认可核证机关
业务守则

由政府资讯科技总监根据
《电子交易条例》（第 553 章）
第 33 条刊登

二零零四年十二月公布

(第二．一版)

香港特别行政区政府
政府资讯科技总监办公室

修订史				
更改编号	修订说明	受影响的页数	版本编号	日期
1.	第二版至第二．一版的更新如下： • 修改第 1.9 段以反映版本编号的更新 • 因应《2004 年专业会计师(修订)条例》而修改第 12.4(a)段	 1 28	二．一	2004 年 12 月

目录

1 引言

1.1 认可核证机关业务守则(“业务守则”)是政府资讯科技总监(“总监”)根据《电子交易条例》(第553章)(“条例”)第33条刊登的。

1.2 本业务守则指明认可核证机关在执行其功能时须采用的标准及程序。本业务守则应与条例一并阅读。

1.3 总监根据条例第21条决定某申请人是否适合认可为认可核证机关时，须考虑该申请人是否有能力遵守本业务守则。

1.4 总监根据条例第22条对个别证书或某类型、类别或种类的证书批给认可时，须考虑该个别证书或该类型、类别或种类的证书是否或会否由某认可核证机关按照本业务守则发出。

1.5 总监根据条例第22、23、24或27条可考虑因某认可核证机关未能遵守本业务守则而暂时吊销或撤销以下认可或不将其续期：批给该核证机关的认可，或对由该认可核证机关发出或拟发出的个别证书或某类型、类别或种类证书批给的认可(视乎属何种情况而定)。

1.6 如本业务守则任何部分与条例内的任何条文不符，则以条例内的有关条文为准。

1.7 总监会不时对本业务守则作出修订，并可就日后的修订项目谘询业界(包括根据条例第21及34条认可的核证机关）。谘询业界的主要渠道是透过认可核证机关业务守则谘询委员会。该委员会由总监担任主席。

1.8 本业务守则的中文与英文版本之间如出现差异而引起任何冲突，须以英文版本为准。

1.9 业务守则第二.一版取代2004年7月出版的业务守则第二版。

2 用语定义

2.1 本业务守则内有关用语的定义如下：

证书 指符合以下所有说明的纪录：

(a) 由核证机关为证明数码签署的目的而发出，并且该数码签署的用意是确认持有某特定配对密码匙的人的身分或其他主要特征的；

(b) 识别发出纪录的核证机关；

(c) 指名或识别获发给纪录的人；

(d) 包含该获发给纪录的人的公开密码匙；并且

(e) 由发出纪录的核证机关签署；

核证机关	指向他人（可以是另一核证机关）发出证书的人；
核证机关证书	指由核证机关发出的证书或向核证机关发出的证书，用以证明该机关所发出的证书。该证书可以是核证机关发给本身的证书，或是某核证机关发给另一核证机关的证书；
核证机关披露纪录	就任何认可核证机关而言，指根据条例第 31 条为该机关备存的纪录；
证书政策	指一套订明的规则，表明证书对特定群体及／或有共同保安规定的使用类别的适用性；
核证作业准则	指认可核证机关所发出的以指明其在发出证书时使用的作业实务及标准的准则；
证书撤销清单	指由核证机关备存及公布的清单，列明其发出及已撤销的证书；
数码签署	就电子纪录而言，指签署人的电子签署，而该签署是用非对称密码系统及杂凑函数将该电子纪录作数据变换而产生的，使持有原本未经数据变换的电子纪录及签署人的公开密码匙的人能据之确定：

(a) 该数据变换是否用与签署人的公开密码匙对应的私人密码匙产生的；及

(b) 在产生数据变换之后，该原本的电子纪录是否未经变更；

电子纪录　指资讯系统所产生的数码形式的纪录，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；并且

(b) 能储存在资讯系统或其他媒介内；

适当人选　在决定某人是否适当人选时，总监除考虑其认为有关的任何其他事宜外，还须考虑是否有以下情况：

(a) 该人曾在香港特别行政区或其他地方被裁定犯任何罪行，而该项定罪必然包含该人曾有欺诈性、舞弊或不诚实的作为的裁断；

(b) 该人曾被裁定犯本条例所订的罪行；

(c) 如该人是个人，该人是未获解除破产的破产人，或在先前 5 年内曾订立《破产条例》(第 6 章)所指的债务重整协议、债务偿还安排或自愿安排；及

(d) 如该人是一间公司，该公司正在清盘中，或是清盘令的标的，或有接管人就该公司而获委任，或该公司在先前 5 年内曾订立《破产条例》(第 6 章)所指的债务重整协议、债务偿还安排或自愿安排；

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的系统：

(a) 处理资讯的；

(b) 记录资讯的；

(c) 能用作使资讯记录或储存在不论位于何处的其他资讯系统内，或能用作将资讯在该等系统内以其他方式处理的；及

(d) 能用作检索资讯的（不论该等资讯是记录或储存在该系统内或在不论位于何处的其他资讯系统内）；

发出 就某证书而言，指：

(a) 制造该证书，继而通知在该证书内指名或识别为获发给该证书的人，关于该证书内所载与该人有关的资讯；或

(b) 通知将会在该证书内指名或识别为获发给该证书的人，关于将会在该证书内所载与该人有关的资讯，继而制造该证书，

再继而提供该证书，供该人使用；

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的公开密码匙，而该公开密码匙是能核实该私人密码匙所产生的数码签署的；

个人资料 指《个人资料（私隐）条例》（第486章）所界定的个人资料；

邮政署署长 指《邮政署条例》(第98章)所指的署长；

获适当授权人 指获授予权力代表登记人行事的人；

私人密码匙 指配对密码匙中用作产生数码签署的密码匙；

公开密码匙 指配对密码匙中用作核实数码签署的密

码匙；

认可证书	指下述证书：
	(a) 根据条例第 22 条认可的证书；
	(b) 属根据条例第 22 条认可的证书的类型、类别或种类的证书；或
	(c) 邮政署署长所发出的指明为认可证书的证书；
认可核证机关	指根据条例第 21 条认可的核证机关，或邮政署署长；
纪录	指在有形媒介上注记、储存或以其他方式固定的资讯，亦指储存在电子或其他媒介的可藉可理解形式还原的资讯；
倚据限额	指就认可证书的倚据而指明的金钱限额；
储存库	指用作储存及检索证书及其他与证书有关的资讯的资讯系统；
负责人员	就某核证机关而言，指在该机关与本条例有关的活动方面身居要职的人；
签及签署	包括由意图是认证或承认纪录的人签立或采用的任何符号，或该人使用或采用的任何方法或程序；
登记人	指符合以下所有说明的人（该人可以是另一核证机关）：
	(a) 在某证书内指名或识别为获发给证书；
	(b) 已接受该证书；及
	(c) 持有与列于该证书内的公开密码匙对应的私人密码匙；
稳当系统	指符合以下所有条件的电脑硬件、软件及程序：

(a) 是合理地安全可免遭受入侵及不当使用的；

(b) 在可供使用情况、可靠性及操作方式能于合理期间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) 依循获广泛接受的安全原则；

核实数码签署　就某数码签署、电子纪录及公开密码匙而言，指确定：

(a) 该数码签署是否用与列于某证书内的公开密码匙对应的私人密码匙而产生的；及

(b) 该电子纪录在其数码签署产生后是否未经变更，

而凡提述数码签署属可核实者，须据此解释。

3 认可核证机关的一般责任

3.1 认可核证机关须遵守总监根据条例第 21 条批给认可时附加的条件，或根据条例第 27 条将认可续期时附加的条件。

3.2 认可核证机关可委任代理人或分包商执行其部分或所有运作，但须符合下列条件：

- 该代理人或分包商应具备同等能力以遵守本业务守则内适用于其运作的规定；及
- 认可核证机关须由始至终对其代理人或分包商所执行或其本意是执行条例就该机关规定的功能、权力、权利和职责负责。

3.3 认可核证机关在向其登记人发出证书时，须在合理范围内尽量小心，及须在合理范围内尽量小心处理可能倚据由该机关发出的证书的人。

3.4 认可核证机关须向总监提供其用以签署认可证书的核证机关证书。总监须在为该机关备存的核证机关披露纪录内公布该核证机关证书。有关的披露纪录可在该机关终止服务后的最少 7 年内，提供额外途径，使有需要核实由该机关发出的认可证书有效性的人，可取得有关的证书。

3.5 凡本业务守则规定认可核证机关把资讯及纪录加以记录、保留或存档，该机关须把该等资讯及纪录记录、保留或存档为期最少 7 年，或由总监指明的较长或较短的期间，并须以能确保该等资讯及纪录的安全、完整及可供接达的方式处理，以便检索和查阅。

3.6 认可核证机关须遵守有关个人资料私隐的所有适用条例及规例。认可核证机关尤须：

(a) 列明其有关以下事项的私隐政策：资料当事人（例如证书申请人及登记人）的个人资料的收集、持有和使用；

(b) 在向资料当事人收集个人资料之前或之时，向资料当事人发出一项书面的收集个人资料声明；

(c) 包括一项目的声明（例如在其储存库或核证作业准则内），阐明保存其储存库的目的，以及储存库内所载个人资料的许可用途；及

(d) （作为一项最低限度的规定）按照个人资料私隐专员出版的《遵守〈个人资料（私隐）条例〉规定自我评估资料套》或同类性质的文件进行自我评估，以确保与个人资料私隐有关的所有适用条例和规例得以遵守。认可核证机关须定期或每当其运作发生重大变化以致影响其处理资料当事人的个人资料时，进行此类自我评估。

