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（伺服器）

核证作业准则

日期：二零二二年九月三十日
物件识别码：1.3.6.1.4.1.16030.1.7.14

目录

前言 9
1. 引言 11
1.1 概述 11
1.2 文档名称与标识 11
1.3 公匙基建参与者 13
1.3.1 核证机关 13
1.3.2 注册机构 13
1.3.3 登记人 13
1.3.4 倚据人士 14
1.3.5 其他参与者 14
1.4 证书用途 14
1.4.1 适当证书用途 14
1.4.2 限制的证书应用 14
1.5 策略管理 14
1.5.1 策略文档管理机构 14
1.5.2 联系人 15
1.5.3 确定核证作业准则符合策略的人 15
1.5.4 核证作业准则批准程序 15
1.6 定义和缩写 15
2. 公布与储存库责任 16
2.1 储存库 16
2.2 认证资料的公布 16
2.3 公布的时间或频率 16
2.4 储存库进入控制 16
3. 鉴别及认证 17
3.1 命名 17
3.1.1 名称类型 17
3.1.2 名称需有意义 17
3.1.3 登记人的匿名或伪名 17
3.1.4 诠释各个名称规则 17
3.1.5 名称独特性 18
3.1.6 商标注册的认可、认证和角色 18
3.2 首次身份确认 18
3.2.1 证明拥有私人密码匙之方法 18
3.2.2 组织机构身份的鉴别 18
3.2.3 个人身份认证 20
3.2.4 没有验证的登记人资料 20
3.2.5 授权确认 20
3.2.6 互操作准则 20
3.3 密码匙更新请求的鉴别及认证 20
3.3.1 常规密码匙更新的鉴别及认证 20

3.3.2 证书撤销后密码匙更新的鉴别及认证 20
3.4 证书撤销申请的鉴别及认证 20
4. 证书生命周期操作要求 22
4.1 证书申请 22
4.1.1 谁能递交证书申请 22
4.1.2 登记过程与责任 22
4.2 处理证书申请 22
4.2.1 履行鉴别及认证职能 22
4.2.2 证书申请批准和拒绝 22
4.2.3 处理证书申请的时间 23
4.3 证书签发 23
4.3.1 证书签发期间核证机关的行为 23
4.3.2 核证机关向登记人发出签发证书通告 23
4.4 证书接受 23
4.4.1 构成接受证书的行为 23
4.4.2 核证机关对证书的发布 23
4.4.3 核证机关对其他实体的通告 24
4.5 配对密码匙和证书的使用 24
4.5.1 登记人私人密码匙和证书的使用 24
4.5.2 倚据人士公开密码匙和证书的使用 24
4.6 证书续期 24
4.6.1 证书续期的情形 24
4.6.2 谁能要求证书续期 25
4.6.3 证书续期请求的处理 25
4.6.4 发出新证书时对登记人的通告 25
4.6.5 构成接受续期证书的行为 25
4.6.6 核证机关对续期证书的发布 25
4.6.7 核证机关对其他实体的通告 25
4.7 证书密码匙更新 25
4.7.1 证书密码匙更新的情形 25
4.7.2 谁能要求证书公开密码匙更新 25
4.7.3 证书密码匙更新请求的处理 26
4.7.4 发出新证书时对登记人的通告 26
4.7.5 构成接受密码匙更新证书的行为 26
4.7.6 核证机关对密码匙更新证书的发布 26
4.7.7 核证机关对其他实体的通告 26
4.8 证书变更 26
4.8.1 证书变更的情形 26
4.8.2 谁能要求证书变更 26
4.8.3 证书变更请求的处理 26
4.8.4 发出新证书时对登记人的通告 26
4.8.5 构成接受变更证书的行为 26

4.8.6 核证机关对变更证书的发布 26
4.8.7 核证机关对其他实体的通告 26
4.9 证书撤销和暂时吊销 26
4.9.1 证书撤销的情形 27
4.9.2 谁能要求证书撤销 28
4.9.3 撤销请求的程序 28
4.9.4 撤销请求宽限期 29
4.9.5 核证机关处理撤销请求的时限 29
4.9.6 供倚据人士检查证书撤销的规定 29
4.9.7 证书撤销清单发布频率 30
4.9.8 发布证书撤销清单的最大滞后时间 30
4.9.9 线上撤销/状态查询的可用性 30
4.9.10 线上撤销查询规定 30
4.9.11 撤销公告的其他发布形式 30
4.9.12 密码匙资料外泄的特殊规定 30
4.9.13 证书暂时吊销的情形 30
4.9.14 谁能要求暂时吊销证书 31
4.9.15 要求暂时吊销的程序 31
4.9.16 暂时吊销的期限限制 31
4.10 证书状态服务 31
4.10.1 操作特征 31
4.10.2 服务可用性 31
4.10.3 运作特点 31
4.11 登记使用期结束 31
4.12 密码匙托管与复原 31
4.12.1 密码匙托管与复原的策略与实施 31
4.12.2 工作阶段密码匙的封装与复原的策略与实施 31
5. 设施、管理及运作控制 32
5.1 实体控制 32
5.1.1 选址及建造 32
5.1.2 实体访问 32
5.1.3 电力及空调 32
5.1.4 水患 32
5.1.5 火灾防护 32
5.1.6 媒体存储 32
5.1.7 废物处理 32
5.1.8 场外备存 32
5.2 程序控制 33
5.2.1 受信职责 33
5.2.2 每项任务需要的人数 33
5.2.3 每个职责的鉴别及认证 33
5.2.4 需要职责分离的角色 33

5.3 人员控制 33
5.3.1 资格、经验和清白要求 33
5.3.2 背景调查程序 33
5.3.3 培训要求 33
5.3.4 再培训周期和要求 34
5.3.5 工作岗位轮换周期和顺序 34
5.3.6 未授权行为的处罚 34
5.3.7 独立承办商的要求 34
5.3.8 向人员提供之文件 34
5.4 审计日志程序 34
5.4.1 记录事件的类型 34
5.4.2 处理纪录之次数 35
5.4.3 审核纪录之存留期间 35
5.4.4 审核纪录之保护 35
5.4.5 审核纪录备存程序 35
5.4.6 审核收集系统 (内部对外部) 35
5.4.7 事件主体的通告 35
5.4.8 脆弱性评估 35
5.5 纪录存档 35
5.5.1 存档纪录类型 35
5.5.2 存档保存期限 35
5.5.3 存档保护 36
5.5.4 存档备份程序 36
5.5.5 电子邮戳要求 36
5.5.6 存档收集系统 (内部对外部) 36
5.5.7 获取和验证存档资料的程序 36
5.6 密码匙变更 36
5.7 资料外泄与灾难复原 36
5.7.1 事件和资料外泄处理程序 36
5.7.2 计算机资源、软件和/或数据的损坏 36
5.7.3 私人密码匙资料外泄之程序 36
5.7.4 灾难复原计划 37
5.8 核证机关及核证登记机关终止服务 37
6. 技术保安控制 38
6.1 密码匙之产生及安装 38
6.1.1 产生配对密码匙 38
6.1.2 私人密码匙交付予登记人 38
6.1.3 公开密码匙交付予证书登记人 38
6.1.4 核证机关公开密码匙交付予倚据人士 38
6.1.5 密码匙大小 38
6.1.6 公开密码匙参数的生成和品质检查 38
6.1.7 密码匙用途 (按照 X.509 v3 密码匙使用方法栏位) 38

6.2 私人密码匙保护和加密模组控制 38
6.2.1 加密模组的标准和控制 38
6.2.2 私人密码匙(m 选 n)多人式控制 39
6.2.3 私人密码匙托管 39
6.2.4 私人密码匙备存 39
6.2.5 私人密码匙存档 39
6.2.6 私人密码匙于加密模组之间传递 39
6.2.7 私人密码匙在加密模组的存储 39
6.2.8 启动私人密码匙的方法 39
6.2.9 停用私人密码匙的方法 39
6.2.10 销毁私人密码匙的方法 39
6.2.11 加密模组的评估 39
6.3 配对密码匙管理其他范畴 39
6.3.1 公开密码匙存档 39
6.3.2 证书运作期限和配对密码匙使用期限 40
6.4 启动数据 40
6.4.1 启动数据的产生和安装 40
6.4.2 启动数据的保护 40
6.4.3 启动数据的其他方面 40
6.5 电脑保安控制 40
6.5.1 特定电脑保安技术要求 40
6.5.2 电脑保安评估 41
6.6 生命周期技术控制 41
6.6.1 系统开发控制 41
6.6.2 保安管理控制 41
6.6.3 生命周期的保安控制 41
6.7 网络保安控制 41
6.8 电子邮戳 41
7. 证书、证书撤销清单及线上证书状态应答结构 42
7.1 证书结构 42
7.1.1 版本编号 42
7.1.2 证书延伸栏位 42
7.1.3 算式物件识别码 42
7.1.4 名称格式 42
7.1.5 名称限制 42
7.1.6 证书策略物件识别码 42
7.1.7 策略限制延伸栏位使用的政策 42
7.1.8 策略限定资格的语法和语义的政策 42
7.1.9 关键证书策略延伸栏位的语义处理 42
7.2 证书撤销清单结构 42
7.2.1 版本编号 45
7.2.2 证书撤销清单及证书撤销清单资料延伸栏位 45

7.3 线上证书状态应答结构 45
7.3.1 版本编号 46
7.3.2 线上证书状态应答延伸栏位 46
8. 遵守规定审核和其他评估 47
8.1 评估的频率及情形 47
8.2 评估者的资格 47
8.3 评估者与被评估实体之间的关系 47
8.4 评估内容 47
8.5 对问题与不足采取的措施 47
8.6 评估结果的传达与发布 47
8.7 自我评估 47
9. 法律责任和其他业务条款 48
9.1 费用 48
9.1.1 证书签发和续期费用 48
9.1.2 证书查询费用 48
9.1.3 证书撤销或状态资讯的查询费用 48
9.1.4 其他服务费用 49
9.1.5 退款政策 49
9.2 财务责任 49
9.2.1 保险范围 49
9.2.2 其他资产 49
9.2.3 对最终实体的保险或担保 49
9.3 业务资料机密 49
9.3.1 机密资料范围 49
9.3.2 不属于机密的资料 49
9.3.3 保护机密资料的责任 49
9.4 个人资料隐私 49
9.4.1 隐私方案 50
9.4.2 视作隐私的资料 50
9.4.3 不被视作隐私的资料 50
9.4.4 保护隐私的责任 50
9.4.5 使用隐私资料的通告与同意 50
9.4.6 依法律或行政程序的资料披露 50
9.4.7 其他资料披露情形 50
9.5 知识产权 50
9.6 陈述与担保 50
9.6.1 核证机关的陈述与担保 50
9.6.2 核证登记机关的陈述与担保 51
9.6.3 登记人的陈述与担保 51
9.6.4 倚据人士的陈述与担保 52
9.6.5 其他参与者的陈述与担保 52
9.7 担保免责 52

