



Hongkong Post Bank-Cert
香港郵政銀行證書

以香港郵政署長
根據電子交易條例作為認可核證機關
之
銀行證書核證作業準則

目录

| | |
|----------------------------------|----|
| 前言..... | 4 |
| 1. 引言..... | 6 |
| 1.1 概述..... | 6 |
| 1.2 社区及适用性..... | 6 |
| 1.2.1 核证机关..... | 6 |
| 1.2.2 最终实体..... | 6 |
| 1.2.3 登记人之级别..... | 7 |
| 1.2.4 证书之期限..... | 7 |
| 1.2.5 在香港邮政批核之处所进行申请..... | 7 |
| 1.3 联络资料..... | 8 |
| 1.4 处理投诉程序..... | 8 |
| 2. 一般规定..... | 9 |
| 2.1 义务..... | 9 |
| 2.1.1 核证机关之义务..... | 9 |
| 2.1.2 核证登记机关之义务及责任..... | 9 |
| 2.1.3 承办商之义务..... | 9 |
| 2.1.4 登记人之义务..... | 9 |
| 2.1.5 倚据证书人士之义务..... | 10 |
| 2.2 其他规定..... | 10 |
| 2.2.1 合理技能及谨慎..... | 10 |
| 2.2.2 非商品供应..... | 11 |
| 2.2.3 法律责任限制..... | 11 |
| 2.2.4 香港邮政对已接收但有缺陷之证书所承担之责任..... | 13 |
| 2.2.5 登记人转让..... | 13 |
| 2.2.6 陈述权限..... | 13 |
| 2.2.7 更改..... | 13 |
| 2.2.8 保留所有权..... | 14 |
| 2.2.9 条款冲突..... | 14 |
| 2.2.10 受信关系..... | 14 |
| 2.2.11 交相核证..... | 14 |
| 2.2.12 财务责任..... | 14 |
| 2.3 解释及执行（管辖法律）..... | 14 |
| 2.3.1 管辖法律..... | 14 |
| 2.3.2 可分割性、尚存、合并及通知..... | 14 |
| 2.3.3 争议解决程序..... | 14 |
| 2.3.4 诠释..... | 14 |
| 2.4 收费..... | 14 |
| 2.5 公开发表资料及储存库..... | 14 |
| 2.5.1 证书储存库控制..... | 15 |
| 2.5.2 证书储存库进入要求..... | 15 |
| 2.5.3 证书储存库更新周期..... | 15 |
| 2.5.4 核准使用证书储存库内的资料..... | 15 |
| 2.6 遵守规定之评估..... | 15 |
| 2.7 机密性..... | 15 |
| 3. 鉴别及认证..... | 16 |
| 3.1 首次申请..... | 16 |
| 3.1.1 名称类型..... | 16 |
| 3.1.2 名称需有意义..... | 16 |

| | | |
|-------|---------------------|----|
| 3.1.3 | 诠释各个名称规则..... | 16 |
| 3.1.4 | 名称独特性..... | 16 |
| 3.1.5 | 名称申索争议决议程序..... | 16 |
| 3.1.6 | 侵犯及违反商标注册..... | 17 |
| 3.1.7 | 证明拥有私人密码匙之方法..... | 17 |
| 3.1.8 | 机构申请人身份认证..... | 17 |
| 3.1.9 | 个人申请人身份认证..... | 17 |
| 3.2 | 证书续期..... | 17 |
| 3.2.1 | 银行证书（个人）..... | 17 |
| 3.2.2 | 银行证书（机构）..... | 17 |
| 3.2.3 | 已续期银行证书之有效期..... | 18 |
| 4 | 运作要求..... | 19 |
| 4.1 | 证书申请..... | 19 |
| 4.2 | 发出证书..... | 19 |
| 4.3 | 公布证书..... | 19 |
| 4.4 | 证书撤销..... | 20 |
| 4.4.1 | 撤销..... | 20 |
| 4.4.2 | 撤销程序请求..... | 20 |
| 4.4.3 | 服务承诺及证书撤销清单更新..... | 21 |
| 4.4.4 | 撤销效力..... | 22 |
| 4.5 | 电脑保安审核程序..... | 22 |
| 4.5.1 | 记录事件类型..... | 22 |
| 4.5.2 | 处理记录次数..... | 22 |
| 4.5.3 | 审核记录之存留期间..... | 22 |
| 4.5.4 | 审核记录之保护..... | 23 |
| 4.5.5 | 审核记录备存程序..... | 23 |
| 4.5.6 | 审核资料收集系统..... | 23 |
| 4.5.7 | 事件主体向香港邮政发出通知..... | 23 |
| 4.5.8 | 脆弱性评估..... | 23 |
| 4.6 | 记录存档..... | 23 |
| 4.6.1 | 存档记录类型..... | 23 |
| 4.6.2 | 存档保存期限..... | 23 |
| 4.6.3 | 存档保护..... | 23 |
| 4.6.4 | 存档备存程序..... | 23 |
| 4.6.5 | 电子邮戳..... | 23 |
| 4.7 | 密码匙变更..... | 23 |
| 4.8 | 灾难复原及密码匙资料外泄计划..... | 24 |
| 4.8.1 | 灾难复原计划..... | 24 |
| 4.8.2 | 处理密码匙资料外泄计划..... | 24 |
| 4.8.3 | 密码匙的替补..... | 24 |
| 4.9 | 核证机关终止服务..... | 24 |
| 4.10 | 核证登记机关终止服务..... | 24 |
| 5 | 实体、程序及人员保安控制..... | 24 |
| 5.1 | 实体保安..... | 24 |
| 5.1.1 | 选址及建造..... | 25 |
| 5.1.2 | 进入控制..... | 25 |
| 5.1.3 | 电力及空调..... | 25 |
| 5.1.4 | 自然灾害..... | 25 |
| 5.1.5 | 防火及保护..... | 25 |
| 5.1.6 | 媒体存储..... | 25 |

| | |
|----------------------------------|----|
| 5.1.7 场外备存 | 25 |
| 5.1.8 保管印刷文件 | 25 |
| 5.2 程序控制 | 25 |
| 5.2.1 受信职责 | 25 |
| 5.2.2 港邮政与核证登记机关之间的文件及资料传递 | 25 |
| 5.2.3 年度评估 | 25 |
| 5.3 人员控制 | 26 |
| 5.3.1 背景及资格 | 26 |
| 5.3.2 背景调查 | 26 |
| 5.3.3 培训要求 | 26 |
| 5.3.4 向人员提供之文件 | 26 |
| 6. 技术保安控制 | 26 |
| 6.1 产生及安装配对密码匙 | 26 |
| 6.1.1 产生配对密码匙 | 26 |
| 6.1.2 登记人公开密码匙交付 | 26 |
| 6.1.3 公开密码匙交付予登记人 | 26 |
| 6.1.4 密码匙大小 | 26 |
| 6.1.5 加密模组标准 | 26 |
| 6.1.6 密码匙用途 | 26 |
| 6.2 私人密码匙保护 | 27 |
| 6.2.1 加密模组标准 | 27 |
| 6.2.2 私人密码匙多人式控制 | 27 |
| 6.2.3 私人密码匙托管 | 27 |
| 6.2.4 香港邮政私人密码匙备存 | 27 |
| 6.3 配对密码匙管理其他范畴 | 27 |
| 6.4 电脑保安控制 | 27 |
| 6.5 生命周期技术保安控制 | 27 |
| 6.6 网络保安控制 | 27 |
| 6.7 加密模组工程控制 | 27 |
| 7. 证书及证书撤销清单结构 | 27 |
| 7.1 证书结构 | 27 |
| 7.2 证书撤销清单结构 | 28 |
| 8. 准则管理 | 28 |
| 附录 A - 词汇 | 29 |
| 附录 B - 香港邮政银行证书格式 | 32 |
| 附录 C - 香港邮政证书撤销清单(CRL)格式 | 36 |
| 附录 D - 香港邮政银行证书 — 服务摘要 | 38 |
| 附录 E - 香港邮政银行证书核证登记机关名单 | 39 |
| 附录 F - 核证机关根源证书的有效期限 | 40 |

