# 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
# 政府电子证书（个人）
# 政府电子证书（功能单位）

# “具安全电子邮件功能”

# 核证作业准则

日期：二零二六年十一月一日
物件识别码：1.3.6.1.4.1.16030.1.8.15

# 目录


前言 ..... 9
1. 引言 ..... 11
1.1 概述 ..... 11
1.2 文件名称及识别资料 ..... 11
1.3 公匙基建参与者 ..... 12
1.3.1 核证机关 ..... 12
1.3.2 核证登记机关 ..... 12
1.3.3 中央管理通讯系统 ..... 13
1.3.4 登记人 ..... 13
1.3.5 倚据证书人士 ..... 14
1.3.6 其他参与者 ..... 14
1.4 证书用途 ..... 15
1.4.1 证书的适用用途 ..... 15
1.4.2 证书的禁止用途 ..... 15
1.5 策略管理 ..... 15
1.5.1 管理本文件的机构 ..... 15
1.5.2 联络人 ..... 15
1.5.3 决定本核证作业准则是否符合证书政策的人员 ..... 16
1.5.4 核证作业准则的审批程序 ..... 16
1.6 定义和缩写 ..... 16
2. 公开资料及储存库责任 ..... 17
2.1 储存库 ..... 17
2.2 认证资料公布 ..... 17
2.3 公布时间或频率 ..... 17
2.4 储存库进入控制 ..... 17
3. 鉴别及认证 ..... 18
3.1 命名 ..... 18
3.1.1 名称类型 ..... 18
3.1.2 名称需有意义 ..... 18
3.1.3 登记人的匿名或假名 ..... 18
3.1.4 诠释名称规则 ..... 18
3.1.5 名称独特性 ..... 19
3.1.6 商标的认可、验证及角色 ..... 19
3.2 初始身分验证 ..... 19
3.2.1 证明拥有私人密码匙之方法 ..... 19
3.2.2 机构申请人身分认证 ..... 20
3.2.3 个人身分认证 ..... 20
3.2.4 没有验证的登记人资讯 ..... 20
3.2.5 权限及邮箱控制验证 ..... 20
3.2.6 互操作准则 ..... 20
3.3 密码匙更新请求的标识与鉴别 ..... 20
3.3.1 密码匙更新时的身分识别及身分认证 ..... 21
3.3.2 证书撤销后密码匙更新时的身分识别及身分认证 ..... 21
3.4 撤销请求的标识与鉴别 ..... 21

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 ..... 23
4.2.3 证书申请的处理期限 ..... 23
4.3. 证书签发 ..... 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 ..... 23
4.5 配对密码匙和证书的使用 ..... 23
4.5.1 登记人私人密码匙及证书用途 ..... 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 ..... 24
4.6.3 证书续期请求的处理 ..... 24
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 ..... 25
4.7.4 发出新证书时对登记人的通告 ..... 25
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 请求证书变更的实体 ..... 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 ..... 26
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 ..... 28

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 ..... 29
4.9.8 发布证书撤销清单的最大滞后时间 ..... 29
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 ..... 30
4.9.15 要求暂时吊销的程序 ..... 30
4.9.16 暂时吊销的期限限制 ..... 30
4.10 证书状态服务 ..... 30
4.10.1 操作特征 ..... 30
4.10.2 服务可用性 ..... 30
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及实施 ..... 31
4.12.2 工作阶段密码匙封装及复原政策与实施 ..... 31
5. 设施、管理和运作控制 ..... 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 每个角色的鉴别及认证 ..... 33
5.2.4 需要职责分割的角色 ..... 33
5.3 人员控制 ..... 33
5.3.1 资格、经验和无过失要求 ..... 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 ..... 36
5.5.3 存档保护 ..... 36
5.5.4 存档备份程序 ..... 36
5.5.5 电子邮戳的要求 ..... 36
5.5.6 存档收集系统（内部对外部） ..... 36
5.5.7 获取及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 ..... 37
5.7.1 事故和外泄处理程序 ..... 37
5.7.2 计算机资源、软件和 / 或数据的损坏 ..... 37
5.7.3 私人密码匙资料外泄之程序 ..... 37
5.7.4 灾难后的持续营运能力 ..... 37
5.8 核证机关或核证登记机关终止服务 ..... 38
6. 技术保安控制 ..... 39
6.1 密码匙之产生及安装 ..... 39
6.1.1 产生配对密码匙 ..... 39
6.1.2 私人密码匙交付予登记人 ..... 39
6.1.3 公开密码匙交付予证书发出人 ..... 39
6.1.4 核证机关公开密码匙交付予倚据人士 ..... 39
6.1.5 密码匙大小 ..... 39
6.1.6 公开密码匙参数的生成和品质检查 ..... 39
6.1.7 密码匙用途（按照 X.509 v3 密码匙使用方法栏位） ..... 39
6.2 私人密码匙保护和加密模组控制 ..... 40
6.2.1 加密模组的标准和控制 ..... 40
6.2.2 私人密码匙（m 选 n）多人式控制 ..... 40
6.2.3 私人密码匙托管 ..... 40
6.2.4 私人密码匙备存 ..... 40
6.2.5 私人密码匙存档 ..... 40
6.2.6 私人密码匙于密码模组之间传递 ..... 40
6.2.7 私人密码匙在加密模组的存储 ..... 40
6.2.8 启动私人密码匙的方法 ..... 40
6.2.9 解除私人密码匙启动状态的方法 ..... 40
6.2.10 销毁私人密码匙的方法 ..... 40
6.2.11 加密模组的评估 ..... 40
6.3 配对密码匙管理其他范畴 ..... 41

6.3.1 公开密码匙存档 ..... 41
6.3.2 证书操作期和配对密码匙使用期限 ..... 41
6.4 启动数据 ..... 41
6.4.1 启动数据的产生和安装 ..... 41
6.4.2 启动数据的保护 ..... 41
6.4.3 启动数据的其他范畴 ..... 41
6.5 电脑保安控制 ..... 41
6.5.1 特定电脑保安技术要求 ..... 41
6.5.2 电脑安全评估 ..... 41
6.6 生命周期技术控制 ..... 42
6.6.1 系统开发控制 ..... 42
6.6.2 保安管理控制 ..... 42
6.6.3 生命周期的保安控制 ..... 42
6.7 网络保安控制 ..... 42
6.8 电子邮戳 ..... 42
7. 证书、证书撤销清单及线上证书状态应答结构 ..... 43
7.1 证书结构 ..... 43
7.1.1 版本编号 ..... 43
7.1.2 证书延伸栏位 ..... 43
7.1.3 算式物件识别码 ..... 43
7.1.4 名称格式 ..... 43
7.1.5 名称限制 ..... 43
7.1.6 证书策略物件识别码 ..... 43
7.1.7 策略限制延伸栏位使用的政策 ..... 43
7.1.8 策略限定资格的语法和语义的政策 ..... 43
7.1.9 关键证书策略延伸栏位的语义处理 ..... 43
7.2 证书撤销清单结构 ..... 43
7.2.1 版本编号 ..... 46
7.2.2 证书撤销清单及证书撤销清单资料延伸栏位 ..... 46
7.3 线上证书状态应答结构 ..... 46
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. 认证机构审计和其他评估 ..... 48
8.1 评估的频率及情形 ..... 48
8.2 评估者的资格 ..... 48
8.3 评估者与被评估实体之间的关系 ..... 48
8.4 评估内容 ..... 48
8.5 对问题与不足采取的措施 ..... 48
8.6 评估结果的传达与发布 ..... 48
8.7 自我审核 ..... 48
9. 法律责任和其他业务条款 ..... 49
9.1 登记费用 ..... 49
9.1.1 证书发出或续期费用 ..... 49
9.1.2 证书查询费用 ..... 49
9.1.3 证书撤销或状态资讯的查询费用 ..... 49

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 业务信息机密 ..... 49
9.3.1 机密资料范围 ..... 50
9.3.2 不属于机密的资料 ..... 50
9.3.3 保护机密资料的责任 ..... 50
9.4 个人资料私隐 ..... 50
9.4.1 私隐方案 ..... 50
9.4.2 视作隐私的资料 ..... 50
9.4.3 不被视作私隐资料 ..... 50
9.4.4 保护私隐的责任 ..... 50
9.4.5 使用私隐资料的通告与同意 ..... 50
9.4.6 根据法律或行政程序作出的披露 ..... 51
9.4.7 其他资料披露情况 ..... 51
9.5 知识产权 ..... 51
9.6 陈述及担保 ..... 51
9.6.1 核证机关的陈述与担保 ..... 51
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 ..... 53
9.7 免责声明 ..... 54
9.8 有限责任 ..... 54
9.9 赔偿 ..... 56
9.10 有效期限与终止 ..... 57
9.10.1 有效期限 ..... 57
9.10.2 终止 ..... 57
9.10.3 终止与保留效力 ..... 57
9.11 参与人士的个别通告与通知 ..... 58
9.12 修订 ..... 58
9.12.1 修订程序 ..... 58
9.12.2 通知机制和期限 ..... 58
9.12.3 必须修改物件识别码的情形 ..... 58
9.13 争议处理 ..... 58
9.14 管辖法律 ..... 58
9.15 符合适用法律规定 ..... 59
9.15.1 司法管辖权 ..... 59
9.16 一般条款 ..... 59
9.16.1 完整协议 ..... 59
9.16.2 转让 ..... 59
9.16.3 分割性 ..... 59

9.16.4 执行（不可放弃权利） ..... 59
9.16.5 不可抗力 ..... 59
9.17 其他条款 ..... 59
9.17.1 非商品供应 ..... 59
附录 A - 词汇 ..... 61
附录 B - 香港邮政政府电子证书格式 ..... 65
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)格式 ..... 69
附录 D - 香港邮政政府电子证书 – 服务摘要 ..... 72
附录 E - 香港邮政政府电子证书登记人机构 / 核证登记机关名单及中央管理通讯系统（若有的话） ..... 73
附录 F - 香港邮政政府电子证书服务 - 翘晋电子商务有限公司之合约分判商名单（若有的话） 79
附录 G - 核证机关根源证书的有效期 ..... 80
附录 H - 香港邮政政府电子证书相对应之指定应用 ..... 81

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

# 前言

香港法例第 553 章《电子交易条例》（“条例”）列载公开密码匙基础建设（公匙基建）之法律架构。公匙基建利便电子交易作商业及其他用途。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。经公开密码匙保护的信息只可用其配对私人密码匙解密；而利用私人密码匙作数码签署的信息亦只可用其配对公开密码匙验证。

设计公匙基建之目的，为支援香港特别行政区内安全电子交易及通讯，包括以安全 / 多用途互联网邮件延伸功能（S/MIME）进行安全电子邮件通讯。

根据条例所载规定，香港邮政署长为认可核证机关。香港邮政署长透过香港邮政署职员履行核证机关之职能并提供服务。在本核证作业准则中，香港邮政署长称为**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。香港邮政已批出合约予翘晋电子商务有限公司（“合约”），以营运和维持香港邮政核证机关的系统和服务，合约期由 2023 年 7 月 1 日至 2026 年 6 月 30 日，并延长至 2027 年 6 月 30 日（包括当日）。凡提述由香港邮政执行的所有行为，均包括由翘晋电子商务有限公司代表香港邮政执行的所有该等行为。