9.8 有限责任 53
9.9 赔偿 54
9.10 有效期限与终止 55
9.10.1 有效期限 55
9.10.2 终止 55
9.10.3 终止与保留效力 55
9.11 参与人士的个别通告与通知 55
9.12 修订 55
9.12.1 修订程序 55
9.12.2 通知机制和期限 56
9.12.3 必须修改物件识别码的情形 56
9.13 争议处理 56
9.14 管辖法律 56
9.15 适用法律的符合性 56
9.16 一般条款 56
9.16.1 完整协议 56
9.16.2 转让 56
9.16.3 分割性 56
9.16.4 执行 (律师费和放弃权利) 56
9.16.5 不可抗力 57
9.17 其他条款 57
9.17.1 非商品供应 57
附录 A - 词汇及缩写 58
附录 B - 香港邮政电子证书格式 63
附录 C - 香港邮政证书撤销清单(CRL) 及香港邮政授权撤销清单(ARL) 73
附录 D - 香港邮政线上证书状态应答(OCSP Response)格式 80
附录 E - 香港邮政电子证书 – 服务摘要 82
附录 F - 香港邮政电子证书核证登记机关名单（若有的话） 83
附录 G - 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） 84
附录 H - 核证机关根源证书的有效期 85

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。

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 2020 年 1 月 1 日至 2022 年 6 月 30 日，并延长至 2023 年 6 月 30 日(包括当日)。

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 G** 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、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（伺服器）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（确认网域名称的职能除外）。**附录 F** 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。

本核证作业准则符合 RFC3647 互联网 X.509 公匙基建:证书策略及核证作业架构。

本核证作业之设计旨在符合以下计划最新版本的要求：

- 核证机关/浏览器论坛(CA / Browser Forum) 发布有关发行和管理公开可信证书的基线要求(“基线要求”)；
- 核证机关/浏览器论坛发布有关发行和管理延伸认证证书的准则（"延伸认证 SSL 证书准则"）；
- WebTrust 有关核证机关的原则及准则；
- WebTrust 有关核证机关的原则及准则 – 具网络安全的 SSL 基线
- WebTrust 有关核证机关的原则及准则 – 延伸认证 SSL

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、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。

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（伺服器），香港邮政已指明为认可证书。**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、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。

本准则符合 RFC 3647 的格式要求。 虽然某些章节标题根据 RFC 3647 的结构包含在本准则中, 但该主题不一定适用于香港邮政的服务， 这些章节会说明为 "没有规定"。标准结构的小节在有需要时会提供额外资讯。符合 RFC 3647 的格式要求增强和利便与其他第三方核证机关的对应和互操作性, 并预先为依据人士提供香港邮政作业实务和程序的通知。

附录 E 载有根据本准则发出之电子证书的特点摘要。

1.2 文档名称与标识

本文档为香港邮政核证机关之核证作业准则，自创建本文档以来, 已进行了下列修订。

修订编号	修订摘要	生效日期
1	首个与 RFC 3647 一致的香港邮政电子证书（伺服器）核证作业准则版本，以代替现有核证作业准则(物件识别码 1.3.6.1.4.1.16030.1.1.37)。	2018 年 5 月 31 日
2	更新第 4.2.1 条以符合基线要求(Baseline Requirement) 的网域验证做法	2018 年 7 月 30 日
3	更新香港邮政核证机关外判营运合约之合约期	2018 年 10 月 31 日
4	修正证书撤销和暂时吊销的程序； 更新前言：“核证登记机关履行香港邮政若干职能（确认网域名称的职能除外）”；及	2019 年 2 月 1 日

	更新第 4.9.1 条，纳入所有证书撤销的原因，以符合基线要求(Baseline Requirement)。	
5	由根源证书 Root CA 3 签发的电子证书（伺服器）及更改香港邮政核证机关域名有关的证书格式	2019 年 7 月 1 日
6	更新香港邮政核证机关外判营运合约之合约期	2020 年 1 月 1 日
7	为配合主要浏览器的根源证书政策有关「TLS 伺服器证书有效期不得超过 398 天」之要求，仅签发有效期为 1 年的证书。	2020 年 8 月 31 日
8	修正实体访问控制纪录的保存期限，以及 FIPS 的操作模式。	2021 年 3 月 8 日
9	更新第 4.9.12 条中与密码匙资料外泄相关的处理程序	2021 年 8 月 31 日
10	更新香港邮政核证机关外判营运合约之合约期	2021 年 12 月 31 日
11	延伸认证电子证书（伺服器）的推出	2022 年 1 月 21 日
12	更新公开登记/注册机关	2022 年 4 月 12 日
13	为符合核证机关/浏览器论坛(CA/Browser Forum)第 SC47v2 号表决获通过的要求，签发不包含"Organisational Unit"（OU）栏位的电子证书（伺服器）	2022 年 8 月 30 日
14	更新第 7.2 条，有关与电子证书（伺服器）对应的证书撤销清单资料中撤销原因代码的延伸栏位，可包含的指定撤销理由识别码	2022 年 9 月 30 日

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。**「1.3.6.1.4.1.16030.1.7.14」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）。除了此物件识别码外，所有符合基线要求的证书亦将包括以下由核证机关/浏览器论坛分配之其中一个额外识别码：

机构验证 SSL 证书 **“2.23.140.1.2.2”或**
延伸认证 SSL 证书 **“2.23.140.1.1”**

1.3 公匙基建参与者

1.3.1 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。

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、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。

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 2.3 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) 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 4.9 条），及
d) 通知登记人有关已撤销的证书（见第 4.9.5 条）。

1.3.2 注册机构

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、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。**

参阅**附录 F** -香港邮政电子证书核证登记机关名单（若有的话）

1.3.3 登记人

根据本核证作业准则，登记人指于**附录 A** 内所指的“登记人”或 “登记人机构”。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 1.3.2 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。

1.3.3.1 登记人之类别

根据本准则香港邮政仅发出电子证书（伺服器）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。

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。电子证书（伺服器）“通用版”之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“*”）。

电子证书（伺服器）乃根据核证机关/浏览器论坛 “基线要求”的机构验证规则进行验证。

若电子证书（伺服器）附设延伸认证（亦称延伸认证电子证书（伺服器）），则需根据核证机关/浏览器论坛 的“延伸认证 SSL 证书准则”进行验证。然而延伸认证电子证书（伺服器）只支援一个或多个伺服器名称，但不支援包含通配符之伺服器名称。

1.3.4 倚据人士

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。

1.3.5 其他参与者

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。

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。

参阅**附录 G** -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）

1.4 证书用途

1.4.1 适当证书用途

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。

电子证书（伺服器）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。

1.4.2 限制的证书应用

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。

1.5 策略管理

1.5.1 策略文档管理机构

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、撤销及公

布电子证书时采用之做法及标准。

1.5.2 联系人

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@eCert.gov.hk

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。

1.5.3 确定核证作业准则符合策略的人

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。

1.5.4 核证作业准则批准程序

本准则之更改一律须经香港邮政核准及公布。香港邮政有权更改此准则而不另行通知（见第 9.12 条）。

1.6 定义和缩写

参阅附录 A - 词汇及缩写

2. 公布与储存库责任

2.1 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。

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。

2.2 认证资料的公布

香港邮政储存库可透过下述 URL 接达：

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

或

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

2.3 公布的时间或频率

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。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。
香港邮政每年审查此准则并在必要时对其进行更新。此准则的新版本或修改版通常在其批准后七 (7) 天内发布。

2.4 储存库进入控制

储存库所在位置可供在线浏览，并可防止擅进。

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。

3. 鉴别及认证

3.1 命名

3.1.1 名称类型

3.1.1.1 主体名称

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；及

b) 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。

3.1.1.2 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（伺服器）之申请手续，然而该证书并不会辨识此获授权代表身分。

3.1.1.3 机构中文名称

电子证书（伺服器）以英文发出，其包含的机构名称可以是中文或英文。如电子证书（伺服器）之登记人机构在申请表格内提供中文机构名称，他们可选择在电子证书（伺服器）内显示中文机构名称。如机构未有选择，电子证书（伺服器）内将显示其英文机构名称。对于只有中文机构名称或只提供中文机构名称的电子证书（伺服器）登记人机构，机构的中文名称将显示在电子证书（伺服器）内。

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 登记人的匿名或伪名

香港邮政不会发出以匿名或假名进行伺服器验证的证书。

3.1.4 诠释各个名称规则

电子证书（伺服器）会载入之登记人名称(主体名称)类型见第 3.1.1 条。有关电子证书（伺服器）主体名称之诠释应参照**附录 B**。

3.1.5 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。域名的唯一性由网际网路名称与数字地址分配机构(ICANN)控制。

3.1.6 商标注册的认可、认证和角色

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。

香港邮政可酌情处理有关商标权、服务商标、商用名称、公司名称或知识产权之争议之事宜并享有最终决定权。

3.2 首次身份确认

所有电子证书（伺服器）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（伺服器）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。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 3.2.2 条所述身分证明。申请获批准后，香港邮政即准备证书并按第 4.3 条所述向申请人发出通知，说明如何发出证书。

3.2.1 证明拥有私人密码匙之方法

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.eCert.gov.hk 的指定网页传送给香港邮政。

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。

3.2.2 组织机构身份的鉴别

电子证书（伺服器）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。

3.2.2.1 电子证书（伺服器）

每份电子证书（伺服器）之申请须附有以下文件供香港邮政验证：

a) 盖上申请机构“For and on behalf of”（代表机构签署）印章及附有该机构申请人的获授权签署 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) 由香港特别行政区政府部门或有关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。