本文之版权属香港邮政署长所有。未经香港邮政署长明确认可，不得复制本文之全部或部份内容。

前言

香港法例第 553 章之电子交易条例（「条例」）刊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，其身份为**香港邮政**。

随着香港特别行政区政府决定外判香港邮政核证机关之营运，香港特别行政区政府已通过公开招标于 2006 年 10 月 27 日向香港亿软信息技术有限公司（“承办商”）批出合约（“合约”）以使其于 2007 年 4 月 1 日至 2011 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系统及服务。其后，该合约年期延至 2012 年 3 月 31 日。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，香港邮政作为认可之核证机关，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接受之数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“银行证书”。**

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关于本核证作业准则之若干职能。**附录 E** 刊载核证登记机关之清单。香港邮政透过该等核证登记机关发出两类银行证书予个人（银行证书（个人））及某些机构之成员或雇员（银行证书（机构））。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银行证书之职能或提供服务的行为负责。

本核证作业准则刊载香港邮政银行证书（个人）及香港邮政银行证书（机构）之作业标准，其结构如下：

- 第 1 条载有概述及联络资料
- 第 2 条刊载各方责任及义务
- 第 3 条刊载申请及身份确认程序
- 第 4 条概述运作要求
- 第 5 条介绍保安监控措施
- 第 6 条刊载如何产生及监管公开/私人配对密码匙
- 第 7 条简介技术要求
- 第 8 条概述如何管理本核证作业准则
- 附录 A 载有词汇表
- 附录 B 载有香港邮政银行证书格式

附录 C 载有香港邮政证书撤销清单格式
附录 D 载有香港邮政银行证书服务摘要
附录 E 载有香港邮政银行证书核证登记机关清单
附录 F 载有核证机关根源证书的有效期

香港邮政根据本核证作业准则所发出的银行证书均为条例下的认可证书。而在本核证作业准则范围之外，香港邮政亦签发一张非认可证书，称为「Hongkong Post Commercial 1」的根源证书。由于此根源证书在条例下并非认可证书，因此任何由此根源证书所签发的证书均为非认可证书。香港邮政不会对任何人士因倚据该类非认可证书所造成的损失或损害承担任何责任，本作业准则内的业务守则及标准亦不适用于该类非认可证书。该类非认可证书中的「发行者」栏内会显示「Hongkong Post Commercial 1」以资识别。有关香港邮政所签发的「Hongkong Post Commercial 1」根源证书的详细资料，可见于香港邮政核证机关的网站 <http://www.hongkongpost.gov.hk/>。

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银行证书时采用之做法及标准。

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.2.10」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）。

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）申请人身份之程序，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的银行证书将得到倚据证书人士之倚据并用来核实数码签署。利用由香港邮政发出之证书之各倚据证书人士须独立确认基于公匙基建之数码签署乃属适当及充份可信，可用来认证各倚据证书人士特定之公匙基建应用程序上之参与者身份。

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银行证书，香港邮政已指明为认可证书。对登记人及倚据证书人士而言，根据该条例香港邮政在法律上有义务使用稳当系统，发出、暂时吊销或撤销及在可供公众使用之储存库公布获认可及接受之数码证书(包括银行证书)。换言之，香港邮政指定为认可证书者（如银行证书）均为认可证书，而其内容不但准确，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）。香港邮政已指定银行证书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，亦无变更银行证书作为获认可证书具有之特性。

附录 D 载有银行证书特点摘要。

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获授权发出证书之核证机关（见第 2.1.1 条）。

1.2.1.1 香港邮政所作之陈述

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

1.2.1.2 生效

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定合约承担有关职务，香港邮政可把履行本准则及登记人协议之部份或全部工作之义务，进一步批予分包商执行。无论有关职务是否批出予分包商执行，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，共有两类最终实体：登记人及倚据证书人士。登记人指于附录 A 内所指的“登记人”或“登记人机构”。倚据证书人士乃倚据香港邮政发出之任何类别或种类证书，包括但不限于用于交易之银行证书。特此澄清，倚据证书人士不应倚据核证登记机关。香港邮政透

过其代理人核证登记机关发出银行证书，而核证登记机关对倚据证书人士并无任何谨慎职责，亦不需对倚据证书人士就发出银行证书而负责（见第 2.1.2 条）。倚据其他登记人之证书（包括银行证书）以用于交易之申请人或登记人乃为有关此证书之倚据证书人士。**请倚据证书人士留意：银行证书可能不会发予未成年人（见附录 E）。**

1.2.2.1 登记人之保证及陈述

各申请人(如申请银行证书（机构），获授权代表会代表登记人机构)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（尤其是倚据证书人士）作出陈述，在证书之有效期间，以下事实乃属真实并将保持真实：

- a) 除登记人及银行证书（机构）之授权用户外，并无其他人士曾取用登记人之私人密码匙。
- b) 使用与登记人银行证书所载之公开密码匙相关之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) 证书所载之所有资料及由登记人作出之陈述均属真实。
- d) 证书将只会用于认可及合法用途。
- e) 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、商用名称、公司名称或任何知识产权。
- f) 银行证书（机构）只会由授权用户用于授权应用中，请参阅以下第 1.2.3.2 条。

1.2.3 登记人之级别

根据本准则香港邮政仅发出证书予其申请已获批准并以适当形式签署或确定接受登记人协议之申请人士。根据本准则，香港邮政会发出两类银行证书，但各核证登记机关可决定及与香港邮政同意其是否接受两类申请并于证书内予以识别或仅接受一类，如为一类，则属那一类。

就银行证书(机构)而言，根据本准则之规定，只有登记人机构须成为登记人。

1.2.3.1 银行证书（个人）

银行证书（个人）发给持有香港身份证及十八岁或以上人士。此等证书可用来从事商业用途。

1.2.3.2 银行证书（机构）

银行证书（机构）发给获香港特别行政区政府签发有效商业登记证之机构及获香港法例认可之本港法定团体（即“登记人机构”），并识别已获该登记人机构授权使用该银行证书（机构）之私人密码匙之成员或雇员(即“授权用户”）。

经由核证登记机关发出之银行证书（机构）只会由授权用户用于**附录 E** 中相对该核证登记机关之服务或系统(“获授权应用”）。

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之证书可能有不同期限，取决于核证登记机关就各证书之规定。香港邮政将就核证登记机关规定之证书期限与核证登记机关达成一致意见。证书之期限载于**附录 E（证书续期见第 3.2 条）**。

1.2.5 在香港邮政批核之处所进行申请

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

1.3 联络资料

登记人可经由以下途径作出查询、建议或投诉：
邮寄地址：东九龙邮政信箱 68777 号香港邮政核证机关
电话：2921 6633
传真：2775 9130
电邮地址：enquiry@hongkongpost.gov.hk

