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）

核证作业准则

日期：二零二五年十一月一日
物件识别码：1.3.6.1.4.1.16030.1.8.12

目录

前言

香港法例第 553 章电子交易条例（“条例”）列载公开密码匙基础建设（公匙基建）之法律架构。公匙基建利便电子交易作商业及其他用途。公匙基建由多个元素组成，包括法律责任、政策、硬体、软件、资料库、网络及保安程序。

公匙密码技术涉及运用一条私人密码匙及一条公开密码匙。公开密码匙及其配对私人密码匙在运算上有关连。电子交易运用公匙密码技术之主要原理为：经公开密码匙加密之信息只可用其配对私人密码匙解密；和经私人密码匙加密之信息亦只可用其配对公开密码匙解密。

设计公匙基建之目的，为支援以上述方式在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 2023 年 7 月 1 日至 2026 年 6 月 30 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 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、暂时吊销或撤销及利用公开储存库公布已认可及已接受之数码证书作为在网上进行稳妥的身分辨识。**根据本核证作业准则发出的政府电子证书（个人）及政府电子证书（功能单位）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”。**

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。而根据数字政策专员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。

本核证作业准则列载政府电子证书的实务守则，其结构如下：

第 1 条 载有概述及联络资料
第 2 条 列载各方责任及义务
第 3 条 列载申请及身分确认程序

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、撤销及公布政府电子证书时采用之做法及标准。

香港邮政已获 Internet Assigned Numbers Authority (IANA) 分配私人企业号码 (Private Enterprise Number) 16030 号。「1.3.6.1.4.1.16030.1.8.12」为本准则的物件识别码 (Object Identifier, OID) （见**附录 B** 内关于核证政策(Certificate Policies)的说明）。

本准则列载参与香港邮政所用系统之人士之角色、职能、义务及潜在责任。本准则列出核实证书(即根据本作业准则发出的证书)申请人身分的程序，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式上之参与者之身分。倚据人士不得在**附录 H** 所列证书的登记人机构的指定应用以外的任何公匙基建应用程式上使用香港邮政发行的证书。

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。

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）、政府电子证书（功能单位），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）。香港邮政已指定其代理人或承办商或分包商之事实并无减轻香港邮政使用稳当系统之义务，亦无变更政府电子证书作为获认可证书具有之特性。

附录 D 载有政府电子证书特点摘要。

1.2 社区及适用性

1.2.1 核证机关

根据本准则，香港邮政履行核证机关之职能并承担其义务。香港邮政乃唯一根据本准则授权发出证书之核证机关（见第 2.1.1 条）。

1.2.1.1 香港邮政所作之陈述

根据本准则而发出之证书，香港邮政向根据本准则第 2.1.6 条及其他有关章条之倚据人士表明，香港邮政已根据本准则发出证书。透过公布本准则所述之证书，香港邮政即向根据本准则第 2.1.6 条及其他有关章条之倚据人士表明，香港邮政已根据本准则发出证书予其中已辨识之登记人。

1.2.1.2 生效

香港邮政将于储存库公布经由登记人接受并已发出之认可证书。 （见第 2.5 条）

1.2.1.3 香港邮政进行分包合约之权利

只要分包商同意与香港邮政签订合约承担有关职务，香港邮政可把履行本准则及登记人协议之部分或全部工作之义务，批予分包商执行。无论有关职务是否批出由分包商执行，香港邮政仍会负责履行本准则及登记人协议。

1.2.2 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。

1.2.3 最终实体

根据本核证作业准则，存在两类最终实体，包括登记人及倚据证书人士。登记人指于**附录 A** 内所指的 “登记人”或 “登记人机构”。倚据证书人士乃倚据香港邮政发出之任何类别或种类政府电子证书用于**附录 H** 内所指的指定应用之交易的人士。特此澄清，倚据证书人士不应倚据政策局/部门/办公室或承办商。香港邮政透过政策局/部门/办公室或承办商发出政府电子证书，政策局/部门/办公室及承办商对倚据证书人士并无任何谨慎职责，亦不需对倚据证书人士就发出政府电子证书而负责（见第 2.1.4 条）。于**附录 H** 内所指的指定应用之交易中依据其他登记人政府电子证书之登记人乃为有关此证书之倚据证书人士。

1.2.3.1 登记人之保证及陈述

每位申请人（如申请政府电子证书，提出要求者会代表申请人）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（尤其是倚据证书人士）作出陈述，在证书之有效期间，以下事实乃属真实并将保持真实：

a) 证书已被接受并在有效期内正常运作，使用对应于包含在证书内的公开密码匙的私人密码匙进行指定应用乃登记人自己的行为；
b) 证书所载之所有资料及由登记人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) 登记人将会在**附录 H** 内所指的指定应用中使用证书;

e) 登记人同意本作业准则的条款和条件以及香港邮政的其他协议和政策声明;
f) 登记人已授权中央管理通讯系统在**附录 H** 内所指的指定应用中取阅登记人证书的私人密码匙;
g) 在证书申请过程中所提供之所有资料，均并无侵犯或违反任何第三方之商标、服务标记、品牌、公司名称或任何知识产权。

1.2.4 登记人之类别

根据本准则香港邮政仅发出证书予其申请已获批准并已以适当形式确定接受登记人协议之申请人士。

1.2.4.1 政府電子證書（個人）

政府电子证书 (个人)发给政策局/部门/办公室（即**附录E**内所列出的「登记人机构」）之下的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申请人士。

此类型证书仅限在中央管理通讯系统中使用：

a) 加密、解密和签署电子信息;
b) 签署文件;
c) 在中央管理通讯系统内进行身分认证；及
d) 就中央管理通讯系统与其他机构交换信息方面，发出认收信息并附加其数码签署以证实其收件者身分，藉此确认已收讫送出之加密信息。

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E**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加密、解密和签署电子信息，签署文件，在中央管理通讯系统中进行认证及数码签署以外，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。

证书产生的签署并不旨在用作《电子交易条例》("ETO") (第553章) 所定义之交易的数码签署。

1.2.4.2 政府電子證書（功能单位）

政府电子证书（功能单位）发给政府政策局/部门/办公室（即**附录E**内所列出的「登记人机构」）之下的中央管理通讯系统功能单位; 并识别已获该登记人机构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申请人士。

此类型证书仅限在中央管理通讯系统中使用：

a) 加密和解密电子信息； 及
b) 发出认收信息并附加其数码签署以证实其收件者（收件者为功能单位）身分，藉此确认已收讫送出之加密信息。

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E**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加密和解密电子信息及数码签署以外，不会授权予中央管理通讯系统用户使用政府电子证书（功能单位）于任何其他用途。

证书产生的签署并不旨在用作《电子交易条例》("ETO") (第553章) 所定义之交易的数码签署。

1.2.5 证书之期限

证书的有效期由产生自香港邮政系统当日起即日生效。

政府电子证书（个人）的证书有效期范围为一年至二年。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）的证书有效期范围为一年至二年。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。

根据本核证作业准则发出之电子证书会根据不同登记人机构有不同之有效期。香港邮政将同意该登记人机构为该机构用户所申请的政府电子证书之有效期。**附录G**内列出证书的有效期（有关证书续期，请参阅第3.2条）。