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。

3.2.2.2 延伸认证电子证书（伺服器）

香港邮政根据核证机关/浏览器论坛发布的延伸认证 SSL 证书准则第 11 条，按照下列各项，核实申请人机构身分的合法存在、实体存在和营运存在：

政府实体或私人机构

a) 如该机构于延伸认证 SSL 证书准则的定义中被视为政府实体或私人机构，每份延伸认证电子证书（伺服器）的申请必须附有与第 3.2.2.1 条所述相同的文件。香港邮政依据注册机关和登记机关发出的有关文件，核实该机构的合法存在。

商业实体

b) 如该机构于延伸认证 SSL 证书准则的定义中被视为商业实体，则除了第 3.2.2.1 条所述由登记机关发出的的文件外，其获授权代表须同时递交由第三方核证人（即香港公证人、执业会计师或执业律师）发出之"专业核证函件"， 其中需列明以下附加文件（验证文件）已由第三方核证人核证：

i) 申请人之个人声明，包括其个人目前或曾经使用的全名或名称（包括所有其他使用过的名称）、其可供联络的居住地址、出生日期，以及确认所有证书内容资料皆为真实且正确无误之声明。个人声明须由申请人签署，并须与申请表之签署相同;
ii) 申请人的香港身份证或护照副本;
iii) 至少两份包括申请人姓名以证明申请人身分的证明文件，其中一份证明文件必须来自金融机构。（1）可接受的金融机构文件包括信用卡/签账金融卡（该卡须列出到期日期，且该卡尚未到期）或物业按揭账单/银行账单（发出时间在过去六个月内），及（2）可接受的非金融文件包括能确认固定地址收取服务费用的近期水电煤费账单正本（不可是移动/手提电话账单）或租金付款账单的副本（该证明须列出日期，且日期必须为过去六个月内）;
iv) 商业登记证副本; 及
v) 申请人机构之有效的银行存款账户文件副本。

所有上述的验证文件之正本，必须提供给香港邮政作核实用途。 香港邮政会与申请人面对面核实及核对以下验证文件之正本：

i) 核对个人声明的内容，以确定包括申请人姓名、申请人签署和居住地址在内的资料和验证文件正本和申请表中的相对应资料一致;及
ii) 核对验证文件（包括申请人的香港身份证或护照的副本）是完整、真实和准确复制正本之文件。

香港邮政在收到 "专业核证函件"连同已核对的验证文件后，香港邮政会核实第三方核证人是否为香港合法公证人、执业会计师或执业律师，并会确认第三方核证人是否已验证了该验证文件。

所有申请：

c) 如果申请表中提供的业务地点地址资料无法在相关的香港政府部门或登记机构得到核实时，香港邮政或承办商可以实地考察业务地点，以获取显示申请人业务的记录（例如拍摄固定招牌、业务地点外部、业务地点内部接待区或工作区等照片）。

香港邮政在有怀疑的情况下，可拒绝有关申请。

3.2.3 个人身份认证

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 3.2.2 条所述身分证明。

3.2.4 没有验证的登记人资料

香港邮政按照核证机关/浏览器论坛基线要求第 7.1.4.2 条中定义的主体名称和主体别名进行认证。任何其他包含在电子证书 (伺服器)的未经认证的指定资料，香港邮政不须就此等提交给香港邮政的未经验证之登记人资料负责。

3.2.5 授权确认

授权确认包含确定获授权代表是否具有特定权限、权利或许可(包括允许代表登记人机构)以获得电子证书 (伺服器)。

所有电子证书 (伺服器) 的申请，获授权代表的授权均通过使用核证机关/浏览器论坛基线要求第 3.2.2.4 条中列出的一个或多个程序进行验证，以及根据基线要求第 3.2.5 条的可靠的通信方法进行。

就延伸认证电子证书（伺服器）而言，申请人的授权会根据延伸认证 SSL 证书准则第 11.8.3 条作进一步核实。 按照该准则第 11.5 条，香港邮政须发出电邮及获取申请人回复，以确认申请表格内提供的电话号码及电邮地址为核实的通讯方法，并确认透过该电话号码能可靠地联络申请人及验证获授权代表获申请人 的授权以代表申请人提交延伸认证电子证书（伺服器）的申请。

3.2.6 互操作准则

香港邮政根据本核证作业准则而发出的电子证书（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。

3.3 密码匙更新请求的鉴别及认证

香港邮政支援在证书期满前为现有证书提供密码匙更换以满足两个需要：

i) 证书替补，即在申请证书后更改了某些 (或没有更改) 主体资料，并且登记人希望(或不希望)更换新证书的配对密码匙;
ii) 证书续期，即登记人希望延长现有证书的使用期限，并更换证书的配对密码匙。

在以上两种情况下，必须依据第 4.2.1 条再次确认身份鉴别及认证。

3.3.1 常规密码匙更新的鉴别及认证

香港邮政不支援证书常规更换密码匙以作密码匙替补的请求。一般证书的密码匙会于证书续期过程中或因应香港邮政的酌情权于证书替补过程中被更换。

3.3.2 证书撤销后密码匙更新的鉴别及认证

香港邮政不得为已过期或已撤销的证书更换密码匙。

登记人或登记人机构的获授权代表必须按照第 3.2 条所述的首次登记手续申请证书。

3.4 证书撤销申请的鉴别及认证

香港邮政接到登记人或透过代理人提交的首次撤销证书要求后，会验证该请求及其原因。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(1)登记人在其提交要求的香港邮政网站的指定网页上进行身份认证，(2)收到由登记人以其私人密码匙进行数码签署之电子邮件,(3)登记人亲笔签署之信件正本或(4)登记人亲笔签署之撤销证书申请表格正本。

4. 证书生命周期操作要求

4.1 证书申请

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。

4.1.1 谁能递交证书申请

获香港特别行政区政府签发有效商业登记证之申请人其获授权代表，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，均可向香港邮政递交证书申请。

4.1.2 登记过程与责任

电子证书申请人必须完成登记程序, 其中包括:

a) 填妥申请表格并于香港邮政指定处所或香港邮政指定的其他机构的处所用递交；
b) 在登记过程中提供申请表格所规定的证明文件；
c) 缴交所需费用；
d) 产生私人密码匙及公开密码匙；
e) 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.eCert.gov.hk 的指定网页传送给香港邮政。

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 处理证书申请

4.2.1 履行鉴别及认证职能

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 3.2.2 条及第 3.2.3 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。同时，香港邮政会对列于证书上的域名进行核证机关授权记录的检查。若核证机关授权记录存在，但记录并未将香港邮政之域名”eCert.gov.hk”列入为获授权证书发出人的域名，则其证书申请将不会被继续处理。若列于证书上的域名并没有核证机关授权记录，则香港邮政认为申请人同意让香港邮政为其域名发出证书。

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)的完整网域名称(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 所规定) ; 或
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 所规定)。

4.2.2 证书申请批准和拒绝

在核对身分手续后，香港邮政有义务通知申请人其申请已被接纳或拒绝。申请被拒绝的申请人随后可重新申请。香港邮政有绝对酌情权保留拒绝申请的权力, 且无须对因拒绝申请而产生的任何损失或

费用承担任何责任。

4.2.3 处理证书申请的时间

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（伺服器）及延伸认证电子证书（伺服器）	十个工作天

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 4.2.3 条而言，一律不视作工作日计算。

4.3 证书签发

4.3.1 证书签发期间核证机关的行为

至少两名可直接参与证书签发并且已使用双重认证登入香港邮政系统的香港邮政人员输入并审核申请人的资料。在成功完成对申请人证书申请所需的核对后, 香港邮政批准其电子证书 (伺服器) 的申请。

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。

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。为按照 RFC6962 以支持证书透明度(Certificate Transparency)，香港邮政会将该证书发送到两个或以上的证书透明度日志(Certificate Transparency Logs)，以获取并附加证书签署时间戳(signed certificate timestamp)于电子证书上。

4.3.2 核证机关向登记人发出签发证书通告

在核对身分手续成功后, 香港邮政将发电子邮件到申请人指定的电子邮件地址通知其申请已被接纳。

4.4 证书接受

4.4.1 构成接受证书的行为

申请人于香港邮政指定网页 http://www.eCert.gov.hk 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。当申请人使用电子证书时, 即被视为已接受电子证书。

申请人可浏览证书档案或经香港邮政核证机关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。

4.4.2 核证机关对证书的发布

所有已获接受并已发出的电子证书将根据《电子交易条例》的规定在香港邮政储存库公布。

4.4.3 核证机关对其他实体的通告
核证登记机关如有参与发出证书的过程, 将可能会收到发出证书的通知。

4.5 配对密码匙和证书的使用

4.5.1 登记人私人密码匙和证书的使用
登记人负责：

a) 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。
b) 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）。
c) 在登记人明确知晓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香港邮政知会，香港邮政拟根据本准则之条款撤销证书后，均不得在交易中使用证书。
d) 在明知香港邮政可能据以撤销证书之任何事项之情况下，或登记人作出撤销申请或经香港邮政知会拟撤销证书时，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，因情形乃属如此，故倚据人士不得就交易而倚据证书。
e) 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。

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。

4.5.2 倚据人士公开密码匙和证书的使用
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 F**)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) 执行所有适当证书路径认可程序。
e) 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。

4.6 证书续期

4.6.1 证书续期的情形
香港邮政会于证书的有效期届满前，向电子证书（伺服器）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 6.3.2 条指明的证书有效期：

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

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

4.6.2 谁能要求证书续期

电子证书（伺服器）不会自动续期。若香港邮政接收到续期申请，即会根据 3.2.2 条所述“组织机构身份的鉴别”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.eCert.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。

4.6.3 证书续期请求的处理

续期申请规定和程序与首次申请发出证书时的规定和程序大致相同，并将根据第 3.2.2 条所述的 "组织机构身份的鉴别"之过程进行认证。 香港邮政将要求申请人更换其新证书的密码匙。