3.7 认可核证机关不得使用任何有损经济效益或自由贸易的限制性作业实务。

3.8 如认可核证机关向公众发出的证书中有认可的证书和非认可的证书，该机关须在其核证作业准则和储存库中公布其发出该两种不同类目的证书的事实。该机关如此公布事实时，须清楚识别其所发出的个别证书或某类型、类别或种类的证书中何者属根据条例获认可的证书而何者属非认可的证书。

3.9 认可核证机关须按照有关防止对残疾人士施行歧视性的做法的所有条例和规例，在提供服务时顾及残疾人士的需要。

4 核证作业准则

4.1 认可核证机关须就其发出的各类型、类别或种类的认可证书，向公众公布及备存其最新的核证作业准则。

4.2 认可核证机关须在其核证作业准则内述明该机关、其登记人及倚据其发出的证书的人的法律责任、法律责任限额、权利和责任，以及该机关在其证书内设定的倚据限额的重要性。认可核证机关须透过以下方法，使其登记人及倚据该机关发出的证书的人注意到该等法律责任、法律责任限额、权利和责任及倚据限额的重要性：

- 在与登记人订立的任何合约内适当地另行指明该等资讯；及
- 以书面及联机的和可供公众接达的电子媒介提供该等资讯。

4.3 认可核证机关须在其核证作业准则内，就其发出的各类型、类别或种类的认可证书的认可情况，提供最新的资讯。

4.4 认可核证机关须令其登记人及可能倚据其发出的非认可的证书的人，知悉使用及倚据该等证书的影响。

4.5 认可核证机关须令其证书的申请人知悉，当该机关把申请人的个人资料纳入在向申请人发出的认可证书，及把该证书在该机关的储存库公布时，该等资料便会成为公开资讯的程度。该机关的核证作业准则必须明确述明有关的认可证书的内容。

4.6 认可核证机关须在公布核证作业准则后，向总监提交该准则的副本，并于切实可行范围内尽快以书面通知总监其后有关该准则的任何变更。认可核证机关亦须于切实可行范围内尽快记录该准则的所有变更及每项变更的生效日期。

4.7 如认可核证机关发出已在某证书政策指明的某类型、类别或种类的认可证书，该证书政策会当作核证作业准则的一部分。

4.8 认可核证机关须保留其核证作业准则每个版本的副本，并须列明核证作业准则的生效日期及停止生效日期（如适用）。

4.9 认可核证机关在发出某类型、类别或种类的认可证书时，须遵守关于该类型、类别或种类的认可证书的核证作业准则。

4.10 认可核证机关须确保其核证作业准则可随时在联机的及可供公众接达的储存库内查阅。核证作业准则有任何变更时，储存库内的资讯须尽快予以更新。

4.11 有关核证作业准则内容的标准及程序载于附录 1。

4.12 认可核证机关拟对其运作或与该机关发出的一个或多个类型、类别或种类的认可证书对应的核证作业准则作出重大变更前，须以书面通知总监有关变更的详情。总监将会考虑该机关拟作出的重大变更是否符合条例及本业务守则的有关条文，并可要求该机关按照第 12.1(c)及 13.1(c)段向总监呈交有关重大变更的报告及/或法定声明。认可核证机关的运作方面或其核证作业准则的重大变更包括但不限于以下例子：

(a) 会减低认可证书可靠性的有关识别程序的变更；

(b) 认可证书的依据限额的变更；或

(c) 密码匙的产生、储存或使用程序的变更。

4.13 凡有任何事件会不利于及严重影响其核证作业准则的全部或部分有效性，认可核证机关须立即通知总监、登记人及倚据人士。该机关须立即处理该事件。该等事件的解决办法须在切实可行的范围下，尽快在核证作业准则内反映、在该机关的联机的储存库公布及向总监报告。

5 稳当系统

5.1 认可核证机关须使用稳当系统提供服务，包括产生及管理其密码匙，产生及管理登记人的密码匙（如适用），认可证书的发出、续期、暂时吊销或撤销，就认可证书的发出、续期、暂时吊销或撤销发出通知，设置储存库，以及在储存库内公布认可证书及其他资讯。

通用释义

5.2 “系统”一词指系统本身，即硬件和软件，及管制和运作程序（人手及自动操作的程序）。制订有关程序旨在确保该系统能一致、可信及可靠地执行其原定的功能。

5.3 认可核证机关须证明该系统运作的机制、程序及运作环境均足以令系统执行其原定的功能，系统才可获接受为稳当系统。

5.4 量度稳当程度并无一套绝对的标准。稳当程度只能以某一个特定的情况作出评估。

指导原则

5.5 在条例所采取的科技中立及尽量少加规管的原则下，认可核证机关可自行选择支援其运作的技术方案。

5.6 凡认可核证机关有部分运作范围（如与影响保安的功能有关的运作）具高风险，该机关所采用的系统及程序会被预期是可符合国际间广泛接受或认可的标准。此外，就良好的作业实务而言，认可核证机关须就确定其运作的潜在风险进行有系统的评估，并采取合适的对策以控制、减轻及监察有关风险。

须予以考虑的特定范围

5.7 在公开密码匙基础建设下运作的认可核证机关，须应用硬件、软件及密码组件。这些组件须有适当的保安政策及程序作配合，以确保认可核证机关能在稳妥可靠的环境下运作。

5.8 认可核证机关为达致保持系统稳当的目的所采用的方法，会因应不同认可核证机关提供的服务种类、科技状况及业务环境而可能有所不同。认可核证机关须依循以下获广泛认可的良好作业实务。

行业内广泛接受的良好作业实务

5.9 认可核证机关须就其营运环境发展、制订、备存及更新有正式记录及经核准的政策、程序及作业实务，其中包括但并不限于下文的讨论范围。

获广泛接受的保安原则

5.9.1 认可核证机关须根据获广泛接受的保安原则，就其运作发展、制订、备存、更新及推行足够及适当的保安管制措施。保安原则最少须涵盖下列各项：

(a) 资产分类及管理

(i) 认可核证机关须把其资产按适当的方式分类，并为其主要资产识别拥有人。该机关须备存最新及完整的资产清单，并制订程序以保障其资产；

(ii) 认可核证机关须把所备存的资讯当为其中一种资产，并根据业务运作的重要性（包括资料私隐的考虑因素）为该等资讯分类。该机关须制订适当的管制措施，以保证该等资讯不会被人擅自接达或破坏。

(b) 人事保安

(i) 认可核证机关须透过多种机制发展、制订、备存及更新有效的人事保安管制措施，其中包括但不限于：

- 根据其保安政策在正式的工作定义内对工作种类的职责及责任加以界定；
- 根据其保安政策及程序对其员工进行保安审核；及
- 在雇佣合约的正式条款及条件内纳入保持机密性或类似的条款。

(ii) 认可核证机关须为其职员提供适当及足够的培训，目的是维持他们执行任务的能力，以确保保安政策得以有效推行和予以遵守。培训的内容可包括但不限于以下范围：

- 适当的技术培训；
- 组织政策和程序；及
- 处理保安事件及通知高层管理人员有关重大保安事件的程序。

(iii) 认可核证机关须制订适当的管制措施以监察其人员的表现，例如：

- 定期进行的工作表现评核；
- 正式的纪律程序；及
- 正式终止服务的程序。

(c) 实体及环境保安

(i) 认可核证机关须执行有效的实体及环境保安管制措施，其中包括但不限于：

- 识别及界定保安范围，并采取适当的保安管制措施以确保该等范围的安全；
- 就认可核证机关的职员及访客进入该等范围制订正式的程序；

- 设立适当的保安及进入保安范围的监察机制，而认可核证机关用以储存影响保安的设备的范围须特别加以注意；

- 制订适当的管制措施，以保障其设备免受火灾、水灾、停电等环境因素及灾患影响，并须防止有人擅自进入保安范围内；

- 制订一般的保安管制措施，例如：清理桌面政策及对属于认可核证机关的设备、资讯及其他资产的一般管制；及

- 确保其环境管制机制得以维持，并按时进行检讨。

(ii) 凡认可核证机关倚靠第三方提供服务，以保障实体及环境的保安，该等服务须在该机关与第三方供应商订立的正式服务协议内述明。

(d) 系统接达的管理

认可核证机关须就其资讯系统（包括应用系统）的接达发展、制订、维持及更新有效的管制措施及程序。该等管制措施及程序须因应受保护系统的敏感性及关键性而发展、制订、维持及更新，其中包括但不限于：

- 制订适当的业务规定以管制系统的接达；

- 正式厘定用户的责任；

- 就用户识别资料管理及系统接达的监察制订正式程序，其中包括：

  － 分配、修改及撤销用户的接达权；及

  － 利用记录或类似方法监察尝试接达系统的情况；

- 就接达网络、操作系统及应用系统制订适当的管制措施，如防火墙和路由器筛选指令；

- 就监察系统接达及使用制订适当的程序及管制措施；

- 就流动电脑应用及电讯运作制订适当的程序及管制措施；

- 就擅自或非法使用软件制订适当的程序及管制措施；及

- 就与接达网络、操作系统及应用系统有关的保安事件制订适当的处理程序。

操作管理

5.9.2 认可核证机关须就其日常的操作维持有效的管制措施及程序。操作政策及标准操作程序须予以正式制订及记录，其中包括但不限于以下范围：

- 清楚界定其操作人员的职务及责任；
- 制订定期监察系统承担能力的程序，以监察系统的工作表现及找出窒碍系统工作表现的地方；
- 制订适当的程序，以防止其电脑基建设施受有害程式（如电脑病毒等）的影响；
- 制订适当的系统及网络管理程序，包括备份及存档等内务管理；
- 就电子资讯及媒体的处理、分发、储存及处置制订适当的程序；及
- 制订适当的程序处理及解决操作上的问题。