1.2.6 透过中央管理通讯系统进行申请

所有首次申请及政府电子证书撤销或到期后之新政府电子证书申请，提出要求者须依据本作业准则第 3 及 4 条指明的程序透过中央管理通讯系统代表申请人递交申请。

1.3 联络资料

登记人可经由以下途径作出查询、建议或投诉：

邮寄地址：东九龙邮政信箱 68777 号香港邮政核证机关
电话 ：2921 6633
传真 ：2775 9130

电邮地址：enquiry@eCert.gov.hk

1.4 处理投诉程序

香港邮政会尽快处理所有以书面及口头作出的投诉，并在收到投诉后七个工作天内给予详细的答复。若七个工作天内不能给予详细的答复，香港邮政会向投诉人作出简覆。在可行范围内，香港邮政人员会于收到投诉后尽快以电话、电邮或信件与投诉人联络确认收到有关投诉及作出回复。

2. 一般规定

2.1 义务

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

2.1.1 核证机关之义务

根据条例，香港邮政为认可核证机关，负责使用稳当系统发出、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) 透过中央管理通讯系统接受电子证书申请；
b) 透过中央管理通讯系统处理电子证书申请；
c) 根据递交的签发证书要求，发出电子证书，并于储存库公布电子证书；
d) 透过中央管理通讯系统通知申请人有关已批准或被拒绝的申请；
e) 撤销证书并依时公布证书撤销清单，及
f) 透过中央管理通讯系统通知或直接通知登记人有关已撤销的证书。

2.1.2 承办商之义务

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

2.1.3 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)，当中包括了于申请人提交申请时与中央管理通讯系统资料吻合的申请人相关资料，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) 确保登记人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登记人和/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) 在登记人被允许于指定应用中使用政府电子证书前，核实登记人的身份；
m) 分配独特的身份号码给申请人/登记人，此号码于递交政府电子证书申请时用来引用申请人/登记人资料, 其必须与登记人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，则确保该政府电子证书不会用于进行或者完成指定应用；
o) 遵守香港邮政不时发出的所有通知，指示及守则；及
p) 遵守本作业准则。

2.1.4 政策局/部门/办公室之义务

政策局/部门/办公室负责：

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。

2.1.5 登记人之义务

登记人负责:

a) 同意中央管理通讯系统，在硬体安全模组和中央管理通讯系统处所内的环境下代表登记人产生配对密码匙；
b) 准确地按照本准则所载之程序直至证书过期；
c) 不时将与证书有关之登记人资料之任何变动通知核证登记机关；
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核证登记机关；
e) 同意其透过获发出或接受证书向香港邮政保证（承诺）并向所有倚据证书人士表明，在证书之有效期间，以上第1.2.3.1条载明之事实乃属真实并将一直保持真实；
f) 在登记人明知香港邮政，或代表香港邮政的承办商或核证登记机关根据准则条款可能据以撤销证书之任何事项之情况下，或登记人已作出撤销申请或经香港邮政，或代表香港邮政的承办商或核证登记机关所知会，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。
g) 在明知香港邮政，或代表香港邮政的承办商或核证登记机关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或代表香港邮政的承办商或核证登记机关知会拟撤销证书时，须立即通知从事当时仍有待完成之任何交易之倚据证书人士，用于该交易之证书须予撤销(由香港邮政或经登记人申请)，并明确说明，因情形乃属如此，故倚据证书人士不得就交易而倚据证书；及
h) 承认知悉一经递政府电子证书申请表，即批准向其他人或在香港邮政储存库公布其政府电子证书。

2.1.5.1 登记人之责任

各登记人承认，若上述义务未得以履行，则根据登记人协议及/或法例，各登记人有或可能有责任向香港邮政及/或其他人士(包括倚据证书人士)就可能因此产生之责任或损失及损害赔偿损失。

2.1.6 倚据人士之义务

倚据政府电子证书之倚据证书人士负责：

a) 倚据证书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) 于倚据该等政府电子证书前，确定使用政府电子证书乃适合**附录H**规定之相关指定应用之用途，而承办商或中央管理通讯系统并不对倚据证书人士承担任何谨慎职责。
c) 承认知悉若政府电子证书在**附录H**规定之指定应用以外的任何应用中被使用或作为依据，香港邮政、中央管理通讯系统或承办商将不对倚据证书人士承担任何责任或谨慎职责。
d) 于倚据证书前查核证书撤销清单上之证书状态。
e) 执行所有适当证书路径认可程序。

2.2 其他规定

香港邮政对登记人及倚据人士之义务

2.2.1 合理技术及谨慎

香港邮政谨此与各登记人协议，根据本准则香港邮政、承办商及代表香港邮政之核证登记机关向各登记人及倚据证书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证书人士承担任何绝对义务。**香港邮政不保证香港邮政、承办商、中央管理通讯系统或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、中央管理通讯系统或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证书人士、或非登记人的倚据证书人士，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，各登记人及各倚据证书人士同意香港邮政、邮政署、承办商、中央管理通讯系统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、中央管理通讯系统或代表香港邮政之核证登记机关已采取合理程度之技术及谨慎之前提下，若登记人或倚据证书人士因倚据另一登记人由香港邮政所发出之政府电子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、中央管理通讯系统或核证登记机关概不负责。

亦即如在香港郵政（郵政署、承辦商、中央管理通訊系統或核證登記機關）已採取合理程度之技術或謹慎以避免及/或減輕無法控制事件後果之前提下，若登記人或倚據證書人士因香港郵政不能控制之情況遭受不良影響，香港郵政、郵政署、承辦商、中央管理通訊系統或任何核證登記機關概不負責。香港郵政控制以外之情況包括但不限於互聯網或電訊或其他基礎建設系統之可供使用情況，或天災、戰爭、軍事行動、國家緊

急狀態、疫症、火災、水災、地震、罷工或暴亂或其他登記人或其他第三者之疏忽或蓄意不當行為。

2.2.2 非商品供应

特此澄清，登记人协议并非任何性质商品之供应合约。任何及所有据此发出之证书持续为香港邮政之财产及为其拥有且受其控制，证书中之权利、所有权或利益不得转让于登记人，登记人仅有权申请获发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证书人士接达之公开储存库内提供之证书，并非作为对倚据证书人士供应任何商品；亦不会作为对倚据证书人士关于证书为某一特定目的之可商售性或适用性的保证；亦不会作为向倚据证书人士作出供应商品的陈述或保证。香港邮政虽同意将上述物品转让予申请人或登记人作本准则指定用途；但亦合理谨慎确保此等物品适合作本准则所述完成及接受证书之用途。若未能履行承诺，香港邮政须承担下文第 2.2.3-2.2.4 条所述责任。另外，由香港邮政转让的物品可内载其他与完成及接受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。

2.2.3 法律责任限制

2.2.3.1 限制之合理性

各登记人或倚据人士必须同意，香港邮政按本登记人协议及准则所列条件限制其法律责任实属合理。

2.2.3.2 可追讨损失种类之限制

在香港邮政违反：

a) 本登记人协议；或
b) 任何谨慎职责－尤其当登记人或倚据证书人士、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，为登记人或倚据证书人士，而采取合理技巧及谨慎及/或职责；

的情况下，而登记人或倚据证书人士（无论作为根据准则或以其他任何方式定义之登记人或倚据证书人士）蒙受损失及损害，**香港邮政概不负责关乎下述原因之赔偿或其他补救措施：**

a) **任何直接或间接利润或收入损失、信誉或商誉损失或伤害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；或**
b) **任何间接、相应而生或附带引起之损失或损害，而且即使在后者情况下，香港邮政已获提前通知此类损失或损害之可能性。**