1.4 处理投诉程序

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

2. 一般规定

2.1 义务

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

2.1.1 核证机关之义务

根据条例，香港邮政为认可核证机关，负责使用稳当系统发出、暂时吊销或撤销及利用公开储存库公布已认可及已接受之数码证书。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) 通知登记人有关已批准或被拒绝的申请（见第 4.1 条）；
- c) 暂时吊销或撤销证书及依时公布证书撤销清单（见第 4.4 条）；及
- d) 通知登记人有关已暂时吊销或撤销的证书（见第 4.4 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、撤销或公布银行证书，或就收集及保留文件或资料对登记人或倚据证书人士承担任何谨慎职责。核证登记机关之行为仅为履行香港邮政于此事项之义务及责任。核证登记机关有权代表香港邮政实施登记人协议之条款（除非及直至该机关被撤销及登记人正式获通知任何该等撤销）。**在任何情况下，核证登记机关不须就登记人协议或核证登记机关代表香港邮政作为认可核证机关发出之证书对登记人或倚据证书人士承担任何责任。**

2.1.3 承办商之义务

承办商祇会依据与香港邮政及其之合约条款，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。
- 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（如申请银行证书（机构），则由获授权代表签署）；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之陈述准确无误。
- c) 准确地按照本准则所载关于完成证书之程序。
- d) 承认会履行义务，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) 发现其私人密码匙之任何丢失或外泄时，立即向相关证书中指明之核证登记机关呈报丢失或外泄（外泄乃属违反保安，使资料遭受未经授权之进入，从而导致未经授权即对资料进行披露、更改或使用）。

- f) 不时将登记人提供之证书资料或授权用户之任何变动立即通知相关证书中指明之核证登记机关。
- g) 不时把银行证书(机构)的委任变动及获授权代表资料变动立即通知相关证书中指明之核证登记机关。
- 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相关证书中指明之核证登记机关。
- i) 同意其透过获发出或接受证书而向香港邮政保证(承诺)并向所有倚据证书人士表明, 在证书之有效期间, 以上第 1.2.2.1 条载明之事实乃属真实并将一直保持真实。
- j) 在登记人明知香港邮政或相关证书中指明之代表香港邮政之核证登记机关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核证登记机关知会, 核证登记机关(代表香港邮政行事)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) 在明知核证登记机关可能据以撤销证书之任何事项之情况下, 或如上文 g)所述登记人作出撤销申请或经核证登记机关知会拟撤销证书时, 须立即通知从事当时仍有待完成之任何交易之倚据证书人士, 用于该交易之证书须予撤销, 并明确说明, 因情形乃属如此, 故倚据证书人士不得就交易而倚据证书。
- l) 就银行证书(机构)而言, 只适用于授权应用中。
- m) 承认知悉一经递交银行证书申请表, 即批准向其他人或在香港邮政储存库公布其银行证书。

2.1.4.1 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(包括倚据证书人士)就可能因此产生之责任或损失及损害赔偿损失。

2.1.5 倚据证书人士之义务

倚据银行证书之倚据证书人士负责:

- a) 倚据证书人士于倚据证书时如考虑过所有因素后仍确信倚据证书实属合理之举, 方可倚据证书。
- b) 于倚据该等证书前, 确定使用证书乃适合本准则规定之用途, 而核证登记机关(见附录 E)并不对倚据证书人士承担任何谨慎职责。
- c) 于倚据证书前查核证书撤销清单上之证书状态。
- d) 履行所有适当之证书核实程序。

2.2 其他规定

香港邮政对登记人及倚据证书人士之义务

2.2.1 合理技能及谨慎

香港邮政向各登记人及各倚据证书人士承诺, 根据本准则香港邮政、承办商或代表香港邮政之核证登记机关履行及行使作为核证机关所具之义务和权利时, 采取合理程度之技术及谨慎。香港邮政不向登记人或倚据证书人士承担任何绝对义务。香港邮政不保证其本身、承办商或核证登记机关或其他任何一方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关于执行本合约及行使及履行其根据本准则之权利及义务时采取合理程度之技术及谨慎, 若登记人作为本准则定义下之登记人或倚据证书人士或非登记人作为倚据证书人士遭受出自本准则中描述之公开密码匙基建或与之相关任何性质之债务、损失或损害, 包括随后对另外一登记人证书之合理倚据而产生之损失或损害, 各登记人同意及各倚据证书人士须承认香港邮政、香港邮政署、承办商及任何核证登记机关概无需承担任何责任、损失或损害。

即如在香港邮政、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, 若登记人或倚据证书人士因倚据另一登记人由香港邮政所发出之银行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、香港邮政署、承办商及任何该等核证登记机关概不负责。

亦即如在香港邮政（香港邮政署、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，若登记人或倚据证书人士因香港邮政不能控制之情况下遭受不良影响，香港邮政、香港邮政署、承办商或任何该等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建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，登记人仅有权促使证书发出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洽之公开储存库内提供之证书，并非作为对倚据证书人士供应任何商品；亦不会作为对倚据证书人士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登记人作本核证作业准则之指定用途，但亦承诺合理谨慎确保此等物品适合作本核证作业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 至 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银行证书无关之资料。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款决定。

2.2.3 法律责任限制

2.2.3.1 限制之合理性

各登记人或倚据证书人士必须同意，香港邮政按登记人协议及本准则所列之条件限制，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) 登记人协议；或
- b) 任何谨慎职责一尤其就登记人或倚据证书人士而言，当登记人、或倚据证书人士或其他人以任何方式倚据香港邮政根据此公开密码匙基建发出或被代为发出之任何证书时，根据登记人协议香港邮政违反其应合理采取技术或谨慎及/或职责

之情况下，登记人或倚据证书人士（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证书人士）蒙受损失及损害，**香港邮政概不负责关乎下述原因之赔偿或其他补救措施：**

- 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、失去工程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——200,000 港元

除下文所述之例外情况外，在香港邮政违反：

- a) 登记人协议及核证作业准则条文；或
- b) 任何谨慎职责，尤其就登记人或倚据证书人士而言，当登记人或倚据证书人士或其他人士以任何方式倚据香港邮政根据此公开密码匙基建发出之任何证书时香港邮政违反根据本准则其应合理采取技术或谨慎及/或职责

之情况下，登记人或倚据证书人士蒙受损失及损害（无论作为根据准则或以其他任何方式定义之登记人或倚据证书人士），香港邮政对任何登记人或任何倚据证书人士（无论作为根据准则或以其他任何方式定义之登记人或倚据证书人士或以任何其他身份）所负法律责任限制于任何情况下，就每份银行证书（个人）或每份银行证书（机构）而言，不超过 200,000 港元。

2.2.3.4 提出索偿之时限

任何登记人或倚据证书人士欲向香港邮政提出索偿，且该索偿源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，则应在登记人清楚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、核证登记机关及其各自之人员

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，登记人及倚据证书人士必须向香港邮政承认，就登记人及倚据证书人士所知，香港邮政、承办商或任何核证登记机关或其各自之任何职员、雇员或代理人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其任何个人出于真诚以任何方式与香港邮政履行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所做之任何行为或不作为相关之谨慎责任或职责；各登记人及倚据证书人士接受并将继续接受此点，并向香港邮政保证不起诉或透过任何其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）以任何方式与香港邮政履行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所作任何行动或不行动寻求任何形式之追讨或纠正，并承认香港邮政享有充份法律及经济利益以保护香港邮政署及上述个人免受此等法律行动。

