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
「智方便」电子证书

核证作业准则

日期：二零二四年七月十一日
物件识别码：1.3.6.1.4.1.16030.1.9.3

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中华人民共和国香港特别行政区进行商业活动及其他交易。

就条例而言，香港邮政署长为认可核证机关。根据条例，香港邮政署长（其本人或香港邮政署职员）(a)履行核证机关之职能和提供服务，以及与核证机构之职能或服务相关或附带的服务；及(b)为任何合宜举措以履行上述(a)段的目的及与认可核证机关有关的任何条文。

根据政府资讯科技总监颁布之认可核证机关业务守则第 33 条，香港邮政可以指定代理人或合约分判商，在香港邮政全面管理和监控下进行其若干或所有作业.。

香港邮政根据条例赋予的权力提供核证机关服务，并且由 2007 年 4 月 1 日起，在香港邮政的全面管理和监督下，将核证机关服务外判给承办商。

香港邮政依然为条例第 34 条下之认可核证机关，而核证登记机关及承办商（包括核证登记机关及承办商之合约分判商）则为香港邮政根据政府资讯科技总监颁布之认可核证机关业务守则第 3.2 条所委任之代理人，为香港邮政所委任以履行核证机关之职能。

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、撤销及利用公开储存库公布已认可及已接受之數码证书作为在网上进行稳妥的身份辨识。**根据本核证作业准则发出的「智方便」电子证书，均为条例下的认可证书，在本核证作业准则内称为“证书”或“「智方便」电子证书”。**

本核证作业准则列载「智方便」电子证书之实务守则，其结构如下：

第 1 条载有概述及聯络资料
第 2 条列载各方职能及义务
第 3 条列载身份辨识与验证要求
第 4 条概述运作要求
第 5 条介绍保安监控措施

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证书时采用之实务守则。

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。就识别准则之言，“1.3.6.1.4.1.16030.1.9.3”为本准则的物件识别码(Object Identifier, OID)（见**附录** B 内关于证书政策(Certificate Policies)的說明）。

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、撤销及公布的「智方便」电子证书）申请人身份的程序，并介绍香港邮政之运作、程序及保安要求。

为香港居民提供免费的数码个人身份，是 2017 年 10 月公布的数码基础设施项目之一。政府已经展开相关的数码基础设施并命名为「智方便」平台。「智方便」为所有香港居民提供数码个人身份，使他们能够以单一的数码身份和认证与政府和商业进行网上交易。

香港居民可以透过各个提供各种「智方便」版本的登记渠道获取「智方便」。只有按照本准则第 3.1.1 条登记的「智方便」持有人，方有资格申请「智方便」电子证书。

香港邮政根据本准则所签发的「智方便」电子证书，是特别指明为已按照本准则第 3.1.1 条登记的「智方便」持有人，根据条例提供具法律效力的数码签署。除特别声明外，本作业准则各章节中提到的「智方便」版本是指根据本准则第 3.1.1 条获取的「智方便」版本，在本准则内称为「智方便」。

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「智方便」电子证书，香港邮政已指明为认可证书。根据条例，「智方便」电子证书享有认可证书的地位，其用于数码签署的交易受到条例的认可和保护。

「智方便」电子证书支援公匙基建模式，即登记人可以远程接达储存在「智方便」系统所托管的硬体安全模组中的私人密码匙，且登记人的「智方便」电子证书配对密码匙在硬体安全模组中制作并储存。

附录 D 载有「智方便」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。香港邮政乃唯一被授权根据本准则发出「智方便」电子证书之核证机关（见第 2.1.1 条）。

1.2.1.1 生效

香港邮政于储存库公布「智方便」电子证书。

1.2.1.2 香港邮政进行合约分判之权利
香港邮政可指定代理人或合约分判商履行本准则及登记人协议规定之部份或全部职能。无論是否有任何指定，香港邮政仍为认可核证机关及会履行「智方便」电子证书发出人的职能。

1.2.2「智方便」核证登记办事处
香港邮政通常透过「智方便」核证登记办事处处理「智方便」电子证书申请人或登记人之事宜。政府资讯科技总监办公室履行「智方便」核证登记办事处的职能，或指定承办商履行部份或全部「智方便」核证登记办事处的职能。「智方便」核证登记办事处是代表香港邮政的核证登记机关执行以下职责：

a) 接受和处理申请人及登记人的证书申请；
b) 核实申请人及登记人之身份；
c) 保留核实申请人和登记人身份证明文件的文本；及
d) 通知申请人及登记人有关已批准或被拒绝的证书申请，及已撤销的证书。

下文第 2.1.2 条载有「智方便」核证登记办事处需履行的所有职能。

1.2.3 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。

倚据证书人士需注意：十八岁以下的人士亦可按本准则第 3 条及第 4 条，申请「智方便」电子证书。

1.2.3.1 私人密码匙的位置
「智方便」电子证书之私人密码匙将储存于「智方便」系统所托管的硬体安全模组。香港邮政将于储存库公布「智方便」电子证书（连同公开密码匙），供公众下载及核对数码签署。

1.2.3.2 登记人及「智方便」核证登记办事处
登记人必须授权「智方便」核证登记办事处保管和管理私人密码匙，并保存一份由香港邮政发给登记人的「智方便」电子证书。登记人确认「智方便」核证登记办事处亦可同时代表香港邮政履行以上第 1.2.2 条所述的职能。登记人确认并同意「智方便」核证登记办事处的有关职能不会造成利益冲突，「智方便」核证登记办事处担任的职能亦同时对所有人士有利。

1.2.4 证书之类别
「智方便」电子证书是唯一根据本准则由香港邮政发出的证书类别。香港邮政仅签发「智方便」电子证书予已以适当形式确定接受登记人协议，且其身份及其证书申请已根据本准则第 3 条和第 4 条被「智方便」核证登记办事处成功核实及接受之申请人士。登记人可以透过「智方便」系统，与接受「智方便」电子证书数码签署的倚据证书人士进行政府及商业交易。

「智方便」电子证书可发出予十八岁以下的人士 （另见第 3.1.3 条）

1.2.5 证书之期限
根据本准则「智方便」电子证书的有效期由发出自香港邮政当日起即日生效，有效期为一年。

1.2.6 申请
所有「智方便」电子证书的首次申请及续期申请，申请人须符合本准则第 3 及 4 条所述的要求。

1.2.7 适用性
发出予登记人的「智方便」电子证书可用于一般用途，并没有受限制用于特定类型之交易。

1.3 聯络资料

申请人或登记人可经由以下途径就「智方便」电子证书作出查询、建议或投诉：

邮寄地址：东九龍邮政信箱 68777 号香港邮政核证机关
电话：29216633
传真：27759130
电邮地址：enquiry@eCert.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，并在收到投诉后十个工作日内给予详细的答复。若十个工作日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聯络确认收到有关投诉及作出回覆。

2. 一般规定

2.1 职能和义务

香港邮政之职能乃由本准则以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。

2.1.1 核证机关之职能和义务

根据本准则，香港邮政履行以下之职能（「智方便」核证登记办事处或承办商在香港邮政的管理和控制下可以履行以下任何或所有职能）：

a) 透过「智方便」核证登记办事处接受「智方便」电子证书申请；
b) 透过「智方便」核证登记办事处通知申请人有关已批准或被拒绝的申请；
c) 根据「智方便」核证登记办事处递交的签发证书要求，发出「智方便」电子证书，并于储存库公布「智方便」电子证书；
d) 撤销「智方便」电子证书并依时公布修订的证书撤销清单；
e) 提供用于检查「智方便」电子证书状态之线上证书状态应答（“ OCSP”）；
f) 透过「智方便」核证登记办事处通知登记人有关已撤销的「智方便」电子证书。

根据条例，香港邮政负责使用稳当系统履行其服务以（a）发出或撤销「智方便」电子证书；或（b）利用储存库公布已发出之「智方便」电子证书，或給予通知书与已撤销之「智方便」电子证书。

2.1.2「智方便」核证登记办事处之职能及义务

「智方便」核证登记办事处履行以下之职能（承办商在「智方便」核证登记办事处的管理和控制下可以履行以下任何或所有职能）：

<u>代表香港邮政履行核证登记机关之职能（见第 1.2.2 条）</u>

a) 接受和处理申请人之证书申请，申请人必须为「智方便」持有人（見第 3.1.1 條）；
b) 在首次申请或续期申请「智方便」电子证书时核实申请人/登记人之身份（見第 3.1.2 條及第 3.2.1 条），并在「智方便」系统中为身份核实结果作纪录；
c) 为任何撤销「智方便」电子证书的要求核实登记人的身份；
d) 根據本準則条款及登记人协议，在整个证书有效期内及相关证书到期后至少 7 年内，保存所有用作核实申请人为「智方便」持有人身份的记录。
e) 当收到香港邮政通知后，通知申请人/登记人有关证书申请及撤销证书要求已获批准或被拒绝的结果；
f) 告知登记人其义务，包括有责任维护用于透过「智方便」系统接达「智方便」电子证书的「智方便」凭证，以及即时透过「智方便」系统或其他由「智方便」核证登记办事处指定之通讯渠道向「智方便」核证登记办事处呈报任何外泄或怀疑外泄的事件；

<u>其他职能</u>

g) 在申请人确认接受登记人协议条款及条件后，向香港邮政递交证书申请要求；
h) 为登记人制作配对密码匙，并将其私人密码匙储存在「智方便」系统的硬体安全模组内；
i) 保管和管理登记人的私人密码匙，并确保只有登记人才可使用其私人密码匙进行数码签署；

j) 当「智方便」电子证书在储存库、证书撤销清单或线上证书状态应答中显示证书状态为已过期或已撤销状况时，确保登记人或任何其他人士不能再使用该「智方便」电子证书的私人密码匙；
k) 产生并递交签发证书要求给香港邮政，其中包括了与申请人有关的资料以及确认同意接受登记人协议的条款及条件。