2.2.3.3 限额 -- 20 万港元

除下文所述例外情况外，在香港邮政违反：

a) **本登记人协议及核证作业准则条文；或**
b) **任何谨慎职责－尤其当登记人或倚据证书人士、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，为登记人或倚据证书人士，采取合理技巧或谨慎及/或**

职责；

之情况下，而登记人或倚据证书人士蒙受损失及损害（无论作为根据准则或以其他任何方式定义之登记人或倚据证书人士），对于任何登记人、或任何倚据证书人士（无论作为根据准则或以其他任何方式定义之登记人或倚据证书人士或以任何其他身分），香港邮政所负法律责任限制于且任何情况下每份政府电子证书不得超过 20 万港元。

2.2.3.4 提出索償之時限

任何登记人或倚据证书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、撤销或公布政府电子证书相关，则应在登记人或倚据证书人士察觉其有权提出此等索偿的事实之日起一年内、或透过行使合理努力其有可能清楚此等事实之日起一年内（若更早）提出。特此澄清，不知晓此等事实之法律重要性乃无关重要。一年期限届满时，此等索偿必须放弃且绝对禁止。

2.2.3.5 香港郵政署、承辦商、中央管理通訊系統、核證登記機關及各自之人員

无论香港邮政署、承办商、中央管理通讯系统或任何核证登记机关或其各自之任何职员、雇员或其他代理人均非登记人协议之签约人，登记人及倚据证书人士必须向香港邮政承认，就登记人及倚据证书人士所知，香港邮政署、承办商、中央管理通讯系统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、或倚据证书人士担负任何个人责任或谨慎职责；每一位登记人及倚据证书人士接受并将继续接受此点，并向香港邮政保证不起诉或透过任何其他法律途径对前述任何关于该人出于真诚（不论是否出于疏忽）、并与香港邮政履行本登记人协议或由香港邮政作为核证机关发出之任何证书相关，而作出的行动或遗漏事项寻求任何形式之追讨或纠正，并承认香港邮政享有充分法律及经济利益以保护香港邮政署及上述机构及个人免受此等法律行动。

2.2.3.6 蓄意之不当行为或个人伤亡之责任

任何因欺诈或蓄意之不当行为或个人伤亡之责任均不在本准则、登记人协议或香港邮政发出之证书之任何限制或除外规定范围内，亦不受任何此等规定之限制或被任何此等规定免除。

2.2.3.7 证书通知、限制及倚据限额

香港邮政发出之政府电子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 电子交易条例(第 553 章)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 http://www.eCert.gov.hk）。香港特别行政区法律适用于本证书，倚据证书人士须提交因倚据本证书而引致之任何争议或问题予香港特别行政区法庭之非专有司法管辖权。*
>
> *倘阁下为倚据证书人士而不接受本证书据以发出之条款及条件，则不应倚据本证书。*
>
> *香港邮政署长（经香港邮政署、承办商，其各自职员、雇员及代理人，包括但不限于核证登记机关）发出本证书，但无须对倚据证书人士承担任何责任或谨慎*

职责（此准则中列明者除外）。

倚据证书人士倚据本证书前负责：

a. *只有当倚据证书人士于倚据时所知之所有情况证明倚据行为乃属合理及本着真诚时，方可倚据本证书；*
b. *倚据本证书前，确定证书之使用就准则规定用于相关之指定应用之之用途而言乃属适当；*
c. *承认知悉若倚据证书人士倚据本政府电子证书用于准则**附录H**内所指相关之登记人机构相关之指定应用以外的任何应用，香港邮政署长、香港邮政署、承办商、中央管理通讯系统，任何核证登记机关及其各自职员、雇员及代理人将不对倚据证书人士承担任何责任或谨慎职责；*
d. *倚据本证书前，根据证书撤销清单检查本证书之状态；及*
e. *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、中央管理通讯系统、任何核证登记机关及其各自职员、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、中央管理通讯系统、任何核证登记机关及其各自职员、雇员或代理人对倚据证书人士之任何损失或损害概不承担任何责任，在该等情况下根据条例适用于本证书之倚据限额为 0 港元。

若本证书在任何方面不准确或误导，而该等不准确或误导乃因香港邮政署长、香港邮政署、承办商、中央管理通讯系统、任何核证登记机关及其各自职员、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证书人士支付最多 20 万港元，惟该等损失不属于及不包括（1）任何直接或间接利润或收入损失、信誉或商誉损失或伤害、任何商机或契机、失去工程或失去或无法使用任何数据、设备或软件或（2）任何间接、相应而生或附带引起之损失或损害，而且即使在后者情况下，香港邮政已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，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、中央管理通讯系统、任何核证登记机关及其各自职员、雇员或代理人概不对倚据证书人士就本证书承担任何谨慎职责。

索赔时限
任何倚据证书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、撤销或公布本政府电子证书相关，则应在倚据证书人士知悉存在任何有权提出此等索偿事实之日起一年内或透过行使合理努力彼等有可能知悉此等事实之日起一年内（若更早）提出。特此澄清，不知晓此等事实之法律重要性乃无关重要。一年期限届满时，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、中央管理通讯系统、任何登记机关或其职员、雇员或代理人作出之故意或罔顾后果之失实陈述，则本证书并不就彼等对因合理倚据本证书中之失实陈述而遭受损失之倚据证书人士所应承担之法律责任作出任何限制。

本文所载之法律责任限制不适用于个人伤害或死亡之（不大可能发生之）情形。”

2.2.4 香港邮政对已获接收但有缺陷之电子证书所承担之责任

尽管上文已列明香港邮政承担责任之限制，若政府电子证书对应之登记人接收证书后发现，因证书内之私人密码匙或公开密码匙出现差错，导致基于公匙基建预期之交易无法适当完成或根本无法完成，则登记人须将此情况立即通知香港邮政，以便撤销证书及（如愿意接受）重新发出。或倘此通知已于接收证书后三个月内发出且登记人不再需要证书，则香港邮政若同意确有此差错将进行退款。倘登记人于接收证书三个月过后方将此类差错通知香港邮政，则费用不会自动退还，而由香港邮政酌情退回。

2.2.5 登记人的转让

登记人不可转让登记人协议或证书赋予之权利。拟转让之行为均属无效。

2.2.6 陈述权限

除非获得香港邮政授权，香港邮政署、承办商或任何核证登记机关之代理人或雇员无权代表香港邮政对本准则之意义或解释作任何陈述。

2.2.7 更改

香港邮政有权更改本准则，而无须发出预先通知(见第 8 条)。登记人协议不得作出更改、修改或变更，除非符合本准则中之更改或变更规定，或获得香港邮政署长之明确书面同意。

2.2.8 保留所有权

根据本准则发出之证书上所有资料之实质权利、版权及知识产权现属香港邮政所有，日后亦然。

2.2.9 条款冲突

倘本准则与登记人协议或其他规则、指引或合约有冲突，登记人、倚据证书人士及香港邮政须受本准则条款约束，除非该等条款受法律禁止。

2.2.10 受信关系

香港邮政、承办商、中央管理通讯系统或任何核证登记机关并非登记人或倚据证书人士之代理人、受信人、受托人或其他代表。登记人及倚据证书人士无权以合约或其他方式约束香港邮政、承办商、中央管理通讯系统或任何核证登记机关承担登记人或倚据证书人士之代理人、受信人、受托人或其他代表之责任。尤其代表登记人之中央管理通讯系统之“ 提出要求者”绝对不可作为中央管理通讯系统之“业务管理人员”（即核证登记机关之成员），而中央管理通讯系统之“业务管理人员”（即核证登记机关之成员）亦绝对不可作为代表登记人之中央管理通讯系统之“ 提出要求者”。