电脑系统的发展及维修保养

5.9.3 认可核证机关须就系统的发展及维修保养工作发展、制订、维持及更新有效的管制措施及程序，其中包括：

- 制订适当的内部标准，以确保无论由认可核证机关的人员或在外发的情况下由外间机构进行发展工作时，均能保持一贯的标准；
- 制订程序，以确保把用作生产及发展的环境分隔开；
- 制订程序，以确保操作及发展人员的职责得以区分；
- 对接达其用作生产及发展的环境内的资料及系统制订管制措施；
- 对变更管制程序（包括系统及／或数据的紧急变更）制订管制措施；及
- 就采购设备及服务的妥善管理制订程序。

业务运作的持续性

5.9.4 认可核证机关须发展、制订、维持及更新涵盖所有关键的运作范围的业务持续运作计划。

5.9.5 该持续运作计划须定期进行彻底的测试，而计划所载列的有关主要人员须参与进行测试。在可能范围内，须聘用独立人士观察这些测试的进行。

5.9.6 业务持续运作计划须涵盖紧急应变措施，例如：认可核证机关本身用以签署登记人证书的私人密码匙外泄或怀疑外泄后的复原运作，或认可核证机关的系统或其系统的任何组成部分出现重大故障后的复原运作。

备存适当的事件纪录

5.9.7 认可核证机关须备存足够的事件纪录，包括保留与该机关发出及管理认可证书有关的文件。

5.9.8 认可核证机关须为该等事件纪录存档。该机关亦须定期检查事件纪录，并就经识别的任何异常情况采取行动。

5.9.9 认可核证机关须为所有重大事件备存纪录，其中包括但并不限于：

- 对用以产生密码匙的资料及设备的接达；
- 密码匙及证书及其产生、发出、分派、储存、备份、暂时吊销、撤销、撤回、存档、销毁及其他的有关事项；
- 保安事件，包括密码匙资料外泄；及
- 密码设备的采购、安装、使用、解除运作及弃用。

对遵守规定的监察及保证

5.9.10 认可核证机关须发展、制订、维持及更新适当的管制措施，以确保能遵守适用的法律、规管及技术方面的规定，其中包括但不限于：

- 制订适当的功能，以监察认可核证机关的所有运作程序，并确保遵守所适用的规定；
- 确保其遵守监察的功能符合业界的现行标准及作业实务；及
- 就操作系统安排进行适当的检讨。

认可核证机关特定功能的良好作业实务

5.10 认可核证机关需就其特定的功能发展、制订、维持及更新有正式记录及经核准的政策、程序及作业实务，其中包括但不限于下文所载的范围。

核证作业准则的管理

5.10.1 认可核证机关须在核证作业准则内披露业务的作业实务，并对核证作业准则执行有效的管制措施，其中包括但不限于：

- 成立管理小组，并授予制订及核准核证作业准则的权力及责任，包括认可核证机关所采用的任何证书政策；
- 制订有效程序，以持续检讨及更新核证作业准则；及
- 使核证作业准则可供登记人及可能倚据由该机关发出的认可证书的人查阅。

监察认可核证机关的功能以确保其遵守法律和规管

5.10.2 认可核证机关须维持有效程序，以监察及确保其遵守所有法律及规管方面的规定，包括条例有关的条文、根据条例订立的规例及本业务守则。

密码匙的管理

5.10.3 认可核证机关须就该机关本身的密码匙的产生、储存、备份、复原、分发、使用、销毁及存档维持有效的程序及管制措施，其中包括但不限于：

- 有关使用产生密码匙的密码模组的管制措施，包括采用符合适当保安标准的技术方案;
- 有关产生密码匙的操作管制措施，其中包括但不限于：
  - 用以确保用于产生密码匙的设备完整无误的程序；及
  - 用以确保密码匙是由获授权人在受管制的方式下产生的程序；
- 有关密码匙的储存、备份及复原的管制措施，其中包括但不限于：
  - 认可核证机关的运作复原程序的定期彻底测试；

– 用以确保核证机关的私人密码匙得以安全地保管的程序，例如：采用双重接达的保管方法。认可核证机关须制订适当的措施，以确保能侦测任何尝试擅自接达该机关的私人密码匙的情况；及

– 用以确保认可核证机关的私人密码匙的备份得以在双重接达的管制下安全地运作的程序，及该机关的私人密码匙的备份应以稳妥的方式保管；

- 有关分发密码匙程序的保安管制措施，其中包括但不限于：

  – 用以确保认可核证机关提供予总监在其核证机关披露纪录内存放的公开密码匙是完整及真确的程序；及

  – 用以确保认可核证机关本身的公开密码匙是完整及真确的程序；

- 有关使用密码匙的管制措施，包括启动密码匙的程序，例子包括但不限于：

  – 须有一名以上的负责人员才可启动认可核证机关的私人密码匙；及

  – 只有在取得适当的授权经订明的方式以进行原定目的，才可启动认可核证机关的私人密码匙；

- 有关确保安全销毁配对密码匙及任何有关设施的管制措施，包括采取程序以确保销毁私人密码匙的所有副本（令私人密码匙在销毁后再不能复原或重组），以及撤销对应的公开密码匙的程序；及

- 有关确保已存档的密码匙符合在核证作业准则内述明的保安及运作规定的管制措施。

产生密码匙工具的管理

5.10.4 认可核证机关须就产生密码匙工具的采购、接收、安装、验收测试、调试、使用、维修、保养及弃用，维持有效的程序及管制措施，例如：

- 维持程序，以确保密码模组的完整性；

- 维持程序，以确保产生密码匙的工具由获授权人在适当的督导下操作，以防止工具遭擅自改动；并设立管制机制，

以确保密码模组不会在不能侦测的情况下遭人擅自改动；及

- 维持程序，以确保使用密码模组产生的密码匙的强度，是符合认可核证机关及登记人为密码匙的目的所需的适合强度。

由认可核证机关提供的密码匙管理服务（凡适用）

5.10.5 如认可核证机关为登记人提供密码匙管理服务，便须就密码匙的产生、储存、备份、复原、销毁、及存档等方面，执行有效的程序及管制措施。该等程序及管制措施须符合载于本业务守则第 5.10.3 及 5.10.4 段的原则。凡登记人的配对密码匙由认可核证机关产生，该机关须制订程序，以确保私人密码匙以安全的方式及在没有被擅自改动的情况下交付证书申请人；认可核证机关倘没有登记人的书面同意，不得备存登记人的私人密码匙副本。

权标的生命周期管理（凡适用）

5.10.6 认可核证机关须就其所使用的任何权标（如智能卡）的预备、启动、使用、分派及终止使用，维持有效的程序及管制措施。

证书管理

5.10.7 认可核证机关须就证书的管理，维持有效的程序及管制措施，其中包括但不限于下列例子：

- 认可核证机关须根据有关的核证作业准则所载列的程序，核实申请发出证书或将证书续期的人的身分。该机关亦须核实该人的特有名称的独特性；

- 认可核证机关须订立适当程序，使其在登记人的证书的有效期届满前，通知登记人须为证书续期；

- 认可核证机关须采取开放及共通的界面以发出认可证书，而证书的格式须在有关的核证作业准则内述明；

- 认可核证机关须制订适当的政策及程序，以确保该机关的储存库的效能，符合该机关在核证作业准则内就储存库所载列的服务水平；及

- 认可核证机关须在核证作业准则内载列处理登记人投诉的程序。

证书撤销资讯公布的管理

5.10.8 认可核证机关须就证书撤销资讯公布的管理（例如透过其证书撤销清单及任何其他公布有关证书撤销资讯的方式），制订有效的程序及管制措施，例如：

- 认可核证机关须按照在核证作业准则内述明的政策、程序及安排，更新证书撤销清单及任何其他公布有关证书撤销资讯的方式；及
- 认可核证机关须制订程序，以确保只有获授权人才可接达储存库、证书撤销清单及任何其他公布有关证书撤销资讯的方式，以进行修订的工作。

使用稳当系统产生密码匙及保存纪录

5.11 认可核证机关须使用稳当系统为本身及登记人产生配对密码匙。凡其任何认可证书的申请人使用自己的系统产生其配对密码匙，认可核证机关须要求该申请人使用稳当系统以产生其配对密码匙。认可核证机关须向申请人提供指引，并须采取合理地切实可行的措施，以确定申请人在使用稳当系统以产生其配对密码匙方面遵守指引。如该申请人没有遵守指引或没有使用稳当系统以产生配对密码匙，认可核证机关不得接受该申请人的配对密码匙。

5.12 认可核证机关须把本身的私人密码匙及启动数据（如个人识别密码、密码等）以安全的方式分开保存。

5.13 认可核证机关须制备及保留下列纪录：

- 有关认可证书的发出、续期、暂时吊销及撤销的事项（包括向认可核证机关申请认可证书的任何人的身分证明文件）；
- 证书撤销资讯的公布（例如透过证书撤销清单及任何其他公布有关证书撤销资讯的方式）；
- 有关产生认可核证机关本身的配对密码匙的文件；
- 有关产生登记人的配对密码匙的文件；及
- 认可核证机关的电脑设施的行政管理。