「智方便」核证登记办事处负责使用稳当系统交付上述职能。

香港邮政依然对「智方便」核证登记办事处在其执行或声称执行上述涉及核证机关之义务和职责的行为负责。「智方便」核证登记办事处仅代表香港邮政执行香港邮政在核证登记机关功能中的义务和职责。

2.1.3 承办商之职能及义务
承办商仅根据其与香港邮政之间之合约之规定向香港邮政承担责任。根据该等合约，香港邮政任命承办商为其代理人营运并维持系统以签发「智方便」电子证书。此外，在香港邮政的全面管理和控制下，香港邮政可以不时任命该承办商或其他任何代理人或承办商，执行所有或任何陈述于本准则之职能。

2.1.4 申请人及登记人之义务

2.1.4.1 申请人之义务
在不影响申请人于本准则和登记人协议规定的其他义务的前提下，申请人对以下所有事项负责：

a) 通过「智方便」系统适当地完成申请程序，并确保在申请证书时作出准确的陈述和保证；
b) 以香港邮政指明的形式确认接受登记人协议，并履行该登记人协议规定其承担之义务；
c) 同意「智方便」系统在收到申请人的「智方便」电子证书申请后，产生签发证书要求并发给香港邮政，其要求包括了申请人相关资料及申请人确认接受登记人协议条款及条件；
d) 确认「智方便」电子证书申请一旦递交，申请人同意「智方便」系统收讫「智方便」电子证书即被视为申请人接受「智方便」电子证书，并授权香港邮政向其他人士或于香港邮政储存库内公布其「智方便」电子证书。

2.1.4.2 登记人之义务
在不影响登记人于本准则和登记人协议规定的其他义务的前提下，登记人对以下所有事项负责：

a) 同意「智方便」核证登记办事处透过「智方便」系统产生登记人之配对密码匙并储存其私人密码匙于「智方便」核证登记办事处处所内的环境下及硬体安全模组内；
b) 按照本准则所载之规定办理证书首次申请与证书续期；
c) 不时将由登记人提供之证书资料之任何变动通知「智方便」核证登记办事处；
d) 如发生可能致使香港邮政有权根据下文第 4 .2 条所载之理由撤销证书的任何事件，立即通知「智方便」核证登记办事处；
e) 同意证书一经发出，即向香港邮政以及所有倚据证书人士保证及表明，在证书之有效期间，本准则第 9.6.2 条载明之保证及陈述乃属并将保持真实、准确及完整；
f) 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，或根据第 4.2 条所述登记人已作出撤销申请或已从香港邮政收到撤销通知书的情况下，均不得在交易中使用证书；
g) 在明知香港邮政可能据以撤销证书之任何事项之情况下，或根据第 4.2 条所述登记人已作出撤

销申请或已香港邮政收到撤销通知书的情况下，须立即通知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被撤销（由香港邮政或登记人本人要求），并明确說明，在此情形下倚据证书人士不得就交易而倚据该证书。

2.1.5 倚据证书人士之义务

在不影响倚据证书人士于本准则和登记人协议规定的其他义务的前提下，倚据「智方便」电子证书之倚据证书人士对以下所有事项负责：

a) 倚据证书人士于倚据「智方便」电子证书时如考虑过所有因素后确信倚据证书实属合理，方可倚据该等证书；
b) 于倚据该「智方便」电子证书前，确定「智方便」电子证书及其支援的任何数码签署用于适当的用途；
c) 履行第 9.6.3 条中列载之所有行为。

2.2 收费

「智方便」电子证书免费提供给登记人。

2.3 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「智方便」电子证书有关之其他资料。除平均每周兩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发出的「智方便」电子证书，尽快在储存库作出公布。香港邮政储存库可通过下述 URL 接达：

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

2.3.1 证书储存库控制

储存库所在位置可供网上浏览，并可防止擅进。

2.3.2 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。

2.3.3 证书储存库更新

储存库会于「智方便」系统收到香港邮政发出「智方便」电子证书或香港邮政透过「智方便」核证登记办事处收到申请人的证书撤销清单更新要求时尽快作出更新。

2.3.4 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。

2.4 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、撤销及公布「智方便」电子证书之系统是否妥善遵守本准则。

3. 身份辨识与验证要求

3.1 首次申请

3.1.1「智方便」持有人为先决条件

香港居民可利用不同的注册渠道获取「智方便」，只有（i）在「智方便」核证登记地点登记或（ii）透过配备近场通讯（NFC）功能的智能手机上的「智方便」流动应用程式登记的「智方便」持有人，方有资格申请「智方便」电子证书。

香港居民在提供香港身份证及其本人成功通过「智方便」核证登记办事处的身份核实后，即可在「智方便」核证登记地点获得「智方便」。他们可到「智方便」核证登记地点，透过配备读卡器的特定装置进行登记，该读卡器可识别香港身份证的真伪，并读取储存在香港身份证晶片内的身份资料（包括英文姓名、中文姓名（如有）、香港身份证号码、签发日期、出生日期及性别）。如该特定装置不配备读卡器，处於「智方便」核证登记地点的人员会核实登记者香港身份证的真伪并输入登记者的身份资料到「智方便」系统。登记者于「智方便」核证登记地点提供的身份资料及现场拍摄的照片将会传递到入境事务处的支援电脑系统，用作核对其与入境事务处的记录是否相符，以确认登记者是否香港居民，其提供的身份资料是否真确，及其现场拍摄的照片与入境事务处的记录是否吻合。如没有於现场拍摄照片，「智方便」核证登记地点的人员会面对面检查登记者的身份证并认证登记者之容貌是否与载于香港身份证上的照片相符。

此外，香港居民亦可以透过配备 NFC 功能的智能手机上的「智方便」流动应用程式进行登记来取得「智方便」。登记者将被要求拍摄自己本人的香港身份证以进行身份核实。完成初步核实真伪后，「智方便」流动应用程式会透过 NFC 身份功能读取储存在香港身份证晶片内的加密身份资料（包括英文姓名、中文姓名（如适用）、香港身份证号码、签发日期、出生日期及性别），并将有关资料传送到「智方便」后端系统进行解密。经解密的身份资料及登记者自己本人的自拍照将会传送到入境事务处的支援电脑系统，以便与入境事务处的记录进行核对，以确定登记者是否香港居民，其身份资料是否真确，以及登记者自己本人的自拍照与入境事务处的记录是否吻合。

3.1.2 初次申请

「智方便」电子证书的申请人必须透过「智方便」系统递交证书申请。「智方便」电子证书的申请人必须为「智方便」持有人（请参阅第 3.1.1 条）。「智方便」核证登记办事处及其承办商将核实申请人「智方便」持有人的身份（i）透过「智方便」系统双重认证程序，或（ii）申请人在「智方便」核证登记地点或透过配备 NFC 功能的智能手机上的「智方便」流动应用程式进行登记，且其身份获得核实并成功登记「智方便」（请参阅第 3.1.1 条）。当身份核实完成后，「智方便」核证登记办事处会将证书申请递交给香港邮政。

香港邮政会透过「智方便」系统向成功递交证书申请的申请人发出「智方便」电子证书。申请人同意「智方便」系统收讫「智方便」电子证书即被视为申请人接受「智方便」电子证书。

3.1.3 「智方便」电子证书上列出的登记人名称

透過證書上的主體名稱，包括依據第 4.1 条中的程序所核实的登記人姓名，可識別「智方便」電子

證書登記人之身份。登记人香港身份证号码会以雜凑數值形式储存于证书内（见**附录 B**）。

就发出予十八岁以下人士的「智方便」电子证书而言，透過上文提及之证书上的主体名称及“iAM Smart-Cert (Minor)”字样（见**附录 B**），可識別登記人之身份，及显示登记人获发出「智方便」电子证书时未满 十八岁。

3.1.4 证明有权使用私人密码匙之方法

「智方便」核证登记办事处通过使用登记人的私人密码匙产生数码签署。登记人的私人密码匙储存在「智方便」系统的硬体安全模组内。登记人在使用私人密码匙来产生数码签署前，必须根据「智方便」核证登记办事处的规定，通过严格的验证程序（即双重认证程序）以核实登记人其「智方便」持有人的身份。

「智方便」核证登记办事处之获授权人员必须通过由「智方便」核证登记办事处设计之严格的验证程序后，方可配置、操作和维护储存了由「智方便」核证登记办事处保管之私人密码匙之「智方便」系统。

3.2 证书续期

3.2.1 「智方便」电子证书续期

「智方便」核证登记办事处将在证书有效期届满前至少一个月通知登记人续期。 证书续期程序如下：

（a）「智方便」核证登记办事处透过电子方式向登记人发出续期通知；
（b）登记人同意授权「智方便」核证登记办事处为「智方便」电子证书续期，并透过「智方便」系统的双重认证程序核实其「智方便」持有人的身份；
（c）登记人透过「智方便」系统向香港邮政递交续期申请。

香港邮政不会为已过期或被撤销的证书续期。

3.2.2 已过期或已撤销的「智方便」电子证书

香港邮政会在储存库中发布所有已过期和被撤销证书的资料，并注明其过期或被撤销的状态。此外，已被撤销的证书也会在证书撤销清单内发布。

下文第 4.2.3（a）条规定了用于显示证书被撤销状态的证书撤销清单的更新时间。至于更新储存库以显示过期「智方便」电子证书状态的时间，香港邮政将在证书到期后在储存库内更新过期状态。香港邮政还会提供线上证书状态应答，以检查「智方便」电子证书的撤销状态。

在允许登记人使用「智方便」电子证书之前，「智方便」核证登记办事处将检查登记人的「智方便」电子证书的有效期以核实「智方便」电子证书是否已过期，并透过检查线上证书状态应答，或者在没有在线上证书状态的情况下检查证书撤销清单，以核实「智方便」电子证书是否被撤销。「智方便」核证登记办事处有责任进行上述核实，以确保「智方便」电子证书在已过期或被撤销的情况下，其登记人或任何其他人都无法再使用该「智方便」电子证书。