2.2.11 相互核证

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

2.2.12 财务责任

保单已经备妥，有关证书之潜在或实质责任以及对倚据限额之索偿均获承保。

2.3 解释及执行（管辖法律）

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

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

2.3.3 争议解决程序
香港邮政关于本准则范围内之事宜之决定为最终决定。如有索偿，请送交下列地址：

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

2.3.4 诠释
本准则中英文本措词诠释若有歧异，以英文本为准。

2.4 登记费用

除获得香港邮政豁免，政府电子证书登记人需缴交证书登记费用。关于政府电子证书登记费用的详细资料，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**附录 H** 内所列出之政府电子证书之登记费用。

2.5 公布资料及储存库

根据条例之规定，香港邮政维持一储存库，内有根据本核证作业准则签发并已经由登记人接受的证书清单、最新证书撤销清单，香港邮政公开密码匙、本准则文本一份以及与本准则政府电子证书有关之其他资料。除平均每周两小时之定期维修及紧急维修外，储存库基本保持每日 24 小时、每周 7 日开放。香港邮政会把经由登记人接受并按本准则确认接受的电子证书，尽快在储存库作出公布。香港邮政储存库可透过下述 URL 接达：

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

或

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

2.5.1 证书储存库控制
储存库所在位置可供在线浏览，并可防止擅进。

2.5.2 证书储存库进入要求
经授权之香港邮政人士方可进入储存库更新及修改内容。

2.5.3 证书储存库更新周期
每份证书一经登记人接受及发出后，以及如更新证书撤销清单等其他相关情况时，储存库会尽快作出更新。

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

2.6 遵守规定之评估

须根据条例以及认可核证机关守则之规定，至少每 12 个月进行一次遵守规定之评估，检视香港邮政发出、撤销及公布政府电子证书之系统是否妥善遵守本准则。

2.7 机密性

在履行与香港邮政发出、撤销及公布政府电子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、中央管理通讯系统及核证登记机关均会依循此条限制事项。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；香港邮政需根据本准则履行其责任之情况除外。除非经法庭发出之传召或命令要求，或香港法例另有规定，否则未经登记人事先同意，不得将该等资料对外发布。除非法庭发出传票或命令，或香港法例另有规定，香港邮政尤其不得发表登记人清单或其资料，惟无法追溯个别人登记人之综合资料除外。

3. 鉴别及认证

3.1 首次申请

所有政府电子证书申请人须通透中央管理通讯系统提交申请。

提出要求者须登录中央管理通讯系统，并在中央管理通讯系统中为申请人完成并递交政府电子证书（个人）或政府电子证书（功能单位）证书申请或续期申请。如果业务管理人员要求，提出要求者亦须向业务管理人员提供证明文件，以便业务管理人员对申请人进行身份认证。

业务管理人员须登录中央管理通讯系统，验证申请人的身份并批准该要求。业务管理人员须核实经由提出要求者提供的政府电子证书（个人）申请人的证明文件。

中央管理通讯系统亦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/办公室系统接收证书申请要求，其要求包括了提出要求者和业务管理人员处理证书申请的工作流程资料。 中央管理通讯系统须对证书申请要求进行验证，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于政府处所内的安全环境下使用没有人为干扰的硬件安全模块（HSM）为申请人或功能单位制作私人密码匙及公开密码匙。

中央管理通讯系统须在安全的环境下产生包含公开密码匙的「签发证书要求」(CSR) 。

中央管理通讯系统须预备一份系统界面档案(system interface file)，该档案包含了申请的资料和其产生的签发证书要求，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产生政府电子证书，并以安全的网上方式传输至中央管理通讯系统，或由中央管理通讯系统以分批处理模式安全接收。

中央管理通讯系统须透过使用了TLS规约的专用及安全连接网络，从香港邮政核证机关接收包含政府电子证书的系统界面档案。

中央管理通讯系统须将政府电子证书连接至中央管理通讯系统用户或中央管理通讯系统功能单位，并通知所有曾参与完成申请过程的中央管理通讯系统用户。

香港邮政核证机关会在香港邮政核证机关储存库中公布该政府电子证书。

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在其身份证明文件显示之姓名或标识；
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。

3.1.1.2 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) 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；
b) 登记人机构内之功能单位之名称。

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

所采用名称之语义必须为一般人所能理解，方便辨识登记人身分。

3.1.3 诠释各个名称规则

香港邮政政府电子证书会载入之登记人名称(主体名称)类型见第 3.1.1 条。有关香港邮政政府电子证书主体名称之诠释应参照**附录 B**。

3.1.4 名称独特性

对登记人而言，主体名称 （于**附录 B** 内指明）应无歧义而具独特性。然而，此准则并不要求名称某一特别部分或成分本身具独特性或无歧义。

3.1.5 名称申索争议决议程序

香港邮政对有关名称争议之事宜的决定为酌情性及最终决定。

3.1.6 侵犯及违反商标注册

申请人及登记人向香港邮政保证（承诺）并向中央管理通讯系统、承办商及倚据证书人士申述，申请政府电子证书过程提供之资料概无以任何方式侵犯或违反第三者之商标权、服务商标、商用名称、公司名称或知识产权。

3.1.7 证明拥有私人密码匙之方法

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。

3.1.8 政府电子证书（个人）申请人身份认证

3.1.8.1 业务管理人员角色可以进一步根据本作业准则第 1.2.4.1 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 证书续期

3.2.1 政府电子证书

中央管理通讯系统会于证书的有效期届满前，向政府电子证书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。

政府电子证书不会自动续期。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。政府电子证书续期申请之身分认证会像新申请一样根据第 3.1.8 条“政府电子证书（个人）申请人身份认证”所述之程序进行认证。

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。

3.2.2 续期后之证书之有效期

因应香港邮政的酌情权，发出给登记人的新政府电子证书可由新证书产生日期起有效，而有效期会于原有证书（即须续期的证书）到期日再加上新证书有效期后届满。由此，新的政府电子证书的有效期可超过 1.2.5 条中指定的证书有效期，但不会超过该证书有效期加一个月。

4. 运作要求

4.1 证书申请

4.1.1 根据本核证作业准则发出之政府电子证书之申请人须透过中央管理通讯系统递交申请。中央管理通讯系统会传送申请予香港邮政。

4.1.2 政府电子证书申请要求一经中央管理通讯系统以电子方式递交，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政府电子证书，并接受香港邮政将发给申请人的政府电子证书。

4.1.3 用以证明申请人身分之文件，于本准则第 3.1.8 条（政府电子证书（个人）申请人身份认证）说明。

4.2 发出证书

4.2.1 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）。

4.2.2 政府电子证书会透过中央管理通讯系统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。

4.2.3 中央管理通讯系统同意，他们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，并且同意，他们将对由于任何情形引起的私人密码匙泄密所造成的任何后果负责。

4.2.4 所有存于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。

4.3 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 2.5 条）。申请人可浏览证书档案或经香港邮政储存库核实证书资料。一旦发现任何不正确的证书资料，登记人机构应立即通知香港邮政。