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

香港邮政依然为条例第 34 条下之认可核证机关而承办商则为香港邮政根据数字政策专员在条例第 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安全电子邮件证书（即政府电子证书）均为条例下的认可证书，在本核证作业准则内称为“证书”或“政府电子证书”。

本核证作业准则列明适用于香港邮政所发出政府电子证书的作业方式及标准。本核证作业准则所规管的证书仅供安全电子邮件（S/MIME）用途，并按照核证机关 / 浏览器论坛（CA / Browser Forum） 的 S/MIME 基线要求（Baseline Requirements for S/MIME）发出。

根据条例，香港邮政可以采取任何适当措施，以履行核证机关职能及提供核证机关服务。而根据认可核证机关作业守则，香港邮政可以指定代理人或合约分判商执行其部分或全部业务。

香港邮政可适当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的特定职能。**附录 E** 列载核证登记机关之清单（若有的话）。

除因核证登记机关疏忽、欺诈、超越其获准权限范围行事或其他类似情况外，香港邮政须对核证登记机关作为其代理人履行香港邮政作为认可核证机关有关发出及撤销政府电子证书之职能或提供服务的行为及活动负责。

本核证作业准则列载政府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：证书政策及核证作业架构。

本核证作业准则之设计旨在符合下列规范最新版本的要求：
• 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 S/MIME 证书的基线要求（“基线要求”）；
• WebTrust 核证机关原则及准则；
• WebTrust 核证机关原则及准则－S/MIME。

# 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，本核证作业准则为一份结合证书政策（“证书政策”）及核证作业准则的文件，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及保障电子邮件通讯安全。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及安全电子邮件乃属适当及充分可信，以供其特定应用使用。

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政府电子证书（个人）及政府电子证书（机构单位），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。

本核证作业准则符合 RFC 3647 的格式要求。虽然本核证作业准则按照 RFC 3647 的结构载有若干章节标题，但有关主题未必适用于香港邮政提供的服务。有关章节会注明“不适用”。如有需要，额外资料会载于标准结构下的分节。符合 RFC 3647 的格式要求有助与其他第三方核证机关进行对照及互操作性，并让倚据人士预先了解香港邮政的作业方式及程序。

附录 D 载有根据本准则发出之电子证书特点摘要。

## 1.2 文件名称及识别资料

本文件为香港邮政核证机关就根据本核证作业准则发出的政府电子证书所制订的核证作业准则（“本准则”）。本文件自制订以来曾作出以下修订。

| 版本编号 | 修订说明 | 生效日期 |
|---|---|---|
| 1（.14） | 根据 RFC 3647 制订首个适用于发出政府电子证书（个人）/ 政府电子证书（机构单位），用以取代现有（OID 1.3.6.1.4.1.16030.1.8.13）的核证作业准则。 | 2026 年 10 月 1 日 |
| 2（.15） | 调整政府电子证书的最长有效期由两年缩短至一年以提升安全性与可靠性。 | 2026 年 11 月 1 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。**“1.3.6.1.4.1.16030.1.8.15”**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）。所有符合 S/MIME 基线要求（Baseline Requirements for S/MIME）的证书，均会载有以下额外识别码：

| **政府电子证书** | **政策物件识别码（OID）** |
|---|---|
| 政府电子证书（个人） | 2.23.140.1.5.3.3<br>（由核证机关 / 浏览器论坛（CA / Browser Forum）编配，适用于符合赞助机构验证严格证书政策（Sponsor-validated Strict Certificate Policy）的证书） |
| 政府电子证书（机构单位） | 2.23.140.1.5.2.3<br>（由核证机关 / 浏览器论坛（CA / Browser Forum）编配，适用于符合机构验证严格证书政策（Organization-validated Strict Certificate Policy） |

## 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（或透过其委任的分判商）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（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 核证登记机关

核证登记机关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。除因疏忽、超越授权范围行事、欺诈、刑事行为或

其他类似因素外，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）。

**附录 E** 载有香港邮政政府电子证书核证登记机关清单（若有的话）。

### 1.3.3 中央管理通讯系统

数字政策办公室辖下的中央管理通讯系统（以下简称“中央管理通讯系统”），是提供在**附录 H** 内的各项指定应用，供香港特别行政区政府各政策局 / 部门 / 办公室（“政策局 / 部门 / 办公室”）使用。中央管理通讯系统将采用由香港邮政核证机关签发 X.509 第三版本之新特别用途数码证书，以处理限阅资料。

香港邮政透过中央管理通讯系统指定的提出要求者角色来处理政府电子证书的申请人或登记人之事宜。在这方面，中央管理通讯系统是政府电子证书申请人和登记人的代理人。

同时，中央管理通讯系统的业务管理人员角色由政策局 / 部门 / 办公室指定来核实政府电子证书申请人的身份。在这方面，业务管理人员作为政府电子证书的核证登记机关（以下称为“核证登记机关”）。

所有其他功能和义务，包括中央管理通讯系统因证书生命周期管理及使用政府电子证书时而引致需要履行的功能，不论指定应用的性质如何，中央管理通讯系统作为其登记人的委托人或代理人（但不作为香港邮政承办商的分包商或香港邮政的代理人），其功能和义务均由中央管理通讯系统承担。

### 1.3.4 登记人

本准则下的登记人为**附录 E** 所列的政策局 / 部门 / 办公室。于本准则内，登记人亦可称为“申请人”、“登记人”、“登记人机构”或“政策局 / 部门 / 办公室”。政府电子证书的实际用户及与登记人相关的用户，分为以下两类。

#### 1.3.4.1 与登记人相关的用户类别

##### 1.3.4.1.1 政府电子证书（个人）

政府电子证书（个人）是应代表政策局 / 部门 / 办公室（即申请人及**附录 E** 所列的“登记人机构”）行事的提出要求者之要求，发给中央管理通讯系统用户；并识别已获该登记人机构授权使用该政府电子证书（个人）私人密码匙的中央管理通讯系统用户。登记人机构必须先与香港邮政作出安排，香港邮政才可以为登记人机构发出政府电子证书（个人）。

中央管理通讯系统用户包括：

a) 公务员及由政府直接聘用的合约雇员；
b) 代理 / 个体聘用合约雇员（包括 T 合约资讯科技人员）；
c) 根据上述（b）项以外的合约安排（例如外判合约）聘用的常驻人员。

根据本准则香港邮政仅发出证书予其证书申请已获批准并已以适当形式确认接受登记人协议之登记人机构。

持有此类证书（政府电子证书（个人））的中央管理通讯平台用户，可于中央管理通讯平台使用该证书作下列用途，惟有关电子讯息不得分类为机密电邮：

a) （作为发送人）利用证书附加密码签署，以对电子讯息作出数码签署；
b) （作为发送人）利用数码封印方式防止电子讯息遭受篡改；
c) （作为接收者）允许发送人使用接收者的公开密码匙加密电子讯息；
d) （作为接收者）当收到电子讯息时将其解密；及
e) （作为接收者）让登记人／登记人机构透过发送附有数码签署的确认讯息，以确认接收者的身分及确认收妥经加密的电子讯息。

政府电子证书（个人）只可由中央管理通讯系统用户用于**附录 H** 内列出对应其登记人机构之指定应用。

登记人机构向香港邮政承诺，除了按**附录H**内所指的指定应用作上述用途外，不会授权予中央管理通讯系统用户使用政府电子证书（个人）于任何其他用途。

#### 1.3.4.1.2 政府电子证书（功能单位）

政府电子证书（功能单位）是应代表政策局／部门／办公室（即申请人及**附录E**所列的“登记人机构”）行事的提出要求者之要求，发给中央管理通讯系统功能单位；并识别已获该登记人机构正式授权使用该政府电子证书（功能单位）私人密码匙的中央管理通讯系统功能单位。登记人机构必须先与香港邮政作出安排，香港邮政才可以为登记人机构发出政府电子证书（功能单位）。

政府电子证书（功能单位） 提供给政策局／部门／办公室之下的功能单位使用。

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确定接受登记人协议之登记人机构。

此类型证书仅限在中央管理通讯系统中使用：

a) 利用证书附加密码签署，以对电子讯息作出数码签署；
b) 利用数码封印方式防止电子讯息遭受篡改；
c) 对电子讯息作保密及解密；及
d) 让登记人／登记人机构透过发送附有数码签署的确认讯息，以确认接收者的身分（功能单位身分）及确认收妥经加密的电子讯息。

政府电子证书（功能单位）只可由中央管理通讯系统功能单位用于 附录 H 内列出对应其登记人机构之指定应用。

登记人机构向香港邮政承诺，除了按附录H内所指的指定应用作上述用途以外，不会授权予中央管理通讯系统功能单位使用政府电子证书（功能单位）于任何其他用途。

### 1.3.5 倚据证书人士

倚据人士乃倚据香港邮政发出之任何类别或种类证书，包括但不限于用作核实数码签署的政府电子证书。

### 1.3.6 其他参与者

只要分判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，批予分判商执行。若发生此类分判情况，除因疏忽、超出授权范围行事、欺诈、犯罪行为或其他类似因素导致的情况外，香港邮政仍须就本准则及登记人协议的履行承担责任，犹如未进行该等分判一样。

如上所述，翘晋电子商务有限公司及其分判商（统称为“承办商”）确实为香港邮政委任的分判商之一。

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。

**附录 F** 载有香港邮政政府电子证书服务 - 翘晋电子商务有限公司之合约分判商名单。

## 1.4 证书用途

### 1.4.1 证书的适用用途

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。

根据本准则发出的证书只可用于安全电子邮件通讯用途，包括对电子邮件作出数码签署及加密。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 证书的禁止用途

根据本准则发出的证书不得用于安全电子邮件通讯以外的用途，包括但不限于传输层保安（TLS）认证、程式码签署或非电子邮件文件签署。

## 1.5 策略管理

### 1.5.1 管理本文件的机构

本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、撤销及公布证书时采用之做法及标准。

### 1.5.2 联络人

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 决定本核证作业准则是否符合证书政策的人员

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 核证作业准则的审批程序

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

本准则所使用的定义及缩写载于**附录 A**。

# 2. 公开资料及储存库责任

## 2.1 储存库

根据条例之规定，香港邮政维持一可供公众查阅的储存库，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、证书撤销清单（CRLs），香港邮政公开密码匙、本准则文本一份以及与本准则证书有关之其他资料。香港邮政会尽快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。

储存库内的资料（包括任何个人资料）乃根据条例发布，以便利进行合法电子通讯。

## 2.2 认证资料公布

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等其他相关情况时，储存库会尽快作出更新。

除不时作出的其他修订外，香港邮政最少每 365 日检讨及更新本准则，并作出适当修订，以确保香港邮政的运作保持准确、透明及符合本文件*“引言”*部分所列的外部要求。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

本节说明根据本准则发出的政府电子证书（个人）及政府电子证书（功能单位）的申请人及登记人所适用的身分识别、身分认证及邮箱验证要求。

## 3.1 命名

根据本准则发出的电子证书会按照**附录 B** 所订明的命名规则及证书结构，利用主体名称识别登记人。

### 3.1.1 名称类型

#### 3.1.1.1 政府电子证书（个人）

透过证书上的主体名称（于**附录 B** 内指明），可识别政府电子证书（个人）登记人之身分，该名称由以下资料组成：

a) 中央管理通讯系统用户所控制邮箱的电邮地址（载于主体别名（Subject Alternative Name）延伸栏位）；
b) 中央管理通讯系统用户于其身份证明文件上显示的姓名；及
c) 登记人机构在获香港法例认可之有关香港政府部门之登记名称；如登记人机构为香港特别行政区政府政策局、部门或办公室，则为该政策局、部门或办公室之正式名称。