5.14 认可核证机关须为其发出的所有认可证书存档，并设置接达该等证书的机制。

数码签署

5.15 所推行的技术就产生数码签署方面须遵守的规定：

(a) 数码签署须在其有关的人的指示下才能产生；及

(b) 在与数码签署有关的人没有参与或不知情的情况下，任何人均不能复制该数码签署及从而产生有效的数码签署。

对稳当系统构成影响的事宜

5.16 若发生任何会对认可核证机关的稳当系统或其发出的认可证书造成重大及不利影响的事件时，该机关须：

- 立即把有关事件告知总监；
- 合理地尽力通知所有已经或将会受该事件影响的人；及
- 按照核证作业准则就处理该类事件所指明的程序（如有指明的话）采取行动。

5.17 认可核证机关须确保其所有人员具备所需知识、技术资格和专业知识，以便有效地履行职责。

5.18 认可核证机关须确保所有负责人员和担当获信任职位的人员，例如保安主任、核证机关行政主管、特别系统操作人员、登记人员、及其他能接达重要资料、密码模组及工作事件纪录的人员，均为适当人选。

保安及风险管理

5.19 认可核证机关须采用按普遍接受的保安原则制订的保安政策。

5.20 认可核证机关须就其运作，制订全面的保安事件汇报和处理程序，以及运作复原的机制和程序。

5.21 认可核证机关须充分地识别及制订程序，以处理与该机关的运作有关的风险。该机关须推行一套风险管理计划，就管理包括但不限于以下的事件作出规定：

- 密码匙资料外泄；
- 认可核证机关的系统或网络出现违反保安事项；
- 认可核证机关的基建设施不可供使用的情况；及
- 擅自制造有关证书及证书的暂时吊销和撤销的资讯。

6 证书及认可证书

6.1 认可核证机关可发出认可证书或非认可的证书。如认可核证机关发出的证书中有认可证书及非认可的证书，该机关须以不同的私人密码匙分别签署这两类证书。

6.2 认可证书内应载有所需资讯，以协助登记人及依据证书的人在进行电子交易时找到有关的核证作业准则。

发出证书

6.3 认可核证机关只有在以下情况才可发出认可证书：

(a) 该机关已收到申请人提出的发出认可证书的要求；及

(b) 该机关已遵守核证作业准则载列的所有作业实务及程序，包括与该类型、类别或种类的认可证书有关的申请人的身分核实程序。

6.4 认可核证机关须为其任何认可证书的申请人提供合理机会，以核实已经或将会收纳入证书内的申请人资讯。申请人资讯是指由申请人提供而认可核证机关已经或将会收纳入证书内的资讯。此外，该机关必须采取一切合理地切实可行的措施，确保已经或将会收纳入证书内的资讯准确无误。

6.5 认可核证机关须在其设置的或由一个或多个第三方为其设置的联机的及可供公众接达的储存库内，公布由该机关发出且获登记人接受的认可证书。如认可核证机关向公众发出的证书中有认可证书及非认可的证书，该机关须用独立的储存库分别公布该两类证书。

6.6 认可核证机关须得到认可证书申请人的同意，才可按该机关的原意把申请人的个人资料收纳入该等将予发给申请人的证书内，并将该等证书载列于联机的及可供公众接达的储存库内。

6.7 认可证书经认可核证机关发出且获登记人予以接受后，倘该机关知道有任何影响认可证书的有效性及可靠性的事实，便须在一段合理时间内，透过所有渠道把该事实通知登记人。

6.8 认可证书须述明其有效性届满的日期。

6.9 凡认可核证机关发出认可证书，即属向任何合理地倚据该证书的人，或向任何合理地倚据该证书内列出的公开密码匙所能核

实的数码签署的人，表述该机关已按照适用的核证作业准则发出该证书。

6.10 所有与发出认可证书有关的交易事项，包括日期和时间，均须予以记录。

暂时吊销及撤销认可证书

6.11 认可核证机关可按下文载列的规定撤销认可证书，亦可按该等规定暂时吊销认可证书。

6.12 认可证书须包含或以提述方式收纳所需资讯，以找出或识别载列与公布该证书的暂时吊销或撤销有关的通知的储存库。

6.13 除非认可核证机关及登记人另有协议，否则发出认可证书予登记人的认可核证机关须在接获下列人士的要求后的一段合理时间内，暂时吊销或撤销该证书：

(a) 认可证书内指名或识别的登记人；或

(b) 获适当授权人。

6.14 认可核证机关须于暂时吊销或撤销认可证书后的一段合理时间内，在其设置的储存库或由外间机构代其设置的储存库内，公布有关暂时吊销或撤销认可证书的通知（例如透过认可核证机关签署的证书撤销清单，或任何其他公布有关暂时吊销或撤销认可证书的资讯的方式）。

6.15 认可核证机关撤销或暂时吊销证书的确实时间，以及由接获撤销或暂时吊销认可证书的要求之时起至证书被撤销或暂时吊销之时止的一段期间，以该证书进行交易的法律责任摊分问题，须由认可核证机关和登记人议定。

6.16 如认可核证机关有合理理由相信其发出的某认可证书不可靠，则无论登记人同意与否，该机关可暂时吊销该证书；但该机关须在一段合理时间内完成有关该证书的可靠性的调查，以及决定是否恢复该证书的有效性或撤销该证书。

6.17 如认可核证机关在考虑所有可取得的资讯后，认为应即时撤销其发出的某认可证书，则无论登记人同意与否，该证书须予以撤销。

6.18 如登记人或获适当授权人要求暂时吊销认可证书，认可核证机关须向该登记人或获适当授权人查询，该将会被暂时吊销的认可证书在暂时吊销后是否须被撤销或会否恢复该证书的有效性。有关的核证作业准则须述明该机关在未能联络该登记人或

获适当授权人时应采取的行动。联络有关人士的目的，是取得有关该证书在暂时吊销后须予撤销或恢复有效性的指示。

6.19 如认可核证机关暂时吊销或撤销所发出的认可证书，该机关须在一段合理时间内，把暂时吊销或撤销该证书之事，通知该证书的登记人或获适当授权人，并向他们提供通知纪录。

6.20 认可核证机关须提供热线电话或其他设施，以供登记人向该机关报告有关影响其证书或私人密码匙的事件，例如遗失密码匙或密码匙资料外泄。

6.21 凡与暂时吊销或撤销认可证书有关的所有交易事项，包括日期和时间，均须予以记录。

认可证书的续期

6.22 认可证书可因应登记人的要求及认可核证机关的酌情权，在认可证书的有效期届满时获得续期。

6.23 与认可证书续期有关的所有交易事项，包括日期和时间，均须予以记录。

7 登记人身分的核实

7.1 认可核证机关须在与某类型、类别或种类的认可证书对应的有关核证作业准则内，指明对向该机关申请该等认可证书的人进行身分核实的程序。

7.2 认可核证机关须保留足以识别登记人身分的文件证据。

8 倚据限额以及为法律责任投保

8.1 认可核证机关在向登记人发出某类型、类别或种类认可证书时，可在与该类型、类别或种类证书对应的有关核证作业准则内指明该等证书的倚据限额。该机关须在有关的核证作业准则指明倚据限额对使用该证书的重要性。

8.2 认可核证机关须安排投购适当的保险或作出其他方式的赔偿安排，以确保该机关有足够能力承担因发出或使用认可证书而引起的或与此有关的潜在法律责任。该机关须特别提供证据，证明本身已投购保险，承保因其错误或不作为而引起的申索，而

投保期内每宗申索的最低弥偿额不得少于以下数额（以较高的数额为准）：

(a) 该认可核证机关在其认可证书的核证作业准则上指明的倚据限额的 10 倍（如在一份保险单内就不同的认可证书指明不同的倚据限额，则采用当中最高的倚据限额）；或

(b) 港币 200,000 元；

此外，该机关为此目的而购买的每一份保险单在任何一段为期 12 个月的投保期内，就该保险单所承保的认可证书的申索总额而设定的投保额，须为上述(a)项或(b)项所述数额的 10 倍（以较高者为准）。上述为法律责任投购的保险必须在任何时候均有效，并须就该机关所发出的所有类型、类别或种类的认可证书提供保障。如该机关选择以其他方式为法律责任作出赔偿安排，则所作出的安排必须提供相同的最低弥偿额，并须由独立的第三方加以管理。所作出的其他方式赔偿安排生效之前，该机关必须先征得总监批准。

8.3 认可核证机关所购买的保险单必须：

(a) 由根据《保险公司条例》（第 41 条）获授权在香港特别行政区进行有关保险业务的保险人（包括劳合社）发出；及

(b) 受香港特别行政区的法律管限并按照该等法律解释。

此外，认可核证机关及保险人均须同意就保险单所引起的申索或其他事宜受香港特别行政区法院的非专有司法管辖权所管辖。

8.4 对于因认可核证机关的错误或不作为而引起的申索，该机关须维持一套程序规则，订明提出申索时所需的证明文件。

9 储存库

9.1 认可核证机关须提供最少一个联机的及可供公众接达的储存库，以公布认可证书及其他有关的资讯。该机关须确保其一个或多个的储存库是由稳当系统所提供，并须在核证作业准则内述明有关储存库运作的服务水平。