3.2.3 定期审核

「智方便」系统至少每月一次审核登记人其「智方便」的有效性，当中包括审核登记人之：

（a）死亡记录；
（b）香港居民身份；
（c）香港身份证上显示的个人资料（包括英文姓名，中文姓名（如有），香港身份证号码，出生日期和性别）； 和
（d）「智方便」持有人的身份。

如果定期审核显示某登记人的「智方便」因登记人死亡或失去其香港居民身份或根据本准则第 3.2.3（c）条更改了其个人资料而失效，则「智方便」核证登记办事处将吊销登记人的「智方便」，并在符合《个人资料（私隐）条例》（第 486 章）第 30（5）条的通报要求后，通知香港邮政撤销登记人的「智方便」电子证书。 当香港邮政撤销登记人的「智方便」电子证书后，「智方便」核证登记办事处将立即通知登记人。

如果定期审核显示根据本准则第 3.2.3（d）条登记人不再是「智方便」的持有人，则「智方便」核证登记办事处将通知香港邮政撤销「智方便」电子证书，并在证书撤销后立即通知登记人。

如果「智方便」电子证书已被撤销，符合资格的登记人仍可申请新的「智方便」电子证书。

4. 运作要求

除特别声明外，此 4.1 条所有规定适用于「智方便」电子证书的申请和发出。

4.1 证书申请、发出和公布

4.1.1 证书申请

4.1.1.1
首次申请「智方便」电子证书的申请人必须为「智方便」持有人（请参阅第3.1.1条），并且必须透过「智方便」系统递交证书申请要求和接受登记人协议条款及条件。

4.1.1.2
香港居民只有在「智方便」核证登记办事处核实其身份资料（包括英文姓名、中文姓名（如有）、香港身份证号码及签发日期、出生日期、性别和香港居民身份）后，才会被获发「智方便」（请参阅第 3.1.1 条）。「智方便」电子证书申请人必须为「智方便」持有人（请参阅第 3.1.1 条）。「智方便」核证登记办事处代表香港邮政核实以确保申请人为「智方便」持有人的身份（i）透过「智方便」系统双重认证程序或（ii）申请人在根据第 3.1.1 条进行「智方便」登记，且其身份获得核实并成功登记「智方便」（请参阅第 3.1.1 条）。在不影响条例第 40 条所述之前提下，香港邮政确认有关该等资料，其将不会进行任何进一步的核实，香港邮政将根据其现有之状态（即“申请人为「智方便」持有人，并且申请人的身份资料已获「智方便」核证登记办事处核实” ）接受该等资料。

4.1.2 发出证书

4.1.2.1
若成功核实申请人「智方便」持有人之身份，「智方便」核证登记办事处会在其处所内的环境下使用「智方便」系统内的硬体安全模组（HSM）产生申请人之私人密码匙和公开密码匙。「智方便」核证登记办事处负责确保私人密码匙不会被篡改。

4.1.2.2
「智方便」核证登记办事处会在其处所内一套可靠的系统及环境下产生包含公开密码匙的「签发证书要求」（CSR）。「智方便」核证登记办事处将准备一个包含申请人资料、申请人接受登记人协议记录和签发证书要求的界面档案。界面档案将以电子形式递交给香港邮政。

4.1.2.3
一旦从「智方便」核证登记办事处收到签发证书要求，香港邮政会通过使用内含的公开密码匙检查证书署名请求架构上的数码签署来核实「智方便」核证登记办事处持有相应的私人密码匙。香港邮政不会拥有申请人的私人密码匙。

4.1.2.4
一旦核实「智方便」核证登记办事处持有相应的私人密码匙，香港邮政会产生包含申请人公开密码匙的「智方便」电子证书，并会以安全的方式将发出的「智方便」电子证书传送到「智方便」核证登记办事处。

4.1.2.5
「智方便」核证登记办事处会连接申请人的「智方便」至「智方便」电子证书，以启动申请人之电子证书，并透过「智方便」系统来通知申请人其「智方便」电子证书申请已完成。

4.1.2.6
申请人透过「智方便」系统递交「智方便」电子证书申请，当「智方便」系统收讫其「智方便」电子证书时，即表示申请人接受「智方便」电子证书。一旦申请人成功申请和接受「智方便」电子证书，其已发出的「智方便」电子证书会根据条例第 36条于香港邮政储存库内公布。

4.1.2.7
「智方便」核证登记办事处一旦收讫申请人的「智方便」电子证书，会保管其私人密码匙。

4.1.2.8
所有于「智方便」核证登记办事处和香港邮政之间以电子形式传输的资料必须采用双方同意的规约进行。

4.1.3 公布证书
香港邮政会尽快在储存库公布已发出并获接受的「智方便」电子证书。申请人可透过储存库核实证书上的资料。

4.2 撤销证书

4.2.1 撤销证书的情况

4.2.1.1
若核证机关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。在核证机关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（请参阅第 4.6.2 条）。

4.2.1.2
若登记人之登入「智方便」的凭证已经或者被怀疑已经外泄，登记人必须立刻遵照本准则中规定的撤销程序向香港邮政（透过「智方便」核证登记办事处）申请撤销证书。

4.2.1.3
若私人密码匙或保存公开密码匙相对应之私人密码匙之硬体安全模组已经或者被怀疑已经外泄，「智方便」核证登记办事处必须立即通知香港邮政并向香港邮政申请撤销「智方便」电子证书。「智方便」核证登记办事处必须立即通知相关「智方便」电子证书的登记人，上述有关通知香港邮政和向香港邮政申请撤销已发给该等登记人之「智方便」电子证书。

4.2.1.4
一旦发生任何以下有关「智方便」电子证书的情况或怀疑有该等情况发生，香港邮政将立即撤销该等「智方便」电子证书，更新证书撤销清单（CRL）并透过线上证书状态应答回应其撤销状态，届时香港邮政将透过「智方便」核证登记办事处通知登记人（「撤销证书通知书」）：

a) 「智方便」电子证书之私人密码匙已外泄；
b) 「智方便」电子证书之细节不真实或已变得不真实或证书不可靠；
c) 「智方便」电子证书并非根据本准则妥当发出；
d) 获得发出「智方便」电子证书之登记人未履行本准则或登记人协议列明之责任；
e) 证书适用之规则或法例有此规定；
f) 获得发出「智方便」电子证书之登记人死亡或丧失香港居民身份或已更改显示于其香港身份证上的个人资料（请参阅第3.2.3(a)-(c)条），导致登记人之「智方便」失效；
g) 登记人停止作为「智方便」的持有人（请参阅第3.2.3(d)条）
h) 「智方便」电子证书（未成年人士）之登记人年满18岁。

4.2.1.5
当香港邮政根据第 4.2.1.4 条发出撤销通知书予「智方便」电子证书之登记人，「智方便」核证登记办事处必须立即停止使用该「智方便」电子证书，并且不得允许「智方便」电子证书之相关的私人密码匙被使用。

4.2.2 撤销程序请求

4.2.2.1
登记人可透过「智方便」核证登记办事处的「智方便」系统或其他「智方便」核证登记办事处指定的沟通渠道向香港邮政提出撤销证书之申请。登记人不得直接向香港邮政提交申请。

4.2.2.2
当登记人发出撤销证书请求，「智方便」核证登记办事处将代表香港邮政就登记人进行身份核实。当登记人身份核实完成后，「智方便」核证登记办事处将立即把撤销请求转交予香港邮政。

4.2.2.3
当香港邮政收到「智方便」核证登记办事处之撤销请求后，香港邮政将立即撤销该证书。

4.2.2.4
所有被撤销证书之有关资料（包括表明撤销证书之原因代码）将刊载于证书撤销清单内（请参阅第 7.2 条），并可以透过线上证书状态应答来检查（请参阅第 7.3 条）。

4.2.3 服务承諾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) 香港邮政根据第 4.2.2 条规定，透过「智方便」核证登记办事处从登记人处确切收到撤销证书之请求后，或(2)香港邮政根据第 4.2.1.4.条规定发出撤销证书通知书后，将证书该撤之状态于证书撤销清单公布。然而，证书撤销清单并不会于各证书撤销后随即在公众目录中公布，而只会在下一份证书撤销清单更新并公布时，才会反映该证书已撤销之狀态。如附录 C 第 2 段所述，证书撤销清单每日于香港时间 0915, 1415 和 1900 公布，并存档至少七年。

香港邮政会以合理的方式，根据第 4.2.1.4.条规定，透过「智方便」核证登记办事处发出撤销证书通知予有关登记人。

b) 在以下任何情况发生之后，登记人均不得使用其姓名登记之证书：

(i) 登记人获悉香港邮政根据本准则中的条款（包括第 4.2.1.4 条规定的事项）可能据以撤销证书之任何情况；或

(ii) 登记人根据第 4.2.2.1.条规定透过「智方便」核证登记办事处向香港邮政提出撤销证书请求。

倘若登记人在以上任何情况发生之后，仍在任何交易中使用该等证书，则香港邮政和「智方便」核证登记办事处无须就任何该等交易向登记人或倚据证书人士承担任何责任。

c) 此外，一旦发生上述 b 项（i）至（ii）中列载的任何有关情况，登记人须立即通知倚据证书人士，告知其不得在交易中倚据登记人之证书。无论登记人是否已通知倚据证书人士不得在交易中倚据登记人之证书，香港邮政和「智方便」核证登记办事处无须就该等交易向登记人和倚据证书人士承担任何责任。