4.6.4 发出新证书时对登记人的通告

向申请人发出关于证书续期的通知与本准则第 4.3.2 条中所述有关新电子证书的方法相同。

4.6.5 构成接受续期证书的行为

申请人构成接受续期电子证书之行为与本准则第 4.4.1 条中所述相同。

4.6.6 核证机关对续期证书的发布

香港邮政发布续期电子证书的方式与本准则第 4.4.2 条中描述的方法相同。

4.6.7 核证机关对其他实体的通告

核证登记机关如有参与发出证书的过程, 将可能会收到发出证书的通知。

4.7 证书密码匙更新

4.7.1 证书密码匙更新的情形

更换证书密码匙包括在保留相同的主体资料之同时使用新的公开密码匙和序号产生新证书。一般证书的密码匙会于证书续期过程中或因应香港邮政的酌情权于证书替补过程中被更换。

4.7.2 谁能要求证书公开密码匙更新

香港邮政只会接受来自同一登记人有关电子证书更换密码匙的请求, 或酌情处理。但是, 香港邮政不会自动为电子证书 (伺服器)续期或要求更换密码匙。

4.7.3 证书密码匙更新请求的处理
证书密码匙更新请求的处理过程与发出新证书程序相同。

4.7.4 发出新证书时对登记人的通告
香港邮政将通过本准则第 4.3.2 条中所描述的方法通知更新了证书密码匙的登记人。

4.7.5 构成接受密码匙更新证书的行为
登记人构成接受密码匙更新的证书之行为与本准则第 4.4.1 条中列出的相同。

4.7.6 核证机关对密码匙更新证书的发布
香港邮政发布密码匙更新证书的方式与本准则第 4.4.2 条中描述的方法相同。

4.7.7 核证机关对其他实体的通告
核证登记机关如有参与发出证书的过程, 将可能会收到证书密码匙更新的通知。

4.8 证书变更
本核证作业准则不允许修改已发出的电子证书。

4.8.1 证书变更的情形
没有规定

4.8.2 谁能要求证书变更
没有规定

4.8.3 证书变更请求的处理
没有规定

4.8.4 发出新证书时对登记人的通告
没有规定

4.8.5 构成接受变更证书的行为
没有规定

4.8.6 核证机关对变更证书的发布
没有规定

4.8.7 核证机关对其他实体的通告
没有规定

4.9 证书撤销和暂时吊销
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 5.7.3 条）。

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

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。

4.9.1 证书撤销的情形

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。

不论何时，若有以下情况，香港邮政会于 24 小时内按准则中程序撤销电子证书（伺服器）：

1) 接到登记人透过香港邮政指定网页 http://www.eCert.gov.hk 的电子证书(伺服器) 撤销要求；
2) 接到登记人通知,电子证书 (伺服器) 的初次申请未经授权, 亦没有给予可追溯之授权；
3) 知道或有理由怀疑登记人的私人密码匙已外泄；或
4) 知道或有理由怀疑电子证书 (伺服器) 上之细节不真实或已变得不真实或证书不可靠, 包括但不限于不可倚据网域名称的确认或电子证书(伺服器) FQDN 的控制权。

不论何时，若有以下情况，香港邮政可在 24 小时内撤销电子证书 (伺服器), 并会在 5 日内按准则中程序撤销电子证书 (伺服器)：

5) 接到登记人透过传真、邮寄信件、电子邮件或亲身递交电子证书(伺服器) 撤销要求；
6) 认为电子证书 (伺服器) 不再符合核证机关/浏览器论坛基线要求第 6.1.5 和 6.1.6 条关于密码匙的大小和公开密码匙参数生成及品质检查的要求；
7) 得到证据显示电子证书(伺服器) 被不正当使用；
8) 认为登记人未有履行本准则或登记人协议列明之责任；
9) 知道或有理由怀疑电子证书（伺服器）中的 FQDN 有不合法律许可使用情况（例如法庭或仲裁员已撤销域名登记人使用网域名称的权利，域名登记人与申请人之间的相关许可或服务协议已终止，或域名登记人未能续订网域名称）；
10) 知道或有理由怀疑电子证书（伺服器）“通用版”被使用作核证属于欺诈误导的中继 FQDN；
11) 知道或有理由怀疑电子证书（伺服器）中的资料有重大变更；
12) 认为电子证书 (伺服器) 并非根据核证机关/浏览器论坛基线要求或本准则妥当发出；
13) 认为、知道或有理由怀疑电子证书（伺服器）中的任何资料不准确；
14) 香港邮政根据核证机关/浏览器论坛基线要求发出证书的权利届满或被撤销或终止时，有此规定（除非香港邮政已安排继续维護撤销证书清单及/或线上证书状态应答）；
15) 电子证书（伺服器）适用之本准则，规例或法例有此规定；
16) 认为登记人未曾缴付登记费；
17) 认为已经证明或证实有方法显示登记人的私人密码匙遭受外泄，已经开发了可以借着公开密码匙轻易计算出私人密码匙的方法（例如 Debian weak key，请参阅 http://wiki.debian.org/SSLkeys ），或者有明确证据显示用于生成私人密码匙的特定方法存在缺陷；
18) 知道或有理由相信电子证书 (伺服器) 中的任何 "主体名称" 或 "主体别名" (如有的话) 所指明的任何伺服器名称已不再为登记人机构所拥有；
19) 知道或有理由相信其资料出现在电子证书（伺服器）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。

现时本准则下的所有中继证书仅由香港邮政运作。如果发生以下一种或多种情况，则中继证书应在七（7）日内被撤销：

1) 香港邮政得到证据证明与中继证书中公开密码匙相对应的中继证书私人密码匙遭受外泄，或不再符合核证机关/浏览器论坛基线要求第 6.1.5 和 6.1.6 条关于密码匙的大小和公开密码匙参数生成及品质检查的的要求；
2) 香港邮政得到证据显示中继证书被不正当使用；
3) 香港邮政确认中继证书并非根据核证机关/浏览器论坛基线要求或本准则发出；
4) 香港邮政认为中继证书中的任何资料不正确或误道；
5) 香港邮政因任何原因停止核证机关之运作, 并且没有安排另一个核证机关为中继证书提供撤销支援;
6) 香港邮政根据核证机关/浏览器论坛基线要求发出证书的权利届满或被撤销或终止时 （除非香港邮政已安排继续维護撤销证书清单及/或线上证书状态应答）；
7) 根据香港邮政核证作业准则要求撤销；或
8) 中继证书的技术内容或格式给应用软体供应商或依据人士带来不可接受的风险。

4.9.2 谁能要求证书撤销

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.eCert.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。此外，登记人，依据人士，应用软体供应商和其他第三方可以提交证书问题报告以通知香港邮政撤销电子证书（伺服器）的合理原因。证书问题报告必须指明要求撤销的机构，并须指明有证据支持的撤销原因。香港邮政可在没有申请及不作事前通知之情况下撤销证书。

4.9.3 撤销请求的程序

香港邮政收到撤销证书要求后，将核证该请求并核实撤销的理由。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（1）登记人在其提交要求的香港邮政网站的指定网页上进行身份认证，（2）收到由登记人以其私人密码匙进行数码签署之电子邮件，（3）登记人亲笔签署之信件正本或（4）登记人亲笔签署之撤销证书申请表格正本。香港邮政将通过更新证书撤销清单，或在适用时更新相关的线上证书状态应答，并按照作业准则程序透过电子邮件（如果有联系电子邮件地址）通知登记人撤销证书（“撤销通知书”）。如果证书支持线上证书状态应答，该证书的线上证书状态应答将在证书到期后保持撤消状态。撤销证书申请表格可于网站 http://www.eCert.gov.hk 下载。

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。

4.9.4 撤销请求宽限期

撤销请求宽限期 ("宽限期") 指登记人必须在其进行撤销请求的期间。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。

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。

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。

4.9.5 核证机关处理撤销请求的时限

在香港邮政指定的网页向香港邮政提交撤销证书请求, 撤销将在 24 小时内反映在证书撤销清单中。对于其他方法的请求, 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，香港邮政决定撤销证书，由下一个工作日开始的 24 小时内，将该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撤销之状态。证书撤销清单每天发布 3 次，并存档至少 7 年。相反，如证书支援线上证书状态通讯规约，则证书的线上证书状态通讯规约应答将立即更新及发布以反映证书的撤销状态。

香港邮政会以合理的方式，尽量在收到撤销证书申请 24 小时内，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。

4.9.6 供倚据人士检查证书撤销的规定

倚据人士在依据本证书之前, 有负责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。

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。

有关香港邮政对于倚据人士暂时未能获取已撤销的证书资料时的政策，已列于本准则第 9.6.4 条(倚据人士之义务)及 9.7 条(合理技术及谨慎)。

4.9.7 证书撤销清单发布频率

当电子认证服务机构本身的证书被撤销时，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）)。

证书撤销清单及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。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.eCert.gov.hk 公布。

4.9.8 发布证书撤销清单的最大滞后时间

香港邮政不采用证书撤销清单的最大滞后时间。证书撤销清单通常在产生后的商业合理时间内自动张贴到储存库中。

4.9.9 线上撤销/状态查询的可用性

线上证书状态应答会依据在**附录 D** 内指明的格式即时更新及公布，以反映证书的撤销状态。

4.9.10 线上撤销查询规定

倚据人士必须在倚据证书之前，根据第 4.9.6 条确认证书的有效性。

4.9.11 撤销公告的其他发布形式

没有规定

4.9.12 密码匙资料外泄的特殊规定

任何能提供证书私人密码匙资料被外泄证据的人士（包括但不限于依据人士及应用软体供应商），可以透过香港邮政核证机关网站的密码匙外泄报告网页递交证据，以"密码匙资料外泄"为理由告知香港邮政。如果香港邮政发现或怀疑有私人密码匙资料被外泄，将以商业合理努力通知登记人，并在发现该等撤销原因之后或根据本准则第 7.2 条（a）之要求将证书撤销清单中的撤销原因代码更新为"密码匙资料外泄"。

透过密码匙外泄报告网页向香港邮政递交的报告包括了密码匙资料被外泄的证据，其证据的格式必须为以下两种之一：

a) 以资料被外泄之私人密码匙签署并以"香港邮政的密码匙资料被外泄证据"为其「通用名称」的「签发证书要求」，其签署可利用存放在香港邮政储存库内之有效证书之公开密码匙得以核实；或
b) 私人密码匙本身

4.9.13 证书暂时吊销的情形

不适用

4.9.14 谁能要求暂时吊销证书
不适用

4.9.15 要求暂时吊销的程序
不适用

4.9.16 暂时吊销的期限限制
不适用

4.10 证书状态服务

4.10.1 操作特征
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(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 7.3 条)。

4.10.2 服务可用性
证书状态服务为 24x7 保持开放。

4.10.3 运作特点
没有规定

4.11 登记使用期结束
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 5.5.2 条指定之最短之时限。

4.12 密码匙托管与复原

4.12.1 密码匙托管与复原的策略与实施
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。

4.12.2 工作阶段密码匙的封装与复原的策略与实施
没有规定

5. 设施、管理及运作控制

5.1 实体控制

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 实体访问
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至少 7 年。