9.2 认可核证机关在维持及管理储存库时，不得进行任何对倚据包含在储存库内的认可证书及其他资讯的人造成不合理风险的活动。

9.3 认可核证机关的储存库须载有：

- 由认可核证机关发出的认可证书；
- 有关暂时吊销或撤销认可证书的通知（包括证书撤销清单，或任何其他公布有关暂时吊销或撤销认可证书的资讯的方式（视何者适用而定））；
- 该机关的核证机关披露纪录；及
- 总监指明的其他资讯。

9.4 认可核证机关的储存库不得载有其明知为不正确或不可靠的资讯。

9.5 认可核证机关须在其储存库内把过去最少 7 年内被暂时吊销或撤销的或有效期届满的认可证书存档。

10 披露资讯

10.1 认可核证机关须在其一个或多个储存库内公布：

(a) 该机关的核证机关证书，其中包含与该机关用以在所发出认可证书作数码签署的私人密码匙对应的公开密码匙；

(b) 其核证机关证书或总监向其作出的认可被暂时吊销、撤销或不获续期的通知；及

(c) 对该机关曾发出的认可证书的可靠性，或该机关提供与条例有关的服务的能力造成重大及不利影响的任何其他事实。

10.2 如认可核证机关在聘用负责人员或任何与负责人员有相同功能的人员方面有任何变更，须在该人员受聘日期起计 3 个工作日内把变更通知总监。

10.3 认可核证机关须每 6 个月一次，向总监提供包含以下资讯的进度报告：

(a) 按类型、类别或种类证书区分的登记人的数目；

(b) 按类型、类别或种类区分的发出、暂时吊销、撤销、有效期届满及获得续期的证书数目；

(c) 服务表现与所述明的服务水平的比较；

(d) 所发出的新类型、类别或种类的证书；

(e) 组织结构或系统的变更；

(f) 认可核证机关所采取的行动，该等行动旨在处理根据条例第 20(3)(b)、第 27(5A)(b)、第 43(1)(a)及第 43A(1)(c)条所拟备及向总监提供的评估报告内所作出的建议或识别出的例外情况或不足之处；及

(g) 自上一次提供进度报告或申请认可为认可核证机关或申请认可续期以来，以上各项目的任何变更情况。

10.4 以上各项资讯如有任何重大改变，认可核证机关须立即向总监报告。在有需要的情况下，总监亦可随时给予一段合理时间的通知，要求该机关提供该等报告及其他与条例有关的资讯。

10.5 认可核证机关发现任何可能或将会导致与该机关的运作产生潜在利益冲突的事项时，须立即向总监报告。

10.6 认可核证机关须就任何可能对其运作构成重大及不利影响的事件，立即向总监报告。

10.7 认可核证机关根据条例及业务守则的规定提交任何报告或资讯时，须确保其本身对该等报告及资讯拥有所需的权力，以致能批予总监或促致他人批予总监特许，俾能为施行条例而复制和发布该等报告和资讯的全部或其中任何部分内容。认可核证机关必须在总监提出要求时批予总监或促致他人批予总监该项特许。认可核证机关须因应总监的要求自费采取行动和签立文件（或促致他人采取行动或签立文件），以使该项特许有效。

10.8 认可核证机关同意让总监披露上述报告及资讯，只要总监认为为施行条例而适宜披露便可。

10.9 认可核证机关不得企图以任何方式阻止总监发布其为施行条例而须发布的资讯。

11 终止服务

11.1 核证机关于申请成为认可核证机关时，须向总监提交一份终止服务计划。认可核证机关于申请将认可续期时，须提交一份最新的终止服务计划。在总监提出要求时，该机关亦须在总监向该机关发出的通告中所指定的时间内，提交一份最新的终止服务计划。

11.2 终止服务计划须订明关于认可核证机关终止服务的安排，尤其是把纪录存档最少 7 年的安排。该等纪录包括该核证机关发出的证书以及该机关本身的核证机关证书。

11.3 终止服务计划须涵盖认可核证机关自愿及非自愿地终止服务两种情况，当中包括总监对该机关作出的认可的有效期届满或认可被撤销的情况。终止服务计划亦须订明有关措施，以确保登记人的利益在认可核证机关终止服务后仍能得到保障。

11.4 认可核证机关公布的任何核证作业准则均须提述该核证机关的终止服务计划。

11.5 认可核证机关在终止运作前，必须：

(a) 在终止其核证服务前最少 90 日，把终止服务的意向告知总监；

(b) 在终止其核证服务前最少 60 日，把终止服务的意向告知其所有登记人；

(c) 在终止其核证服务前最少 60 日，在香港特别行区发行的一份英文报章及一份中文报章刊登有关拟终止服务的启事最少连续 3 日；

(d) 在总监认为有此需要时作出安排，使所有尚未撤销的或有效期仍未届满的证书在该机关终止服务时得以撤销，不论登记人是否有提出撤销证书的要求；及

(e) 作出适当的安排，令认可核证机关储存库内的资讯（包括认可核证机关发出的证书的详情及该机关的公开密码匙），得以有秩序地转移。该等资讯须转移至一名保管人。由认可核证机关终止运作的日期或由资讯完成转移的日期（以较迟的日期为准）起计最少七年之内，该保管人须负责保管资讯。该等资讯的用途必须与认可核证机关的原来服务的用途一致，而接达该等资讯的方法及程序则须公布周知。

12 对遵守条例及本业务守则的评估

12.1 认可核证机关必须向总监提交报告如下：

(a) 最少每 12 个月提交一份报告，该报告须载有一份评估，说明该机关在报告所涵盖的期间是否已遵守附录 2 第 1 段所指明的条例及本业务守则的条文；

(b) 在该机关申请认可续期时提交报告，该报告须载有一份评估，说明该机关是否遵守以及有没有能力遵守附录 2 第 1 段所指明的条例及本业务守则的条文；及

(c) 在总监就该机关的重大变更而提出要求时，提交一份报告。该报告须载有一份说明以下事项的评估：

- 鉴于该机关已出现的重大变更，该机关是否遵守以及有没有能力遵守附录 2 第 3 段所指明的条例及本业务守则的条文；或
- 鉴于该机关将会出现的重大变更，该机关有没有能力遵守附录 2 第 3 段所指明的条例及本业务守则的条文。

12.2 认可核证机关须确保该报告是由一名获总监为此目的而认可为合资格的人所拟备，拟备费用由该机关负担。可获考虑核准为合资格拟备评估报告的人应具备下列条件：

- 独立于接受评估的认可核证机关以外；
- 通过认可的专业团体或协会的评审；及
- 熟识下列工作范围：
  - 对公开密码匙基础建设及有关科技的评估，例如数码签署及证书等；
  - 资讯保安工具及技术的应用；
  - 进行财务检讨；
  - 进行保安检讨；及
  - 进行第三方检讨。

12.3 合资格的人可以是具备以上所有条件的个人，或是合伙经营或机构，而该合伙经营或机构的成员整体上具备以上所有条件。签署评估报告的个人必须：

- 是认可专业团体或协会的注册会员，例如持有有效的执业证书或具备同等资格；
- 承担整体责任，以确保进行评估程序的人在数码签署和证书、公开密码匙基础建设、财务事宜等各方面具备足够的知识；及

- 承担整体责任，以确保评估的质素及评估工作符合为该等评估所订下的标准或作业实务。

12.4 下列符合第 12.2 及 12.3 段所载要求的人士，可向总监申请获核准为有资格进行评估的人：

(a) 执业会计师（即持有根据《专业会计师条例》（第 50 章）发出的执业证书的会计师）；及

(b) 香港工程师学会资讯界别的法定会员，并同时为根据《工程师注册条例》（第 409 条）在同一界别下注册的注册专业工程师。

此外，总监亦可核准由其他人士提出的申请，认可他们为有资格进行评估的人。

12.5 第 12.2 段所提述的专业团体或协会必须备有已确立的制度，以恰当地接纳及规管其会员。该制度的主要特征必须包括但不限于：

- 规范入会条件的规则和规例，例如培训、能力测试、成为会员的合宜程度等；
- 规范会员的专业及道德标准的规则和规例，以及规范会员专业服务表现的指引，例如处理利益冲突、执行和接受指示的表现；
- 推行会员的专业和道德标准及监察会员行为操守的机制，包括但不限于正式的纪律处分程序、质量保证措施（例如同事之间的检讨）；及
- 强制性的接受持续专业进修的规定。

12.6 就第 12.1(a)分段所提述的评估报告而言，认可核证机关须在完成评估后的 4 个星期内向总监提交评估报告的文本。就第 12.1(b)分段所提述的评估报告而言，该机关须向总监提交在申请续期日期之前 4 个星期内完成的评估报告的文本。就第 12.1(c)分段所提述的评估报告而言，总监可于其就该机关的重大变更而发出的通知中，指明该机关须向总监呈交报告的时限。

12.7 认可核证机关向总监提交报告时，须同时向总监呈交关于其对合资格的人在评做报告中提出的例外情况、不足之处或建议的回应。

12.8 总监可能以认可核证机关未能符合条例、根据条例而订立的规例以及业务守则内述明的规定为理由，暂时吊销或撤销批给该机关的认可，或拒绝该机关提出将认可续期的申请。