4.4 撤销证书

4.4.1 撤销证书的情况

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

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

登记人之私人密码匙或内载与某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，或政府电子证书上的登记人资料或其对应之中央管理通讯系统用户的职务有任何改变，各登记人必须立即按照本准则的撤销程序，向决策局／部门／办公室申请撤销证书（见第 2.1.5(e) 条）。

不论何时，若有以下情况，香港邮政和代表香港邮政的决策局／部门／办公室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) 知道或有理由相信政府电子证书上指明之中央管理通讯系统用户已非登记人机构的中央管理通讯系统用户；
h) 证书上指明之中央管理通讯系统用户已非担当登记人机构所提供的职务；
i) 知道或有理由相信其资料出现在政府电子证书上之登记人或中央管理通讯系统用户：
    (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) 其中央管理通讯系统用戶因欺詐、舞弊或不誠實行為，或違反電子交易條例被定罪；
    (iv) 在撤销证书前五年内登记人资产之任何部分托给接管人或管理人接管；或
    (v) 无法证明登记人之存在。

4.4.2 撤销程序请求

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。

中央管理通讯系统亦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(system interface file)，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）。

4.4.3 服务承诺及证书撤销清单的更新

a) 香港邮政将作出合理努力，确保在 (1) 香港邮政从决策局 / 部门 / 办公室核收到撤销证书申请或 (2) 在无此申请之情况下，香港邮政或决策局 / 部门 / 办公室决定撤销证书，两个工作日内，将该撤销证书资料于证书撤销清单公布。然而，证书撤销清单并不会于各证书撤销后随即在公众目录中公布。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。证书撤销清单每日公布，并存档最少七年。

   特此声明，星期六、星期日、公众假期及悬挂热带风暴及暴雨警告信号之工作日，就此 4.4.3（a）条而言，一律不视作工作日计算。

   香港邮政会以合理的方式，尽量在收到撤销证书申请两个工作天内，透过电子邮件（如有电子邮件地址）及更新证书撤销清单的方式向有关登记人发出撤销证书通知。

b) 在登记人明知香港邮政或决策局 / 部门 / 办公室根据准则条款可能据以撤销证书之任何事项之情况下，或登记人已作出撤销申请或经知会香港邮政或决策局 / 部门 / 办公室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，则香港邮政及决策局 / 部门 / 办公室毋须就任何该等交易向登记人或倚据证书人士承担责任。

c) 此外，登记人明知香港邮政或决策局 / 部门 / 办公室的核证登记机关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或决策局 / 部门 / 办公室拟撤销证书时，须立即通知从事当时仍有待完成之任何交易之倚据证书人士，用于该交易之证书须予撤销 (由香港邮政、决策局 / 部门 / 办公室、承办商、或经登记人申请)，并明确说明，因情况乃属如此，故倚据证书人士不得就交易而倚据证书。若登记人未能通知倚据人士，则香港邮政及决策局 / 部门 / 办公室无须就该等交易向登记人承担责任，并无须向虽已收到通知但仍完成交易之倚据证书人士承担责任。

   除非香港邮政或决策局 / 部门 / 办公室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证书人士，否则，香港邮政及决策局 / 部门 / 办公室的核证登记机关无须就香港邮政或决策局 / 部门 / 办公室作出撤销证书(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，决策局 / 部门 / 办公室自身无须对倚据证书人士承担独立谨慎责任（决策局 / 部门 / 办公室只是履行香港邮政之谨慎责任）。因此，即使出现疏忽，决策局 / 部门 / 办公室亦无须对倚据证书人士负责 。

d) 证书撤销清单会依据在**附录 C** 内指明的时间表及格式更新及公布。

e) 有关香港邮政对于倚据证书人士暂时未能获取撤销的证书资料时的政策，已列于本准则第 2.1.6 条(倚据证书人士之义务)及 2.2.1 条(合理技术及谨慎)。

4.4.4 撤销效力
在香港邮政把撤销状况刊登到证书撤销清单，即终止某一证书。

4.5 电脑保安审核程序

4.5.1 记录事件类型
香港邮政核证机关系统内之重要保安事件，均以人手或自动记录在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
  - 实际发出及撤销证书
  - 证书续期
  - 更新储存库资料
  - 汇编撤销证书清单并刊登新资料
  - 核证机关密码匙转换
  - 档案备存
  - 紧急密码匙复原

4.5.2 处理纪录之次数
香港邮政每日均会处理及覆检审核运行纪录，用以审核追踪有关香港邮政核证机关的行动、交易及程序。

4.5.3 审核纪录之存留期间
存档审核纪录文档存留期为七年。

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

4.5.5 审核纪录备存程序
香港邮政每日均会按照预先界定程序(包括多人式控制)为审核纪录作适当备存。备存会另行离机储存，并获足够保护，以免被盗用、损毁及媒体衰变。备存入档前会保留至少一星期。

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

4.5.7 事件主体向香港邮政发出通知
香港邮政拥有自动处理系统，可向适当人士或系统报告重要审核事件。

4.5.8 脆弱性评估
脆弱性评估为香港邮政核证机关保安程序之一部份。

4.6 纪录存档

4.6.1 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
- 定期事件纪录
- 其他需用以核实存档内容之数据

4.6.2 存档保存期限
密码匙及证书资料之存档须妥为保存最少七年。审核跟踪文档须以香港邮政视为适当之方式存放于系统内。

4.6.3 存档保护
香港邮政保存之存档媒体受各种实体或加密措施保护，可避免未经授权进入。保护措施用以保护存档媒体免受温度、湿度及磁场等环境侵害。

4.6.4 存档备份程序
在有需要时制作并保存存档之副本。

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

4.7 密码匙变更

由香港邮政产生，并用以证明根据本准则发出的签约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 G**）。香港邮政核证机关密码匙及证书在期满前至少三个月会进行续期。续发新根源密码匙后，相应之根源证书会在香港邮政网页 http://www.eCert.gov.hk 公布供大众取用。原先之根源密码匙则保留至第 4.6.2 条指定之最短之时限，以供核对用原先密码匙进行产生之签署。

4.8 灾难复原及密码匙资料外泄之应变计划

4.8.1 灾难复原计划
香港邮政已备有妥善管理之程序，包括每天为主要业务资讯及核证系统的资料备存及适

当地备存核证系统的软件，以维持主要业务持续运作，保障在严重故障或灾难影响下仍可继续业务。业务持续运作计划之目的在于促使香港邮政核证机关全面恢复提供服务，内容包括一个经测试的独立灾难复原基地，而该基地现时位于香港特别行政区内并距离核证机关主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。

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。

4.8.2 密码匙资料外泄之应变计划

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

如根据本准则签发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。

4.8.3 密码匙的替补

倘若在密码匙资料外泄或灾难情况下，香港邮政根据本准则签发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。

4.9 核证机关终止服务

如香港邮政停止担任核证机关之职能，即按“香港邮政终止服务计划”所定程序知会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。

4.10 决策局 / 部门 / 办公室的核证登记机关终止服务

如决策局 / 部门 / 办公室的核证登记机关被香港邮政或因核证机关终止服务（第 4.9 条）停止担任核证登记机关之职能，或其授权已予以收回，经由该决策局 / 部门 / 办公室的核证登记机关申请之政府电子证书仍会按其条款及有效期继续有效。