#### 3.1.1.2 政府电子证书（功能单位）

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

a) 中央管理通讯系统用户所控制邮箱的电邮地址（载于主体别名（Subject Alternative Name）延伸栏位）；
b) 登记人机构在获香港法例认可之有关香港政府部门之登记名称；如登记人机构为香港特别行政区政府政策局、部门或办公室，则为该政策局、部门或办公室之正式名称。

#### 3.1.1.3 中央管理通讯系统之提出要求者、业务管理人员、决策局 / 部门 / 办公室管理人员

决策局 / 部门 / 办公室指定的提出要求者、业务管理人员及决策局 / 部门 / 办公室管理人员虽替登记人机构于中央管理通讯系统办理政府电子证书之申请手续，然而政府电子证书并不会辨识此人员身分。

### 3.1.2 名称需有意义

根据本准则发出证书所采用主体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 登记人的匿名或假名

根据本准则香港邮政不会发出匿名或假名证书。

### 3.1.4 诠释名称规则

电子证书会载入之登记人名称（主体名称）类型见第 3.1.1 条。有关证书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。

### 3.1.6 商标的认可、验证及角色

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、网域名称、商用名称、公司名称或知识产权。

香港邮政可酌情处理任何有关商标权、服务商标、网域名称、商用名称、公司名称或任何其他知识产权拥争议之事宜并享有最终决定权。

## 3.2 初始身分验证

业务管理人员角色可以进一步根据本作业准则第 1.3.4.1 条中提到的不同人员类别再作定义，以处理不同的验证要求：

| 人员类别 | 说明 |
|---|---|
| 公务员及由政府直接聘用的合约雇员 | 须由具有业务管理人员角色的中央管理通讯系统用户为这类人员执行“认证”步骤。该用户负责核对证书持有人的证明文件*，与政府保存的人事记录是否一致。 |
| 代理／个体聘用合约雇员（包括 T 合约资讯科技人员） | 须由具有业务管理人员角色的中央管理通讯系统用户为这类人员执行“认证”步骤。该用户负责核对证书持有人的证明文件*，与代理保存的聘用记录或决策局／部门／办公室保存的个体聘用合约记录及相关文件是否一致。 |
| 合约安排聘用的常驻人员 | 须由具有业务管理人员角色的中央管理通讯系统用户为这类人员执行“认证”步骤。该用户负责核对证书持有人的证明文件*，与用于决策局／部门／办公室跟外判商订立业务关系的合约、协议、单据或其他种类之法律文件内保存之可以证明证书持有人身份之记录是否一致。 |

*证明文件可以是香港身份证，护照或决策局／部门／办公室用于认证身份的其他文件。

如有疑问，香港邮政可拒绝接受该政府电子证书申请。

### 3.2.1 证明拥有私人密码匙之方法

中央管理通讯系统在其处所内的稳当的系统及环境下使用硬件安全模块（HSM）为登记人提供制作密码匙服务，以确保私人密码匙不被篡改，及产生并传送含公开密码匙的「签发证书要求」（CSR）至香港邮政。香港邮政会在其处所内产生证书。包含了申请人公开密码匙的证书在发出后会以安全的方式发送给申请人。

### 3.2.2 机构申请人身分认证

登记人机构为香港特别行政区政府的政策局、部门或办公室，其身分乃透过其作为政府认可机构的地位及参与中央管理通讯平台而获确认。

政府电子证书的申请由登记人机构指定的获授权角色透过中央管理通讯平台递交。中央管理通讯平台的使用及获授权角色的委任，以证明登记人机构的身分及权限。

香港邮政采用以下登记方案：

a) GOVHK：适用于政府实体。

### 3.2.3 个人身分认证

就政府电子证书（个人）而言，中央管理通讯平台倚赖相关登记人机构先行核实个别人士的身分，以及于中央管理通讯平台内委派获授权用户角色。

中央管理通讯平台用户帐户的使用及角色委派，以证明与政府电子证书（个人）相关联的人士已通过登记人机构的身分认证。（BR 第 3.2.4.1（6） 节）

### 3.2.4 没有验证的登记人资讯

香港邮政会按照 S/MIME 基线要求（Baseline Requirements for S/MIME）核实主体栏位及主体别名延伸栏位中的邮箱栏位（Mailbox Field）。未按照 S/MIME 基线要求（Baseline Requirements for S/MIME）核实的申请人资料，不得载于政府电子证书内。

### 3.2.5 权限及邮箱控制验证

在初始身分验证过程中，香港邮政会采用以下验证方法，确认与政府电子证书相关的邮箱地址的权限或控制权。：

a） 透过网域验证邮箱权限（S/MIME BR 第 3.2.2.1 条）
香港邮政可透过验证邮箱地址中网域部分的控制权，确认申请人或登记人机构已获授权代表有关邮箱持有人行事。如采用网域验证方式，香港邮政只会使用核证机关 / 浏览器论坛《TLS 伺服器证书基线要求》第 3.2.2.4.12 条所订明的认可网域验证方法。

就邮箱授权或控制权的验证而言，任何重复使用的资料、文件或已完成的验证，均须于发出政府电子证书前不超过 30 日内取得或完成。

### 3.2.6 互操作准则

香港邮政根据本准则而发出的政府电子证书，在所有情况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 密码匙更新请求的标识与鉴别

香港邮政支援在证书有效期届满前为现有证书进行密码匙更新，以作以下两种用途：

i） 更换证书：即申请后部分（或全部没有）主体资料有所更改，而登记人可选择（或不选择）更改与新证书相关连的密码匙；

ii） 证书续期：即登记人希望延长现有证书的有效期，并可同时更改与该证书相关连的密码匙。

在上述两种情况下，均须按照第 4.2.1 条的规定重新进行身分识别及身分认证。

### 3.3.1 密码匙更新时的身分识别及身分认证

香港邮政不支援应登记人要求为更换证书而进行例行密码匙更新。证书的密码匙更新通常会作为证书续期程序的一部分进行，或由香港邮政酌情决定作为证书更换程序的一部分进行。

### 3.3.2 证书撤销后密码匙更新时的身分识别及身分认证

香港邮政不容许对已届满有效期或已撤销的证书进行密码匙更新。

透过提出要求者行事的登记人，必须按照第 3.2 条所述重新办理首次登记程序。

## 3.4 撤销请求的标识与鉴别

香港邮政接到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可由中央管理通讯平台透过采用 TLS 协定的专用及安全网络连线向香港邮政核证机关提交载有证书撤销资料的系统介面档案作出。

# 4. 证书生命周期操作要求

## 4.1 证书申请

所有首次申请，以及在政府电子证书被撤销或有效期届满后申请新的政府电子证书，申请人均须透过中央管理通讯平台递交申请。中央管理通讯平台会完成申请程序并将申请传送至香港邮政。

### 4.1.1 谁能递交证书申请

就政府电子证书（个人）及政府电子证书（功能单位）而言，申请须由提出要求者透过中央管理通讯平台代表申请人递交。

### 4.1.2 登记过程与责任

政府电子证书申请人必须完成登记程序，包括：

a) 申请人透过中央管理通讯平台以电子方式提交政府电子证书申请，即授权香港邮政向任何人士或在香港邮政储存库公布其政府电子证书，并接受香港邮政向其发出政府电子证书。；
b) 缴交所需费用；
c) 产生私人密码匙及公开密码匙。

申请人透过中央管理通讯平台以电子方式提交政府电子证书申请，即授权香港邮政向任何人士或在香港邮政储存库公布其政府电子证书，并接受香港邮政向其发出政府电子证书。

## 4.2 处理证书申请

### 4.2.1 履行鉴别及认证职能

用以证明申请人身分的文件，于本准则第 3.2 条说明。电子证书密码信封将于获授权代表在指定香港邮政处所递交申请时当面接收，或于完成身分认证程序后，以安全方式交付予获授权代表，例如挂号邮件。

同时，香港邮政在发出政府电子证书前，会按照 RFC 9495 检索及处理核证机关授权纪录（Certification Authority Authorisation Record）（「CAA 纪录」）。若 CAA 纪录存在，但记录并未将香港邮政之域名「eCert.gov.hk」或「hongkongpost.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。若拟载于证书内的域名并没有 CAA 纪录，则香港邮政认为申请人允许香港邮政为该域名签发证书。

### 邮箱授权验证

完成第 3.2 条所述的身分认证、权限及邮箱控制验证后，香港邮政会按照本核证作业准则所订明的程序处理证书申请。

### 核实证书资料

申请人可浏览证书档案或经香港邮政储存库核实证书资料。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。

## 公布政府电子证书

根据《电子交易条例》的规定，香港邮政会尽快在储存库公布已获接受并已发出的政府电子证书（见第 2 条）。申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

### 4.2.2 证书申请批准和拒绝

完成身分认证程序后，香港邮政有义务通知申请人其申请获接纳或被拒绝。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，且无须对因拒绝而产生的任何损失或费用承担任何责任。

### 4.2.3 证书申请的处理期限

不适用。

## 4.3. 证书签发

4.3.1 在核对身分手续后，中央管理通讯系统会在其处所内之稳当系统及环境下以硬件安全模块（HSM）为登记人提供代制密码匙服务，以保证私人密码匙不受干扰，并生产及传送包含公开密码匙的签发证书要求（CSR）至香港邮政。香港邮政会在其处所内的稳当系统及环境下，产生各中央管理通讯系统用户／中央管理通讯系统功能单位的政府电子证书（包含公开密码匙）。

4.3.2 政府电子证书会以电子方式交付予中央管理通讯系统用户／中央管理通讯系统功能单位。

4.3.3 中央管理通讯系统同意，一旦接获政府电子证书，即须完全为私人密码匙的安全保管负责，并同意将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。

4.3.4 所有存于中央管理通讯系统处所内之稳当系统及环境下的硬件安全模块（HSM）内的私人密码匙均经加密。中央管理通讯系统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。

## 4.4 证书接受

### 4.4.1 构成接受证书的行为

申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，申请人应立即通知香港邮政。

### 4.4.2 核证机关对证书的发布

所有已获接受并发出的政府电子证书均会根据《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

不适用。

## 4.5 配对密码匙和证书的使用

### 4.5.1 登记人私人密码匙及证书用途

登记人必须按照本核证作业准则及核证机关 / 浏览器论坛（CA / Browser Forum）S/MIME 基线要求（Baseline Requirements for S/MIME），仅将政府电子证书及相应的私人密码匙用于安全电子邮件（S/MIME）用途。

登记人机构负责：

a) 承认会履行义务，使用合理预防措施来保护其政府电子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) 发现其政府电子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) 用于身份鉴别的政府电子证书，其私人密码匙只可以在证书有效期内使用。
d) 获授权使用者已获登记人机构授权，并实际按照本核证作业准则，仅将证书及相关私人密码匙用于安全电子邮件用途；
e) 此等证书只可用以按照核证机关 / 浏览器论坛（CA / Browser Forum）S/MIME 基线要求（Baseline Requirements for S/MIME），仅用于安全电子邮件通讯，包括电子邮件的加密及解密，以及电子邮件的数码签署（如适用）；
f) 不会试图使用政府电子证书的私人密码匙用于本核证作业准则所允许的安全电子邮件通讯以外的任何用途；及
g) 获授权使用者采取合理预防措施以维护私人密码匙之安全。