13 声明遵守条例及本业务守则的规定

13.1 认可核证机关必须向总监提交法定声明如下：

(a) 最少每 12 个月提交一份法定声明，述明该机关在法定声明所涵盖的期间是否已遵守附录 2 第 2 段所指明的条例及本业务守则的条文；

(b) 在该机关申请认可续期时提交一份法定声明，述明该机关是否遵守以及有没有能力遵守附录 2 第 2 段所指明的条例及本业务守则的条文；及

(c) 在总监就该机关的重大变更而提出要求时，提交一份述明以下事项的法定声明：

- 鉴于该机关已出现的重大变更，该机关是否遵守以及有没有能力遵守附录 2 第 3 段所指明的条例及本业务守则的条文；或

- 鉴于该机关将会出现重大变更，该机关有没有能力遵守附录 2 第 3 段所指明的条例及本业务守则的条文。

13.2 认可核证机关须确保法定声明是由该机关的负责人员作出，并由该机关负担费用。

13.3 就第 13.1(a)分段所提述的法定声明而言，认可核证机关须于作出法定声明后的 4 个星期内向总监提交该份法定声明。就第 13.1(b)分段所提述的法定声明而言，该机关须向总监提交在申请续期日期之前 4 个星期内作出的法定声明。就第 13.1(c)分段所提述的法定声明而言，总监可于其就该机关的重大变更而发出的通知中，指明该机关须向总监呈交法定声明的时限。

14 标准及技术的采用

14.1 认可核证机关须不断检讨并在适当时改善和更新所采用的标准和技术，以保持登记人对该机关的信心及保障登记人的利益。该机关必须：

(a) 为执行不断检讨及在适当时更新标准和技术的职务而制订明确的政策、管制措施和程序规则；

(b) 将上述职务指派予该机关内指定的组织；及

(c) 定期重新评估上述政策、管制措施和程序规则，以及有关组织的表现。

15 互通性

15.1 为使认可证书所证明的数码签署在减少障碍的情况下取得广泛接受，认可核证机关须尽可能采用开放及共通的界面，以协助其他人核实其认可证书所证明的数码签署。

15.2 认可核证机关须在核证作业准则内，述明其所支援的开放及共通的界面，以及与其他核证机关所建立的互通安排。

16 消费者的保障

16.1 认可核证机关就其服务所作的广告，须内容得体、正确真实。在广告内作出比较时亦须公平和不会产生误导作用，而声称的所有事项均可逐一予以独立地证实。

附录 1－有关核证作业准则内容的标准及程序

1 引言

本附录载列的标准及程序，是政府资讯科技总监（“总监”）根据《电子交易条例》（第 553 章）（“条例”）第 33 条发出的。该等标准及程序主要以互联网工程专责小组（The Internet Engineering Task Force）的第2527号RFC文件《证书政策及核证作业架构》(RFC 2527 “Certificate Policy and Certification Practices Framework”) (一般称为《IETF PKIX第四部分》（IETF PKIX Part 4）)作为基础。所载列的标准及程序是总监预期认可核证机关在发出核证作业准则[1]时，须予采用及遵守的最低标准。

下文载列总监预期认可核证机关须符合的最低标准及最基本的程序。

2 主要特征及核证作业准则简介

2.1 主要特征

认可核证机关须考虑就该机关发出的各类型、类别或种类证书的主要特征作出概述。主要特征会帮助登记人及倚据证书人士迅速了解根据核证作业准则发出的证书的有关特征。

该等特征须包括每类型、类别或种类证书的认可情况、证书的倚据限额及其他重要特征，例如可影响登记人或倚据证书人士对证书的信心及信任程度的规定识别方式。此外，认可核证机关须提述由该机关用作提供其认可状况及由总监备存的核证机关披露纪录的网址或其他资讯来源。

2.2 核证作业准则简介

2.2.1 概论

认可核证机关须就核证作业准则的目的及范围提供高层次的摘要。该摘要应指明总监对该机关认可的范围（例如认可的附带条件），有关该认

[1] 核證作業準則的概念最先在美國律師公會數碼簽署指引(American Bar Association Digital Signature Guidelines) 中獲得明確闡述。美國律師公會的指引把核證作業準則界定爲“核證機關用以發出證書的作業準則”。選用這個詞語的部分原因，是防止其與“政策”一詞造成含糊或混亂。核證作業準則不得與證書政策混淆，因爲兩者就作者、目的、具體程度及方法等方面均各有不同。

可对登记人及倚据人士的意义的概述及有关事宜。认可核证机关亦可强调核证服务的范围、条款及条件。

2.2.2 识别

认可核证机关须就其核证作业准则提供适当的物件识别项目（如有的话）。如认可核证机关就其根据核证作业准则发出的认可证书而支援特定的证书政策，则该机关须识别该等政策，并须在核证作业准则的有关部分提供该证书政策的适当物件识别项目（如有的话）。此外，该机关须确保在可供登记人和准登记人以联机方式接达的地点，公布所识别的政策的全文。

2.2.3 识别参与核证服务运作及维持核证服务的各方以及证书应用的范围

认可核证机关须识别所有已知构成或参与认可核证机关运作及维持核证服务的团体或功能，例如核证机关功能、注册功能、储存库及目标终端用户（即登记人及倚据人士）。如有一项或以上的主要核证服务是以外发形式提供的（例如使用第三方注册功能），须清楚述明。

此外，认可核证机关在适当的情况下，须载列该机关发出的每类型、类别或种类证书在应用方面的限制，例如：

- 所发出证书的适用情况，例如电子邮件、零售交易、合约等；
- 所发出证书在使用上的限制；及
- 所发出证书在使用上的禁制。

2.2.4 联络资料

认可核证机关须最少提供一个联络点，以处理登记人及倚据人士作出有关规管及其他事宜的查询。一般来说，认可核证机关最少会列出一个电话号码、邮递地址及电子邮址供登记人和倚据证书人士联络该机关。此外，认可核证机关须向登记人提供用作向该机关报告事件的热线电话或其他途径，以供登记人报告遗失密码匙或密码匙资料外泄等事件。

3 一般条文

3.1 责任

3.1.1 认可核证机关的职责和责任

认可核证机关须清楚述明该机关为其提供的服务所承担的职责和责任，包括条例载列的特定责任，连同作出认可的条件及本业务守则。该等责任的例子包括：

- 就发出证书一事向登记人（即该证书的发出对象）作出通知（包括作出该等通知的时间）；及
- 就撤销或暂时吊销证书一事向该证书的登记人作出通知（包括作出该等通知的时间）。

凡认可核证机关以外发形式执行其任何功能，与该等功能有关的职责和责任须另行阐述。

3.1.2 登记人的职责和责任

认可核证机关须阐述指配与该机关的登记人的职责及责任，包括在该机关支援的证书政策内载列的规定，例如：

- 确保在申请证书时所作的陈述准确无误；
- 保障登记人的私人密码匙；
- 对私人密码匙及证书的使用施加限制；及
- 就私人密码匙资料外泄或遗失作出通知。

3.1.3 倚据人士的责任

认可核证机关须按照核证作业准则的规定，清楚述明须向倚据人士作出的所有陈述，包括该机关所支援的任何证书政策，例如：

- 倚据人士须了解使用该证书的目的；

- 倚据人士须核实数码签署的责任；
- 查证撤销及暂时吊销证书的责任；及
- 确认接受适用的法律责任限制及保证。

3.1.4 储存库的责任

认可核证机关须清楚述明该机关就提供储存库服务所承担的责任，包括条例载列的特定责任，其中包括核证机关的认可条件及本业务守则。该等责任的例子包括及时公布证书及撤销证书（包括在适合的情况下暂时吊销证书）的资讯，以及有关储存库可供接达和可供使用的条款。

3.2 法律责任

认可核证机关须清楚指明任何与摊分责任有关的适用条文，包括在登记人及本业务守则内界定的获适当授权的人提出撤销或暂时吊销证书的要求之时起，至该机关实际撤销或暂时吊销证书之时止的一段期间内，利用证书作为支援而进行的交易的处理方法。

此外，认可核证机关须清楚指明每项述明的倚据限额的影响。在任何情况下，本部分均不得被视为豁免或弥偿该机关，使其免负任何法律上不能豁免的法律责任。

3.2.1 保证及保证的限制

认可核证机关须就其发出的每类型、类别或种类的证书，清楚指明其有意采用的任何保证及／或施加的限制。

3.2.2 损害赔偿的涵盖范围及卸责声明

认可核证机关须就其发出的每类型、类别或种类的证书，清楚指明其法律责任的涵盖范围（例如直接的、间接的、特别的、相应的、突发的及算定损害赔偿）以及任何卸责声明和责任限制的范围。

3.2.3 损失限制

认可核证机关须就其发出的每类型、类别或种类的证书，清楚指明每张证书或每宗交易的损失限制。

3.2.4 其他豁免事项

认可核证机关须就其发出的每类型、类别或种类的证书，清楚指明其他适用的豁免事项。

3.3 财务责任

认可核证机关须指明与该机关及其他任何在核证作业准则内识别的人士的财务责任的有关事宜，范围包括：

- 受信关系会否在核证作业准则内识别的人士之间出现，或会否因发出证书而在有关人士之间出现；
- 行政程序的财政责任；
- 认可核证机关就其潜在或实际的法律责任以及针对其证书的倚据限额而提出的申索，向登记人及倚据人士提供的财务保证；及
- 其他财务方面的事宜，例如履约保证金、保险单，或其他由认可程序引致的责任（例如作为认可条件之一的责任）。