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 水患
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。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。

5.1.5 火灾防护
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。

5.1.6 媒体存储
媒体存储及处置程序已经开发备妥。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。

5.1.7 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。

5.1.8 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 5.7.4 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。

5.2.2 每项任务需要的人数

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。

5.2.3 每个职责的鉴别及认证

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。

5.2.4 需要职责分离的角色

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

5.3 人员控制

5.3.1 资格、经验和清白要求

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 背景调查程序

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 再培训周期和要求
香港邮政及承办商或其核证登记机关应为其工作人员提供适当和足够的培训 (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。

5.3.5 工作岗位轮换周期和顺序
没有规定

5.3.6 未授权行为的处罚
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。

5.3.7 独立承办商的要求
被指派履行受信职责的承办商人员应遵守第 5.3 条定明的职责, 并受上述第 5.3.6 条处罚的约束。

5.3.8 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。

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。

5.4 审计日志程序

5.4.1 记录事件的类型
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：
  - 处理撤销证书之要求
  - 实际发出、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
  - 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

5.4.2 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。

5.4.3 审核纪录之存留期间
存档审核纪录文档存留期为七年。

5.4.4 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。

5.4.5 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。

5.4.6 审核收集系统 (内部对外部)
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。

5.4.7 事件主体的通告
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。

5.4.8 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。

5.5 纪录存档

5.5.1 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。

5.5.2 存档保存期限
密码匙及证书资料以及 5.5.1 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。

5.5.3 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。

5.5.4 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。

5.5.5 电子邮戳要求
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。

5.5.6 存档收集系统 (内部对外部)
存档资料由香港邮政内部收集。

5.5.7 获取和验证存档资料的程序
有关获取和验证存档资料的程序详情见第 5.5.4 条。

5.6 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二十五年（见**附录 H**）。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.eCert.gov.hk 公布供大众取用。原先之根源密码匙则保留至第 5.5.2 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。

5.7 资料外泄与灾难复原

5.7.1 事件和资料外泄处理程序
香港邮政维护事件处理程序, 以指导人员应对安全事件、自然灾害以及可能引起系统破坏的类似事件。为了维持证书服务的完整性, 香港邮政定立、汇编和定期测试适当的应急和灾害复原计画和程序。

5.7.2 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。

5.7.3 私人密码匙资料外泄之程序
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（伺服器）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。

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（伺服器）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。

5.7.4 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。

5.8 核证机关及核证登记机关终止服务

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。

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。

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。

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，其级别至少达到 FIPS 140-2 第 3 级。

6.1.2 私人密码匙交付予登记人

申请人自行产生私人密码匙。

6.1.3 公开密码匙交付予证书发出人

申请人将自行产生公开密码匙，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。

6.1.4 核证机关公开密码匙交付予倚据人士

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.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。

6.1.5 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。

6.1.6 公开密码匙参数的生成和品质检查

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。

6.1.7 密码匙用途 (按照 X.509 v3 密码匙使用方法栏位)

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 私人密码匙保护和加密模组控制

6.2.1 加密模组的标准和控制

香港邮政的加密模组其级别至少达到 FIPS 140-2 第 3 级。

6.2.2 私人密码匙(m 选 n)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 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 140-2 第 3 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。

6.2.5 私人密码匙存档
所有私人密码匙均不会存档。

6.2.6 私人密码匙于加密模组之间传递
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。

6.2.7 私人密码匙在加密模组的存储
香港邮政私人密码匙在加密模组产生，其级别至少达到 FIPS 140-2 第 3 级。

6.2.8 启动私人密码匙的方法
有关启动私人密码匙的方法的详情见第 6.2.2 条。

6.2.9 停用私人密码匙的方法
有关停用私人密码匙的方法的详情见第 6.2.2 条。

6.2.10 销毁私人密码匙的方法
香港邮政之核证机关密码匙使用期不超过二十五年（见第 5.6 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 5.5 条详述香港邮政公开密码匙纪录存档之工作。

6.2.11 加密模组的评估
有关加密模组分级的详情见本准则第 6.2.1 条。

6.3 配对密码匙管理其他范畴

6.3.1 公开密码匙存档
密码匙及证书资料以及第 5.5.1 条提及之存档纪录均妥为保存最少七年。

香港邮政之核证机关密码匙使用期不超过二十五年（见第 5.6 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 5.5 条详述香港邮政公开密码匙纪录存档之工作。

6.3.2 证书运作期限和配对密码匙使用期限

香港邮政之核证机关密码匙使用期不超过二十五年（见第 5.6 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 5.5 条详述香港邮政公开密码匙纪录存档之工作。

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（伺服器），包括电子证书（伺服器）“通用版 " 或“多域版 "	一年
延伸认证电子证书（伺服器）	一年

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 4.6 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**。

6.4 启动数据

6.4.1 启动数据的产生和安装

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。

6.4.2 启动数据的保护

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。

6.4.3 启动数据的其他方面

没有规定

6.5 电脑保安控制

6.5.1 特定电脑保安技术要求

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关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 8 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。

6.5.2 电脑保安评估
没有规定

6.6 生命周期技术控制

6.6.1 系统开发控制
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关人员或在特殊情况下由其它机关进行开发工作，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。

6.6.2 保安管理控制
香港邮政透过程序实施对其核证机关系统的保安相关配置和保安软体更改的控制。这些程序包括检查应用程式和保安软体的完整性。

6.6.3 生命周期的保安控制
没有规定

6.7 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关网络环境的安全，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。

6.8 电子邮戳
香港邮政使用网路时间协定 (NTP) 与可靠的时间服务至少每八小时一次同步更新其电脑上的系统时间(Windows 预设)。香港邮政不向公众提供任何电子邮戳服务。

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）。**附录 E** 载有电子证书（伺服器）之特点摘要。

7.1.1 版本编号

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**）。

7.1.2 证书延伸栏位

本准则提及之证书格式详情见**附录 B**。

7.1.3 算式物件识别码

本准则提及之证书格式详情见**附录 B**。

7.1.4 名称格式

本准则提及之证书格式详情见**附录 B**。

7.1.5 名称限制

本准则提及之证书格式详情见**附录 B**。

7.1.6 证书策略物件识别码

本准则提及之证书格式详情见**附录 B**。

7.1.7 策略限制延伸栏位使用的政策

本准则提及之证书格式详情见**附录 B**。

7.1.8 策略限定资格的语法和语义的政策

本准则提及之证书格式详情见**附录 B**。

7.1.9 关键证书策略延伸栏位的语义处理

本准则提及之证书格式详情见**附录 B**。

7.2 证书撤销清单结构

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电子证书的资讯。

当电子证书（伺服器）因以下其中一个原因被撤销时，证书对应的证书撤销清单的撤销原因代码延伸栏位必须包含指定的撤销理由识别码。 当撤销理由识别码不是以下其中一个时，证书撤销原因代码延伸栏位将不会提供撤销理由识别码：

撤销原因	撤销理由识别码 （RFC5280 中指明的证书撤销清单原因 （CRLReason））
密码匙資料外泄	1 = 密码匙資料外泄（keyCompromise）
特权被撤销	9 = 特权被撤销（privilegeWithdrawn） （撤销理由识别码“特权被撤销”不需要作为撤销原因选项提供给证书登记人，因使用该撤销理由识别码是由核证机关操作员决定而不是登记人。）
终止营运	5 = 终止营运（cessationOfOperation）
联系变更	3 = 联系变更（affiliationChanged）
证书被取代	4 = 证书被取代（superseded）

以下说明香港邮政核证机关或登记人有义务使用撤销理由识别码的各个撤销情况：

a） 撤销理由识别码（1）“密碼匙資料外泄”

当发生以下一个或多个情况时，将会使用撤销理由识别码“密码匙资料外泄”：

- 香港邮政核证机关得到可核实的证据，证明与证书中公开密码匙相对应的证书登记人私人密码匙遭受外泄；或
- 香港邮政核证机关得知已经证明或证实有方法显示证书登记人的私人密码匙遭受外泄；或
- 有明确证据显示用于生成私人密码匙的特定方法存在缺陷；或
- 香港邮政核证机关得知一种已经证明或证实有方法，该方法可以藉着证书中的公开密码匙轻易计算出证书登记人的私人密码匙（例如 Debian weak key，请参阅 https://wiki.debian.org/SSLkeys）；或
- 证书登记人要求香港邮政核证机关以此撤销理由撤销证书，撤销范围说明如下。

如要求以“密码匙资料外泄” 理由撤销证书的任何人士，透过本准则第 4.9.12 条所述的香港邮政核证机关网站上的密码匙外泄报告网页证明其以往或目前拥有证书的私人密码匙，则香港邮政核证机关将撤销涵盖所有登记人有出现该密码匙的所有情况。

如证书登记人以“密码匙资料外泄”理由要求香港邮政核证机关撤销证书，并且没有证明其以往或目前拥有证书的相关私人密码匙，香港邮政核证机关可以撤销与该登记人相关的所有包含该公开密码匙的证书。

当香港邮政核证机关得到可核实的证据证明证书私人密码匙外泄，但证书撤销清单资料并不包含原因代码延伸栏位，或包含非“密码匙资料外泄”理由于原因代码延伸栏位时，则香港邮政核证机关可以更改证书撤销清单将“密码匙资料外泄”理由作为撤销理由识别码加入原因代码延伸栏位。此外，当香港邮政核证机关确定证书的私人密码匙在证书撤销清单中指示的撤销日期之前已被外泄时，可以更改该证书在证书撤销清单中的撤销日期。

（注意：根据 RFC 5280 第 5.3.2 条中描述，将撤销日期追溯至过去某时是最佳做法的一个例外情况；但是，本准则为支援应用软体供应商，会使用证书首次外泄日期作为撤销日期。）

否则，不得使用“密码匙资料外泄”撤销理由识别码。

b) 撤销理由识别码（9）“特权被撤销”

撤销理由识别码“特权被撤销”旨在用于登记人涉及未导致“密码匙资料外泄”的违规行为的情况，例如证书登记人在其证书申请中提供了误导性信息，或登记人未坚守其在登记人协议或使用条款之重大义务。