2.2.3.6 蓄意之不当行为、个人伤害或死亡之责任

任何因欺诈或蓄意之不当行为、个人伤害或死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

香港邮政发出之银行证书包括下列倚据限额及/或法律责任限制通知：

「香港邮政署及承办商之职员按香港邮政署长之核证作业准则所载条款及条件适用于本证书之情况下，根据电子交易条例作为认可核证机关发出本证书。」

因此，任何人士倚据本证书前均应阅读适用于银行证书之核证作业准则，可浏览香港邮政之网址 <http://www.hongkongpost.gov.hk>，或前往该证书中指明之代表香港邮政之核证登记机关处所及浏览其网址（见附录 E）。香港特别行政区法律适用于本证书，倚据证书人士须提交因倚据本证书而引致之任何争议或问题予香港特别行政区法庭之非专有司法管辖权。

倘阁下为倚据证书人士而不接受本证书据以发出之条款及条件，则不应倚据本证书。

香港邮政署长（经香港邮政署、承办商，其各自职员、雇员及代理人包括但不限于核证登记机关）发出本证书，但无须对倚据证书人士承担任何责任或谨慎职责（准则中列明者除外）。

倚据证书人士倚据本证书前负责：

- a. 只有当倚据证书人士于倚据时所知之所有情况证明倚据行为乃属合理及本着真诚时，方可倚据本证书；*
- b. 倚据本证书前，确定证书之使用就准则规定之用途而言乃属适当；*
- c. 倚据本证书前，根据证书撤销清单检查本证书之状态；及*
- d. 履行所有适当证书路径认可程序。*

若尽管香港邮政署长、香港邮政署、承办商、本证书中指明之任何核证登记机关及其各自之职员、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、本证书中指明之任何核证登记机关及其各自之职员、雇员或代理人对倚据证书人士之任何损失或损害概不承担任何责任，在该等情况下根据条例适用于本证书之倚据限额为 0 港元。

若本证书在任何方面不准确或误导，而该等不准确或误导乃因香港邮政署长、香港邮政署、承办商、本证书中指明之任何核证登记机关或其各自之职员、雇员或代理人之疏忽所导致，则香港邮政署长将就因合理倚据本证书中之该等不准确或误导事项而造成之经证实损失向每名倚据证书人士支付最多 200,000 港元，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，香港邮政已获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 200,000 港元，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、本证书中指明之核证登记机关及其各自之任何职员、雇员或代理人概不对倚据证书人士就本证书承担任何谨慎职责。

提出索赔时间限制

任何倚据证书人士如拟向香港邮政署长索赔，且该索赔源起于或以任何方式与发出、暂时吊销、撤销或公布任何证书相关，则应在倚据证书人士知悉存在任何有权提出此等索偿事实之日起一年内或透过行使合理努力彼等有可能知悉此等事实之日起一年内（若更早）提出。特此澄清，不知晓此等事实之法律重要性乃无关重要。一年期届满时，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、本证书中指明之任何核证登记机关及其各自之职员、雇员或代理人作出之故意或罔顾后果之失实陈述，则本证书并不就彼等对因合理倚据本证书中之失实陈述而遭受损失之倚据证书人士所应承担之法律责任作出任何限制。

本文所载之法律责任限制不适用于个人伤害或死亡之（不大可能发生之）情形。」

2.2.4 香港邮政对已接收但有缺陷之证书所承担之责任

尽管上文已列明香港邮政承担责任之限制，若登记人接获证书后发现，因银行证书（个人）或银行证书（机构）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，登记人须将此情况立即通知证书中指明之核证登记机关，以便撤销证书及（如愿意接收）重新发出。登记人须即时通知有关核证登记机关，以撤销证书及（如愿意接收）重新发出。若登记人于接收证书后三个月内发出通知，且不再需要证书，而代表香港邮政之有关核证登记机关同意确有此差错，有关费用将会退还。若登记人于接收证书三个月过后方将任何此类差错通知有关核证登记机关，则费用将不会退还，而仅可由代表香港邮政之有关核证登记机关酌情退回。

2.2.5 登记人转让

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，承办商、任何核证登记机关、香港邮政署、承办商或任何核证登记机关之代理人或雇员均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，登记人及倚据证书人士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在任何时候均非登记人或倚据证书人士之代理人、受信人、受托人或其他代表。登记人及倚据证书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证书人士之代理人、受信人、受托人或其他代表之责任。

2.2.11 交相核证

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

2.2.12 财务责任

保单已经备妥，有关证书之责任以及对倚据限额之索偿均获承保。

2.3 解释及执行（管辖法律）

2.3.1 管辖法律

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

2.3.2 可分割性、尚存、合并及通知

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

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，则以英文本为准。

2.4 收费

银行证书之收费详情载于附录 E 相关核证登记机关一节。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。根据香港邮政及承办商之合约条款、承办商可向银行证书申请人收取登记年费及续期费用。

2.5 公开发表资料及储存库

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、香港邮政公开密码匙、本准则文本一份以及与本准则有关银行证书之其他资料。除每周最多两小时之定期维修及紧急维修外，储存库基本保持每日 24 小时、每

周 7 日开放。香港邮政会把经由登记人接受并按本准则发出的银行证书，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网上浏览，并可防止擅进。

2.5.2 证书储存库进入要求

经香港邮政授权之人士方可进入储存库更新及修改内容。

2.5.3 证书储存库更新周期

每份证书一经登记人接受及发出后，以及当发生如撤销证书等任何相关情况，储存库均会即时作出更新。

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，查清香港邮政发出、暂时吊销或撤销及公布证书之系统是否妥善遵守本准则。

2.7 机密性

在履行与香港邮政发出、暂时吊销或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银行证书之组成部份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登记人资料，惟根据香港法例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

银行证书(个人)之申请人须亲身到核证登记机关之处所或香港邮政指定机构之处所,并出示第 3.1.9 条所述之身份证明。

银行证书(机构)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,并出示第 3.1.8 条所述身分证明。在银行证书(机构)上列明之授权用户,则无须亲身递交申请。

所有银行证书申请人必须向申请表中指明之核证登记机关呈交一份填妥并经签署之申请表。银行证书(机构)之申请表亦须经申请人所属登记人机构获授权代表填妥及签署,而登记人机构亦会成为登记人。申请获申请表中指明之代表香港邮政之核证登记机关确认后,香港邮政即准备银行证书并向申请人直接发出通知,或按登记人之选择由申请表中指明之核证登记机关通知,说明如何发出证书。

3.1.1 名称类型

3.1.1.1 银行证书(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,可识别银行证书(个人)登记人之身份。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 银行证书(机构)

透过证书上的主体名称可识别银行证书(机构)登记人机构之身份,该名称由以下资料组成:

- 授权用户香港身份证/护照上显示之姓名;
- 登记人机构在有关香港政府部门或登记机关之登记名称;及
- 登记人机构之香港公司注册/商业登记号码。

3.1.1.3 获授权代表

登记人机构获授权代表虽替登记人机构办理银行证书(机构)申请手续,但该人士不会于银行证书(机构)中得到识别。

3.1.1.4 机构中文名称

银行证书一律只用英文发出。只有中文名称或只提供中文名称作登记之机构,其名称不会显示在银行证书上。

3.1.2 名称需有意义

所采用名称之词义必须为一般人所理解,方便辨识登记人身份。

3.1.3 诠释各个名称规则

该数码证书会载入之登记人名称(主体名称)类型见第 3.1.1 条。有关银行证书主题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,此准则不要求名称某一特别部份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