3.4 释义及执行

3.4.1 管限法律

认可核证机关须述明该机关及其核证作业准则，登记人协议及倚据人士协议的管限法律及司法管辖区。

3.4.2 解决争议程序

认可核证机关须述明该机关所制订的、用以解决有关其运作及因该机关向登记人或倚据人士所作陈述所引致的争议及申索的程序。该等程序须

最少指出向该机关提出争议或申索的程序，以及该机关对于在接获申索或争议的通知程序后所采取的步骤。

3.5 收费

认可核证机关须就其发出的每一类别、类型或种类证书的发出、撤销、暂时吊销、检索或核实证书状况，清楚述明向登记人及倚据人士收取的所有费用。

3.6 公布及储存库

认可核证机关须指明该机关所采用的政策及机制，以向其登记人及倚据人士提供有关其证书、其核证作业准则（包括该机关所支援的任何证书政策细节）、以及该机关的现行认可状况及其发出证书的现行认可状况等资讯。该机关应最少述明包括公布办法、公布频密程度、资讯是否可供取阅、接达储存库的管制措施及储存库的细节。

核证作业准则的全文，或一份删去运作细节以免对认可核证机关及其组成部分的完整性产生负面影响的删短版本，须在该机关的网页或其他可供方便接达的地点清楚展示出来。

由于认可核证机关所依循的实际程序预期会逐趋完善，核证作业准则的更新内容须在切实可行的范围内尽快公布。所有变更须在展示核证作业准则的同一地点清楚展示出来，并在切实可行的范围内尽快向总监报告。

3.7 关于遵守规定的评估

认可核证机关须述明有关该机关的遵守规定评估的机制及频密程度，包括根据条例及本业务守则的任何强制性规定。具体范围可包括：

- 就认可核证机关及其任何以外发形式执行功能进行遵守规定评估的频密程度；
- 执行评估的独立评估人的身分和资历；
- 评估人与接受评估的认可核证机关之间的关系；
- 评估内容涵盖范围；及

- 有关传达遵守规定评估的结果的政策（即报告文本的收件人）及跟进行动的政策。

3.8 保密政策

认可核证机关须指明该机关维持资讯保密的政策。须特别注意的事项包括：

- 认可核证机关（包括任何以外发形式执行的功能）须保持机密的资讯的类型；
- 不属机密的资讯的类型；
- 有权获告知证书被撤销或暂时吊销的原因的人；
- 发放资讯的政策，例如：提供资讯给执法人员，在法律程序下被要求披露等；
- 有关发放纪录及资讯的政策；
- 认可核证机关（包括任何其以外发形式执行的功能）可因应资讯拥有人的要求／同意而披露资讯的情况；及
- 任何其他可以披露机密资讯的情况。

总括来说，认可核证机关须遵守有关个人资料的私稳的所有适用规例，而核证作业准则的条文则不得抵触香港特别行政区现行有关私稳的规例及条例第 46 条的规定。

3.9 知识产权

认可核证机关须顾及关于证书、证书的撤销／有效性的资讯、核证作业准则、证书政策、作业实务／政策的规定、名称及密码匙的知识产权。

4 识别及认证

认可核证机关须载列该机关或其外发的注册机构功能（如适用的话）在发出证书前对证书申请人进行核实的程序。该机关发出的每一类别、类型或种类证书的程序均须予以阐述。

此外，认可核证机关须涵盖证书密码匙更新或在撤销后证书密码匙更新的核实程序。该机关亦须顾及与命名有关的作业实务，例如：名称拥有权、名称争议及解决方法。

认可核证机关须指明其接受的各种识别方式，例如：香港身分证、护照、公司章程及商业登记证等。

4.1 初步核证

认可核证机关须指明在发出新证书时采取的身分证明和认证程序及命名方式。认可核证机关须涵盖该机关用以证明证书申请人身分而所采取的特定程序，包括该机关在发出证书给证书申请人前该个人或团体须提交的特定文件。

4.1.1 名称种类

认可核证机关须指明该机关所采用的命名常规，如“X.500 特定名称”(X.500 Distinguished Names)或适用于网站证书的其他命名方式。其他的命名方式（例如电子邮址或个人识别号码）也可包括在内，以确保个人的证书可清楚地加以识别。

认可核证机关亦须指明所有命名方式的细节，包括可能会采用的前缀及常规，以防止相同名称的出现。

4.1.2 名称是否应具意义

认可核证机关须指明证书内的名称是否须具有意义（即使用获广泛理解的语义以描述个人或机构的身分）。如证书内的名称应该具有意义，则应指明该机关所采取的程序，以确保所发给登记人的特定名称具有意义并能适当地识别登记人。

4.1.3 阐释不同命名形式的规则

认可核证机关须提供为根据核证作业准则发出的证书所载的名称格式而设的阐释指引。这范围的深入程度取决于证书所载的名称格式。一般来说，如证书所载名称的阐释有可能为倚据人士误解，认可核证机关须考虑向倚据人士提供指引以减少产生错误阐释的风险。

4.1.4 名称的独特性

如证书所载的名称规定须具有独特性，认可核证机关须制定规格以供依循。如证书的名称须保存独特性，认可核证机关须披露其规定或任何适用的统一命名规则，以确保特定名称的独特性。

4.1.5 解决命名争议的程序

在适合的情况下，认可核证机关须指明该机关解决命名争议的有关程序。

4.1.6 证明管有私人密码匙的办法

如证书申请人产生本身的配对密码匙，而且只有其本人能控制该私人密码匙，认可核证机关必须述明该机关如何核实申请人的私人密码匙与申请人送交该机关以供核证的公开密码匙是对应的。

4.1.7 登记人身分的核实

认可核证机关须指明该机关为确保证书上的登记人与获发证书的证书申请人的名称相符而采取的程序。如认可核证机关采取特别的程序，以核实载于或将会载于证书上的申请人资讯（申请人名称除外），该机关须列明该等特别程序。该等资讯将有助于使申请人了解根据核证作业准则取得数码证书的所需规定，以及帮助倚据人士了解并推断出根据核证作业准则发出的证书的可靠性。

4.2 例行密码匙更新及证书续期

认可核证机关须阐述该机关为进行例行密码匙更新及为证书续期而采取的程序；如用以证明登记人身分的程序与证书首次注册及发出时所采取的程序不同，尤须作此阐述。该机关须在其核证作业准则内述明证书是否可不作密码匙更新而续期。

4.3 撤销证书后的密码匙更新

认可核证机关须指明该机关在撤销证书后再进行补发时，会否采用与首次发出证书时不同的程序。

4.4 撤销证书的要求

认可核证机关须指明在认证及处理撤销证书的要求时所采取的程序及机制，例如：

- 何人获授权提出撤销证书的要求，以及在何种情况下提出此要求；
- 撤销证书的影响；
- 证书撤销后，关于该证书的有效性的资料最快会在何时公布；
- 登记人对于引致证书须予撤销的事件作出报告的责任；及
- 在有人提出撤销证书的要求时对登记人所给予的保障，包括该核证机构与登记人的法律责任摊分的情况。

4.5 暂时吊销证书的要求

认可核证机关须指明该机关是否支援暂时吊销证书服务，如该机关提供这项服务，则须详细列明暂时吊销证书的条件及其影响。认可核证机关须具体指明暂时吊销证书将如何执行，并且在适合的情况下，亦须包括第 4.4 段中就吊销证书而提及的相同的事项。

5 操作方面的规定

5.1 申请证书

认可核证机关须说明与证书申请人申请新证书有关的详情，包括：

- 申请证书的方法及规定提交用以证明申请人身分的文件；

- 有关的资讯，包括但不限于登记人的责任，认可核证机关的陈述、证书的条款及条件、核证机关及证书的认可状况及认可状况对登记人的意义（证书并非认可证书时尤须注意这点）；及

- 用以提交申请的界面规定。

5.2 发出证书

认可核证机关须说明该机关在发出证书时所依循的具体程序详情。发出证书的程序包括：

- 密码匙的产生；

- 把密码匙交付适合人士（即是，如密码匙由证书申请人所产生，该公开密码匙必须与申请证书的要求一并交付认可核证机关，而该机关必须核实申请人管有对应的私人密码匙。如密码匙由认可核证机关所产生，私人密码匙必须稳妥地交付申请人，而该机关必须列明所采取的适合措施，以确保其所管有的密码匙得到适当的处理）；

- 在未取得登记人书面同意的情况下，认可核证机关不得管有登记人的私人密码匙；

- 证书的产生；

- 把证书交付申请人；及

- 在储存库公布证书。

5.3 接受证书

认可核证机关须界定技术或程序方面的机制，以：

- 向证书申请人解释第 3.1.2 段所界定的他们作为登记人的责任；

- 通知申请人证书已经发出及证书所载的关于申请人的资讯；

- 容许申请人接受或拒绝接受该证书；及

- 协助申请人从核证机关取得证书。

认可核证机关须确保申请人在接受证书前有机会核实已经或将会载于证书的关于申请人的资讯。

5.4 暂时吊销及撤销证书

认可核证机关须解释用以暂时吊销或撤销证书的程序。此外，该机关须说明登记人或获适当授权人指示该机关暂时吊销或撤销证书的程序。

5.4.1 暂时吊销证书

认可核证机关须提供暂时吊销证书的详细程序，包括：

- 暂时吊销证书的条件（包括但不限于何人可以指令／撤回暂时吊销证书）；
- 要求／指令暂时吊销证书的方式；
- 暂时吊销证书的公告方式（例如透过通告、电子邮件、把该证书纳入证书撤销清单内或任何其他公布有关暂时吊销资讯的方式）；
- 撤回暂时吊销证书或把暂时吊销证书改为撤销证书的条件，例如时限；
- 认可核证机关暂时吊销认可证书的所需时间，以及在登记人或获适当授权人要求暂时吊销证书与证书实际被暂时吊销之间的一段期间内，因使用证书进行交易引致的法律责任的摊分；
- 认可核证机关向登记人或获适当授权人查证该遭暂时吊销的认可证书于暂时吊销期过后应否予以撤销或是恢复其有效性的预计时限；及
- 如认可核证机关不能接触登记人或获适当授权人以确定该遭暂时撤销证书的最终安排时，该机关所采取的行动。