除非 “密码匙资料外泄”撤销理由识别码已被使用，否则在以下情况下必须使用撤销理由识别码“特权被撤销”：

- 香港邮政核证机关得到证书被不正当使用的证据；或
- 香港邮政核证机关得知证书登记人违反了登记人协议或使用条款中的一个或多个重大义务；或
- 香港邮政核证机关得知电子证书（伺服器）“通用版” 证书被使用作核证属于欺诈误导的中继完整网域名称（FQDN）；或
- 香港邮政核证机关得知证书中的所载资料有重大变动；或
- 香港邮政核证机关确定或得知证书中的任何资料不准确；或
- 香港邮政核证机关得知证书的初次申请未经授权，且登记人亦没有给予可追溯之授权。

否则，不得使用“特权被撤销”撤销理由识别码。

c) 撤销理由识别码（5）“终止营运”

撤销理由识别码“终止营运”旨在用于使用证书的网页在证书到期前关闭的情况，或登记人不再拥有或控制证书中指明的网域名称。 此撤销理由识别码旨在以下情况使用：

- 证书登记人不再控制或不再被授权使用证书中指明的所有网域名称；或
- 证书登记人因为将终止其网站而不再使用证书；或
- 香港邮政核证机关得知任何情况表明使用在证书中的完整网域名称（FQDN）不再合法（例如法庭或仲裁员已撤销域名登记人使用网域名称的权利，域名登记人与申请人之间的相关许可或服务协议已终止，或域名登记人未能续订网域名称）。

除非“密码匙资料外泄”撤销理由识别码已被使用，否则在以下情况下必须使用撤销理由识别码“终止营运”：

- 证书登记人已为此原因要求撤销其证书；或
- 香港邮政核证机关收到可核实的证据，证明证书登记人不再控制或不再被授权使用证书中指明的所有网域名称。

否则，不得使用“终止营运”撤销理由识别码。

d) 撤销理由识别码（3）“联系变更”

撤销理由识别码“联系变更”旨在用于表明证书中的主体名称或其他主体识别资料已更改，但没有理由怀疑证书的私人密码匙已被外泄。

除非“密码匙资料外泄”撤销理由识别码已被使用，否则在以下情况下必须使用撤销理由识别码“联系变更”：

- 证书登记人已为此原因要求撤销其证书；或
- 香港邮政核证机关因证书的主体资料转变而重新发出证书，而且核证机关并没有用其他撤销证书原因（包括“密码匙资料外泄”、“证书被取代”、“终止营运”或“特权被撤销”）更换此证书。

否则，不得使用“联系变更”撤销理由识别码。

e） 撤销理由识别码（4）“证书被取代”

撤销理由识别码“证书被取代”旨在用于显示以下情况：

- 证书登记人已要求以新证书替换现有证书；或
- 香港邮政核证机关得到合理证据，证明不可倚据网域名称的确认或证书之完整网域名称（FQDN）的控制权；或
- 香港邮政核证机关基于要遵守守则的原因撤销证书，例如证书不符合本准则、核证机关/浏览器论坛（CA/Browser Forum）的基线要求或主要的根源证书计划的核证政策（例如 Mozilla 根源证书存储政策）。

除非“密码匙资料外泄”撤销理由识别码已被使用，否则在以下情况下必须使用撤销理由识别码“证书被取代”：

- 证书登记人已为此原因要求撤销其证书；或
- 香港邮政核证机关因域名授权或遵守守则出现问题（而不是与“密码匙资料外泄”或“特权被撤销”相关的问题）而撤销证书。

否则，不得使用“证书被取代”撤销理由识别码。

有关证书撤销清单结构详情见**附录 C**。

7.2.1 版本编号

香港邮政之证书撤销清单一律以 X.509 第二版本之格式发出（见**附录 C**）。

7.2.2 证书撤销清单及证书撤销清单资料延伸栏位

证书撤销清单及证书撤销清单资料延伸详情见**附录 C**。

7.3 线上证书状态应答结构

通过发布一个包含以下主体名称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 CA 及中继证书进行线上证书状态通讯规约的签署。

根源证书：

证书主体名称 (CN)	线上证书状态通讯规约签署人证书主体名称 (CN)

“Hongkong Post Root CA 1”	“Hongkong Post Root CA 1 OCSP Responder”
“Hongkong Post Root CA 3”	“Hongkong Post Root CA 3 OCSP Responder”

中继证书：

证书主体名称 (CN)	**线上证书状态通讯规约签署人证书主体名称 (CN)**
“Hongkong Post e-Cert CA 1 - 15”	“Hongkong Post e-Cert CA 1 - 15 OCSP Responder”
“Hongkong Post e-Cert SSL CA 3 - 17”	“Hongkong Post e-Cert SSL CA 3 - 17 OCSP Responder”
“Hongkong Post e-Cert EV SSL CA 3 - 17”	“Hongkong Post e-Cert EV SSL CA 3 - 17 OCSP Responder”

有关线上证书状态应答结构详情见**附录 D**。

7.3.1 版本编号

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

7.3.2 线上证书状态应答延伸栏位

线上证书状态应答延伸栏位详情见**附录 D**。

8. 遵守规定审核和其他评估

本准则中的实务守则旨在满足或超过行业标准 (如 WebTrust 对核证机关) 的要求。香港邮政作为认可核证机关, 须根据条例 43 (1)编写和提交评估报告。

8.1 评估的频率及情形

遵守规定审核及评估须至少每 12 个月进行一次。

8.2 评估者的资格

需聘请符合条例及认可核证机关业务守则规定资格的之独立外部审计人员进行遵守规定评估。WebTrust 审计员必须符合核证机关/浏览器论坛基线要求第 8.2 条的要求。

8.3 评估者与被评估实体之间的关系

根据条例及认可核证机关业务守则所规定，香港邮政须聘请与之不相关之独立外部审计人员进行遵守规定评估。

8.4 评估内容

须根据条例以及认可核证机关业务守则之规定进行遵守规定之评估，检视香港邮政发出、撤销及公布证书之系统是否妥善遵守本准则。

8.5 对问题与不足采取的措施

如审核报告指出有任何不符合法律、本准则或任何其他与香港邮政服务相关之其他构成合约之义务, 则 (1) 审计人员将记录其差异, (2) 审计员将人及时通知香港邮政, (3) 视差异的性质和程度, 香港邮政将制定一个适当的修正行动计画以消除不符合的地方, 并决定是否对已经发出的电子证书采取任何补救行动。

8.6 评估结果的传达与发布

核证机关的 WebTrust 审核报告在 http://www.eCert.gov.hk/product/cps/ecert 提供给公众。根据条例 43 (1) 条所订的遵守规定评估报告,则会呈交政府资讯科技总监。

8.7 自我评估

香港邮政至少每季度对自上次自我审计以后发布的电子证书中随机选择至少 3%的样本进行自我审核。电子证书的自我审核须按照核证机关/浏览器论坛通过的准则进行。

9. 法律责任和其他业务条款

9.1 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，香港邮政可撤销证书（见第 4.9.1(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.eCert.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。

9.1.1 证书签发和续期费用

电子证书（伺服器）收费	一年有效期的电子证书
不属于“通用版＂或“多域版＂之 新申请或续期	每份电子证书 港币 2,500 元
“通用版＂之 新申请或续期	每份电子证书港币 8,700 元 + 每个附加伺服器 港币 500 元
	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。承办商就电子证书（伺服器）("通用版")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.eCert.gov.hk 或经由第 1.5.2 条所列之途径向香港邮政核证机关作出查询。
“多域版＂之 新申请或续期	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
	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。
延伸认证电子证书（伺服器）之 新申请或续期	每份电子证书 港币 3,000 元
延伸认证电子证书（伺服器）“多域版＂之 新申请或续期	每份电子证书港币 3,500 元 + 每个额外伺服器名称 港币 2,500 元
	延伸认证电子证书（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。

9.1.2 证书查询费用

香港邮政可能对直接进入其证书资料库收取合理费用。

9.1.3 证书撤销或状态资讯的查询费用

香港邮政不会收取撤销证书费用，亦不会对使用证书撤销清单或线上证书状态应答查阅已发出证书的有效性收取费用。

9.1.4 其他服务费用
没有规定

9.1.5 退款政策
尽管已列明在第 9.8 条中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。

9.2 财务责任

9.2.1 保险范围
香港邮政维持一般商业责任保险涵盖至少 200 万美元，及延伸认证 SSL 证书准则中规定的职业责任/过失保险至少 500 万美元。 此外，另一独立之保单已经备妥，有关证书之潜在或实质责任以及根据电子交易条例的规定对倚据限额之索偿均获承保。

9.2.2 其他资产
没有规定

9.2.3 对最终实体的保险或担保
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 业务资料机密

9.3.1 机密资料范围
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；香港邮政或承办商需根据本准则履行其责任之情况除外。

9.3.2 不属于机密的资料
任何未列为机密的资讯都被视为公共资讯。已发布的证书和撤销资料被视为公共资讯。

9.3.3 保护机密资料的责任
在履行与香港邮政发出、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。

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。

9.4 个人资料隐私

9.4.1 隐私方案
香港邮政实施了一项符合本准则的隐私政策。香港邮政隐私政策在香港邮政网站 http://www.eCert.gov.hk 发布。

9.4.2 视作隐私的资料
任何不在已发出的证书、储存库和证书撤销清单公开的登记人资料均视作隐私资料。

9.4.3 不被视作隐私的资料
已发布的证书及撤销资料均被视作公开资料。证书状态资讯和任何证书内容均视作非隐私资料。

9.4.4 保护隐私的责任
在履行与香港邮政发出、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。

9.4.5 使用隐私资料的通告与同意
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；香港邮政或承办商需根据本准则履行其责任之情况除外。

9.4.6 依法律或行政程序的资料披露
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。

9.4.7 其他资料披露情形
没有规定

9.5 知识产权
香港邮政拥有与其资料库、网站、电子证书、商标和来自香港邮政的任何其他出版物（包括本准则）相关的所有知识产权。

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。

9.6 陈述与担保

9.6.1 核证机关的陈述与担保
认可证书一经登记人接受及发出后，香港邮政发布在其储存库中（见第 2 条）。

根据本准则而发出之证书，香港邮政向根据本准则第 9.6.4 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 9.6.4 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。

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。

9.6.2 核证登记机关的陈述与担保

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、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。**