香港邮政或代表香港邮政之核证登记机关对有关名称争议之事宜的决定为酌情性及最终决定。

3.1.6 侵犯及违反商标注册

申请人及登记人向香港邮政保证（承诺）并向核证登记机关及倚据证书人士申述，申请银行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、公司名称或任何其他知识产权。

3.1.7 证明拥有私人密码匙之方法

登记人将拥有经由香港邮政代制密码匙服务产生之私人密码匙。利用代制密码匙服务，香港邮政将在其处所内使用稳当系统，在安全的环境下代登记人产生配对密码匙及制作证书，以保证私人密码匙不被干扰。私人密码匙连同证书将被存储在软碟或电子证书档案卡或替代之存储媒介上，并以申请表中指明的安全方式交付予登记人。所有登记人承认其须对银行证书内与公开密码匙相关之私人密码匙负上保安责任。

3.1.8 机构申请人身份认证

银行证书（机构）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递交，获授权代表亦须出示其香港身份证或护照。每份银行证书（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银行证书（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。

3.1.9 个人申请人身份认证

各个银行证书（个人）申请人身份之确认将透过如下运作完成：

各证书申请人须亲身到核证登记机关之处所，出示填妥并已签署之银行证书申请表以及申请人之香港身份证。该前述处所人员将复核并认证所有申请文件，随后将申请递交香港邮政核证机关处理。

3.2 证书续期

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。香港邮政或核证登记机关均不会为过期、已吊销或已撤销之证书续期。香港邮政会于证书的有效期届满前以电子邮件向登记人发出续期通知。

3.2.1 银行证书（个人）

于办理续期手续时，登记人须向核证登记机关递交一份已填妥及签署之证书续期表格，并缴足应缴费用。一经续期，必须运用香港邮政之代制密码匙服务产生新的配对密码匙。登记人与香港邮政就产生此等新密码匙之责任与上文所述产生原密码匙之责任相同。证书续期表格可于核证登记机关网址（见附录 E）下载，或于核证登记机关办事处索取。于办理续期手续时，原登记人协议中的条款将仍适用于已续期之证书，除非有条款与当时之核证作业准则中的条款发生冲突。倘若确实发生任何冲突，则须以核证作业准则中的条款为准。申请续期之申请人应于递交续期表格前先细阅申请续期当日适用之核证作业准则中的条款。

3.2.2 银行证书（机构）

银行证书（机构）不会自动续期。若香港邮政接收到续期申请，即会根据第 3.1.8 条所述「机构申请人身份认证」之过程重新进行认证。

3.2.3 已续期银行证书之有效期

因应香港邮政的酌情权，发出给登记人的新银行证书可由新证书产生日期起有效，而有效期会于原有证书（即须续期的证书）到期日的三年后（适用于银行证书（个人））、或到期日的一年后（适用于银行证书（机构））届满。由此，新的银行证书（个人）的有效期可超过三年，但不会超过三年另一个月。新的银行证书（机构）的有效期可超过一年，但不会超过一年另一个月。

4 运作要求

4.1 证书申请

4.1.1 按本准则申请银行证书之申请人必须填妥香港邮政与核证登记机关共同编定之表格，并须到核证登记机关处所、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。

4.1.2 申请人可于递交银行证书申请表时，要求额外一份银行证书的副本，此副本可被逐一储存于由申请人所提供的可录光碟、USB 记忆体及/或 PKCS#11 兼容装置内。如香港邮政认为该要求可以接受，则此银行证书副本会被逐一储存于该可录光碟、USB 记忆体及/或 PKCS#11 兼容装置内。第 4.2 条所述程序适用于此银行证书副本，尤其是此银行证书副本会受银行证书个人密码所保护，并以安全方式交付予申请人。

4.1.3 有关用以确定申请人身份所需文件，可参阅本准则第 3.1.8 条（机构申请人身份认证）及第 3.1.9 条（个人申请人身份认证）。在核证登记机关代表香港邮政完成核对身份手续后，各银行证书「个人密码信封」会以安全方式送递给申请人或获授权代表（适用于银行证书（机构）申请）。

4.1.4 核证登记机关会通知申请人申请已获批准，并可能列印由登记人提供之所有资料及要求登记人确认该等资料之准确性及真实性。若香港邮政 / 核证登记机关未能根据本准则列明的要求成功核实有关申请，香港邮政 / 核证登记机关会拒绝有关申请并通知申请人。核证登记机关与香港邮政经电子方式传送之所有申请资料须使用由香港邮政订明之规约。

4.1.5 银行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银行证书，并接受香港邮政将发给申请人的银行证书。

4.2 发出证书

4.2.1 香港邮政进行产生配对密码匙及制作证书的工序。在香港邮政的处所内有一套可靠的系统及环境来进行上述作业，以保证私人密码匙不受干扰。

4.2.2 以密码保护的私人密码匙及证书将随后被存储在软碟或电子证书档案卡或替代存储介质上。软碟或电子证书档案卡或替代存储介质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。

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

4.2.4 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。在完成送递银行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。

4.2.5 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 公布证书

根据《电子交易条例》的规定，香港邮政会即时在储存库公布已获接受并已发出的银行证书（见

第 2.5 条)。

4.4 证书撤销

4.4.1 撤销

若香港邮政私人密码匙资料外泄，会导致香港邮政迅速地撤销所有经由该私人密码匙发出的证书。在私人密码匙资料外泄的情况下，香港邮政会根据在业务持续运作计划内定明的程序迅速地撤销所有已发出给登记人的证书（见第 4.8.2 条）。

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

登记人之私人密码匙或内载与某银行证书公开密码匙相关私人密码匙之媒介，若已外泄或怀疑已外泄，各登记人必须立即按照本准则的撤销程序，直接向香港邮政或证书中所指明之核证登记机关申请撤销证书（见第 2.1.4(h)条）。

不论何时，若有以下情况，香港邮政及证书中所指明之代表香港邮政之核证登记机关均可按准则中程序暂时吊销或撤销证书并会以书面（证书撤销通知书）通知登记人：

- a) 知悉或有理由怀疑登记人之私人密码匙已外泄；
- b) 知悉或有理由怀疑证书上任何细节乃不真实或已变得不真实或证书由于其他原因不可靠；
- c) 认为证书并未根据准则妥当发出；
- 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) 任何适用于该证书之规例或法例有此规定；
- f) 认为登记人未曾缴付登记费；
- g) 知悉或有理由相信其出现在证书上之银行证书（个人）登记人：
 - i) 死亡或已死亡；或
 - 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新协议或债务偿还安排或自愿安排；
 - 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银行证书（机构）上指明之授权用户已非登记人机构之成员或雇员；
或
- i) 知道或有理由相信其资料出现在银行证书（机构）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新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，或违反条例被定罪；
 - iv) 在撤销证书前五年内登记人资产之任何部份托给接管人或管理人接管。

4.4.2 撤销程序请求

登记人，或登记人机构的获授权代表，可透过香港邮政位于 <http://www.hongkongpost.gov.hk> 的指定网页、传真、邮寄信件、电子邮件或亲身前往邮局，向香港邮政提出撤销证书要求。登记人亦可透过传真、邮寄信件、电子邮件或亲身前往核证登记机关式视乎何种方式可为所联系机关接纳而定，向证书中指明之核证登记机关提出撤销要求（见附录 E）；而该核证登记机关会将撤销证书要求转递给香港邮政。