对于从香港邮政由做出撤销证书之决定（不论是应要求或是自行作出该等决定）至该等证书撤销出现在证书撤销清单上之间的期间内或至线上证书状态应答更新了回应证书撤销状态之间的期间内所发生的交易，以及在此之后使用任何已撤销证书所引起之任何交易，香港邮政和「智方便」核证登记办事处无须就该等交易向登记人和倚据证书人士承担任何责任。

d) 证书撤销清单、香港邮政授权撤销清单（ARL）会依据在**附录 C** 内指明的时间表及格式更新及公布。

4.2.4 撤销之生效时间

在不影响上述第 4.2.3 条 b 至 d 项的前提下，在撤销状态出现在证书撤销清单上，或在线上证书状态应答更新了撤销状态之时，该证书即告终止。尽管有上述关于终止证书之生效时间（或在其之后）之规定，对违反第 4.3.3 条 b 项或其他可适用之规定而使用证书的行为，香港邮政和「智方便」核证登记办事处概不负责。倚据证书人士在倚据「智方便」电子证书进行交易前，必须查核储存库、证书撤销清单和/或相关之线上证书状态应答。然而，如果「智方便」核证登记办事处已妥当地履行了第 3.2.2 条列载的义务，已过期或已撤销之「智方便」电子证书均不可能再被授权使用（如适用）。

4.3 电脑保安审核程序

4.3.1 记录事件類型

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审核追踪保安档案内。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：

- 处理撤销证书之要求
- 实际发出及撤销证书
- 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
- 产生及签署线上证书状态应答
- 核证机关密码匙转换
- 档案备存
- 密码匙紧急复原

4.3.2 处理纪录之次数
香港邮政每日均会处理及覆检审核运行记录，用以审核追踪有关香港邮政的行动、交易及程序。

4.3.3 审核记录之存留期间
存档审核记录文档存留期为至少七年。

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

4.3.5 审核记录备存程序
香港邮政每日均会按照预先界定程序（包括多人式控制）为审核记录作适当备存。备存会另行離机储存，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。

4.3.6 审核资料收集系统
香港邮政系统审核记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。

4.3.7 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。

4.3.8 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。

4.4 记录存档

4.4.1 存档记录類型
香港邮政须确保存档记录记下足够资料，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）存有以下數据：

a) 系统设备结构档案
b) 评估结果及/或设备合格 覆检(如曾进行)
c) 核证作业准则及其修订本或最新版本

d) 对香港邮政具约束力而构成合约之协议
e) 所有发出或公布之证书及证书撤销清单，以及所有线上证书状态应答
f) 定期事件记录
g) 其他需要以核实存档内容之数据，以及
h) 证书申请的相关文件，证书批准或拒绝的资料以及登记人协议。

4.4.2 存档保存期限
密码匙及证书资料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。

4.4.3 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，可避免未经授权之进入。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。

4.4.4 存档备存程序
在有需要时制作并保存存档之副本。

4.4.5 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。

4.5 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「智方便」电子证书的香港邮政核证机关根源证书，在**附录 E** 列载其有效期由产生之时起计算不超过二十五年。香港邮政核证机关根源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，相連之根源证书会在香港邮政网页 http://www.eCert.gov.hk 公布，供大众取用。原先之根源密码匙则保留至第 4.4.2 条指定之最短之时限，以供核实用原先之根源密码匙产生的任何签署。

4.6 灾难复原及密码匙资料外泄之应变计划

4.6.1 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保证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離核证机关主要营运设施不少于十千米的地点。业务持续运作计划每年均会检讨及进行演练。

如发生严重故障或灾难，香港邮政即时知会政府资讯科技总监，并公布将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離设施并锁于其他臨时设施内；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。

在发生灾难后但稳妥可靠的环境尚未重新确立前的这一期间内，香港邮政将无法更新证书撤销清单，也无法返回线上线上证书状态应答。登记人可以继续使用「智方便」电子证书，但须自负风险。香港邮政亦无法发出证书，撤销证书或开放储存库供下载公共密码匙和证书。

4.6.2 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「智方便」电子证书的核证机关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。核证机关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。

4.6.3 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的「智方便」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核证机关公开密码匙及如何向登记人重新发出证书。

4.7 核证机关终止服务

如香港邮政停止担任认可核证机关之职能，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至少七年（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。

根据香港邮政终止服务计划，香港邮政会在终止服务生效前至少九十天知会政府资讯科技总监其准备终止「智方便」电子证书有关服务。香港邮政会在终止服务生效前至少六十日，透过电子邮件、信件或者透过「智方便」系统通知所有登记人其准备终止作为认可核证机关之服务。香港邮政认可核证机关将会在香港发行的一家英文日报（如可行）以及一家中文日报上刊载其准备终止作为认可核证机关之服务。该等公告必须在终止服务生效前至少六十日刊发，且必须持续刊载三天。

4.8 「智方便」核证登记办事处终止服务

无论是什么原因的情况下，若「智方便」核证登记办事处停止担任根据本准则之核证登记机关，经「智方便」核证登记办事处发出的「智方便」电子证书也将同时被撤销。香港邮政和「智方便」核证登记办事处无须对任何人因证书撤销所引起的索赔、法律程序、债务、损失（包含任何直接或间接的损失、任何收益损失、利润、商业机会、合约或预期存款）、损害（包含任何直接、特殊、间接或从属的任何性质的损害）或任何损失或费用承担任何责任。

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。

5.1.2 进入控制
香港邮政实施商业上具备合理之实体保安控制措施，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），而可使用该等硬体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。

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 防火及消防保护
核证机关设施备妥防火计划及灭火系统。

5.1.6 媒体存储
媒体存储及处理程序已经开发备妥。

5.1.7 场外备存
香港邮政核证机关系统數据之适当备存会另行储存于其他场所，并获足够保护，以免被盗用、损毁及媒体衰变。(另见第 4.6.1 条)。

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、使用或撤销带來重大影响（包括进入香港邮政核证机关资料库受限制之运作）之香港邮政、「智方便」核证登记办事处或承办商之雇员、合约分判商以及顾问（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「智方便」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。香港邮政进行按角色及责任订定各级实体及系统接达控制，以及采取职责分离措施，以维护有关程序之完整性。

5.2.2 香港邮政、承办商与「智方便」核证登记办事处之间的文件及资料传递
香港邮政、「智方便」核证登记办事处与承办商之间的所有文件及资料的传递，均使用香港邮政规定且获得「智方便」核证登记办事处和承办商同意之协约，以惯常的控制及安全方式进行。

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 2.4 条）。

5.3 人员控制

5.3.1 背景及资格
香港邮政、「智方便」核证登记办事处及承办商采用之人员及管理政策，可合理确保各自之人员（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
根据本准则之规定，香港邮政会调查及 /或要求「智方便」核证登记办事处和承办商调查担任受信职责之人员（在其受聘/加入前及其后有需要时定期进行），以核实该等人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
香港邮政人员、「智方便」核证登记办事处人员与承办商人员均已接受了履行其职责所需要之初步培训。有需要时，香港邮政、「智方便」核证登记办事处与承办商亦会提供持续培训，使其人员能掌握所需最新工作技能。

5.3.4 向人员提供之文件
香港邮政人员、「智方便」核证登记办事处人员及承办商人员会收到综合用户手册，其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

本条說明香港邮政特别为保障加密密码匙及相关數据所订之技术措施。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由多人式控制之可防止篡改硬件装置内进行。

6.1 产生及安装配对密码匙

6.1.1 产生配对密码匙

除非程序被获授权使用者外泄，否则香港邮政核证机关根源证书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。香港邮政产生核证机关根源证书配对密码匙，用于发出符合本准则之「智方便」电子证书。「智方便」核证登记办事处在其处所内的的环境下使用「智方便」系统内的硬体安全模组产生「智方便」电子证书申请人之配对密码匙。

6.1.2 登记人公开密码匙交付

「智方便」核证登记办事处会在产生申请人/登记人的配对密码匙后产生包含公开密码匙的「签发证书要求」（CSR），并透过系统界面将该要求传送至香港邮政。

6.1.3 公开密码匙交付予登记人

香港邮政核证机关根源证书之公开密码匙可从网页 http://www.eCert.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。「智方便」电子证书的登记人配对密码匙为 2048 位元 RSA。

6.1.5 加密模组标准

香港邮政进行之签署密码匙的产生、存储及签署操作均在硬体加密模组内进行。

6.1.6 密码匙用途

「智方便」电子证书之密码匙用于进行数码签署。香港邮政核证机关根源证书密码匙（用于产生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。此外，线上证书状态应答签署人之证书用于签署线上证书状态应答。

6.2 私人密码匙保护

6.2.1 加密模组标准

香港邮政核证机关根源证书私人密码匙利用加密模组产生，其级别至少达到 FIPS140-1 第 4 级。

6.2.2 私人密码匙多人式控制

香港邮政核证机关根源证书私人密码匙储存在可防止篡改加密硬体装置内。香港邮政采用多人式控制启动、使用、终止香港邮政私人密码匙。

6.2.3 私人密码匙托管
香港邮政并无为香港邮政核证机关根源证书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
香港邮政核证机关根源证书私人密码匙的备存，是使用达到 FIPS 140-1 第 4 级保安标准的装置加密及储存。香港邮政核证机关根源证书私人密码匙的备存程序须超过一名人士参与完成。备存的私人密码匙亦须由超过一名人士启动。其他私人密码匙均不设备存。所有私人密码匙不会存档。

6.3 配对密码匙管理其他范畴
香港邮政核证机关根源证书及相关密码匙使用期不超过二十五年（同见第 4.5 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，均于硬体加密模组内进行。第 4.4 条详述香港邮政核证机关根源证书公开密码匙记录存档之工作。

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香港邮政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 2.4 条详述遵守规定之评估。

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。

6.6 网络保安控制
香港邮政核证机关系统有防火墙以及其他接达控制机制保护，其配置只允许根据本准则所载已获授权之核证机关服务者接达。

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份及核实该等讯息是否完整之公开密码匙（即用于核实數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「智方便」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

通过发布一个包含主体名称“Hongkong Post Root CA 2 OCSP Responder”的线上证书状态应答签署人证书，香港邮政已授权一个线上证书状态应答伺服器为根证书 “Hongkong Post Root CA 2” 进行线上证书状态应答的签署。通过发布包含主体名称“Hongkong Post e-Cert CA 2 - 19 Responder”的线上证书状态应答签署人证书，授权线上证书状态应答伺服器为中继证书 “Hongkong Post e-Cert CA 2 - 19” 进行线上证书状态应答的签署。