9.6.3 登记人的陈述与担保

各申请人（申请电子证书（伺服器），获授权代表会代表申请人）须签署或确定接受一份协议（按本准则规定之条款），其中载有一条款，申请人据此条款同意，申请人一经接受根据本准则发出之证书，即表示其向香港邮政保证（承诺）并向所有其他有关人士（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（伺服器）登记人的授权用户外，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 1.4 条指明的用途。
d) 证书所载之所有资料及由登记人作出之陈述均属真实。
e) 证书将只会用于符合本核证作业准则之认可及合法用途。
f) 在证书申请过程中所提供之所有资料，均并无侵犯或违反任何第三方之商标、服务标记、品牌、公司名称或任何知识产权。

登记人负责：

a) 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（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。
b) 准确地按照本准则所载关于证书之程序直至证书过期。
c) 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。
d) 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。
e) 在登记人明确知晓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香港邮政知会，香港邮政拟根据本准则之条款撤销证书后，均不得在交易中使用证书。
f) 在明知香港邮政可能据以撤销证书之任何事项之情况下，或登记人作出撤销申请或经香港邮政知会拟撤销证书时，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，因情形乃属如此，故倚据人士不得就交易而倚据证书。
g) 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。
h) 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。

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。

9.6.4 倚据人士的陈述与担保

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 F**)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) 执行所有适当证书路径认可程序。
e) 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。

9.6.5 其他参与者的陈述与担保

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。

9.7 担保免责

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。

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。

9.8 有限责任

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。

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。

除下文所述例外情况外，在香港邮政违反：

c) 本登记人协议及核证作业准则条文；或
d) 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（伺服器）不得超过 20 万港元。

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、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。

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。

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。

9.9 赔偿

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.eCert.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、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没有规定于个人伤害或死亡之（不大可能发生之）情形。”

9.10 有效期限与终止

9.10.1 有效期限

有关准则一经香港邮政在网页 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。

9.10.2 终止

本准则 (包括所有修订和增编) 继续有效, 直到被更新版本取代为止。

9.10.3 终止与保留效力

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。

9.11 参与人士的个别通告与通知

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。

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@eCert.gov.hk

9.12 修订

9.12.1 修订程序

香港邮政批准更新其核证作业准则后，有关准则一经香港邮政在网页 http://www.eCert.gov.hk 或香港邮政储存库公布，更改即时生效，并对当时及之后获发证书的申请人以及登记人均具约束力。

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。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。

9.12.2 通知机制和期限
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.eCert.gov.hk 或香港邮政储存库浏览此份准则以及其旧有版本。

9.12.3 必须修改物件识别码的情形
香港邮政有权决定核证作业准则的修订是否需要同时更改物件识别码(OID)。

9.13 争议处理

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@eCert.gov.hk

9.14 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。

9.15 适用法律的符合性
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。

9.16 一般条款

9.16.1 完整协议
本准则中英文本措词诠释若有歧异，以英文本为准。

9.16.2 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。

9.16.3 分割性
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。

9.16.4 执行 (律师费和放弃权利)

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@eCert.gov.hk

9.16.5 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；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。

9.17 其他条款

9.17.1 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 9.8 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。

附录 A - 词汇及缩写

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”指自然人或法人并已申请电子证书。

“应用软体供应商”指互联网浏览器软件或其他依据人士应用软件的供应商，该软件显示或使用证书并包含香港邮政根源证书。

“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。

“商业实体”指任何根据延伸认证 SSL 证书准则定义的非私人机构、非政府实体及非商贸实体之登记人机构，登记人机构并非有限公司且仅持有香港特别行政区政府税务局发出 的商业登记证（BR）。

“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发出证书。

“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。

“证书问题报告” 指对涉嫌密码匙泄露，证书滥用或其他类型的欺诈，妥协，滥用或与证书相关的不当行为的投诉。

“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。

“证书透明度”指按照 RFC6962 和 Google 的要求，所提供给公开审核及监视的一个有关核证机关发出电子证书的日志。

“证书透明度日志”是一个加密的、可公开审核的、仅限附加记录伺服器电子证书的一个简单的网络服务。

“密码匙外泄报告网页”是香港邮政核证机关网站上的一个网页，用於向香港邮政报告与证书相关的怀疑私人密码匙资料外泄。

“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 2020 年 1 月 1 日至 2022 年 6 月 30 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。该合约年期已延长至 2023 年 6 月 30 日(包括当日)。

“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 G**，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。

“网域名称”表示网域名称系统中分配的节点标签。

“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。

“延伸认证”就支援延伸认证的香港邮政电子证书（伺服器）而言，是指包含延伸认证 SSL 证书准则中指定的主体资料，并已根据延伸认证 SSL 证书准则进行认证的电子证书。

“延伸认证 SSL 证书准则”指核证机关/浏览器论坛在 http://www.cabforum.org 发布有关发行和管理延伸认证证书的准则。

“完整网域名称”指包含网域名称系统中所有上级节点标签的网域名称。

“政府实体”指香港特别行政区政府政策局或部门，或获香港特别行政区法律认可之本港法定团体。

“ 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。

“香港”指中华人民共和国香港特别行政区。

“注册机关”就延伸认证电子证书（伺服器）而言：

(a) 在“私人机构”的文意下，指香港特别行政区政府公司注册处（见 https://www.cr.gov.hk/），在其职能下登记核实实体的合法存在；或
(b) 在“政府实体”的文意下，指制定香港特别行政区法例、规例或判令以成立政府实体合法存在的实体。

“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。

“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。

“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。

“公证人"指持有有效公证人委任证明书并在香港特别行政区高等法院备存的公证人注册纪录册上注册之律师。

“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》。

“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。

“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。

“香港邮政署长”指香港法例第 98 章《邮政署条例》所指署长。

“执业会计师”指持有根据《专业会计师条例》（第 50 章）发出有效执业证书的会计师。

“执业律师”指持有有效执业证书并在香港特别行政区高等法院备存的律师登记册上登记的律师。

“私人密码匙”指配对密码匙中用作产生数码签署之密码匙。

“私人机构”指任何持有公司注册处签发的公司注册证书 （CI） 及香港特别行政区政府税务局签发的商业登记证（BR）的登记人机构。

“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。

“登记机关” 指为组建业务或根据许可证、契约或其他证明授权开展业务的实体进行登记商业资讯的香港特别行政区政府税务局（见 https://www.ird.gov.hk/）。

“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。

“可靠的通讯方法”指除由获授权代表提供以外的已核实通讯方法, 如邮寄快递地址、电话号码或电邮地址。

“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。

“证书签署时间戳”指当提交一张有效的伺服器电子证书到一个证书透明度日志后，该日志会发出一个证书签署时间戳，以表示容许将该证书在某特定时间内加到日志内。

“智能身份证”指可将电子证书载入其中的身份证。

“S/MIME”即保密／多功能互联网邮递伸延的缩写

“SSL”即保密插口层的缩写

“中继证书”指由香港邮政的根源证书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。

“主体名称”指证书持有者名字的信息。

“TLS”即传输层保安协定的缩写

“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。

“专业核证函件”指根据延伸认证 SSL 证书准则中规定之已核实的会计师函件或已核实的法律意见书 。

“WebTrust for Certification Authorities” 即在 http://www.webtrust.org 公布之现有的加拿大注册会计师（CPA）WebTrust 计划。

“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。

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"、"Hongkong Post e-Cert CA 1-15"、"Hongkong Post e-Cert SSL CA 3-17"及"Hongkong Post e-Cert EV SSL CA 3-17"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) 根源证书“Hongkong Post Root CA 1”之下的电子证书（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）:-

(香港邮政核证机关自 2016 年 1 月 1 日起已停止由中继证书" Hongkong Post e-Cert CA 1 - 10" 签发电子证书 (伺服器)。)

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		

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 "
	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		
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）:-

(香港邮政核证机关自 2016 年 9 月 1 日起已停止由中继证书" Hongkong Post e-Cert CA 1 - 14" 签发电子证书 (伺服器)。)

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]		

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 "
	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）:-

（香港邮政核证机关自 2019 年 7 月 1 日起已停止由中继证书″Hongkong Post e-Cert CA 1-15″签发电子证书 （伺服器）。）

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		
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)]		

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 "
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] Policy Identifier =2.23.140.1.2.2 (附注 13) 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		
	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）		
1.3.6.1.4.1.11129.2.4.2		证书签署时间戳 (signed certificate timestamp)		
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：*.eCert.gov.hk, *.subdomain.eCert.gov.hk。唯延伸认证电子证书（伺服器）不支援“通用版 " 功能。
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 3.1.1.3 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 1.2 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：*.eCert.gov.hk 及 eCert.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

13. 此栏位中添加了核证机关/浏览器论坛物件识别码, 用于标识根据核证机关/浏览器论坛基线要求发出的证书-组织标识声明。

2) 根源证书“Hongkong Post Root CA 3”之下的电子证书（伺服器）格式

以下为适用于由中继证书"Hongkong Post e-Cert SSL CA 3 - 17”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)		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 SSL CA 3 - 17 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） o=[登记人机构名称]（附注2） 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3）				
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 (OCSP)	[线上证书状态应答 URL]（附注 9）		
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)		数码签署，密码匙加密		
		（此栏为“关键”栏位）		

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 "
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 4） Policy Qualifier Id = CPS Qualifier : [核证作业准则的URL] Policy Identifier = 2.23.140.1.2.2（附注 11） 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5）	[主体名称内之伺服器名称] + [0 至 49] [额外伺服器名称]（附注6）
	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)		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7）		
1.3.6.1.4.1.11129.2.4.2		证书签署时间戳		

以下为适用于由中继证书”Hongkong Post e-Cert EV SSL CA 3 - 17”发出的延伸认证电子证书（伺服器）：-

栏位名称		栏位内容
標準欄 (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 (Issuer)		cn=Hongkong Post e-Cert EV SSL CA 3 - 17 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]

栏位名称		栏位内容
標準欄 (Standard fields)		
主体名称 (Subject name)		cn=[伺服器名称]（附注1） o=[登记人机构名称]（附注2） l=Hong Kong s=Hong kong c=HK Object Identifier （2.5.4.9） =[街道地址] Object Identifier （2.5.4.5） = [主体注册编号] Object Identifier （2.5.4.15） =[业务分类，例如"私人机构"/"政府实体"/"商业实体"/"非商贸实体"]（附注10） Object Identifier (1.3.6.1.4.1.311.60.2.1.3)=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3）		
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 (OCSP)	[线上证书状态应答 URL]（附注 9）
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)		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 4） Policy Qualifier Id = CPS Qualifier : [核证作业准则的URL] Policy Identifier = 2.23.140.1.1（附注 12） 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] + [0 至 49] [额外伺服器名称]（附注6）
	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)		伺服器验证 用户端验证