5. 实体、程序及人员保安控制

5.1 实体保安

5.1.1 选址及建造
香港邮政核证机关运作位于商业上具备合理实体保安条件之地点。在场地建造过程中，香港邮政已采取适当预防措施，为核证机关运作作好准备。

5.1.2 进入控制
香港邮政实施商业上具合理实体保安之控制，限制进入就提供香港邮政核证机关服务而使用之硬件及软件（包括核证机关伺服器、工作站及任何外部加密硬件模组或受香港邮政控制之权标）。可使用该等硬件及软件之人员只限于本准则第 5.2.1 条所述之履行受信职责之人员。在任何时间都对该等进入进行控制及人手或电子监控，以防发生未经授权入侵。

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

5.1.4 自然灾害
核证机关设施在合理可能限度内受到保护，以免受自然灾害影响。

5.1.5 防火及防水处理
核证机关设施备妥防火计划及灭火系统。

5.1.6 媒体存储
媒体存储及处置程序已经开发备妥。

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

5.1.8 保管印刷文件
用于验证申请人的身分证明由决策局 / 部门 / 办公室妥為保存。獲授權人員方可以取閱該等紀錄。

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。

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

5.2.2 香港邮政、承办商、中央管理通讯系统与核证登记机关之间的文件及资料传递

香港邮政、承办商、中央管理通讯系统与核证登记机关之间的所有文件及资料的传递，均使用香港邮政所惯常规定在控制及安全的方式进行。

5.2.3 年度评估

评估工作每年执行一次，以确保符合政策及工作程序控制之规定。（见第 2.6 条）

5.3 人员控制

5.3.1 背景及资格

香港邮政及承办商采用之人员及管理政策可合理确保香港邮政、承办商或核证登记机关的人员，包括雇员、承包商及顾问之可信程度及胜任程度，并确保他们以符合本准则之方式履行职责及表现令人满意。

5.3.2 背景调查

香港邮政对担任受信职责之人员进行调查（其受聘前及其后有需要时定期进行），及/或香港邮政要求承办商、中央管理通讯系统及核证登记机关进行调查，以根据本准则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。

5.3.3 培训要求

香港邮政、承办商、中央管理通讯系统及核证登记机关人员已接受履行其职责所需要之初步培训。有需要时香港邮政及承办商亦会提供持续培训，使其各自人员能掌握所需最新工作技能。

5.3.4 向人员提供之文件

香港邮政、承办商、中央管理通讯系统及核证登记机关人员会收到综合用户手册，详细载明证书之制造、发出、更新、续期及撤销程序及与其职责有关之其他软件功能。

6. 技术保安控制

本条说明香港邮政特别为保障加密密码匙及相关数据所订之技术措施。控制香港邮政核证机关密码匙之工作透过实体保安及稳妥密码匙存储进行。产生、储存、使用及毁灭香港邮政核证机关密码匙只能在由多人式控制之可防止篡改硬件装置内进行。

6.1 密码匙之产生及安装

6.1.1 产生配对密码匙

除非程序被中央管理通讯系统用户外泄，否则香港邮政配对密码匙之产生程序可使配对密码匙的中央管理通讯系统用户以外人士无法取得私人密码匙。香港邮政产生配对根源密码匙，用以发出符合本准则之证书。

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) 为申请人/登记人代制配对密码匙，以确保私人密码匙不被篡改。

6.1.2 登记人公开密码匙交付

中央管理通讯系统会以硬件安全模块(HSM)代表申请人 / 登记人生产配对密码匙。登记人之公开密码匙须连同签发证书要求送递至香港邮政以产生证书。香港邮政将使用方法以确保：

- 公开密码匙在传输过程中不会被更改；及
- 发送人拥有与传送的公开密码匙对应的私人密码匙。

6.1.3 公开密码匙交付予倚据证书人士

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。

6.1.4 密码匙大小

香港邮政之签署配对密码匙为 2048 位元 RSA。政府电子证书登记人配对密码匙为 2048 位元 RSA。

6.1.5 加密模组标准

香港邮政进行之产生签署密码匙、存储及签署操作在硬件加密模组进行 。

6.1.6 密码匙用途

香港邮政政府电子证书之密码匙可用于**附录 H** 内所指的指定应用之数码签署及数据加密。香港邮政根源密码匙（用于制造或发出符合本准则证书之密码匙）只用于签署(a)证书及(b)证书撤销清单。

6.2 私人密码匙保护

6.2.1 加密模组标准

香港邮政私人密码匙利用加密模组产生，其级别至少达到 FIPS 140-1 第 3 级。

6.2.2 私人密码匙多人式控制

香港邮政私人密码匙储存在可防止篡改加密硬件装置内。香港邮政采用多人式控制启动、

使用、终止香港邮政私人密码匙。

6.2.3 私人密码匙托管

香港邮政使用之电子证书系统并无为香港邮政私人密码匙及登记人私人密码匙设计私人密码匙托管程序。有关香港邮政私人密码匙的备存，见第 6.2.4 条。

6.2.4 香港邮政私人密码匙备存

香港邮政私人密码匙的备存，是使用达到 FIPS 140-1 第 2 级保安标准的装置加密及储存。香港邮政私人密码匙的备存程序须经超过一名人士参与完成。备存的私人密码匙亦须超过一名人士启动。其他私人密码匙均不设备存。所有私人密码匙不会存档。

6.3 配对密码匙管理其他范畴

香港邮政核证机关根源密码匙使用期不超过由香港邮政产生之签署根源密码匙及证书的有效期（见**附录 G** 及第 4.7 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 4.6 条详述香港邮政公开密码匙纪录存档之工作。

6.4 电脑保安控制

香港邮政实行多人控制措施，控制启动数据（如个人辨识密码及接达核证机关系统密码的生命周期）。香港邮政已制定保安程序，防止及侦测未获授权进入核证机关系统、更改系统及系统资料外泄等情况。此等保安控制措施接受第 2.6 条遵守规定之评估。

6.5 生命周期技术保安控制

香港邮政制定控制程序，为香港邮政核证机关系统购置及发展软件及硬件。并已定下更改控制程序以控制并监察就有关系统部件所作的调整及改善。

6.6 网络保安控制

香港邮政核证机关系统有防火墙以及其他接达控制机制保护，其配置只允许已获授权使用本准则所载核证机关服务者接达。

6.7 加密模组工程控制

香港邮政使用之加密装置至少达到 FIPS140-1 第 2 级。

7. 证书及证书撤销清单结构

7.1 证书结构

本准则提及之证书内有用于确认电子讯息发送人身分及核实该等讯息是否完整之公开密码匙（即用于核实数码签署之公开密码匙）。本准则提及之证书一律以 X.509 第三版本之格式发出（见**附录 B**）。**附录 D** 载有各类香港邮政政府电子证书之特点摘要。

7.2 证书撤销清单结构

香港邮政证书撤销清单之格式为 X.509 第二版本（见**附录 C**）。

8. 准则管理

本准则之更改一律须经香港邮政核准及公布。有关准则一经香港邮政在网页 http://www.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。申请人、登记人及倚据证书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。

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) 在某人在該證書內指名或識別為獲發給該證書的人的情況下，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”指中央管理通讯系统用户 或决策局 / 部门 / 办公室的功能单位并已申请政府电子证书。政府电子证书一旦成功申请及发出，申请人即为登记人。