线上证书状态应答结构详情见**附录 C**。

8. 本准则管理

本准则之更改一律须经香港邮政批准并公布。有关准则一经香港邮政在香港邮政核证机关网页 http://www.eCert.gov.hk 或香港邮政储存库公布，更改即时生效，并对获发证书的申请人以及登记人均具约束力。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、登记人及倚据证书人士可从香港邮政核证机关网页 http://www.eCert.gov.hk 浏览此份准则以及其旧有版本。

9. 法律责任和其他业务条款

此部分为有关「智方便」电子证书之法律陈述，保证和限制条款。

9.1 费用

9.1.1 证书发出或续期费用
「智方便」电子证书免费提供予登记人。

9.1.2 证书查询费用

香港邮政保留对查询其证书数据库确定和收取合理费用之权利。

9.1.3 撤销或状态资料查询费用
香港邮政不会就撤销证书或倚据证书人士透过使用证书撤销清单或线上证书状态应答查看证书的撤销状态收取费用。

9.1.4 香港邮政对已获接收但有缺陷之证书所承担之责任
尽管下文已列明香港邮政承担责任之限制，若登记人接收「智方便」电子证书后发现，因「智方便」核证登记办事处产生的「智方便」电子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，及登记人将此情况立即通知「智方便」核证登记办事处以便撤销证书及（如愿意）重新发出证书，则「智方便」电子证书将重新发出给登记人。

9.2 财务责任

9.2.1 保险范围
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。

9.3 业务资料之保密

9.3.1 保密资料范围
在无意减损其根据条例第 46 条的规定必须承担之义务之情况下，香港邮政特别将以下类别的资料保密（统称“保密资料”），并维持合理地控制以防止该等记录泄露给非受信工作人员。

a) 所有香港邮政拥有及保管的，用于签署和向登记人发出证书的根源认可核证机关/次认可核证机关的私人密码匙；
b) 任何业务连续性，应急反应，意外事件及灾难恢复计划；
c) 任何其他用于保护资料保密性，完整性和可用性的安全实务，措施，机制，计划或程序；
d) 任何根据第 9.4 条作为隐私资料被香港邮政保管之资料；
e) 任何第 4.4.1 条指明之交易记录，审计记录及档案记录，包括证书申请记录以及提交用于辅助申请证书之文件，无论该等申请最后成功或被拒；
f) 交易记录，财务审计记录和外部或内部审计记录及任何审计报告（审计师确认本准则规定之

控制的有效性的信函除外）。

9.3.2 不属于保密的资料

9.3.2.1
公布于「智方便」电子证书内的登记人申请数据被视为公开且不属于保密资料。登记人确认所有香港邮政核证机关发出的证书的撤销数据是公开资料并于储存库中公布。

9.3.2.2
私人密码匙由「智方便」核证登记办事处保管，香港邮政不会保存任何「智方便」电子证书的私人密码匙。私人密码匙由「智方便」核证登记办事处在其处所内的环境下产生，并储存在「智方便」系统内的硬体安全模组中。提醒申请人和登记人在申请或续期或接受或使用「智方便」电子证书前，他们应符合「智方便」核证登记办事处采取适当的有关确保私人密码匙保密性和安全性的保安措施。

9.4 个人资料隐私保密

9.4.1 隐私保密方案
香港邮政已施行隐私政策，以符合本准则之规定。香港邮政的隐私政策于此网页公布：https://www.hongkongpost.hk/sc/privacy/index.html。

9.4.2 视作隐私的资料
在证书或证书撤销清单中不提供于公众的有关人士之个人资料被视作隐私（统称“隐私资料”）。

9.4.3 不被视作隐私的资料
证书、证书撤销清单以及出现在证书、证书撤销清单内的个人资料不被视为隐私资料。

9.4.4 使用隐私资料的告知及同意
在得到对象书面同意，或因应适用之法律或法院命令或其他于条例第 46（2）条规定的情况之要求，香港邮政可以使用对象之隐私资料。

9.4.5 倚据司法及行政程序的资料披露
除条例第 46（2）（a）至（d）条之情况，香港邮政不得泄露任何机密资料。无意减损第 46（2）条规定的除外范围的情况下，香港邮政可以（a）不时向「智方便」核证登记办事处、承办商、其他承办商、顾问或咨询人披露机密资料，如果该等披露是为了按照条例规定履行某职能或者为了条例之目的。或（b）向「智方便」核证登记办事处披露机密资料，如果该等机密资料与登记人或登记人的证书申请、续期和撤销有关。

9.5 知识产权
香港邮政、「智方便」核证登记办事处及承办商拥有所有有关其数据库、系统、网页和包括本准则在内的任何源自香港邮政之公开之知识产权。

商标“香港邮政（HKPost）”和“香港邮政电子证书(Hongkong Post e-Cert)”乃香港邮政之注册商标。

香港邮政可拥有其他未被注册的商标或服务商标，但其仍为香港邮政的财产。

证书乃香港邮政独家拥有之财产。倘若证书按照非独占性及免专利的准则下进行完全复制及分发，则香港邮政允许该等复制和分发的进行。香港邮政保留于任何时候酌情撤销证书的权利。

9.6 声明与保证

9.6.1 香港邮政之声明与保证

9.6.1.1
香港邮政仅向登记人和所有在有效期内实际倚据该类证书的倚据证书人士作出以下保证和声明（“证书保证”）。

9.6.1.2
在下述限定下，证书保证特别包含保证如下事项：

(A) 一经发出「智方便」电子证书，香港邮政即向任何合理倚据包含于「智方便」电子证书内的资料之人士，或合理倚据可由列载于「智方便」电子证书内的公开密码匙核实的数码签署之人士声明，香港邮政已根据本准则发出证书。

(B) 一经公布「智方便」电子证书，香港邮政即向任何合理倚据包含于「智方便」电子证书内的资料之人士声明，香港邮政已向证书辨识之登记人发出证书。

9.6.1.3
对于包含于证书中的其他任何资料，或者由香港邮政，或代表香港邮政编辑、公布或传播的任何其他资料，香港邮政对于其准确性、真实性、完整性或适当性不做任何保证。

9.6.1.4
香港邮政不保证任何软件或硬体装置的质量，功能或性能。

9.6.1.5
由于香港邮政不可控制之原因导致证书无法撤销，香港邮政不承担责任。

9.6.2 登记人之声明与保证

9.6.2.1
各登记人必须亲身签署或确认接受登记人协议。作为登记人同意的登记人协议的一部分，下列所有承诺与保证皆由或皆视为由登记人作出，并明确为了香港邮政、「智方便」核证登记办事处以及所有倚据证书人士之利益而做出，并在申请、发出以及以其名字发出之证书的有效期内保持真实、完整和准确:

(A) 资料准确性：有义务并且保证在任何时候，在申请「智方便」电子证书或者不时被香港邮政提出要求（不论直接或经由「智方便」核证登记办事处要求）的情况下向香港邮政和「智方便」核证登记办事处提供准确和完整之资料以及其他陈述，该等资料包括但不限于发出和接受证书所需要的资料和陈述；

(B) 接受证书：有责任并保证登记人不会使用证书直到登记人审核和核实了证书内数据的准确性；

(C) 证书之使用：有责任并保证仅在遵守所有适用的法律的情况下使用证书，并仅根据登记人协议来使用证书；

(D) 因资料外泄进行的报告和撤销：一旦发生任何列载于第 4.2.1.4 条的情况，有责任并保证透过「智方便」核证登记办事处要求香港邮政撤销证书；以及

(E) 终止使用证书：有责任并保证根据第 4.2.3(b)条，立即停止使用证书及其私人密码匙。

9.6.2.2
在未限制本准则规定之登记人的其他义务的情况下，登记人仅就于证书内发表的任何失实声明向合理倚据该声明之第三方承担责任。

9.6.2.3
一旦接受证书，登记人即从其接受证书之时开始并在证书的有效期向香港邮政、「智方便」核证登记办事处及倚据证书人士声明、保证并负担以下义务：

(A) 使用对应于包含在证书内的公开密码匙的私人密码匙进行的交易是登记人自己的行为，并且证书在当时以及证书的有效期内已被接受并可正常使用；

(B) 登记人向香港邮政（无论直接或透过「智方便」核证登记办事处）及「智方便」核证登记办事处作出的声明均为真实，准确和完整；

(C) 所有包含于证书内的资料为真实，准确和完整；

(D) 证书仅用于经授权和合法的用途，符合本准则规定，并且登记人将于附录 D 中列载之用途中使用证书；

(E) 登记人同意本准则之条款和条件；

(F) 登记人遵守适用于其国家和地区之法律；

(G) 登记人均已授权「智方便」核证登记办事处，保管登记人证书之私人密码匙，及每当登记人进行数码签署时，接达其证书之私人密码匙；

(H) 在使用登记人的证书之私人密码匙前，登记人已提交「智方便」核证登记办事处规定的严格的验证程序以核实其「智方便」持有人的身份；

(I) 使用登记人证书中的公开密码匙对应之私人密码匙而产生的数码签署，乃登记人之数码签署。

9.6.3 倚据证书人士之声明与保证
倚据证书人士接受，为了合理倚据一份「智方便」电子证书，倚据证书人士必须履行以下所有事项：

(A) 做出合理努力以获取有关使用电子证书及公匙基建的足够知识；

(B) 阅读附录 D 中所列载电子证书的用途及其使用限制，并透过本准则了解香港邮政对于倚据发出的「智方便」电子证书之法律责任的限制；

(C) 通过使用该等人士之名称，搜索储存库以核实登记人是否具有有效的未过期之「智方便」电子证书。停止倚据已经过期之「智方便」电子证书；

(D) 通过参考证书撤销清单或相关的线上证书状态应答核实「智方便」电子证书。被撤销之「智方便」电子证书会在证书撤销清单或相关的线上证书状态应答中显示相应的状态。停止倚据已经被撤销之「智方便」电子证书；