### 4.5.2 倚据人士公开密码匙和证书的使用

倚据政府电子证书的人士须负责：

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。
c) 于倚据证书前查核证书撤销清单上之证书状态。
d) 执行所有适当证书路径认可程序。
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

电子证书可于证书有效期届满前续期，但须符合本核证作业准则的规定。

### 4.6.2 谁能要求证书续期

登记人机构的提出要求者须透过中央管理通讯系统以电子方式递交证书续期申请，及缴付续期费用。若香港邮政接收到续期申请，即会根据第 3.2.3 条所述“个人身分认证“之过程进行认证，如同收到新申请一样。

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，方可透过中央管理通讯系统递交续期要求。

### 4.6.3 证书续期请求的处理

#### 4.6.3.1 政府电子证书续期

根据本核证作业准则发出或续期的证书，其有效期不得超过核证机关／浏览器论坛（CA / Browser Forum）S/MIME 基线要求（Baseline Requirements for S/MIME）所容许的最长有效期。

4.6.3.1.1　中央管理通讯平台会于证书的有效期即将届满前，向政府电子证书登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或已撤销的证书续期。

政府电子证书（个人）的证书有效期为一年。政策局／部门／办公室可根据业务需要为证书持有人选择证书的有效期。

政府电子证书（功能单位）的证书有效期为一年。政策局／部门／办公室可根据业务需要为证书持有人选择证书的有效期。

证书续期以后，中央管理通讯平台会透过其中央密码匙产生服务为登记人产生新的配对密码匙。证书续期以后，只要登记人协议原有之条款及条件与续期当日有效的核证作业准则条款并无抵触，则原订的条文仍适用于新续期的证书。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。

### 4.6.4　发出新证书时对登记人的通告

向登记人发出关于证书续期的通知与本准则第 4.3.2 条中所述有关新政府电子证书的方法相同。

### 4.6.5　构成接受续期证书的行为

登记人构成接受续期政府电子证书的行为，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

香港邮政发布续期政府电子证书的方式，与本准则第 4.4.2 条中所描述的方法相同。

### 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。然而，香港邮政不会自动为政府电子证书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

证书密码匙更新要求的处理程序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 条中所述的方式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 条中所列的相同。

### 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 条中所述的方法相同。

### 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政府电子证书。

### 4.8.1 证书变更的情形
不适用。

### 4.8.2 请求证书变更的实体
不适用。

### 4.8.3 证书变更请求的处理
不适用。

### 4.8.4 发出新证书时对登记人的通告
不适用。

### 4.8.5 构成接受变更证书的行为
不适用。

### 4.8.6 核证机关对变更证书的发布
不适用。

### 4.8.7 核证机关对其他实体的通告
不适用。

## 4.9 证书撤销和暂时吊销
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。暂时吊销证书并不适用。

### 4.9.1 证书撤销的情形

4.9.1.1 若香港邮政私人密码匙资料外泄，会导致香港邮政迅速地撤销所有经由该私人密码匙发出的证书。在私人密码匙资料外泄的情况下，香港邮政会根据在密码匙资料外泄计划内定明的程序迅速地撤销所有已发出的登记人证书（见第 5.7.3 条）。

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

4.9.1.3 登记人之私人密码匙或内载与某电子证书公开密码匙相关私人密码匙之储存媒体，**若已外泄或怀疑已外泄，或电子证书上由登记人提供之资料有任何改变，或相关政府电子证书所对应的中央管理通讯平台用户角色有所改变或失效**，各登记人**必须立即**按照本准则的撤销程序，向其政策局 / 部门 / 办公室申请撤销证书。

4.9.1.4 不论何时，若有以下情况，香港邮政均可按准则中程序撤销证书，并会以电子邮件（证书撤销通知书（如有电子邮件地址））及透过更新证书撤销清单的方式通知登记人：

a) 知道或有理由怀疑登记人之私人密码匙已外泄；
b) 知道或有理由怀疑证书之细节不真实或已变得不真实或证书不可靠；
c) 认为证书并非根据准则妥当发出；
d) 认为登记人未有履行本准则或登记人协议列明之责任；
e) 证书适用之规例或法例有此规定；
f) 认为登记人未曾缴付登记费；
g) 知道或有理由相信在政府电子证书上指明之中央管理通讯平台用户已非登记人机构之中央管理通讯平台用户；或
h） 知道或有理由相信在政府电子证书上指明之中央管理通讯平台用户已不再拥有其于登记人机构内之角色。

4.9.1.5 香港邮政会于下列任何事件发生后 24 小时内撤销政府电子证书：

1) 香港邮政收到登记人以书面提出撤销政府电子证书要求当日后的下一个工作日；
2) 香港邮政收到登记人通知，表示原来的证书申请未经授权，且登记人不会追溯给予有关授权当日后的下一个工作日；
3) 香港邮政取得证据，证明与政府电子证书内公开密码匙相对应的登记人私人密码匙已遭外泄；
4) 香港邮政认为已经证明或证实有方法，可借着政府电子证书中的公开密码匙轻易计算出登记人的私人密码匙（例如 Debian weak key，请参阅 https://wiki.debian.org/SSLkeys）；
5) 香港邮政取得证据，证明政府电子证书内任何邮箱地址的网域授权或邮箱控制验证结果不应被信赖。

4.9.1.6 香港邮政可于下列任何事件发生后 24 小时内撤销政府电子证书，并且在任何情况下最迟会于 5 日内撤销政府电子证书：

1) 政府电子证书不再符合 S/MIME 基线要求（Baseline Requirements for S/MIME）第 6.1.5 及第 6.1.6 条的规定；
2) 香港邮政取得证据，显示政府电子证书被不正当使用；
3) 香港邮政得悉登记人违反登记人协议中一项或多项条款列明之责任；
4) 香港邮政得悉有任何情况显示政府电子证书内使用的电邮地址或完整网域名称（Fully-Qualified Domain Name）已不再获合法允许使用（例如法院或仲裁机构已撤销使用有关电邮地址或网域名称的权利、登记人所订立的相关牌照或服务协议已终止，或帐户持有人未能维持该电邮地址或网域名称的有效状态）；

5) 香港邮政得悉政府电子证书所载资料有重大变更；
6) 香港邮政得悉政府电子证书并非按照 S/MIME 基线要求（Baseline Requirements for S/MIME）或香港邮政证书政策及／或核证作业准则发出；
7) 香港邮政确定或得悉政府电子证书所载任何资料并不准确；
8) 香港邮政根据 S/MIME 基线要求（Baseline Requirements for S/MIME）发出政府电子证书的权利已届满、被撤销或终止，除非香港邮政已作出安排继续维持证书撤销清单或线上证书状态通讯规约储存库；
9) 香港邮政证书政策及／或核证作业准则规定必须撤销证书；或
10) 香港邮政得悉存在已被证实或已获证明的方法，会导致登记人的私人密码匙遭受外泄，或有明确证据显示用以产生该私人密码匙的特定方法存在缺陷。

4.9.1.7 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。

### 4.9.2 谁能要求证书撤销

提出要求者须登录中央管理通讯系统，在中央管理通讯系统中为政府电子证书（个人）申请人或政府电子证书（功能单位）的功能单位完成并递交撤销证书要求。

业务管理人员须登录中央管理通讯系统，并于决策局／部门／办公室设定的预定工作日内批准该要求。

### 4.9.3 撤销请求的程序

中央管理通讯系统可提供应用程式接口（API），透过专用和安全连接网络从政策局／部门／办公室系统接收撤销证书要求，其要求包括了提出要求者和业务管理人员处理撤销证书申请的工作流程资料。中央管理通讯系统须对撤销证书要求进行验证，并按照中央管理通讯系统记录对提出要求者和业务管理人员的工作流程进行权限查核。

中央管理通讯系统须预备一份系统界面档案，该档案包含了撤销证书资料，并透过专用和安全连接网络以 TLS 规约递交给香港邮政核证机关。

香港邮政核证机关会撤销证书，该证书撤销后即会永久失效。所有已撤销的证书之有关资料将刊载于证书撤销清单内。香港邮政核证机关将按照时间表公布证书撤销清单。

中央管理通讯系统会透过专用且安全的网络以 TLS 规约从香港邮政核证机关接收包含撤销证书结果的系统界面档案。因此，中央管理通讯系统须停止使用该政府电子证书，并通知所有涉及撤销请求的中央管理通讯系统用户。

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）。

### 4.9.4 撤销请求宽限期

撤销要求宽限期（“宽限期”）指登记人必须在其进行撤销要求的期间。登记人之私人密码匙或内载与某政府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，或政府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。

### 4.9.5 核证机关处理撤销请求的时限

香港邮政将尽合理努力，确保于以下日期的下一个工作日起计 24 小时内，把撤销资料刊载于证书撤销清单：（1）收到登记人的撤销证书要求或撤销证书的最终确认；或（2）在未有收到该等要求的情况下，香港邮政决定撤销证书之日。然而，香港邮政不会于每次撤销证书后立即更新及公布供公众查阅的证书撤销清单。只有在下一次证书撤销清单更新及公布时，证书的已撤销状态才会反映于证书撤销清单内。证书撤销清单每日公布三次，并最少保存七年。

香港邮政会尽合理努力，在撤销证书后 24 小时内，透过更新证书撤销清单的方式及电子邮件（如有电子邮件地址）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

倚据人士在倚据本证书前，有负责于倚据证书前查核证书撤销清单上之证书状态。

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

当电子证书被撤销时，香港邮政会适时发布有关信息（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（CRL）及香港邮政授权撤销清单（ARL）会按照附录 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站 http://www.eCert.gov.hk 发布。

### 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。一般而言，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
香港邮政现时不会就按照本准则发出的电子证书提供线上证书状态应答（OCSP）服务。

### 4.9.10 线上撤销查询规定
倚据人士必须在倚据证书之前，按照第 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
不适用。

### 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（包括但不限于倚据人士及应用程式软件供应商），可以透过香港邮政核证机关网站的密码匙外泄报告网站递交证据，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，将尽商业上合理的努力通知登记人，并在发现该等撤销原因后或按照本准则第 7.2(a)条之要求将证书撤销清单内的撤销原因代码更新为“密码匙外泄”。

透过密码匙外泄报告网站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
政府电子证书不设暂时吊销安排。

### 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，包括表明撤销证书的原因代码将刊载于证书撤销清单内（见第 7.2 条）。

### 4.10.2 服务可用性
证书状态服务 24x7 保持开放。

### 4.10.3 运作特点
不适用。

## 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） 证书登记使用期满，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及实施
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 工作阶段密码匙封装及复原政策与实施
不适用。

# 5. 设施、管理和运作控制

## 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 每个角色的鉴别及认证

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 需要职责分割的角色

香港邮政已为所有涉及香港邮政政府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、经验和无过失要求

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、承办商及核证登记机关须尽合理努力确保其所有人员（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、承办商及核证登记机关须尽合理努力，为其人员提供适当及充足的培训（担任核心职位的人员每年至少接受一次培训），以确保其有能力履行职责，以及有效推行及遵守保安政策。