″应用程式接口″指一个界定了中央管理通讯系统与指定决策局/部门/办公室系统之间互动的应用程式接口。 当指定决策局/部门/办公室管理其系统用户的账户时，中央管理通讯系统透过应用程式接口从决策局/部门/办公室系统接收用户的帐户资料。

“非對稱密碼系統”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。

“业务管理人员” 指中央管理通讯系统中的用户角色，负责核证申请人的身份（即担任核证登记机关）并批准中央管理通讯系统中的证书申请，续期和撤销要求。

“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”**指核證機關發出以指明其在發出證書時使用之作業實務及標準之準則。

“证书撤销清单”列舉證書發出人在證書原定到期時間前宣佈無效之公開密碼匙證書（或其他類別證書）之資料。

“签发证书要求”指中央管理通讯系统发送给香港邮政包含登记人公开密码匙的信息，以申请证书。

“中央管理通讯系统”指在**附录E**中列出由数字政策办公室集中管理和支援的平台，允许决策局 / 部门 / 办公室指定人员作预先设定的用户角色，管理密码匙及证书并存储在硬件安全模块（“HSM”），以执行本准则中所述的职责。

“中央管理通讯系统用户”指由数字政策办公室提供给决策局 / 部门 / 办公室用户登入中央管理通讯系

统并执行各种指定应用的帐户。

“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。

“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。

“指定应用”指**附件 H** 内列明的登记人机构（若有的话）的相关之可使用政府电子证书的系统或服务。

“数码签署”就电子纪录而言，指签署人之电子签署，该签署用非对称密码系统及杂凑函数将该电子纪录作数据变换产生，使持有原本未经数据变换之电子纪录及签署人之公开密码匙者能据此确定：
(a) 该数据变换是否用与签署人之公开密码匙对应之私人密码匙产生；以及
(b) 产生数据变换后，原本之电子纪录是否未经变更。

“电子纪录”指资讯系统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。

“硬件安全模块” 指用于存储和管理证书以及保护密码匙不被篡改，导出或复制的硬件安全设备。

“资讯”包括资料、文字、影像、声音编码、电脑程式、软件及资料库。

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

“发出”就证书而言，指
(a) 制造该证书，然后将该证书包含的关于在该证书内指名或识别为获发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。

“条例”指香港法例第 553 章《电子交易条例》。

“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碼匙。

“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”指由香港邮政核证机关委任之机构（列载于**附录 E**，若有的话），按照此核证作业准则所详述核实申请人身份。

“倚据限额”指就认可证书倚据而指明之金钱限额。

“**倚据证书人士**”指在登记人机构指定应用之授权交易中倚据任何类别或级别的政府电子证书的自然人或法人。

“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”指在中央管理通讯系统中为需要证书的中央管理通讯系统用户（申请人）提出证书申请、续期和撤销要求之用户角色。拥有此角色的中央管理通讯系统用户也可以为自己提出证书要求。

“角色”指证记人机构援予中央管理通讯系统用户的职能或责任。

“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。

“中继证书”指由根源证书"Hongkong Post Root CA 2"所签发的中继核证机关证书，并用于签发香港邮政认可证书。

“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”指决策局 / 部门 / 办公室之下的中央管理通讯系统用户或功能单位：

(i) 在某证书内指名或或识别为决策局 / 部门 / 办公室的人士或功能单位而获发给证书；
(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；

注解 * :-“持有 " 对私人密码匙而言，指私人密码匙已为其保管，及只有该证书内指名或识别为获发给证书的人士可以使用该证书内的公开密码匙对应之私人密码匙，并且该名人士已获其登记人机构授权成为中央管理通讯系统用户。

“**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**” 指决策局 / 部门 / 办公室；而其提出要求者已签署登记人协议，及根据此核证作业准则，该决策局 / 部门 / 办公室为合资格并获发出政府电子证书之机构。

“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 。

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。

附錄 B

附录 B - 香港邮政政府电子证书格式

本附錄詳述由中繼證書“Hongkong Post e-Cert CA 2 - 17”根據本核證作業準則簽發的政府電子證書（個人）及政府电子证书（功能单位）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 e-Cert CA 2 – 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=[中央管理通讯系统用户姓名]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人机构分行/部门名称] ou=[登记人机构名称] ou=[分行/部门名称缩写] ou=[登记人参考编号]（附注3） o= Hongkong Post g-Cert (Individual) c=HK
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元
发出人识别名称 (Issuer unique identifier)		未使用
登记人识别名称 (Subject unique identifier)		未使用
标准延伸栏位 (Standard extension)（附注4）		
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	序号 (Serial number)	[从发出人处获取]
密码匙使用方法 (Key usage)		不可否认，数码签署，密码匙加密 **（此栏为“关键”栏位）**
证书政策 (Certificate policy)		Policy Identifier = [物件识别码]（附注 5） Policy Qualifier ID = CPS Qualifier : [核证作业准则的URL]

栏位名称		栏位内容
主体别名 (Subject alternative name)	DNS	未使用
	1st Directory Name	ou=[类别] (Note 6) ou=[登记人机构分行/部门中文名称] ou=[登记人机构中文名称]
	rfc822	[证书持有人电子邮箱地址]（附注2）
发出人别名 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	主体类型 (Subject type)	最终实体
	路径长度限制 (Path length constraint)	无
延伸密码匙使用方法 (Extended key usage)		SSL Client, S/MIME
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL]（附注7）

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（如没有电子邮箱地址，此栏将会留空）
3. 登记人参考编号： 10 位数字
4. 除非另外注明，所有标准延伸栏位均为“非关键”延伸栏位。
5. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅本准则第 1.1 条。
6. “类别” 指决策局 / 部门 / 办公室个别用户的类别。
7. 证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL2.crl，此为中继证书"Hongkong Post e-Cert CA2 - 17"所发出的「分割式证书撤销清单」。

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 e-Cert CA 2-17 o=Hongkong Post l=Hong Kong, s=Hong Kong, c=HK

栏位名称		栏位内容
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=[功能单位名称]（附注1） e=[电子邮箱地址]（附注2） ou=[登记人机构分行/部门名称] ou=[登记人机构名称] ou=[分行/部门名称缩写] ou=登记人参考编号(附注 3) o= Hongkong Post g-Cert (Functional Unit) c=HK
主体公开密码匙资料 (Subject public key info)		算式识别 (Algorithm ID)：RSA 公开密码匙 (Public key)：密码匙长度为2048位元
发出人识别名称 (Issuer unique identifier)		未使用
登记人识别名称 (Subject unique identifier)		未使用
标准延伸栏位 (Standard extension)（附注4）		
机关密码匙识别名称 (Authority key identifier)	**发出人 (Issuer)**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	序号 (Serial number)	[从发出人处获取]
密码匙使用方法 (Key usage)		数码签署，密码匙加密 **（此栏为“关键”栏位）**
证书政策 (Certificate policy)		Policy Identifier =[物件识别码]（附注 5） Policy Qualifier ID = CPS Qualifier : [核证作业准则的URL]
主体别名 (Subject alternative name)	**DNS**	未使用
	第一目錄名称 (First Directory Name)	**ou=[类别]** (附注 6) ou=[登记人机构分行/部门中文名称] ou=[登记人机构中文名称]
	rfc822	[证书持有人电子邮箱地址]（附注2）
发出人别名 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主体类型 (Subject type)**	最终实体
	路径长度限制 (Path length constraint)	无
延伸密码匙使用方法 (Extended key usage)		SSL client, S/MIME
证书撤销清单分发点 (CRL distribution point)		分发点名称 = [证书撤销清单分发点URL]（附注7）