(E) 采取任何其他合理的措施将倚据无效的，撤销的，届满的或被拒的「智方便」电子证书产生或以未被授权的方式使用的「智方便」电子证书而产生的数码签署所导致的风险最小化；及

(F) 考量以下因素，并仅在根据实际情形确为合理之情况下才倚据「智方便」电子证书：

(a) 确认一方身份所需要的任何法律要求，保护资料的保密性或隐私性，或根据任何适用的法律，该交易具有的法律可执行性；
(b) 倚据证书人士已经注意到或者应当注意到的，列载于证书和本准测中的所有事实；
(c) 交易的经济价值；
(d) 因为在申请、交易或者交流过程中发生验证错误、丧失资料的保密性或私密性造成的潜在损失或潜在损害；
(e) 特定的司法管辖区的法律的适用性，包括列载于与登记人协议或本准则中的司法管辖权；
(f) 倚据证书人士之前与登记人交易的过程，若有；
(g) 贸易惯例，包括与基于计算机的贸易方式有关的的经验；及
(h) 任何其他可靠或不可靠的标记，以及倚据证书人士知道或注意到的其他关于登记人和/或申请、沟通或交易之事实。

9.7 法律责任限制

9.7.1
登记人有权在由「智方便」核证登记办事处（如有）提供的机制内酌情决定可使用「智方便」电子证书的交易的最大金额。「智方便」电子证书本身不会就登记人和倚据证书人士之间的交易的最大金额设置限定。

9.7.2
一般免责声明：在法律允许的最大限度下，香港邮政及「智方便」核证登记办事处无须对任何人因以下任何事项造成的，或起因于以下任何事项，或与以下任何事项有关联之任何索赔、诉讼、债务、损失（包含任何直接或间接的损失、任何收益损失、利润、业务、合约或预期存款）、损害（包含任何直接、特殊、间接或附加的任何性质的损害）或任何损失或开销承担任何责任：(a)香港邮政行使本准则中列载之职能或权力；(b)使用或倚据任何「智方便」电子证书及(c)倚据或使用虚假或伪造的并由「智方便」电子证书支援的登记人数码签署，而对该证书而言香港邮政已经遵

守条例及业务守则中的要求；及(d)以未获授权或不诚实或欺诈手段使用「智方便」电子证书；(e)「智方便」电子证书中或储存库中的任何资料（根据条例第 40 条要求陈述的资料除外）不真实、不准确或不完整。

9.7.3
除列载于条例第 39 条及第 40 条的声明外，即使本准则中有相反之规定，香港邮政不会向任何人（包括任何登记人，任何倚据证书人士和任何承办商）作出任何声明或保证，包括(a)确认证书或储存库中（根据条例第 40 条要求确认的资料除外）的任何资料是准确的，正确的或完整的；及(b)透过使用「智方便」电子证书产生的数码签署进行的任何交易的有效性和合法性。

9.7.4
除列载于条例第 39 条及第 40 条的声明外，在法律允许的最大限度下，无论是根据本准则、条例、业务守则或任何登记人协议或者其他法律，香港邮政不会对任何人（包括任何登记人，任何倚据证书人士和任何承办商）承担谨慎职责(Duty of Care)。如未有违反列载于条例第 39 条和第 40 条的规定，香港邮政或其雇员在其雇用期内的行为或疏忽不能被视为可提起诉讼之疏忽或故意违约行为。

9.7.5
除了条例第 39 条和第 40 条规定的陈述以及其他依法不能予以排除之陈述与保证之外，香港邮政不提供任何类型的陈述、保证和义务，包括特定目的适用性以及对于提供的未经核实之资料的准确性所做的保证。

9.7.6
若有任何不符或违反本准则或登记人协议或条例第 39 条或第 40 条之情况，对于登记人因为上述一次或多次不符或违反而遭受损失或损害而提出的可以获得法律认可且可以证明之索赔，香港邮政就一张「智方便」电子证书的责任而言最高不超过 200,000 港元（总计，如果多过一次不符或违反），或就一张签发予未满 18 岁人士的「智方便」电子证书（未成年人士）的责任而言 0 港元。

9.7.7
若有任何不符或违反本准则或列载于条例第 39 条或第 40 条的声明之情况，对于倚据证书人士因为上述一次或多次不符或违反而遭受的损失或损害而提出的可以获得法律认可且可以证明之索赔，香港邮政就一张「智方便」电子证书的责任而言最高不超过 200,000 港元（总计，如多过一次不符或违反），或就一张签发予未满 18 岁人士的「智方便」电子证书（未成年人士）的责任而言 0 港元。

9.7.8
承办商乃由香港邮政按照香港邮政与承办商之间的独立合约任命之承办商，且此任命只以该独立合约为条件。本准则不给予承办商任何额外的权力或要求香港邮政向承办商承担额外的义务。至于条例第 39 条和第 40 条中的声明，承办商有责任确保其在为香港邮政履行任何条例中列载之职能的限度内遵守条例中规定的内容。承办商不是条例第 40 条提及的合理倚据证书内的资料的人士。

9.7.9
所有申请人、登记人、承办商、倚据证书人士及其他人士、实体和机构同意，除非同意香港邮政于第 9.7 条和第 9.8 条中作出之声明、保证和条件以及规定的法律责任限制，香港邮政将不会向登记人发出证书，香港邮政也不会提供有关证书的服务，这些条款对合理分摊风险十分必要。

9.7.10
本第 9.7 条和第 9.8 条中的各个条款须独立诠释并不得影响本准则其他任何之条款，且除非有明确规定，不得通过参考任何其他条款或由其他条款推断而受限制。

9.8 关于可追讨损失类型的限制及免责声明

9.8.1
在不影响第 9.7 条免责声明的情况下，在任何情况下（除诈骗或故意之不正当行为），香港邮政或「智方便」核证登记办事处无须就以下任何或全部事项，以及所造成之结果承担责任：

9.8.1.1
任何间接的、不确定的或附加的损失或损害（即使香港邮政或「智方便」核证登记办事处已被告知出现此类损失或损害的可能性）；

9.8.1.2
（无论是否视为直接或间接损失）任何利润损失、名誉或声誉上的损失或伤害，机会损失或项目损失；

9.8.1.3
任何死亡或人身伤害（除了任何香港邮政或「智方便」核证登记办事处的疏忽，“疏忽”参照《管制免责条款条例》（香港法律第 71 章）的定义）；

9.8.1.4
任何数据损失；

9.8.1.5
任何由证书或数码签署的使用、传播、许可使用、履行或不履行引起的或者与之有关的其他任何间接的、附加的或惩罚性损害；

9.8.1.6
任何索赔、诉讼、损失或损害（直接或间接或不确定或特殊），但是因为倚据条例第 39 条与第 40 条之声明而造成的除外；

9.8.1.7
任何因倚据证书、证书或储存库内的资料而发生的索赔责任，且该等非正常情况是由于申请人或登记人或任何其他人士之欺诈或故意不正当行为而导致的；

9.8.1.8
任何因未按照本准则使用证书引起的责任；

9.8.1.9
任何因使用无效的证书（过期或已撤销）引起的责任；

9.8.1.10

任何因使用证书超过适用的使用限制而引起的责任；

9.8.1.11
任何因安全性、可用性、产品的完整性而引起的责任（包括申请人/登记人使用的硬体和软件）；

9.8.1.12
任何由证书之私人密码匙外泄引起的责任。

9.8.2 非商品供应
特此澄清，登记人协议并非任何性质之商品之供应合约。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、所有权或利益均不得转让于登记人，登记人仅有权申请发出证书及根据概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或服务；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应商品或服务的陈述或保证。

9.8.3 提出索赔的时限
在不影响第 9.7 条和第 9.8 条及于本准则其他地方规定之免责声明和限制的情况下，任何登记人或倚据证书人士或任何其他人士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、撤销或公布「智方便」电子证书相关，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。

9.8.4「智方便」核证登记办事处、香港邮政署、承办商及其各自之人员
香港政府或香港政府之任何职员、雇员港或其代理人（除了香港邮政）均非登记人协议之签约人。登记人及倚据证书人士必须承认，据登记人及倚据证书人士所知，香港政府、香港政府的任何职员、雇员或代理人（包括「智方便」核证登记办事处和香港邮政的职员、雇员和代理人）（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认可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。各登记人及倚据证书人士向香港政府、其职员与雇员以及代理人（包括「智方便」核证登记办事处和香港邮政的职员、雇员和代理人）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）、并与香港邮政履行登记人协议或由香港邮政作为认可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这些机构及个人免受此等法律行动。

9.8.5 欺诈责任
香港邮政因欺诈造成之责任不属 本准则规定的任何限定或除外规定范围之内，任何登记人协议或由香港邮政发出之证书亦不受任何此等规定之限制或被任何此等规定限制或免除。

9.8.6 证书通知，限制及倚据限额
在不影响本准则余下条款约束力的情况下，香港邮政发出之「智方便」电子证书应认作已包括本

准则第 9.6 条至第 9.15 条之规定。

9.9 赔偿

一旦接受或使用或倚据证书，各登记人和倚据证书人士即同意赔偿香港邮政以及香港政府，及其（包括「智方便」核证登记办事处和香港邮政）职员、雇员、代理人和承办商因任何责任导致的可能会给香港邮政及上述人士造成之任何责任，任何损失或损害以及债务，及任何类别的索赔、法律程序、成本、费用和开支，包括全额赔偿之法律费用，并承诺香港邮政以及香港政府，及其（包括「智方便」核证登记办事处和香港邮政）职员、雇员、代理人和承办商免受上述责任、损失、损害或费用之损害。该等责任、损失、损害或费用等是由于该等人士在使用或公布证书的过程中有如下行为而造成：（i）为获取或使用证书而对重要事实进行了虚假陈述或者未能陈述重要事实（无论此类虚假陈述或遗漏是有意或是由于疏忽或草率造成）；（ii）违反登记人协议、本准则或任何适用的法律；（iii）因该等人士而非因香港邮政的疏忽导致资料外泄或未授权使用证书或私人密码匙；或（iv）误用证书或私人密码匙。