### 5.3.5 工作岗位轮换周期和顺序
不适用。

### 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
获被委派执行受信职务的承办商人员应遵守第 5.3 条就该等职务所订明的职责及要求，并受上文第 5.3.6 条处罚所约束。

### 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、承办商及核证登记机关之间传送的所有文件及资料，均须按照香港邮政不时订明的规程，以受控及安全的方式交付。

## 5.4 审计日志程序

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

核证机关证书及密码匙生命周期事件，包括：

- 密码匙的生成、备份、储存、复原、存档及销毁；
- 证书的申请、续期、密码匙更新要求及撤销；
- 批准及拒绝证书申请；
- 加密硬件装置生命周期管理事件；
- 产生证书撤销清单；及
- 推出新的证书结构及停用现有证书结构。

登记人证书生命周期管理事件，包括：

- 证书的申请、续期、密码匙更新要求及撤销；
- 本准则规定的所有验证行为；
- 批准及拒绝证书申请；
- 证书签发；及

- 产生证书撤销清单。

保安事件，包括：

- 成功及不成功的公匙基建系统存取尝试；
- 已执行的公匙基建及保安系统操作；
- 保安设定档变更；
- 在证书系统上安装、更新及移除软件；
- 系统崩溃、硬件故障及其他异常情况；
- 防火墙及路由器的活动；及
- 进出核证机关设施。

日志记录必须包括下列资料：

a） 事件发生的日期及时间；
b） 作出日志记录的人员身分；及
c） 事件描述。

### 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：

a) 系统设备结构档案
b) 评估结果及／或设备合格覆检（如曾进行）
c) 核证作业准则及其修订本或最新版本
d) 对香港邮政具约束力而构成合约之协议
e) 所有发出或公布之证书及证书撤销清单
f) 定期事件纪录
g) 其他需用以核实存档内容之数据
h) 证书系统建设和升级文档；
i) 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；
j) 审计记录；
k) 员工资料，包括但不限于背景调查、录用、培训等资料；
l) 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第 5.5.1 条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 电子邮戳的要求

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在内部收集。

### 5.5.7 获取及验证存档资料的程序

有关获取及验证存档资料的程序详情载于第 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政府电子证书有效期为不超过二十五年（见**附录 G**）。香港邮政核证机关密码匙及证书在期满前至少三个月会进行续期。续发新根源密码匙后，相应之根源证书会在香港邮政网站 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 事故和外泄处理程序

香港邮政备有事故处理程序，以指引人员应对保安事故、自然灾害及其他可能导致系统受损的类似事件。为维持证书服务的完整性，香港邮政制定、记录及定期测试适当的应变及灾难复原计划和程序。

香港邮政备有全面而可行的大规模撤销事件应变计划，并每年对计划进行测试，以及将测试中获得的经验纳入计划，以不断改进应对能力。

### 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政府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数字政策专员并作出公布。倘若在计算机资源、软件和／或数据损坏的情况下，中央管理通讯平台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。

如根据本准则签发政府电子证书的香港邮政私人密码匙资料外泄，香港邮政会即时知会数字政策专员并作出公布。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政府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数字政策专员并作出公布。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，必须经过数字政策专员确定后才可以进行。

### 5.7.4 灾难后的持续营运能力

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数字政策专员，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 核证机关或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”所定程序知会数字政策专员并作出公布。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

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。

就根源证书及中继证书配对密码匙，香港邮政会：

a) 准备并采用密码匙产生程序；
b) 由合资格的审计人员见证核证机关配对密码匙之产生过程，或录制整个核证机关配对密码匙之产生过程；及
c) 由合资格的审计人员提交报告，报告发表意见认为香港邮政在其根源密码匙和电子证书生成过程中已采用密码匙产生程序及用于确保配对密码匙完整性和机密性的控制措施。

### 6.1.2 私人密码匙交付予登记人

中央管理通讯平台会代表申请人 / 登记人按照代制密码匙的要求产生政府电子证书的配对密码匙。

### 6.1.3 公开密码匙交付予证书发出人

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站 http://www.eCert.gov.hk 取得。香港邮政采取保护措施，以防该等密码匙被人更改。

### 6.1.4 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站 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 4096 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）

政府电子证书之密码匙只可用于加密电子通讯及列于第 1.3.4.1 条的其他用途。如电子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，政府电子证书的数码签署只可用于提供身分认证、资料完整性及不可否认性。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
所有私人密码匙不会存档。

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

### 6.2.7 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 解除私人密码匙启动状态的方法
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
香港邮政核证机关根源密码匙使用期不超过 25 年（另见第 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，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。

香港邮政核证机关根源密码匙使用期不超过 25 年（另见第 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，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 证书操作期和配对密码匙使用期限
香港邮政核证机关根源密码匙使用期不超过 25 年（另见第 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，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。

证书的有效期由发出自香港邮政系统当日起即日生效。

根据本核证作业准则在登记使用期内而发出之证书有效期可不同于上述之有效期（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 启动数据的其他范畴
不适用。

## 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构软件和存储数据文件的系统是安全、可信赖的系统，不会受到未经授权的内部和外部访问。此等保安控制措施接受第 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，清除所有可能载有与政府电子证书服务保安有关资料的储存内容，并加以确认。

### 6.5.2 电脑安全评估
不适用。

## 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构人员或在特殊情况下由其它机构进行开发工作，均能使用一致和有效的内部标准；
b) 将生产及开发的环境分隔开的有效程序；
c) 将操作、运维、开发人员的职责得以区分的有效程序；
d) 对用于生产及开发的环境内的资料及系统进行有效访问的控制措施；
e) 对变更控制程序（包括但不限于系统和数据的正常和紧急变更）的有效控制措施（包括但不限于版本的控制、严格的测试验证等）；
f) 系统上线前进行安全性的检查和评估的程序，检查和评估内容包括有否安全漏洞和被入侵的危险等；
g) 对采购设备及服务进行妥善管理的有效程序；
h) 硬件密码匙设备的生命周期（从设备开始运作到逻辑 / 物理销毁）过程中，对该设备的访问至少有 3 名可信人员共同参与。

### 6.6.2 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件变更的控制。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

不适用。

## 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构网络环境的安全，适时更新版本，定期针对网络环境进行风险评估和审计，以检测有否被入侵的危险，其配置只允许已获授权使用本准则所载核证机关服务者接达，尽可能降低来自网络的风险。

香港邮政至少每季进行一次漏洞扫描，并至少每年进行一次渗透测试。所有已识别的漏洞会被即时修复，通常在保安修补程式发布后一个月内完成。香港邮政会进行风险评估，以决定适当的漏洞缓解策略及时间表，并妥善记录评估结果。如未能于一个月内完成修复，香港邮政会评估相关风险，并制订及执行有记录的缓解计划。

## 6.8 电子邮戳

香港邮政使用网络时间协定（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 D** 载有政府电子证书之特点摘要。

香港邮政核证机关系统会透过密码学安全伪乱数生成器（CSPRNG）产生包含至少 64 位元并且大于零（0）的非连续电子证书序号。

### 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政府电子证书的资讯。

当政府电子证书因下列其中一项原因被撤销时，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**<br>**（RFC 5280 中指明的证书撤销清单原因（CRLReason））** |
|---|---|
| 密码匙资料外泄 | 1 = 密码匙资料外泄（keyCompromise） |
| 特权被撤销 | 9 = 特权被撤销（privilegeWithdrawn）<br>（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）“密码匙资料外泄”

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，该方法可以借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某政府电子证书曾被用作认证具欺诈性及误导性的下级完整网域名称；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并不准确；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站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获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悉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称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”：

- 证书登记人已为此此原因撤销其证书；或
- 香港邮政核证机关收到可核实的证据，证明证书登记人已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，否则在下列情况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情见**附录 C**。

## 7.3 线上证书状态应答结构
不适用。

### 7.3.1 版本编号
不适用。

### 7.3.2 线上证书状态应答延伸栏位
不适用。

# 8. 认证机构审计和其他评估

本核证作业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》第 43（1）条编写和提交评估报告。

## 8.1 评估的频率及情形

遵守规定审核评估须至少每十二个月进行一次。

## 8.2 评估者的资格

独立外部审计员进行合规评估所须具备的资历，须符合《条例》及《认可核证机关业务守则》所订明的要求。WebTrust 审计员亦须符合 S/MIME 基线要求第 8.2 条的规定。

## 8.3 评估者与被评估实体之间的关系

合规评估由独立于香港邮政的外部审计员进行，有关审计员须符合《条例》及《认可核证机关业务守则》所订明的要求。

## 8.4 评估内容

香港邮政就其发出、撤销及公布电子证书的系统进行合规评估，以确定本核证作业准则是否获妥善遵循。该等评估须按照《条例》及《认可核证机关业务守则》所订明的要求进行。

## 8.5 对问题与不足采取的措施

如审计员在审核中发现不符合适用法律、本核证作业准则或与香港邮政服务有关的任何其他合约责任的重大情况，则：（1）审计员须记录有关差异；（2）审计员须立即通知香港邮政；及（3）香港邮政须根据有关差异的性质及影响范围，制定适当的纠正措施计划以纠正有关不符合情况，并决定是否就已发出的政府电子证书采取任何补救措施。

## 8.6 评估结果的传达与发布

核证机关的 WebTrust 审核报告会于 http://www.eCert.gov.hk/product/cps/ecert 供公众查阅。根据《条例》第 43（1）条编制的合规评估报告，则会提交予数字政策专员。

## 8.7 自我审核

香港邮政每季最少进行一次自我审核，抽样检查自上次自我审核以来所发出的电子证书中最少百分之三的随机样本。电子证书的自我审核须按照核证机关 / 浏览器论坛（CA / Browser Forum）采纳的指引进行。

# 9. 法律责任和其他业务条款

## 9.1 登记费用

### 9.1.1 证书发出或续期费用

除获得香港邮政豁免，否则一切登记费用须由政府电子证书登记人付清。有关政府电子证书的收费详情，请参阅**附录 H**。香港邮政保留绝对权力，不时检讨及订定登记费的收费水平，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向政府电子证书登记人收取**附录 H** 所列的登记费。

### 9.1.2 证书查询费用

香港邮政可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查阅已发出证书的有效性收取费用。

### 9.1.4 其他服务费用

香港邮政会不时检讨。

### 9.1.5 退款政策

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

香港邮政维持专业责任 / 错误及遗漏保险，保额不少于一百万美元。此外，该保险亦涵盖根据《电子交易条例》条文就证书所订倚据限额而可能产生或实际产生的责任及申索。

### 9.2.2 其他资产

不适用。

### 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 业务信息机密

### 9.3.1 机密资料范围

作为根据本准则申请政府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；但登记人名称、中央管理通讯平台用户名称，以及香港邮政或承办商在履行本准则下香港邮政责任所必需的其他资料除外。

### 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。已发布的证书及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，不得将包括上文第 9.3.1 条所述的资料对外发布。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，惟无法追溯个别登记人之综合资料除外。