附注：

1. 由登记人机构提供的功能单位名称。
2. 登记人机构提供之功能单位电子邮箱地址（如没有电子邮箱地址，此栏将会留空）
3. 登记人参考编号： 10 位数字
4. 除非另外注明，所有标准延伸栏位均为“非关键”延伸栏位。
5. 本栏已包括本核证作业准则的物件识别码 (Object Identifier, OID)。关于本准则的物件识别码，请参阅本准则第 1.1 条。
6. “类别” 指决策局 / 部门 / 办公室功能单位的用户类别。
7. 证书撤销清单分发点 URL 为 http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL2.crl ，此为中继证书"Hongkong Post e-Cert CA 2 - 17"所发出的「分割式证书撤销清单」。

附录 C - 香港邮政证书撤销清单(CRL) 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 - 17"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政府电子证书的资讯：

a) **「分割式证书撤销清单」(Partitioned CRL)** 包含分组已撤销证书的资料。公众可于下述位址(URL)获取相关的「分割式证书撤销清单」：

http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL2.crl

b) **「整体证书撤销清单」 (Full CRL)** 包含分别由中继证书"Hongkong Post e-Cert CA 2 - 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」：

http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL1.crl; 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 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 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。

（I） 由中继证书"Hongkong Post e-Cert CA 2 - 17"根据本准则发出的分割式及整体证书撤销清单格式:-

标准栏位 (Standard Fields)	子栏位 (Sub-fields)	分割式证书撤销清单栏位内容	整体证书撤销清单栏位内容	备注
版本 (Version)		v2		此栏显示证书撤销清单格式的版本为 X.509 第二版
签署算式识别 (Signature algorithm ID)		Sha256RSA		此栏显示用以签署证书撤销清单的算法的识别码
发出人 (Issuer name)		cn=Hongkong Post e-Cert CA 2 - 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

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
	撤销日期 (Revocation date)	[UTC 时间]		此栏显示撤销证书的时间
	证书撤销清单资料延伸栏位 (CRL entry extensions)			
	原因代码 (Reason code)	[撤销理由识别码]		（附注 1）
标准延伸栏位 (Standard extension) （附注 2）				
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	cn=Hongkong Post Root CA 2 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK		此栏提供有关资料以识别用作签署证书撤销清单的私人密码匙的配对公开密码匙。
	序号 (Serial number)	[发出人证书的序号]		此栏显示发出人证书的序号
证书撤销清单号码 (CRL number)		[由核证系统产生]		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） 由根源证书"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)	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 e-Cert CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	此栏显示签署及发出授权撤销清单的机构
此次更新 (This update)		[UTC 时间]	此栏显示本授权撤销清单的发出日期 (是次更新)
下次更新 (Next update)		[UTC 时间]	表示下次授权撤销清单将于显示的日期或之前发出 (下次更新)，而不会于显示的日期之后发出。根据核证作业准则的规定，授权撤销清单是每年更新及发出
撤销证书 (Revoked certificates)	用户证书 (User certificate)	[证书序号]	此栏列出已撤销证书的证书序号
	撤销日期 (Revocation date)	[UTC 时间]	此栏显示撤销证书的时间
	授权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）

标准栏位 (Standard Fields)	子栏位 (Sub-fields)	栏位内容	备注
标准延伸栏位 (Standard extension) （附注 2）			
机关密码匙识别名称 (Authority key identifier)	发出人 (Issuer)	cn=Hongkong Post Root CA 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	此栏提供有关资料以识别用作签署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
授权撤销清单号码 (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)		只显示用户证书=No 只显示核证机关证书=Yes 间接授权撤销清单=No **（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：

   0 = 未注明；1 = 密码资料外泄；2 = 核证机关资料外泄；3 = 联号变更；
   4 = 证书被取代；5 = 核证机关终止运作；6 = 证书被暂时吊销

   由于登记人无须提供撤销证书的原因，所以「原因代码」会以「0」表示（即「未注明」）。

2. 除非另外注明，所有标准延伸栏位均为 “非关键” (Non-Critical) 延伸栏位。

附录 D - 香港邮政政府电子证书 – 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 3.1.8 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。 ▪ 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）） ▪ **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 ▪ 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）） ▪ 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）） ▪ 由香港邮政核证机关系统产生的登记人参考编号
登记费用及有效期	证书有效期为一年到二年，请参阅**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 建筑署 审计署 医疗辅助队 屋宇署 政府统计处 行政长官办公室 特首政策组 政务司司长办公室 – 政府档案处 政务司司长办公室及财政司司长办公室 民众安全服务处 民航处 土木工程拓展署 公务员事务局 商务及经济发展局 公司注册处 政制及内地事务局 惩教署 文创产业发展处 文化体育及旅游局 香港海关 卫生署 律政司 发展局规划地政科 发展局工务科	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： – 根据第 3.1 条及第 4.1 条所述提供证书申请服务。 – 根据第 3.2 条所述提供证书续期请求服务。 – 根据第 4.4.1 条；第 4.4.2 条及第 4.4.3 条所述提供证书撤销请求服务。 – 根据第 5.1.8 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
渠务署		
教育局		
机电工程署		
环境及生态局		
环境保护署		
财经事务及库务局财经事务科		
财经事务及库务局库务科		
消防处		
食物环境卫生署		
政府飞行服务队		
政府化验所		
政府物流服务署		
政府产业署		
医务卫生局		
路政署		
民政事务总署		
民政及青年事务局		
香港金融管理局		
香港天文台		
香港警务处		
房屋局		
房屋署		
入境事务处		
廉政公署		
独立监察警方处理投诉委员会		
政府新闻处		
税务局		
创新科技及工业局		
创新科技及工业局 – 数字政策办公室		
创新科技及工业局 – 创新科技署		

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
知识产权署 投资推广署 薪谘会联合秘书处 司法机构 劳工及福利局 劳工处 土地注册处 地政总署 法律援助署 康乐及文化事务署 海事处 电影、报刊及物品管理办事处 通讯事务管理局办公室 申诉专员公署 破产管理署 规划署 邮政署 公务员敍用委员会 香港电台 差饷物业估价署 选举事务处 截取通讯及监察事务专员秘书处 保安局 社会福利署 香港特别行政区政府驻北京办事处 工业贸易署 运输及物流局 运输署 库务署 大学教育资助委员会秘书处		

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
水务署 在职家庭及学生资助事务处（学生资助处） 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： -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； -为证书申请，续期和撤销提供审批工作流程； -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； -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； -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： - 为中央管理通讯系统中用户角色作出定义，使策局 / 部门 / 办公室能指定人员作为核证登记机关以执行如第 2.1.3 条所述核证申请人身份。 - 如第 3.1.7, 3.2 及 4.2 所述产生密码匙。 -承担第 2.1.3 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

根源证书名称	有效期	备注
Hongkong Post Root CA 2	2015年9月5日 至 2040年9月5日	
Hongkong Post e-Cert CA 2 - 17	2017年8月12日 至 2032年8月12日	此中继证书由2019年7月19日开始发出认可政府电子证书给申请者。

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 年到 2 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。 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 1.3 条所列之途径向香港邮政核证机关作出查询。	第 1.2.4.1 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 年到 2 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 1.2.4.2 条所述政府电子证书（功能单位）的用途