9.10 期限与终止

9.10.1 期限

本准则及其任何修改由香港邮政在香港邮政核证机关网站 http://www.eCert.gov.hk 或在储存库公布时生效，并将维持有效直至根据本准则第 9.10 条终止为止。

9.10.2 终止

本准则可经不时之修改并维持有效，直至被新的版本所取代或者根据本准则第 9.10 条终止为止。

9.10.3 终止的生效与效力续存

本准则终止的条件和效力将在其终止时于香港邮政的储存库（http://www.eCert.gov.hk）予以通告。该通告中将简述不受终止之影响而在终止后持续有效之条款。保护商业秘密和个人隐私之责任终止后继续有效，对于已经存在之证书中的条款和条件将在该证书有效期之剩余期间内继续有效。

在此特别声明，香港邮政可在无需得到任何人之同意的情况下，终止本准则。

9.11 对参与者的个别通知与沟通

香港邮政接受通过电子形式或信件形式寄往本准则第 1.3 条规定地址与本准则有关的通知。当收到来自香港邮政之有效认收信息时，通知的发出者可以藉此确认其沟通已经生效。

9.12 修改

9.12.1

所有对于本准则的修改由有权决定此等修改的香港邮政公布。**在此特别声明，香港邮政可在无需得到任何人之同意的情况下，修改本准则。**有关准则一经香港邮政在香港邮政核证机关网页 http://www.eCert.gov.hk 或香港邮政储存库公布，更改即时生效，并对所有申请人、登记人、「智方便」核证登记办事处、倚据证书人士、承办商以及在登记人协议中被视为第三方人士之其他人士均具有约束力（无需事先考虑或取得任何该等人士之同意）。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。此份准则以及其旧有版本可在香港邮政核证机关网页 http://www.eCert.gov.hk 浏览。**对于那些不同意本准则前述更改的登记人，自这些修改**

生效起一个月内，可以根据第 4.2.2.1 条规定向香港邮政发出通知要求停止使用「智方便」电子证书并透过「智方便」核证登记办事处撤销「智方便」电子证书。在上述的一个月期限内若无任何来自登记人的通知，将视作登记人同意这些更改。

9.12.2
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。在上述规定约束下，所有其他改变都须获得登记人协议各方的同意。登记人协议的变更 (不论是由香港邮政单方进行或登记人与香港邮政达成协议进行) 可在无需取得任何第三方的同意下, 进行上述任何修改。

9.12.3
根据本准则之条款任何一方（不论是由香港邮政单方进行或登记人与香港邮政达成协议进行）终止登记人协议、终止或撤销任何「智方便」电子证书无需取得任何第三方同意。

9.12.4 已经采取合理措施以确保该等第三方会透过公布本准则而了解到本准则第 9.12 条。

9.13 争议之解决程序
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：

香港邮政核证机关
东九龙邮政信箱 68777 号
电邮：enquiry@eCert.gov.hk

9.14 管辖法律
本准则受香港法律规管并依香港法律解释。该等法律选择是为了确保本准则解释一致性，而与香港邮政数码证书的所在地和使用地无关。

双方均同意服从香港法院的专属司法管辖权，以解决因本准则或登记人协议引起的或与之相关的任何争议。

9.15 完整协议

9.15.1
本准则应当持续在符合商业习惯、商业上合理的条件以及本准则涉及之产品或服务的目标用途之范围内进行解释。在解释本准则时，各方应当考虑到香港邮政的服务和产品范围和应用以及其在商业交易中适用之诚信原则。虽有前述之规定，由香港邮政发出的用于其他类型证书的核证作业准则将不被用于解释本准则的规定。

9.15.2
本准则中的标题、副标题以及其他章节仅为方便参考之用，而不应用于解释、解读或执行本准则的任何规定。

9.15.3
本准则的附录和定义对所有人士而言为本准则整体之不可分离且具有约束力之组成部分。

9.15.4

如果/当本准则（包括不时的修改）与其他规则、指南或合约相冲突时，本准则（除非本准则的条款被条例所禁止）优先适用于登记人和其他当事人并具有约束力。如果本准则的条款之间存在冲突，或与香港邮政有关的其他文件存在冲突时，香港邮政可酌情决定优先适用有利于香港邮政、保留香港邮政最佳利益的条款，约束有关的各方。

9.16 转让

没有香港邮政之书面同意，本准则之各方不能转让其在本准则或者适用的协议项下的任何权利或义务。

9.17 可分割性

9.17.1

如果本准则的任何规定或其应用由于任何原因在某些程度上被认定为无效或者无强制力的，本准则的剩余内容将维持有效，并为了能在最大可能限度内事实各方最初之目的而进行解释。

9.17.2

本准则内的每一条限制责任或免责声明或损害排除之条款，均为可分割的且不受其他条款约束，并可按此执行。

9.18 执行（律师费和放弃权利）

香港邮政保留向任何与在本准则第 9.9 条规定的行为有关的一方寻求损害赔偿和法律费用之权利。除非本准则规定了时间架构，任何一方延迟或者疏于行使任何基于本准则之权利、救济或权力，将不会妨碍或者被解释为放弃该等权利、救济或权力。任何一方放弃本准则规定之任何违约或者义务，不得被解释为对其他任何后续毁约或义务的弃权。香港邮政与本准则各方之间的双边协议可以对本准则之执行包含追加规定。

9.19 不可抗力

如果香港邮政由于以下原因被阻止、被禁止或者延迟履行或无法履行任何行为或要求，香港邮政将不承担责任：由于任何适用的法律、条例或者命令之规定；由于任何民政当局或军事当局；断电、通信中断或由任何香港邮政无法控制之人士提供之其他系统失效；火灾、洪水或其他紧急状态；罢工、恐怖袭击或战争；不可抗力；香港出现传染病爆发；或者其他类似超出香港邮政合理控制并且非因其无疏忽过错而造成之情形。

9.20 其他规定

9.20.1

本准则对适用本准则的各方之继承者、执行者、后代、代表者、管理者和受让人（不论是明示还是暗示形式）均有约束力。

9.20.2 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。

9.20.3 受信关系

无论在任何时候，香港邮政、「智方便」核证登记办事处或承办商并非登记人或倚据证书人士之代理人、受信人、收托人或其他代表。登记人或倚据证书人士无权以合约或其他方式约束香港邮政、

「智方便」核证登记办事处或承办商承担代理人、受信人、受托人或其他代表的责任。

9.20.4 诠释

本准则中英文本措词诠释若有歧异，以英文本为准。

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) 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；

“申請人”指自然人并已申请「智方便」电子证书。「智方便」电子证书一旦成功申请及发出，申请人即被称为登记人。

“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。

“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。

“证书”或**“「智方便」电子证书”**指符合以下所有说明之纪录：
  a) 由香港邮政发出，其目的为支持数码签署用以确认该证书上标明之人士确实为有权使用与包含在证书中的公共密码匙相对之私人密码匙之人士；
  b) 识别香港邮政为发出其之认可核证机关；
  c) 指名或识别获发纪录之人士；
  d) 包含了获发纪录人士之公开密码匙；并
  e) 经发出纪录的香港邮政作为核证机关签署。

“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”或**“准则”**指本文件及其所有附录。

“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。

“签发证书要求”指「智方便」核证登记办事处收到申请人的「智方便」电子证书申请后生成的讯息，并通过「智方便」系统发送给香港邮政，以申请证书。

“实务守则”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实务守则。

“合约”指香港邮政不时与承办商签订的外判合同，在香港邮政的监督和管理下代表香港邮政履行本作业准则所规定的全部或任何职能。

“承办商”指香港邮政不时订立的合约之承办商;以及该承办商的所有分办商。

“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”指资讯系统產生的数码形式之纪录，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”指根据《人事登记条例》第 177 章发出的身份证。

“香港邮政”指邮政署长为该条例认可的核证机关。

“香港邮政核证机关系统”指香港邮政用以执行核证机关功能的电脑硬件，软件和程序。

“硬体安全模组” 指用于中央存储和管理证书以及保护密码匙不被导出或复制的硬件安全设备。

“「智方便」持有人” 指在根据第3.1.1条获得「智方便」的人，并且其「智方便」在「智方便」系统中仍然有效。

“港元”指香港之合法货币。

“香港”指中华人民共和国香港特别行政区。

“智方便”指香港政府提供给香港居民进行电子交易的电子身份。在本准则中，「智方便」指的是根据第3.1.1条所获得的「智方便」的版本。

“「智方便」核证登记地点”指「智方便」核证登记办事处提供之附有特定装置的指定场所之登记地点，该登记地点提供给香港居民亲身注册「智方便」，其「智方便」版本符合资格申请「智方便」电子证书。

“「智方便」系统”指由政府（通过「智方便」核证登记办事处委任的承办商）开发和管理的系统，该系统向香港居民提供「智方便」功能，包括注册，使用和帐户维护。

“「智方便」核证登记办事处”指第1.2.2节中提及的「智方便」核证登记办事处。

“入境事务处”指香港特区政府入境事务处。

“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) 。

“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该证书的人的资讯，直接通知该人或通过「智方便」核证登记办事处间接通知该人；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该证书的人的资讯，直接通知该人或通过「智方便」核证登记办事处间接通知该人，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。