香港邮政接到此要求后会暂时吊销证书。经登记人，或经初始接收撤销证书要求的核证登记机关，

最后确认撤销证书后，该证书即会撤销且永久失效。撤销证书之最后确认程序包括收到由登记人以其私人密码匙进行数码签署之电子邮件、登记人亲笔签署之信件正本或登记人亲笔签署之撤销证书申请表格。如未有收到登记人的最后确认，证书会继续暂时失效，并列入证书撤销清单，直至证书有效期届满为止。撤销证书申请表格可从香港邮政网页 <http://www.hongkongpost.gov.hk> 下载。香港邮政会考虑登记人的要求，把暂时吊销的证书回复为有效。但香港邮政只会在谨慎的情况下把暂时吊销的证书回复为有效。

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

证书中所指明之核证登记机关（香港邮政之代理人）会在收到撤销申请或相关撤销证书之最后确认程序后，一个工作日内通知香港邮政，以便其将吊销或撤销之证书相应地刊载于证书撤销清单内。

倘若核证登记机关在某一个非工作日之前一天收到撤销申请或撤销证书之最后确认证书，核证登记机关将立即通知登记人，彼等须将其撤销申请或最后确认证书直接送往香港邮政。

核证登记机关及香港邮政只能在正常办公时间内处理撤销申请或及撤销证书之最后确认程序。核证登记机关办理撤销证书事务之办公时间详情请参照附录 E。

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风雨警告信号，处理撤销证书要求将立即暂停。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之间或十时正除下，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（周六、周日或公众假期除外）恢复。

4.4.3 服务承诺及证书撤销清单更新

- a) 香港邮政将作出合理努力，确保（1）于直接从登记人收到或从证书中所指明之核证登记机关处收到撤销申请或撤销证书之最后确认证书时或（2）在无此申请之情况下，香港邮政及/或代表香港邮政之核证登记机关决定暂时吊销或撤销证书时，确保在两个工作日内，将该暂时吊销或撤销证书于证书撤销清单公布。然而，证书撤销清单并不会于各证书暂时吊销或撤销后随即公布。而只会在下一份证书撤销清单更新并公布时，才会反映该证书已被撤销之状态。证书撤销清单每日均会公布，并存档七年。

特此澄清，星期六、星期日、公众假期及悬挂热带风暴及暴雨警报信号之工作日，一律不视作第 4.4.3（a）条所述目的之工作日计算。

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

- b) 在登记人明知香港邮政/或证书中所指明之核证登记机关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或代表香港邮政之核证登记机关，香港邮政或代表香港邮政之核证登记机关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。倘若登记人无视以上

规定，仍确实在交易中使用证书，则香港邮政及核证登记机关毋须就任何该等交易向登记人或倚据证书人士承担责任。

- c) 此外，登记人明知香港邮政及/或证书中所指明之核证登记机关根可能撤销证书之任何事项之情况下，或登记人作出申请或经知会香港邮政或核证登记机关拟撤销证书时，须立即通知从事当时仍有待完成之任何交易之倚据证书人士，用于该交易之证书须予撤销（由香港邮政、核证登记机关或经登记人申请），并明确说明，因情况乃属如此，故倚据证书人士不得就交易而倚据证书。若登记人未能通知倚据证书人士，则香港邮政及核证登记机关无须就该等交易向登记人承担责任，并无须向虽已收到通知但仍完成交易之倚据证书人士承担责任。

除非香港邮政或代表香港邮政之核证登记机关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撤销证书人士，否则，香港邮政及核证登记机关无须就香港邮政及核证登记机关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与证书撤销清单之内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份规限之范畴。在任何情况下，核证登记机关自身无须对倚据证书人士承担独立 谨慎责任（核证登记机关只是履行香港邮政之谨慎责任）。因此，即使出现疏忽，核证登记机关亦无须对倚据证书人士负责。

- d) 证书撤销清单会依据在附录 C 内指明的时间表及格式更新。
- e) 有关香港邮政对于倚据证书人仕暂时未能获取已暂时吊销或撤销的证书的资料时的政策，已列于本准则第 2.1.5 条(倚据证书人士之义务)及第 2.2.1 条(合理技术及谨慎)

4.4.4 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后，即终止某一证书。

4.5 电脑保安审核程序

4.5.1 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审核追踪保安档案内。此等事件包括而限于以下例子：

- 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份的过程
- 定期管理证书之工作包括：
 - 处理撤销及吊销证书之要求
 - 实际发出、撤销及吊销证书
 - 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
 - 核证机关密码匙转换
 - 档案备存
 - 紧急密码匙复原

4.5.2 处理记录次数

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

4.5.3 审核记录之存留期间

存档审核记录文档存留期为七年。

4.5.4 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。

4.5.5 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。

4.5.6 审核资料收集系统

香港邮政核证机关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序、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。

4.5.7 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。

4.5.8 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。

4.6 记录存档

4.6.1 存档记录类型

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）存有以下数据：

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

4.6.2 存档保存期限

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

4.6.3 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。

4.6.4 存档备存程序

在有需要时制作并保存存档之副本。

4.6.5 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。

4.7 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 F）。香港邮政核证机关密码匙及证书在期满前至少三个月会进行续期。续发新根源密码匙后，相连之根源证书会在香港邮政网页<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 4.6.2 条指定之最短之时限，以供核对用原先密码匙进行产生之签署。

4.8 灾难复原及密码匙资料外泄计划

4.8.1 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执行。

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。

4.8.2 处理密码匙资料外泄计划

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

如根据本准则用作发出香港邮政银行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。

4.8.3 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银行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。

4.9 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。

4.10 核证登记机关终止服务

如核证登记机关停止担任核证登记机关之职能，且其代表香港邮政行使之授权已予以收回，香港邮政或相应核证登记机关将知会指明该核证登记机关之证书之登记人。尽管核证登记机关进一步代表香港邮政之权力被终止，银行证书仍按其条款继续有效直至届满（惟登记人必须就先前由核证登记机关处理与银行证书有关之事项直接与香港邮政交涉者除外），且于届满时，前核证登记机关须认可银行证书继续有效。倘代表香港邮政之核证登记机关之权力被撤回，则指明该核证登记机关之银行证书于届满后不得续期。

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，为核证机关运作做好准备。

5.1.2 进入控制

香港邮政实施商业上具合理实体保安之控制，限制进入就提供香港邮政核证机关服务而使用之硬件及软件（包括核证机关伺服器、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）。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。在任何时间都对进入进行控制及人手或电子监控，以防发生未经授权入侵。

5.1.3 电力及空调

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

5.1.4 自然灾害

核证机关设施在合理可能限度内受到保护，以免受自然灾害影响。

5.1.5 防火及保护

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妥。

5.1.7 场外备存

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

5.1.8 保管印刷文件

印刷文件包括登记人协议及身份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记录。

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，以及代表香港邮政行使权利之核证登记机关之雇员、承包商及顾问（统称「人员」），应视作承担受信职责。该等人员包括但不限于系统管理人员、操作员、工程人员及获委派监督香港邮政核证机关运作之行政人员。