## 9.4 个人资料私隐

### 9.4.1 私隐方案

香港邮政已实施符合本核证作业准则的私隐政策。香港邮政的私隐政策于香港邮政网站 http://www.eCert.gov.hk 公布。

### 9.4.2 视作隐私的资料

任何不在已发出的证书、储存库及证书撤销清单公开的登记人资料均视作私隐资料。

### 9.4.3 不被视作私隐资料

已发布的证书及撤销资料均被视作公开资料。证书状态资料及任何证书内容均视作非私隐资料。

### 9.4.4 保护私隐的责任

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 使用私隐资料的通告与同意

作为根据本准则申请政府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 根据法律或行政程序作出的披露
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，不得将包括上文第 9.3.1 条所述的资料在内的机密资料对外发布。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，惟无法追溯个别登记人之综合资料除外。

### 9.4.7 其他资料披露情况
不适用。

## 9.5 知识产权
香港邮政拥有与其资料库、网站、电子证书、商标及香港邮政发布的任何其他刊物（包括本核证作业准则）有关的一切知识产权。

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 陈述及担保

### 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（包括第 3.2 条）所述的核查程序，以验证证书申请人确为证书内所识别之登记人机构。

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。除因疏忽、超越授权范围行事、欺诈、刑事行为或其他类似因素的情况外，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。

核证登记机关代表香港邮政履行其于此等事项下的义务及责任。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）。

### 9.6.3 登记人的陈述与担保
各登记人机构（由提出要求者代表）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，登记人机构据此条款同意，登记人机构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) 使用与证书所载公开密码匙相对应的私人密码匙执行指定应用，即属上文第 1.3.4.1.1 条所述隶属登记人机构的中央管理通讯平台用户的行为，或上文第 1.3.4.1.2 条所述功能单位的行为；且该证书已获接受，并于整个有效期内维持正常运作；
b) 证书所载之所有资料及由登记人机构作出之陈述均属真实。
c) 证书将只会用于符合本核证作业准则之认可及合法用途。
d) 登记人机构将确保证书只限用于**附录 H** 所订明的指定应用；
e) 登记人机构同意遵守本核证作业准则、香港邮政的其他协议及政策声明所载的条款及条件；
f) 登记人机构已授权中央管理通讯平台于**附录 H** 所订明的指定应用中取用该证书的私人密码匙；
g) 在证书发出、接受及整个证书有效期内所提供之所有资料，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登记期届满。
c) 不时将政府电子证书中央管理通讯平台用户的委任或任何资料变动立即通知香港邮政。
d) 将可能致使香港邮政根据本准则第 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（由香港邮政或经申请人或登记人申请），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) 承认知悉一经递交政府电子证书申请表，即授权向其他人或在香港邮政储存库公布其政府电子证书，包括中央管理通讯平台用户或登记人机构的名称。
h) 用于身份鉴别的证书，其私人密码匙只可以在政府电子证书有效期内使用。

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

倚据政府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。
c) 于倚据证书前在适用情况下查核证书撤销清单上之证书状态。
d) 执行所有适当证书路径认可程序。
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。除因疏忽、超越授权范围行事、欺诈、刑事行为或其他类似因素的情况外，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。

#### 9.6.5.1 中央管理通讯系统之义务

中央管理通讯系统负责：

a） 在中央管理通讯系统中为“提出要求者”的用户角色作出定义，以便政策局 / 部门 / 办公室可以指定人员作为“提出要求者”以代表中央管理通讯系统用户（申请人）提出申请证书，证书续期或证书撤销的要求；
b） 在中央管理通讯系统中为“业务管理人员”的用户角色作出定义，以便政策局 / 部门 / 办公室可以指定人员作为核证登记机关，验证申请人的身份并于中央管理通讯系统中批准证书申请、续期和撤销要求；
c） 确保中央管理通讯系统用户不能同时担任“业务管理人员”和“提出要求者”的角色，以达到职责分离的要求；
d） 定义和提供予中央管理通讯系统中的不同用户角色（“提出要求者”，“业务管理人员”）的审批工作流程，以执行证书申请，续期和撤销的相应任务（递交要求，验证和审批要求）；
e） 代表申请人向香港邮政产生并递交「签发证书要求」（Certificate Signing Request），当中包括于提交时与中央管理通讯系统所知悉有关中央管理通讯系统用户或功能单位的资料相符的资料，以及申请人确认的登记人条款及条件；
f） 代表申请人接受香港邮政以安全的方式发出的政府电子证书；
g） 确保登记人配对密码匙只会在中央管理通讯系统的硬体安全模组（“HSM”）内产生和储存；
h） 确保妥善保管登记人的配对密码匙；
i） 确保政府电子证书仅用于**附录 H** 中所规定之指定应用；
j） 确保中央管理通讯平台用户或功能单位不被允许使用政府电子证书于**附录 H** 中规定之指定应用以外的其他用途；
k） 确保只有在政府电子证书中列明的中央管理通讯平台用户和 / 或功能单位才能使用其私人密码匙于有关的指定应用进行数码签署；
l） 在中央管理通讯平台用户或功能单位被允许于指定应用中使用政府电子证书前，核实中央管理通讯平台用户或功能单位的身份；
m） 分配独特的身份号码给中央管理通讯平台用户，此号码于递交政府电子证书申请时用来引用中央管理通讯平台用户资料, 其必须与中央管理通讯平台用户的身份证明具有唯一的相关性；
n） 每次在指定应用中使用政府电子证书时，根据储存库和证书撤销清单中显示的资料确保该政府电子证书并未过期或未被撤销。如果政府电子证书已过期或被撤销，不会使用该政府电子证书进行或完成指定应用；

#### 9.6.5.2 政策局 / 部门 / 办公室之义务

政策局 / 部门 / 办公室除作为登记人所须承担的责任外，亦须负责：

a） 指定“业务管理人员”作为核证登记机关以验证申请人的身份，并透过中央管理通讯系统中的“业务管理人员”批准证书申请，续期和撤销要求；

b） 保存由“业务管理人员”角色用作核证申请人身份的文件证明；

c） 指定“提出要求者”代表申请人提出证书申请、续期或撤销的要求；

d） 确保“提出要求者”妥善完成申请程序, 并代表申请人确认接受登记人条款及条件；

e） 确保政府电子证书正确使用于**附录 H** 中所规定之指定应用；及

f） 确保“业务管理人员”在政策局 / 部门 / 办公室预先订明的工作天内完成批核证书撤销要求。

### 9.7 免责声明

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，以及（对于登记人而言）登记人协议中的相关规定。除因疏忽、欺诈、超越授权范围行事或其他类似情况（统称“例外情况”）外，核证登记机关或承办商的一切作为及不作为均视作香港邮政的作为及不作为，免责声明及倚据限额同样适用于该等情况。即使在例外情况下，在法律允许的范围内，香港邮政、核证登记机关及承办商均应依据本 9.8 条规定的免责声明及倚据限额。

若发生：

a) 香港邮政违反本准则或登记人协议；
b) 香港邮政违反任何谨慎职责－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；
c) 因根据本准则及实务守则规定须由香港邮政确认，并且在该证书或存储库中被错误陈述的任何资讯而造成的损失

之情况下，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，若发生：**

**a) 香港邮政违反本准则或登记人协议（仅适用于登记人）；**
**b) 香港邮政违反任何谨慎职责－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；或**
**c) 因根据本准则及实务守则规定须由香港邮政确认，并且在该证书或存储库中被错误陈述的任何资讯而造成的损失**

**之情况下，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不得超过 20 万港元（不论是政府电子证书（个人）或政府电子证书（功能单位），并且无论上述索赔、违约及／或损失的数量为何。**

**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。**

承办商、任何核证登记机关，以及香港邮政署、承办商或任何核证登记机关的任何职员、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或其各自之任何职员、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。

如因倚据由香港邮政（或其代表香港邮政行事的承办商）发出的证书所支援，而属某登记人或任何声称代表该登记人行事的人士的虚假或伪造数码签署而引致任何损失，而香港邮政已符合《条例》及《认可核证机关业务守则》的规定，则香港邮政、承办商及其各自的高级人员、雇员或代理人，均毋须就登记人及倚据人士所蒙受的任何损失或损害承担责任，而由于上述免责声明，在此等情况下适用于任何证书的倚据限额并无需要适用。

## 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政府电子证书的准则（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，在适用情况下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。*

*若尽管由香港邮政署长（或其代表行事的承办商）签发的证书所支持的订户虚假或伪造数字签名而导致任何损失，并且该署长已就该证书遵守了条例及业务守则的相关规定，则在此情况下，香*

*港邮政署长、香港邮政署承办商及其各自职员、雇员或代理人均无需对倚据人士之任何损失或损害承担任何责任；此外，鉴于上述免责声明，该证书依据条例所适用的任何倚据限额也不再适用。*

*在符合本准则－包括本准则第 9.8 及 9.9 条－以及本证书所载各项规定与例外情况的前提下，若香港邮政违反了任何注意义务（特别是根据本准则或法律规定须尽到的合理技能与注意义务，和／或因倚据人士或任何其他人依赖或使用香港邮政在公开密码匙基础设施计划下签发的证书而可能对倚据人士负有的任何义务），或因依赖本准则及业务守则规定须由香港邮政确认、但却在该证书或资料库中被错误陈述的资讯而导致损失，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不得超过 20 万港元（不论是政府电子证书（个人）或政府电子证书（功能单位）），且无论上述索赔、违约及／或损失的数量为何。*

*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不适用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站 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数字政策专员。

### 9.10.2 终止

本核证作业准则（包括其所有修订及增编）持续有效，直至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”所定程序知会数字政策专员并作出公布。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站 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数字政策专员。申请人、登记人及倚据人士可从香港邮政网站 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

除下文第 9.15 条规限，香港邮政关于本准则范围内之事宜之决定，在没有明显错误的情况下均为最终决定。如声称存在明显错误，有关申索，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接受香港特别行政区法院的非专属司法管辖权。

## 9.15 符合适用法律规定

### 9.15.1 司法管辖权
任何一方（不论是香港邮政、登记人、倚据人士、承办商或核证登记机关（各称为一方））如因本核证作业准则而产生或与之相关的任何争议或分歧，须首先按照当时有效的《香港特别行政区政府调解规则》进行调解。

如上述争议或分歧未能透过调解解决，任何一方均可就该争议或分歧提出诉讼。各方同意，香港法院对该争议或分歧享有专有司法管辖权。

## 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（不可放弃权利）
香港邮政未有执行本核证作业准则的任何条文，并不构成放弃其于日后执行该条文或本核证作业准则任何其他条文的权利。任何放弃权利必须以书面作出并由香港邮政签署，方为有效。

### 9.16.5 不可抗力
香港邮政如因任何适用法律、规例或命令的规定；民事、政府或军事机关的行动；任何由其他人士营运而香港邮政无法控制的电力、通讯或其他系统故障；火灾、水灾或其他紧急情况；罢工；恐怖主义行为或战争；天灾；或其他超出其合理控制范围且并非因其过失或疏忽所引致的类似原因，而被阻止、禁止或延迟履行任何作为或规定，或未能履行任何作为或规定，香港邮政毋须承担任何责任。

## 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，香港邮政须承担第 9.8 条所载责任。另外，由香港邮政转让的物品可内载其他与完成及接受政府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

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”**指附录 E 中所列，透过提出要求者行事的申请人机构。