“近场通讯”或“NFC”是一种无线电技术，适用于多种非触式和近距离的无线电应用，例如支付款项、资讯检索、流动营销和装置配对等。

“OCSP”指在线证书状态通信规约，用于检查证书的状态。

“条例”指香港法例第 553 章《电子交易条例》。

“组织”指除个人之外之任何实体。

“公匙基建”指公开密码匙基础建设。

“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數码签署之密码匙。

“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借理解形式还原之资讯。

“核证登记机关”指代表香港邮政履行核证登记职能，在发出「智方便」电子证书前核实申请人身份之机构。

“倚据限额”指第 9.7 条规定的倚据「智方便」电子证书之金额限额。

“倚据证书人士”指合理地倚据「智方便」电子证书中所包含之资料之人士，但该人士必须遵守第 9.6.3 条规定之声明保证。

“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。

“签”和**“签署”**包括由意图认证或承认记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。

“配备 NFC 功能的智能手机” 就「智方便」使用而言，指根据《人事登记规例》（第 177A 章）第 12(1B)条获政府批准的设施，可以在指明情况下读取储存在身份证所关乎的人的香港身份证晶片内的资料。

“登记人参考编码”指香港邮政系统产生的一个登记人参考编码。

“中继证书”指由根源证书"Hongkong Post Root CA 2"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。

“登记人”指符合以下所有說明的人：

(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) 已授权「智方便」核证登记办事处持有与该证书公开密码匙相对应之私人密码匙。

注：与本准则中提及之私人密码匙相关之"持有"指处在某人之控制之下，以致仅有证

书中指名或识别之人方能使用该私人密码匙。

“登记人协议”就「智方便」电子证书而言，指香港邮政和该证书登记人之协议，其中包括了「智方便」电子证书的《登记人条款及条件》以及本准则。

“稳当的系统”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) 可用性和可靠性达到了合理水准，且可以在合理的期间内保证正确之运作模式；

(c) 合理地适合与执行其原定功能；及

(d) 依循广为接受之安全原则。

解释原则

2.1. 在本准则中，除非前后文另有所指，必须遵从以下之解释规则。

(a) 提及成文法律或者成文法律性条款之内容应被解释为引用该等成文法律或者成文法律性条款之不时之替代、修订、修改或重新生效，并且应该包括根据该等条款所做出之附属性立法；

(b) 词语引用之单数形式包括复数形式，反之亦然。词语引用之性别包括所有性别。词语中的“人”包括任何个人、企业、公司或未经公司设立程序之实体（不论是否设立或是否完成了公司设立程序）；

(c) 条款之标题仅为便于参考之目的，对于本准则之解释没有影响；

(d) 提及某一文件时应：

(i) 包括所有附加于该文件之附件、附录和添附文件；以及

(ii) 包括不时被修改或补充后之该文件。

(e) 提及“登记人”或“申请人”或“倚据证书人士”或“承办商”时应包括该等人之经批准的受让人、所有权继承人或者任何在此之下享有衍生权利之人；

(f) 提及“香港邮政” 或“「智方便」核证登记办事处”时，应包括其受让人、所有权继承人或者任何在此之下享有衍生权利之人，不论该等人士是否在相关条款中有被独立提及；

(g) 提及条文、附录或附件时，除特别声明外，应指本准则之条文、附录或者附件；

(h) 提及“法律”、“法规”时应包括任何具有法律之效力之宪法性条款、条约、公约、条例、附属立法、命令、规则和法规以及任何民事法、普通法以及衡平法之法律规则；

(i) 一天中的某个时间应指香港时间；

(j) 提及一日应指公历日；提及工作日应指除星期六、根据《公众假期条例》（第149章）的所有公众假期、及发出黑色暴雨警告信号或悬挂八号或以上热带气旋信号的日子以外的任何公历日；提及一个月或一个月期间是指一个公历月；

(k) 词语引用某一整体的，应被看作包含了该整体之各部分；

(l) “包括”这一词语不论是否明确做出该种规定都应表示包括但不限于；

(m) 词语或者表现形式如果在本准则中被定义或被引用其他定义，该等词语或表现形式延伸至该其在语法上之变体以及与之同源之表现形式；

(n) 提及“书面”时应包括打字、印刷、微影、摄影、传真或者以电子邮件方式进行之沟通之

印刷版本，也包括以其他可以辨别内容之形式呈现或者重现文字；及

(o) 在数字后提及“章”时代表香港法律之相关章节；

2.2. 本准则之任何内容都不得被用于限制、损害或者干涉任何香港邮政受法律赋予或者依据法律履行的权力与责任，以及香港邮政就此等权力与责任之行使或执行。

附录 B - 香港邮政「智方便」电子证书格式

本附录详述由中继证书"Hongkong Post e-Cert CA 2 - 19"根据本核证作业准则签发的「智方便」电子电子证书格式。

A. 「智方便」电子证书格式

栏位名称		栏位内容	
		香港邮政「智方便」电子证书	发出予未满18岁人士的 香港邮政「智方便」电子证书
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二十位元组十六进制数字]	
签署算式识别 (Signature algorithm ID)		Sha256RSA	
发出人名称 (Issuer name)		cn=Hongkong Post Root CA 2 -19 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=[香港身份证姓名]（附注1） ou=[登记人参考编号]（附注2） o=Hongkong Post iAM Smart-Cert c=HK	cn=[香港身份证姓名]（附注1） ou=[登记人参考编号]（附注2） o= Hongkong Post iAM Smart-Cert (Minor)（附注3） 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4）			
机关资料查询 (Authority Information Access)	**核证机关发出人 (Certification Authority Issuer)**	[发出人公开证书的URL]	
	线上证书状态应答 (OCSP)	[线上证书状态应答URL]（附注9）	

栏位名称		栏位内容	
		香港邮政「智方便」电子证书	发出予未满18岁人士的 香港邮政「智方便」电子证书
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	cn=Hongkong Post e-Cert CA 2 o=Hongkong Post l=Hong Kong s=Hong Kong 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，不可否认 **（此栏为“关键”栏位）**	
证书政策 (Certificate policies)		Policy Identifier = [物件识别码]（附注 5） 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6） Policy Qualifier Id = CPS Qualifier = [核证作业准则的URL]	Policy Identifier = [物件识别码]（附注5） 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7）	
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	
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）	

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. 登记人参考编号： 10 位数字
3. “iAM Smart-Cert (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 3.1.3 条）。
4. 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。
5. 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。
6. 本栏已增加一个支持 Adobe PDF 签名的物件识别码。
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：

$$cert\_hkid\_hash = \text{SHA-256}\left(\text{RSA}_{privatekey,\ sha\text{-}256}\left(hkid\_number\right)\right)$$

*SHA-256*为一杂凑函数而*RSA*则为签署函数

8. 证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1_<xxxxx>.crl，由中继证书“Hongkong Post e-Cert CA 2 - 19”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。
9. 线上证书状态通讯规约应答伺服器的 URL 为 http://ocsp1.eCert.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)及香港邮政线上证书状态应答(OCSP) 格式

本附录 C 详述有关由中继证书"Hongkong Post e-Cert CA 2 - 19"所发出的证书撤销清单的更新及公布安排和其格式，以及由"Hongkong Post Root CA 2"所发出的授权撤销清单(ARL) 的更新及公布安排和其格式。

此外，通过发布一个包含主体名称为“Hongkong Post Root CA 2 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源证书“Hongkong Post Root CA 2”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称为“ Hong Kong Post e-Cert CA 2-19 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“ Hong Kong Post e-Cert CA 2-19”进行线上证书状态通讯规约的签署。除此之外，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“证书策略”栏位。在本附录 C 的最后章节，还提供了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撤销的「智方便」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」：

> 「智方便」电子证书：
> 由中继证书"Hongkong Post e-Cert CA 2 - 19"所发出 http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1_<xxxxx>.crl，其中 <xxxxx> 为包含 5 个数字或字符的字串。

b) **「整体证书撤销清单」 (Full CRL)** 包含由中继证书"Hongkong Post e-Cert CA 2 - 19"所发出的所有已撤销证书的资料。公众可分别于下述位址(URL)获取「整体证书撤销清单」：

> http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1.crl；或 ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA2 - 19 CRL1, o=Hongkong Post, c=HK)

上述的证书撤销清单包含已撤销证书的资料，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.eCert.gov.hk 公布补充证书撤销清单。

由中继证书"Hongkong Post e-Cert CA 2 - 19"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)		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 2 - 19, 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)			
	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 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, 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 – 每一分割式证书撤销清单有其自己的序列]		此栏显示证书撤销清单的编号，该编号以顺序形式产生。

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
发出人分发点 (Issuer distribution point)		分发点名称=分割式证书撤销清单 URL 只存有用户证书=是 只存有核证机关证书=否 间接的 CRL=否 **（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。

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.eCert.gov.hk/crl/RootCA2ARL.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 2, o=Hongkong Post, c=HK)

由根证书"Hongkong Post Root CA 2"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)		sha256RSA	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 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, 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)		

标准栏位 (Standard fields)	子栏位 (Sub-fields)	授权撤销清单栏位内容	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 CA2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, 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）**	

根据本准则发出的线上证书状态应答(OCSP response)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 • 发出人主体名称的杂凑值 • 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「智方便」电子证书 – 服务摘要

要点	「智方便」电子证书
登记人	持有「智方便」的香港居民（请参阅第 3.1.1 条）
证书之授权用户	与登记人相同
倚据限额	• 每张「智方便」电子证书HK$200,000，或 • 每张发出予未满18岁人士的「智方便」电子证书HK$0 （请参阅第 9.7.6 条及 9.7.7 条）
认可证书	是
配对密码匙长度	2048 位元 RSA
产生配对密码匙	由「智方便」核证登记办事处代制产生
于申请「智方便」电子证书时核实身份	如第 4.1.1 条所述
证书用途	不可否认的数码签署
证书内包含登记人的资料	• 登记人的英文姓名； • 登记人香港身份证号码的杂凑数值 (hash value)；及 • 登记人参考编号（由香港邮政系统产生）
登记及行政费用	免费
证书有效期	一年

附录 E - 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 2	2015年9月5日 至 2040年9月5日	此根源证书由 2015 年 9 月 5 日起开始发出中继证书
Hongkong Post e-Cert CA 2 – 19	2019年7月29日 至 2034年7月29日	此中继证书由2020年10月7日起开始发出「智方便」电子证书给申请者。