范围	2.2.15	
9.2.2 其他资产	2.2.15	
9.2.3 对最终实体的保险或担保	2.2.15	
9.3 业务信息保密	2.7	
9.3.1 保密信息范围	2.7	
9.3.2 不属于保密的信息	2.7	
9.3.3 保护保密信息的责任	2.7	
9.4 个人隐私保密	2.7	
9.4.1 隐私保密方案	2.7	
9.4.2 作为隐私处理的信息	2.7	
9.4.3 不被视为隐私的信息	2.7	
9.4.4 保护隐私的责任	2.7	
9.4.5 使用隐私信息的告知与同意	不适用	本准则参照 RFC2527 制定，不披露此部分内容
9.4.6 依法律或行政程式的信息披露	2.7	
9.4.7 其他信息披露情形	2.7	
9.5 知识产权	1.2.2.1	
9.6 陈述与担保	2	
9.6.1 电子认证服务机构的陈述与担保	2.2.3	
9.6.2 注册机构的陈述与担保	2.1.1	
9.6.3 登记人的陈述与担保	2.1.4	
9.6.4 倚据人士的陈述与担保	2.1.6	
9.6.5 其他参与者的陈述与担保	不适用	本准则参照 RFC2527 制定，不披露此部分内容
9.7 担保免责	2.2.10	
9.8 有限责任	2.2.3	

RFC3647 的章节	本准则的相关章节	说明
9.9 赔偿	2.2.3	
9.10 有效期限与终止	不适用	暂无规定
9.10.1 有效期限		
9.10.2 终止		
9.10.3 效力的终止与保留		
9.11 对参与者的个别通告与沟通	2.3.2	
9.12 修订	8	
9.12.1 修订程式	8	
9.12.2 通知机制和期限	8	
9.12.3 必须修改业务规则的情形	8	
9.13 争议处理	2.3.3	
9.14 管辖法律	2.3.1	
9.15 与适用法律的符合性	2.3.1	
9.16 一般条款	2.3	
9.16.1 完整协议	2.3.2	
9.16.2 转让	2.2.5	
9.16.3 分割性	2.3.2	
9.16.4 强制执行	2.3.3	
9.17 其他条款	不适用	本准则参照 RFC2527 制定，不披露此部分内容