香港邮政已为所有涉及香港邮政电子核证服务而承担受信职责之人员订立、汇编及推行相关程序。执行下列工作，有关程序即可完整进行：

- 按角色及责任订定各级实体及系统接达控制
- 职责划分

5.2.2 港邮政与核证登记机关之间的文件及资料传递

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

5.2.3 年度评估

评估工作每年执行一次，以确保符合政策及工作程序控制之规定。（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该等人员，以及代表香港邮政行使权利之核证登记机关人员，包括其雇员、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

香港邮政调查及 / 或要求承办商及核证登记机关调查其担任受信职责之人员（其受聘前及其后按需要定期进行），以按本准则之规定核实该等雇员之可信度及是否适任。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

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

5.3.4 向人员提供之文件

香港邮政人员及承办商人员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能措施。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 产生及安装配对密码匙

6.1.1 产生配对密码匙

除非程序被授权用户外泄，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授权用户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，在完成送递银行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银行证书（个人）及银行证书（机构）配对密码匙。

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址 <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。登记人配对密码匙则为 1024 位元 RSA。

6.1.5 加密模组标准

香港邮政进行之签署产生密码匙、存储及签署操作在硬件加密模组进行。

6.1.6 密码匙用途

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

6.2 私人密码匙保护

6.2.1 加密模组标准

香港邮政私人密码匙利用加密模组产生，其级别至少达到 FIPS140-1 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核证系统并无为香港邮政私人密码匙及登记人私人密码匙设计整体性密码匙托管程序。有关香港邮政私人密码匙的备存，见第 6.2.4 条。

6.2.4 香港邮政私人密码匙备存

香港邮政私人密码匙的备存，是使用达到 FIPS 140-1 第 2 级保安标准的装置加密及储存。香港邮政私人密码匙的备存程序须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。

6.3 配对密码匙管理其他范畴

香港邮政之公开及私人密码匙使用期不超过二十年。所有香港邮政密码匙之产生、销毁、储存以及证书及撤销清单签署运作程序，均于硬件加密模组内进行。第 4.6 条详述香港邮政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核证机关系统密码的生命周期）。香港邮政已制定保安程序，防止及侦测未获授权进入核证机关系统、更改系统及系统资料外泄等情况。此等保安控制措施接受第 2.6 条遵守规定之评估。

6.5 生命周期技术保安控制

香港邮政控制为香港邮政核证机关系统购置及发展软件及硬件之程序。现已定下更改控制程序以控制并监察就该等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，其配置只允许已获授权使用本准则所载核证机关服务者接达。

6.7 加密模组工程控制

香港邮政使用之加密装置至少达到 FIPS140-1 第 2 级。

7. 证书及证书撤销清单结构

7.1 证书结构

本准则提及之证书内有用于确认电子讯息发送人身份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 载有银行证书之特点摘要。

7.2 证书撤销清单结构

香港邮政证书撤销清单之格式为 X.509 第二版本（见附录 C）。

8. 准则管理

更改本准则一律须经香港邮政核准及公布。有关准则一经香港邮政在网址 <http://www.hongkongpost.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员及登记人均具约束力。就任何对本准则作出的更改，香港邮政会实际可行地尽快通知政府资讯科技总监。登记人及倚据证书人士可从香港邮政网址 <http://www.hongkongpost.gov.hk> 或有关核证登记机关网址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) 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。

“申请人” 指申请银行证书之自然人或法人。

“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。

“授权应用” 指核证登记机关发出之银行证书可能只适用于附录 E 第五栏中相对该核证登记机关之服务或系统。

“获授权代表” 指登记人机构之授权代表。

“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银行证书（机构）的私人密码匙。

“证书”或“银行证书” 指符合以下所有说明之记录：

- (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份或其他主要特征；
- (b) 识别发出记录之核证机关；
- (c) 指名或识别获发给记录者；
- (d) 经发出记录的核证机关签署。

“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” 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。

“承办商” 指香港亿软信息技术有限公司。其为由香港邮政根据认可核证机关业务守则第 3.2 段所委任为香港邮政核证机关于 2007 年 4 月 1 日至 2012 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系统及服务之代理人。

“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” 就电子记录而言，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

电子记录作数据变换产生,使持有原本未经数据变换之电子记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, 原本之电子记录是否未经变更。

“电子证书档案卡” 为一张智能卡, 是储存银行证书的储存媒体。

“电子记录” 指资讯系统产生之数码形式之记录, 而该记录:

- (a) 能在资讯系统内传送或由一个资讯系统传送到另一个资讯系统; 并
- (b) 能储存在资讯系统或其他媒介内。

“电子签署” 指与电子记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记录之目的订立或采用者。

“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) 记录资讯;
- (c) 用作使资讯记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 (不论该等资讯记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” 就某特定电子记录而言, 指代他人发出、接收或储存该记录, 或就该记录提供其他附带服务者。

“发出” 就证书而言, 指

- (a) 制造该证书, 然后将该证书包含的关于在该证书内指名或识别为获发给该证书的人的资讯, 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。

“线上即时认证” 指经由互联网确认证书有效性之协定。

“条例” 指香港法例第 553 章电子交易条例。

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

“PKCS#11 兼容装置” 指一种装置 (例如智能卡), 除可储存银行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 第三级或以上的认证。

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

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

“记录”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，代表香港邮政行使香港邮政核证机关一定职能，并提供香港邮政核证机关之若干服务之机构。

“倚据限额”指就认可证书倚据而指明之金额限额。

“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。

“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。

“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；或
- (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为合资格获签发银行证书(机构)之机构。

“稳当系统”指符合以下所有条件之电脑硬件、软件及程序：

- (a) 合理地安全可免遭受入侵及不当使用；
- (b) 在可供使用情况、可靠性及操作方式能于合理期内维持正确等方面达到合理水平。
- (c) 合理地适合执行其原定功能；及
- (d) 依循广为接受之安全原则。

为执行电子交易条例，如某数码签署可参照列于某证书内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 - 香港邮政银行证书格式

本附录详述由中继证书"Hongkong Post e-Cert CA 1 - 10"根据本核证作业准则签发的银行证书格式。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银行证书格式，请根据银行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) 银行证书（个人）证书格式

| 栏位名称 | 栏位内容 | |
|--|---|---|
| 标准栏 (Standard field) | | |
| 版本 (Version) | | X.509 V3 |
| 序号 (Serial number) | | [由香港邮政系统设置] |
| 签署算式识别 (Signature algorithm ID) | | sha1RSA |
| 发行者名称 (Issuer Name) | | cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK |
| 有效期 (Validity period) | 不早于 (Not before) | [由香港邮政设置的UTC 时间] |
| | 不迟于 (Not after) | [由香港邮政设置的UTC 时间] |
| 主体名称 (Subject name) | | cn=[香港身份证姓名] (附注1) e=[电子邮箱地址] (附注2) ou=[登记人参考编号] (附注3) o=Hongkong Post Bank-Cert (XXX- Personal) (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1024-bit |
| 发出人识别名称 (Issuer unique identifier) | | 未使用 |
| 登记人识别名称 (Subject unique identifier) | | 未使用 |
| 标准延伸栏位 (Standard extension) (附注5) | | |
| 机关密码匙识别名称 (Authority key identifier) | 发行者 (Issuer) | cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK |
| | 序号 (Serial number) | [从发出人处获取] |
| 密码匙的使用 (Key usage) | | 不可否认, 数码签署, 密码匙加密 (此栏为“关键”栏位) |
| 证书政策 (Certificate policy) | | PolicyIdentifier = [物件识别码] (附注6) PolicyQualifierID = CPS Qualifier = www.hongkongpost.gov.hk |
| 主体其他名称 (Subject alternative name) | DNS | [经加密的香港身份证号码] (附注7) |
| | rfc822 | [证书持有人电子邮箱地址] (附注2) |
| | 第一目录名称的共同名称 (1 st Directory) | [核证登记机关参考资料] |