**“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。

**“应用程式接口”**指一种应用程式介面，用于定义中央管理通讯系统与特定政策局 / 部门 / 办公室系统之间的交互作用。当政策局 / 部门 / 办公室在其系统中管理使用者帐户时，中央管理通讯系统可透过此应用程式接口从特定的政策局 / 部门 / 办公室系统接收使用者帐户资讯。

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

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

**“核证机关 / 浏览器论坛 S/MIME 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 S/MIME 证书的基线要求。

**“核证机关 / 浏览器论坛 TLS 伺服器证书基线要求”**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 TLS 伺服器证书的基线要求。

**“业务管理人员”**指中央管理通讯系统中的一种使用者角色，负责核实申请人的身分（即担任核证登记机关的角色），并审核中央管理通讯系统中的证书申请、续期及撤销请求。

**“核证机关”**指向他人（可以为另一核证机关）发出证书者。

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

**“证书”**或**“政府电子证书”**指符合以下所有说明之纪录：

a） 由核证机关为证明数码签署之目的而发出而该数码签署用意为确认持有某特定配对密码匙者身分或其他主要特征；
b） 识别发出纪录之核证机关；
c） 指名或识别获发给纪录者；
d） 包含该获发给纪录者之公开密码匙；并
e） 经发出纪录的核证机关签署。

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

**“证书问题报告”**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。

**“提交签发证书要求”**指由中央管理通讯系统发送给香港邮政、包含登记人的公开密码匙，旨在申请证书的讯息。

**“中央管理通讯系统”**指由数字政策办公室管理和支援的、在**附录 E** 中列出的集中式管理服务平台，该平台提供上文第 9.6.5.1 节所概述的功能。

**“中央管理通讯系统用户”**指由数字政策办公室提供帐户、可登入中央管理通讯系统并存取各类指定应用的政策局 / 部门 / 办公室使用者。

**“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，用于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 2023 年 7 月 1 日至 2026 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 2027 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 F**，若有的话）。其为香港邮政根据认可核证机关业务守则第 3.2 段所委任之代理人，根据合约条款，为香港邮政营运及维持香港邮政核证机关之服务及系统。

**“对应”**就私人或公开密码匙而言，指属同一配对密码匙。

**“业务守则”**指由数字政策专员在条例第 33 条下颁布之认可核证机关业务守则。

**“指定应用”**指在**附录 H** 中列出的指定应用。

**“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。

**“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。

**“政府电子证书（个人）”或“政府电子证书（功能单位）”**指政府电子证书或证书。

**“硬体安全模组”**是指一种硬体安全设备，用于储存和管理证书，并保护配对密码匙，防止其被篡改、汇出或复制。

**“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。

**“香港”**指中华人民共和国香港特别行政区。

**“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。

**“邮箱栏位”**在电子证书而言，指包含主体邮箱位址的字段，该位址透过 rfc822Name 或其他类型为 id-on-SmtpUTF8Mailbox 的 otherName 值储存在 subjectAltName 延伸栏位。

**“OCSP”**指线上证书状态应答。

**“线上证书状态应答”**指一种线上证书核对规约，允许倚据人士查明政府电子证书的状态。

**“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。

**“香港邮政署长”**指香港法例第 98 章《邮政署条例》所指署长。

**“私人密码匙”**指配对密码匙中用作产生数码签署之密码匙。

**“公开密码匙”**指配对密码匙中用作核实数码签署之密码匙。

**“认可证书”**指：

（a） 根据电子交易条例第 22 条认可之证书；
（b） 属根据电子交易条例第 22 条认可之证书之类型、类别或种类之证书；或
（c） 电子交易条例第 34 条所述核证机关所发出指明为认可证书之证书。

**“认可核证机关”**指根据电子交易条例第 21 条认可之核证机关或第 34 条所述核证机关。

**“纪录”**指在有形媒界上注记、储存或以其他方式固定之资讯，亦指储存在电子或其他媒界可藉理解形式还原之资讯。

**“核证登记机关”**指由香港邮政指定，代表香港邮政核证机关行使一定职能，并提供香港邮政核证机关之若干服务（包括核实申请人身分）之机构。

**“倚据限额”**指就认可证书倚据而指明之金钱限额。

**“倚据人士”**指透过使用中央管理通讯系统，来验证另一中央管理通讯系统用户或功能单位的身份，并据此决定是否信任该用户或功能单位的数位签署资讯的登记人机构的中央管理通讯系统用户或功能单位。

**“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。

**“提出要求者”**指中央管理通讯系统中的一种使用者角色，负责代表登记人机构提出证书申请、证书续约及证书撤销请求。

**“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。

**“角色”**指登记人机构赋予中央管理通讯系统用户的职能或职责。

**“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。

**“S/MIME”** 指安全／多用途互联网邮件延伸（Secure/Multipurpose Internet Mail Extensions）的缩写。

**“SSL”** 指安全通讯端层（Secure Sockets Layer）的缩写。

**“中继证书”**指由香港邮政根源证书所签发的中继核证机关证书“Hongkong Post Root CA 2”，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”**指登记人机构。

**“登记人协议”**指由登记人及香港邮政（即香港邮政署长，代表香港政府）订立的协议，该协议包括政府电子证书的登记人条款及条件，以及本核证作业准则。此协议属于谅解备忘录性质，不具法律约束力。

**“登记人机构”**指**附录 E** 所列的实体。

**“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。

**“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。

**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 - 香港邮政政府电子证书格式

本附录详述由中继证书“Hongkong Post g-Cert CA 2 - 26”根据本核证作业准则签发的政府电子证书格式。

## 1） 政府电子证书（个人）格式

| 栏位名称 | | 栏位内容 |
|---|---|---|
| **标准栏 （Standard fields）** | | |
| **版本 （Version）** | | X.509 V3 |
| **序号 （Serial number）** | | [由香港邮政系统设置的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 Root CA 2 - 26<br>o=Hongkong Post<br>l=Hong Kong<br>s=Hong Kong<br>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=[中央管理通讯系统用户姓名] （附注1）<br>g=[中央管理通讯系统用户名]<br>sn=[中央管理通讯系统用户姓氏]<br>e=[电子邮箱地址] （附注2）<br>ou=[登记人机构分行 / 部门名称]<br>o=Hong Kong SAR Government<br>c=HK<br>Object Identifier (2.5.4.5) SERIALNUMBER=[登记人参考编号] （附注3）<br>Object Identifier (OID: 2.5.4.97)=GOVHK |
| **主体公开密码匙资料 （Subject public key info）** | | 算式识别 （Algorithm ID）：RSA<br>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）** | | |
| **机关信息访问 (Authority Information Access)** | **核证机关发出人 (Certification Authority Issuer)** | URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt |
| **机关密码匙识别名称 (Authority Key Identifier)** | **KeyID** | [发出人证书的主体密码匙标识符] |
| **发出人证书的主体密码匙标识符 (Subject Key Identifier)** | | [由主体公开密码匙衍生] |
| **密码匙使用方法 （Key usage）** | | 不可否认，数码签署，密码匙加密<br><br>**（此栏为“关键”栏位）** |

| 栏位名称 | | 栏位内容 |
|---|---|---|
| **证书政策 （Certificate policies）** （附注4） | | Policy Identifier = [本准则的物件识别码] （附注 5）<br>Policy Identifier = 2.23.140.1.5.3.3 （附注 6）<br>Policy Identifier = 1.3.6.1.4.1.16030.1.10.4 （附注7） |
| **主体别名 （Subject alternative name）** | rfc822 | [证书持有人电子邮箱地址] （附注2） |
| **发出人别名（Issuer alternative name）** | | 未使用 |
| **基本限制 （Basic constraints）** | **主体类型 （Subject type）** | 未使用 |
| | **路径长度限制 （Path length constraint）** | 未使用 |
| **延伸密码匙使用方法（Extended key usage）** | | S/MIME |
| **证书撤销清单分发点（CRL distribution point）** | | 分发点名称 = [证书撤销清单分发点URL] （附注8） |

附注：

1. 中央管理通讯系统用户格式：以英文格式 记载- 姓氏（大写）+ 名（例如: CHAN Tai Man David）。
2. 登记人机构提供之中央管理通讯系统用户电子邮箱地址。
3. 登记人参考编号：10 位数字。
4. 由中继证书签发的证书符合本准则、核证机关 / 浏览器论坛 S/MIME 基线要求。
5. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。请参阅本准则第 1.2 条。
6. 证书策略物件识别码由核证机关 / 浏览器论坛分配给符合赞助机构验证严格证书政策的电子证书。
7. 香港邮政分配物件识别码显示，其持有人是政府电子证书（个人）之登记人。
8. 证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL2.crl，此为中继证书"Hongkong Post e-Cert CA 2 - 26"所发出的「整体证书撤销清单」。

## 2） 政府电子证书（功能单位）格式

| 栏位名称 | | 栏位内容 |
|---|---|---|
| **标准栏 （Standard fields）** | | |
| **版本 （Version）** | | X.509 V3 |
| **序号 （Serial number）** | | [由香港邮政系统设置的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 Root CA 2 - 26<br>o=Hongkong Post<br>l=Hong Kong<br>s=Hong Kong<br>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=Hong Kong SAR Government<br>e=[电子邮箱地址] （附注1）<br>ou=[登记人机构分行 / 部门名称]<br>o=Hong Kong SAR Government<br>c=HK<br>Object Identifier (2.5.4.5) SERIALNUMBER=[登记人参考编号] （附注3）<br>Object Identifier (OID: 2.5.4.97)=GOVHK |
| **主体公开密码匙资料 （Subject public key info）** | | 算式识别 （Algorithm ID）：RSA<br>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）** | | |
| **机关信息访问 (Authority Information Access)** | **核证机关发出人 (Certification Authority Issuer)** | URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt |
| **机关密码匙识别名称 (Authority Key Identifier)** | KeyID | [发出人证书的主体密码匙标识符] |
| **发出人证书的主体密码匙标识符 (Subject Key Identifier)** | | [由主体公开密码匙衍生] |
| **密码匙使用方法 （Key usage）** | | 数码签署，密码匙加密<br><br>**（此栏为“关键”栏位）** |
| **证书政策 （Certificate policies）** （附注3） | | Policy Identifier = [本准则的物件识别码] （附注 4）<br>Policy Identifier = 2.23.140.1.5.2.3 （附注 5）<br>Policy Identifier = 1.3.6.1.4.1.16030.1.10.5 （附注6） |
| **主体别名 （Subject alternative name）** | rfc822 | [证书持有人电子邮箱地址] （附注1） |
| **发出人别名（Issuer alternative name）** | | 未使用 |
| **基本限制 （Basic constraints）** | **主体类型 （Subject type）** | 未使用 |
| | **路径长度限制 （Path length constraint）** | 未使用 |
| **延伸密码匙使用方法 （Extended key usage）** | | S/MIME |

| 栏位名称 | | 栏位内容 |
|---|---|---|
| **证书撤销清单分发点**<br>**（CRL distribution point）** | | 分发点名称 = [证书撤销清单分发点URL] （附注7） |