栏位名称		栏位内容
標準欄 (Standard fields)		
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）
1.3.6.1.4.1.11129.2.4.2		证书签署时间戳

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)）。除英文伺服器名称外，还支援 ISO / IEC 10646 中编码的中文伺服器名称字符。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：*.eCert.gov.hk, *.subdomain.eCert.gov.hk。
2. 电子证书（伺服器）以英文发行，机构名称为英文或中文。申请电子证书并在申请表格中提供其公司中文名称的机构，他们可决定是否在电子证书上显示中文公司名称。如机构未有提供此区分，则该公司的英文名称将显示在其电子证书内。对于只有中文公司名称的公司申请电子证书，或只提供中文公司名称的公司，其中文公司名称会显示在电子证书内（见本核证作业准则第 3.1.1.3 条）)。此外，机构分行/部门名称将以公司名称的相同语言显示。除非另有说明，否则所有标准延伸均设为“非关键”。
3. 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。
4. 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 1.2 条。
5. 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：*.eCert.gov.hk 及 eCert.gov.hk）。除英文伺服器名称外，还支援带有 ISO / IEC 10646 编码字符的中文伺服器名称。
6. 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。除英文伺服器名称外，还支援 ISO / IEC 10646 中编码的中文伺服器名称字符。
7. 对于由中继证书 "Hongkong Post e-Cert SSL CA 3 - 17" 所发出的证书，证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertSCA3-17CRL1.crl，此乃中继证书"Hongkong Post e-Cert SSL CA 3 - 17"所发出的「整体证书撤销清单」。
8. 对于由中继证书 "Hongkong Post e-Cert EV SSL CA 3 - 17" 所发出的证书，证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertESCA3-17CRL1.crl ，此乃中继证书"Hongkong Post e-Cert EV SSL CA 3 - 17"所发出的「整体证书撤销清单」。
9. 线上证书状态通讯规约应答伺服器的 URL 为 http://ocsp1.eCert.gov.hk
10. 本栏包含以下字串其中之一："私人机构"、"政府实体"、"商业实体"或"非商贸实体"，具体视乎登记人机构是否符合延伸认证 SSL 证书准则的相关条款。
11. 此栏位中添加了核证机关/浏览器论坛物件识别码, 用于标识根据核证机关/浏览器论坛基线要求发出的证书-组织标识声明。
12. 此栏位中添加了核证机关/浏览器论坛对延伸认证 SSL 证书准则的物件识别码， 用于标识证书。

附录 C - 香港邮政证书撤销清单(CRL) 及香港邮政授权撤销清单(ARL)

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"、"Hongkong Post e-Cert CA 1 - 15"、"Hongkong Post e-Cert SSL CA 3 - 17"及"Hongkong Post e-Cert EV SSL CA 3 - 17"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"及"Hongkong Post Root CA 3"所发出的授权撤销清单(ARL) 的更新及公布安排和其格式。

香港邮政每天三次更新及公布的证书撤销清单（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电子证书的资讯：

a) **「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"，"Hongkong Post e-Cert CA 1 - 15"及"Hongkong Post e-Cert SSL CA 3 - 17"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」：

   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)

   iv. 由中继证书"Hongkong Post e-Cert SSL CA 3 – 17"所发出的证书：
   http://crl1.eCert.gov.hk/crl/eCertSCA3-17CRL1.crl 或
   ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert SSL CA 3 - 17 CRL1, o=Hongkong Post, c=HK)

   v. 由中继证书"Hongkong Post e-Cert EV SSL CA 3 – 17"所发出的证书：
   http://crl1.eCert.gov.hk/crl/eCertESCA3-17CRL1.crl 或
   ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert EV SSL CA 3 - 17 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 points) 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。

香港邮政会更新及公布授权撤销清单，而清单内载有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：

i. 由根源证书"Hongkong Post Root CA 1"所发出的证书：
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)

ii. 由根源证书"Hongkong Post Root CA 3"所发出的证书：
http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 3, o=Hongkong Post, c=HK)

（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 3）				
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
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 3）			
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

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
	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 3）			
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。

(IV) 由根源证书"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 2）
标准延伸栏位 (Standard extension) （附注 3）			
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) 由中继证书"Hongkong Post e-Cert SSL CA 3-17"根据本准则发出的证书撤销清单格式:-

标准栏位 (Standard fields)	子栏位 (Sub-fields)	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 SSL CA 3 - 17, 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，证书撤销清单是每日更新及发出
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 3）			
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	cn=Hongkong Post Root CA 3 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]	此栏显示证书撤销清单的编号，该编号以顺序形式产生。

(VI) 由中继证书"Hongkong Post e-Cert EV SSL CA 3-17"根据本准则发出的证书撤销清单格式:-

标准栏位 (Standard fields)	子栏位 (Sub-fields)	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 EV SSL CA 3 - 17, 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，证书撤销清单是每日更新及发出

标准栏位 (Standard fields)	子栏位 (Sub-fields)	证书撤销清单栏位内容	备注
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 3）			
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 3 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]	此栏显示证书撤销清单的编号，该编号以顺序形式产生。

(VII) 由根源证书"Hongkong Post Root CA 3"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 3 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)		
	原因代码 (Reason code)	[撤销理由识别码]	（附注 2）
标准延伸栏位 (Standard extension) （附注 3）			
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	cn=Hongkong Post Root CA 3 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。

标准栏位 (Standard fields)	子栏位 (Sub-fields)	授权撤销清单栏位内容	备注
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）**	

附注

1. 有关电子证书（伺服器）及延伸认证电子证书（伺服器）的证书撤销清单，其证书撤销清单资料延伸栏位可包含以下撤销理由识别码：

   1 = 密码匙资料外泄， 3 = 联系变更， 4 = 证书被取代，
   5 = 终止营运， 9 = 特权被撤销

   否则，证书撤销清单资料延伸栏位不会包含撤销理由识别码。

2. 有关根源证书及中继证书的授权撤销清单，包括交叉证书，其证书撤销清单资料延伸栏位必须包含以下其中一个撤销理由识别码：

   0 = 没有注明， 1 = 密码匙资料外泄， 2 = 核证机关资料外泄，3 = 联系变更，
   4 = 证书被取代，5 = 终止营运

3. 除非另有说明，否则所有栏位均将设定为“非关键”。

附录 D - 香港邮政线上证书状态应答(OCSP Response)格式

本附录 D 详述有关香港邮政线上证书状态应答(OCSP Response)格式

通过发布一个包含以下主体名称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 CA 及中继证书进行线上证书状态通讯规约的签署。

根源证书：

证书主体名称 (CN)	**线上证书状态通讯规约签署人证书主体名称 (CN)**
"Hongkong Post Root CA 1"	"Hongkong Post Root CA 1 OCSP Responder"
"Hongkong Post Root CA 3"	"Hongkong Post Root CA 3 OCSP Responder"

中继证书：

证书主体名称 (CN)	**线上证书状态通讯规约签署人证书主体名称 (CN)**
"Hongkong Post e-Cert CA 1 - 15"	"Hongkong Post e-Cert CA 1 - 15 OCSP Responder"
"Hongkong Post e-Cert SSL CA 3 - 17"	"Hongkong Post e-Cert SSL CA 3 - 17 OCSP Responder"
"Hongkong Post e-Cert EV SSL CA 3 - 17"	"Hongkong Post e-Cert EV SSL CA 3 - 17 OCSP Responder"

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 D 的最后章节，还将提供线上证书状态应答的格式。

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 1，2））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).

标准栏位 (Standard Fields)	子栏位(Sub-fields)	子栏位(Sub-fields)	栏位内容	备注
		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. 有关电子证书（伺服器）及延伸认证电子证书（伺服器）的线上证书状态应答，其证书状态栏位可包含以下撤销理由识别码：

   0 = 没有注明， 1 = 密码匙资料外泄， 3 = 联系变更， 4 = 证书被取代，
   5 = 终止营运， 9 = 特权被撤销

2. 有关根源证书及中继证书的线上证书状态应答，包括交叉证书，其证书状态栏位必须包含以下其中一个撤销理由识别码：

   0 = 没有注明， 1 = 密码匙资料外泄， 2 = 核证机关资料外泄，3 = 联系变更，
   4 = 证书被取代，5 = 终止营运

附录 E - 香港邮政电子证书 – 服务摘要

1) 电子证书(伺服器) 及延伸认证电子证书（伺服器）

要点	电子证书（伺服器）	延伸认证电子证书（伺服器）
登记人	获香港特别行政区政府签发有效商业登记证之机构、获香港法例认可之本港法定团体及香港特别行政区政府政策局、部门或机关	
证书持有人	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	由登记人自行产生	
核对身分	核对网域名称(Domain Name)、机构及其获授权代表的身分	核对机构的合法存在、实体存在和营运存在、通信方法，核实域名身份及核实其获授权代表
证书用途	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 ▪ 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	▪ 登记人机构名称、街道地址及业务类别 ▪ 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
登记及行政费用	见本核证作业准则第 9.1 条	
证书有效期	一年	
	（见本核证作业准则第 4.6.1 及 6.3.2 条）	

附录 F - 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 G - 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 H - 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2016年1月1日起停止发出认可证书。
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2016年9月1日起停止发出认可证书。
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2019年7月1日起停止发出认可证书。
Hongkong Post Root CA 3	2017年8月12日至 2023年5月15日	此交叉证书由2017年8月12日起开始发出给根源证书 CA “Hongkong Post Root CA 3”。

根源证书名称	有效期	备注
Hongkong Post Root CA 3	2017 年 6 月 3 日至 2042 年 6 月 3 日	此根源证书由 2017 年 6 月 3 日起开始发出中继证书
Hongkong Post e-Cert SSL CA 3 - 17	2017 年 6 月 3 日至 2032 年 6 月 3 日	此中继证书由 2019 年 7 月 1 日起开始发出电子证书（伺服器）。
Hongkong Post e-Cert EV SSL CA 3 - 17	2017 年 6 月 3 日至 2032 年 6 月 3 日	此中继证书由 2022 年 1 月 21 日起开始发出延伸认证电子证书（伺服器）。

此为本核证作业守则之最终页