| 栏位名称 | | 栏位内容 |
|--|----------------------------------|------------------------------|
| | Name CN) | |
| 发行者其他名称 (Issuer alternative name) | | 未使用 |
| 基本限制 (Basic constraints) | 主体类型 (Subject type) | 最终实体 |
| | 路径长度限制 (Path length constraints) | 无 |
| 延伸密码匙的使用 (Extended key usage) | | 未使用 |
| 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)
3. 登记人参考编号: 10 位数字
4. XXX 为核证登记机关名称 (见附录 E)
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. 申请人的香港身份证号码(包括括号内的数字)(以 hkid_number 表示)将会经申请人的私人密码匙签署并转化为一杂凑数值(以 cert_hkid_hash 表示)后, 存入证书:

$$cert_hkid_hash = SHA-1 (RSA_{privatekey, sha-1} (hkid_number))$$

SHA-1为一杂凑函数而RSA则为签署函数

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

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」。

2) 银行证书（机构）证书格式

| 栏位名称 | | 栏位内容 |
|--|---|--|
| 标准栏 (Standard field) | | |
| 版本 (Version) | | X.509 V3 |
| 序号 (Serial number) | | [由香港邮政系统设置] |
| 签署算式识别 (Signature algorithm ID) | | sha1RSA |
| 发行者名称 (Issuer) | | cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK |
| 有效期 (Validity period) | 不早于 (Not before) | [由香港邮政设置的UTC 时间] |
| | 不迟于 (Not after) | [由香港邮政设置的UTC 时间] |
| 主体名称 (Subject name) | | cn=[授权用户姓名] (附注1) e=[电子邮箱地址] (附注2) ou=[登记人参考编号] (附注3) ou=[商业登记证书编号+注册证书/登记证书编号+其他] (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 Bank-Cert (XXX-Corporate) (附注6) 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1024-bit |
| 发出人识别名称 (Issuer unique identifier) | | 未使用 |
| 登记人识别名称 (Subject unique identifier) | | 未使用 |
| 标准延伸栏位 (Standard extension) (附注7) | | |
| 机关密码匙识别名称 (Authority key identifier) | 发行者 (Issuer) | cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK |
| | 序号 (Serial number) | [从发出人处获取] |
| 密码匙的使用 (Key usage) | | 不可否认, 数码签署, 密码匙加密 (此栏为“关键”栏位) |
| 证书政策 (Certificate policy) | | PolicyIdentifier = [物件识别码] (附注8) PolicyQualifierID = CPS Qualifier = www.hongkongpost.gov.hk |
| 主体其他名称 (Subject alternative name) | DNS | 未使用 |
| | rfc822 | [证书持有人电子邮箱地址] (附注2) |
| | 第一目录名称的共同名称 (1 st Directory Name CN) | [核证登记机关参考资料] |
| 发行者其他名称 (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 |
|---|-------------------------------------|------------------------------|
| | 路径长度限制 (Path length constraints) | 无 |
| 延伸密码匙的使用 (Extended key usage) | | 未使用 |
| 证书撤销清单分发点 (CRL distribution point) | | 分发点名称 = [证书撤销清单分发点URL] (附注9) |
| Netscape 延伸栏位 (Netscape extension) (附注7) | | |
| 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)
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 (首 11 位数字/字母代表商业登记编号)【如无商业登记证书编号, 栏位全部为零(“0”)】，“注册证书 / 登记证书编号”栏位: 一串 8 位数字/字母【如无注册证书 / 登记证书编号, 栏位全部为零(“0”)】“其他”栏位: 最多 30 位字元 (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 3.1.1.4 条)。
6. XXX 为核证登记机关名称 (见附录 E)
7. 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。
8. 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。
9. 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」。

附录C - 香港邮政证书撤销清单(CRL)格式

本附录 C 详述有关由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的证书撤销清单的更新及公布安排和其格式。中继证书"Hongkong Post e-Cert CA 1"由 2010 年 2 月 26 日起停止发出认可证书,但会继续更新及公布证书撤销清单直至其有效期届满为止。如欲了解有关由中继证书"Hongkong Post e-Cert CA 1"所发出的证书撤销清单的更新及公布安排和其格式,请根据银行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。

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银行证书的资讯:

- 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。银行证书(个人)及银行证书(机构)的分割式证书撤销清单可于以下 URL 获取:

<http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl>

- b) 「整体证书撤销清单」(Full CRL)包含所有由中继证书"Hongkong Post e-Cert CA 1 - 10"所发出的已暂时吊销或已撤销证书的资料。公众可于以下 URL 获取「整体证书撤销清单」:

<http://crl1.hongkongpost.gov.hk/crl/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)

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(见本准则第 2.5 条)。在不能预见及有需要的情况下,香港邮政可不作事前通知而更改上述证书撤销清单的更新及公布的时序。

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 field) | 子栏位 (Sub-field) | 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 |
| 发行者 (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] | | 此栏列出已撤销的证书并以证书序号排列次序 |
| | 撤销日期 | [UTC 时间] | | 此栏显示撤销证书的日期 |

| 标准栏位 (Standard field) | 子栏位 (Sub-field) | 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 |
|--------------------------------------|---------------------------------------|--|--------------|--------------------------------------|
| | (Revocation date) | | | |
| | 输入证书撤销清单资料申延栏位 (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) | 发行者 (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。 |

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 - 香港邮政银行证书 — 服务摘要

| 服务 | 银行证书（个人） | 银行证书（机构） |
|-------------|--|--|
| 登记人 | 持有有效香港身份证及 <u>年满 18 岁</u> 人仕 | 获香港特别行政区政府签发有效商业登记证之机构及获香港法例认可之本港法定团体 |
| 证书持有人 | 即登记人 | 登记人机构之成员或雇员并为授权用户 |
| 依据限额 | HK\$200,000 | HK\$200,000 |
| 认可证书 | 是 | 是 |
| 配对密码匙 | 1024-bit RSA | 1024-bit RSA |
| 核证登记机关 | 见附录 E | 见附录 E |
| 制造配对密码匙 | 由香港邮政代制 | 由香港邮政代制 |
| 核实身份 | 须核对登记人的身份 | 须核对机构及其获授权代表的身份 |
| 证书的用途 | 数码签署及加密 | 数码签署及加密 |
| 证书内包含登记人的资料 | <ul style="list-style-type: none"> ▪ 香港身份证上列出的英文姓名； ▪ 香港身份证号码的杂凑数值 (hash value)； ▪ 电邮地址；及 ▪ 登记人参考编号（由香港邮政系统产生） | <ul style="list-style-type: none"> ▪ 登记人机构名称 ▪ 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 |
| 登记费用及证书有效期 | 见附录 E | 见附录 E |

附录E - 香港邮政银行证书核证登记机关名单

由本核证作业准则生效日期起，香港邮政银行证书并无指定之核证登记机关，香港邮政核证机关亦停止发出香港邮政银行证书。

对于在本核证作业准则生效日期前发出的香港邮政银行证书，倚据证书人士请参阅相关的银行证书核证作业准则。

附录F - 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日起停止发出银行证书。 |
| 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日起开始发出银行证书给申请者。 |