附注：

1. 登记人机构提供之中央管理通讯系统功能单位电子邮箱地址。
2. 登记人参考编号：10 位数字。
3. 由中继证书签发的证书符合本准则、核证机关 / 浏览器论坛 S/MIME 基线要求。
4. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。请参阅本准则第 1.2 条。
5. 证书策略物件识别码由核证机关 / 浏览器论坛分配给符合机构验证严格证书政策的电子证书。
6. 香港邮政分配物件识别码显示，其持有人是政府电子证书（功能单位）之登记人。
7. 证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL2.crl，此为中继证书"Hongkong Post e-Cert CA 2 - 26"所发出的「整体证书撤销清单」。

# 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)格式

本附录 C 详述有关由中继证书"Hongkong Post e-Cert CA 2 - 26"所发出的证书撤销清单，以及由根源证书"Hongkong Post Root CA 2"所发出的授权撤销清单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：

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 2 - 26"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 2 - 26"所发出的证书：
http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL1.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 26 CRL1, o=Hongkong Post, c=HK)

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

在正常情况下，香港邮政会于更新时间后，尽快将最新的证书撤销清单公布。在不能预见及有需要的情况下，香港邮政可不作事前通知而更改上述证书撤销清单的更新及公布的时序。香港邮政也会在有需要及不作事前通知的情况下，于香港邮政网页 http://www.eCert.gov.hk 公布补充证书撤销清单。

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. 根源证书"Hongkong Post Root CA2"所签发的中继证书
http://crl1.eCert.gov.hk/crl/RootCA2ARL.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 2, o=Hongkong Post, c=HK)

**（I） 由中继证书"Hongkong Post e-Cert CA 2 - 26"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 2 - 26,<br>o=Hongkong Post,<br>l=Hong Kong,<br>s=Hong Kong,<br>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) |

| 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 |
|---|---|---|---|
| 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) | KeyID | [签发此证书撤销清单之中继证书的主体密码匙标识符] | |
| 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。 |

**(II) 由根证书"Hongkong Post Root CA 2"根据本准则发出的授权撤销清单格式:-**

| 标准栏位 (Standard fields) | 子栏位 (Sub-fields) | 授权撤销清单栏位内容 | 备注 |
|---|---|---|---|
| 版本 (Version) | | v2 | 此栏显示授权撤销清单格式的版本为 X.509 第二版 |
| 签署算式识别 (Signature algorithm ID) | | sha256RSA | 此栏显示用以签署授权撤销清单的算法的识别码 |
| 发出人 (Issuer name) | | cn=Hongkong Post Root CA 2<br>o=Hongkong Post,<br>l=Hong Kong,<br>s=Hong Kong,<br>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） | | | |

| 标准栏位 (Standard fields) | 子栏位 (Sub-fields) | 授权撤销清单栏位内容 | 备注 |
|---|---|---|---|
| 机关密码匙识别名称 (Authority Key Identifier) | 发出人 (Issuer) | cn=Hongkong Post Root CA2<br>o=Hongkong Post,<br>l=Hong Kong,<br>s=Hong Kong,<br>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<br>只存有核证机关证书=是<br>间接的 CRL=否<br><br>**（此栏为“关键”栏位）** | |

附注：

1. 以下为可于撤销证书栏位下列出的理由识别码：

   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 = 未注明；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 - 香港邮政政府电子证书 – 服务摘要

| 要点（附注 1） | 政府电子证书 |
|---|---|
| **登记人机构** | 香港特别行政区政府决策局 / 部门 / 办公室 |
| **登记人** | 中央管理通讯系统 用户 / 中央管理通讯系统 功能单位 |
| **依据限额** | HK$200,000 |
| **认可证书** | 是 |
| **配对密码匙长度** | 2048 位元 RSA |
| **核证登记机关** | 中央管理通讯系统内代表各决策局 / 部门 / 办公室的业务管理人员 |
| **产生配对密码匙** | 由中央管理通讯系统代制产生 |
| **核对身分** | 如第 3.2 条所述 |
| **证书用途** | • 加密 / 解密，及数码签署以确认已收讫送出之信息。<br>• 签署文件并在中央管理通讯系统内进行认证（不用作 ETO 所述的数码签署）（仅限政府电子证书（个人））<br>• **附录 H** 列出对应其政府电子证书的指定应用 |
| **证书内包含登记人的资料** | • 登记人机构名称<br>• 中央管理通讯系统用户英文姓名及其电邮地址（仅限政府电子证书（个人））<br>• 功能单位用户英文姓名及其电邮地址（仅限政府电子证书（功能单位））<br>• 由香港邮政核证机关系统产生的登记人参考编号 |
| **登记费用及证书有效期** | 一年。见**附录 H** |

附注

1. 登记人机构必须先与香港邮政作出安排，香港邮政才可以为登记人机构发出政府电子证书。

# 附录 E - 香港邮政政府电子证书登记人机构 / 核证登记机关名单及中央管理通讯系统（若有的话）

**(I) 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室名单**

| 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室 | 证书类别 | 服务提供 |
|---|---|---|
| 渔农自然护理署<br><br>建筑署<br><br>审计署<br><br>医疗辅助队<br><br>屋宇署<br><br>政府统计处<br><br>行政长官办公室<br><br>特首政策组<br><br>政务司司长办公室 - 政府档案处<br><br>政务司司长办公室及财政司司长办公室<br><br>民众安全服务处<br><br>民航处<br><br>土木工程拓展署<br><br>公务员事务局<br><br>商务及经济发展局<br><br>公司注册处<br><br>政制及内地事务局 | 政府电子证书（个人）及政府电子证书（功能单位） | 为中央管理通讯系统提供以下有关申请政府电子证书之服务：<br>- 根据第3.2条及第4.1条所述提供证书申请服务。<br>- 根据第4.6条所述提供证书续期请求服务。<br>- 根据第4.9.1条；第4.9.3条及第4.9.5条所述提供证书撤销请求服务。<br>- 根据第5.1.6条所述的决策局 / 部门 / 办公室的文件保存。 |

| 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室 | 证书类别 | 服务提供 |
|---|---|---|
| 惩教署<br><br>文创产业发展处<br><br>文化体育及旅游局<br><br>香港海关<br><br>卫生署<br><br>律政司<br><br>发展局规划地政科<br><br>发展局工务科<br><br>渠务署<br><br>教育局<br><br>机电工程署<br><br>环境及生态局<br><br>环境保护署<br><br>财经事务及库务局财经事务科<br><br>财经事务及库务局库务科<br><br>消防处<br><br>食物环境卫生署<br><br>政府飞行服务队<br><br>政府化验所<br><br>政府物流服务署<br><br>政府产业署 | | |

| 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室 | 证书类别 | 服务提供 |
|---|---|---|
| 医务卫生局<br>路政署<br>民政事务总署<br>民政及青年事务局<br>香港金融管理局<br>香港天文台<br>香港警务处<br>房屋局<br>房屋署<br>入境事务处<br>廉政公署<br>独立监察警方处理投诉委员会<br>政府新闻处<br>税务局<br>创新科技及工业局<br>创新科技及工业局 - 数字政策办公室<br>创新科技及工业局 - 创新科技署<br>知识产权署<br>投资推广署<br>薪资会联合秘书处<br>司法机构 | | |

| 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室 | 证书类别 | 服务提供 |
|---|---|---|
| 劳工及福利局<br><br>劳工处<br><br>土地注册处<br><br>地政总署<br><br>法律援助署<br><br>康乐及文化事务署<br><br>海事处<br><br>通讯事务管理局办公室<br><br>申诉专员公署<br><br>破产管理署<br><br>规划署<br><br>邮政署<br><br>公务员叙用委员会<br><br>香港电台<br><br>差饷物业估价署<br><br>选举事务处<br><br>截取通讯及监察事务专员秘书处<br><br>保安局<br><br>社会福利署<br><br>香港经济贸易办事处<br><br>工业贸易署 | | |

| 作为香港邮政登记人机构 / 核证登记机关的决策局 / 部门 / 办公室 | 证书类别 | 服务提供 |
|---|---|---|
| 运输及物流局<br><br>运输署<br><br>库务署<br><br>大学教育资助委员会秘书处<br><br>水务署<br><br>在职家庭及学生资助事务处(学生资助处)<br><br>在职家庭及学生资助事务处(在职家庭津贴办事处) | | |

**(II) 中央管理通讯系统 (CMMP)**

| 中央管理通讯系统（CMMP）行政及支援 | 证书类别 | 提供的服务 | 备注 |
|---|---|---|---|
| 数字政策办公室 | 香港邮政政府电子证书 (个人) 及政府电子证书 (功能单位) | 设置和维护中央管理通讯系统供决策局 / 部门 / 办公室使用：<br>-提供决策局 / 部门 / 办公室的用户角色，让决策局 / 部门 / 办公室以此执行有关政府电子证书的申请；<br>-为证书申请，续期和撤销提供审批工作流程；<br>-为政府电子证书登记人的私人密码匙及其使用提供安全保管；<br>-当决策局 / 部门 / 办公室要求时，向其提供政府电子证书登记人的私人密码匙；<br><br>为决策局 / 部门 / 办公室的政府电子证书申请人的提供以下程序：<br>- 为中央管理通讯系统中用户角色作出定义，使决策局 / 部门 / 办公室能指定人员作为核证登记机关以执行如第 3.2 条所述核证申请人身份。<br>- 如第 3.2.1, 4.3 及 4.6 所述产生密码匙。<br>-承担第 9.6.5.2 条所述的义务责任。 | 为达到职责分离的要求，中央管理通讯系统不容许用户作为“业务管理人员”时批准自己提出的要求，即中央管理通讯系统用户不能就某一要求同时担任“业务管理人员”和“提出要求者”的角色。 |

# 附录 F - 香港邮政政府电子证书服务 - 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，香港邮政政府电子证书服务并无指定之受翘晋电子商务有限公司委任的合约分判商。

# 附录 G - 核证机关根源证书的有效期

| 参考项目 | 香港邮政核证机关根源证书名称 | 有效期 | 备注 |
|---|---|---|---|
| 1 | Hongkong Post Root CA 2 | 2015 年 9 月 5 日 至<br>2040 年 9 月 5 日 | 此根源证书由 2015 年 9 月 5 日起开始发出中继证书。 |
| 主体专有名称 （Subject DN）<br>C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 2<br>SHA-1 Thumbprint<br>DE010808E41EC41930D44095F8FE596B582C8CA2 | | | |
| 2 | Hongkong Post e-Cert CA 2 - 26 | 2026 年 5 月 7 日 至<br>2040 年 9 月 5 日 | 此中继证书由 2026 年 10 月 1 日起开始发出政府电子证书。 |
| 主体专有名称 （Subject DN）<br>C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 26<br>SHA-1 Thumbprint<br>EA9AECB58CB9023AE090235EA2FFFA8ED8420A88 | | | |

# 附录 H - 香港邮政政府电子证书相对应之指定应用

| 政府电子证书类别 | 证书有效期 | 指定应用 | 登记费 | 备注 |
|---|---|---|---|---|
| 政府电子证书（个人） | 1 年 | 由中央管理通讯系统支援的数字政策办公室之应用 | 新申请或续期：每份证书每年港币 20 元。<br><br>承办商就政府电子证书（个人）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。 | 第 1.3.4.1.1 条所述政府电子证书（个人）的用途 |
| 政府电子证书（功能单位） | 1 年 | 由中央管理通讯系统支援的数字政策办公室之应用 | 新申请或续期：每份证书每年港币 20 元。 | 第 1.3.4.1.2 条所述政府电子证书（功能单位）的用途 |