5.4.2 撤销证书

认可核证机关须提供撤销证书的详细程序，包括：

- 撤销证书的条件（包括但不限于何人可指令／撤回撤销证书）；
- 要求／指令撤销证书的方式；
- 作出撤销的公告方式（例如透过通告、电子邮件、把该证书纳入证书撤销清单内、更新载有撤销证书／证书有效性的资讯的伺服器或任何其他公布有关撤销资讯的方式）；及
- 认可核证机关撤销认可证书的所需时间，以及在登记人或获适当授权人要求撤销证书与证书实际被撤销之间的一段期间内，因使用证书进行交易引致的法律责任的摊分。

登记人或获适当授权人可使用能识别将被撤销的证书、能解释撤销证书的理由及能核实撤销证书要求（如数码或人手签署）的界面，提出撤销登记人的证书的要求。撤销证书要求的认证是十分重要的，因为这措施可以防止未获授权人恶意提出撤销证书的要求。传送要求的方式，例如电子邮件及网络界面，须随时可供登记人及获适当授权人使用。

一般来说，证书在下列情况下须予以撤销：

- 证书内的识别资讯或特征在证书有效期届满前有所变更；
- 知悉登记人已违反对应的核证作业准则的规定；
- 登记人怀疑或确认私人密码匙的资料外泄；或
- 登记人不再希望拥有或需要签署电子讯息的能力。

5.4.3 证书撤销清单及其他公布有关撤销资讯的方式

证书撤销清单指明由认可核证机关发出但已经被撤销的证书，并可就每一证书说明其撤销理由。认可核证机关须述明分发证书撤销清单的机制，及倚据人士如何接达该等清单，并须指明更新证书撤销清单的频密程度。

认可核证机关可决定使用或支援任何其他公布有关证书撤销资讯的方式。认可核证机关须说明可供使用的接达资讯机制、有关机制的使用条款和条件及有关资讯的更新频密程度。

5.4.4 就证书撤销清单或其他公布有关撤销资讯的方式而规定的查核要求

认可核证机关须通知登记人及在一般可以接达的地点明显地作出通告，指出如载有公开密码匙以核实数码签署的证书不再有效，倚据该数码签署是具有风险的。

此外，认可核证机关须清楚地及明显地指明其在倚据人士暂时不能取得有关撤销证书的资讯（而如该认可核证机关亦透过证书撤销清单或其他公布有关撤销资讯的方式公布有关证书暂时吊销的资讯，则亦包括有关证书暂时吊销的资讯）的情况下所采取的政策。认可核证机关须特别指出在这种情况下的摊分法律责任的问题。

5.5 保安覆检程序

认可核证机关须阐述该机关所采用的事件记录及覆检系统，以维持一个安全的运作环境。该等系统包括的范围如下：

5.5.1 所记录事件的类型

认可核证机关须阐述该机关将会记录的事件的类型。认可核证机关最少须考虑记录下列事件：

- 电脑设施的行政管理，包括但不限于：
  - 网络上的可疑活动；
  - 重复的未能接达的情况；
  - 与就核证机关的整体运作而设置的设备和软件的安装、修改及组态设定有关的事件；
  - 使用特许方式接达核证机关各部分的事件；及

- 一般的证书管理运作，例如：
  - 撤销及暂时吊销证书的要求；
  - 实际发出（包括向认可核证机关申请认可证书的任何人的身分证明文件）、撤销及暂时吊销证书；
  - 证书续期；
  - 更新储存库；
  - 有关证书撤销及暂时吊销的资讯的产生及公布；
  - 核证机关密码匙的产生以及密码延续（包括有关文件）；
  - 登记人配对密码匙的产生（包括有关文件）；
  - 备份；及
  - 紧急的密码匙运作复原。

在切实可行的范围内，所记录的事件须识别引发该事件的单位或个人，以及包括任何作出回应的行动及采取行动的人员。所有纪录内容须盖上日期及时间。

认可核证机关首先根据现行获接纳的作业实务，对个别与保安有关的事件和趋势的严重性及重要性订立界限，是良好的作业方法。所有超出界限的事件和重要趋势必须加以记录。

认可核证机关须区分特权及实施其他机制或程序，以确保所有纪录完整无误。认可核证机关须阐述用以区分特权的机制及程序。

5.5.2 处理事件纪录的频密程度

认可核证机关须指明处理事件纪录（例如综合审核及检讨）的频密程度。

5.5.3 事件纪录的保存期限

认可核证机关须指明事件纪录的保存期限，而该期限须符合本业务守则的规定。

5.5.4 事件纪录的保护

认可核证机关须指明为保护事件纪录免受意外损毁或蓄意修改而采取的机制。

5.5.5 事件纪录备份的程序

认可核证机关须指明把事件纪录备份的程序及备份的保留期限。良好的作业实务是要确保储存设施能为备份提供足够的保护，以免备份遭盗窃和损毁或出现媒体衰变。此外，必须确保在存档期间，数据的储存和检索方法是现行及有效的方法。

5.6 纪录存档

认可核证机关须阐述关于该机关保留一般纪录的政策。一般来说，认可核证机关须确保其所存档的纪录的详尽程度，足以确立在以往发出的证书的有效性及该机关在以往能妥善运作。认可核证机关可考虑存档的主要数据类型包括：

- 与设立核证机关的设备有关的数据，如：
  - 系统设备的组态设定档案；
  - 设备评估及／或设备评审检讨的结果（如曾经进行）；
  - 核证作业准则；及
  - 认可核证机关须予遵守的任何具合约性质的协议。
- 与认可核证机关的运作有关的数据：
  - 任何上述数据项目的修改或更新；

- 所有已发出的证书及已公布的有关证书撤销及暂时吊销的资讯；
- 定期的事件纪录（根据第 5.5 段的规定）；及
- 其他用以核实存档内容的所需资料。

5.6.1 存档的保留期限

认可核证机关须指明存档纪录的保留期限，而该期限须符合本业务守则的规定。

5.6.2 存档的保护

认可核证机关须指明用以保护存档纪录的程序，例如：

- 该等存档的保管人；
- 接达该等纪录的机制，例如：为覆检或解决争议等目的；及
- 保护存档免受意外损毁或蓄意修改、盗窃或媒体衰变的机制。

5.6.3 存档备份的程序

认可核证机关须指明为存档纪录备份的程序及备份的保留期限。良好的作业实务是要确保储存设施能为备份提供足够的保护，以免备份遭盗窃和损毁或出现媒体衰变。此外，必须确保在存档期间，储存及检索数据的方法是现行及有效的方法。

5.7 密码匙变更

认可核证机关须指明该机关变更其密码匙的程序及把有关程序通知登记人的机制。

5.8 密码匙资料外泄及运作复原

认可核证机关须阐述该机关在密码匙资料外泄或发生灾难时发出通知及运作复原的程序。该机关须特别说明下列事项：

- 认可核证机关在其电脑资源、软件及／或数据遭破坏或泄漏的情况下，或怀疑遭破坏或泄漏的情况下所采取的运作复原程序。该等程序阐述如何重新建立稳妥可靠的环境、须予撤销的证书、认可核证机关本身的密码匙应否予以撤销、如何为登记人提供新的核证机关公开密码匙及如何重新核证登记人的方法；

- 认可核证机关在密码匙资料外泄或怀疑外泄时所采取的运作复原程序，包括通知登记人和倚据人士，及重建核证机关稳当运作的程序；及

- 在发生自然或其他灾害后但在稳妥可靠的环境尚未在原地点或后备地点重新确立前，认可核证机关为其设备作稳妥安排的程序，例如在受损毁的地点保护敏感资料免遭盗窃的程序。

如发生任何上述事件必须立即通知总监。

5.9 核证机关终止服务

认可核证机关须指明该机关终止服务及通知登记人及倚据人士有关其终止服务的安排，包括该机关的存档纪录保管人的身分。该等安排须遵守本业务守则第 11 段载列的规定。

6 实体、程序及人事保安方面的管制措施

认可核证机关须阐述该机关制定的非技术性运作管制措施，以保证其业务以稳当的方式进行。

该等管制措施的主要例子包括核证机关主要功能的实体、程序及人事方面的管制措施；核证机关的主要功能计有密码匙的产生、证书申请人身分的核实、证书的发出、证书的撤销或暂时吊销、审核、存档等。核证机关亦可就储存库及任何以外发形式执行的功能（例如注册功能）制订类似的管制措施。

6.1 实体保安管制措施

认可核证机关须阐述对装载该机关系统的设施的管制措施，其中包括：

- 场地的地点及结构；
- 识别保安范围及实体进入有关范围的考虑因素；
- 环境灾患，例如：电力供应、空气调节、湿度、水灾、火灾等；及
- 媒体储存及处置。

6.2 程序管制措施

就认可核证机关的运作而言，获信任职位指某些职位，其担任人士无论是因意外或蓄意而引致不恰当地执行其职责，便可能令该机关出现保安问题。获信任职位包括负责监管的管理人员及操作人员。获得选择担当该等职位的人必须具备所需才能及足以胜任。该等职位所发挥的功能是整个核证机关进行稳当运作的基础。

认可核证机关须阐述该机关识别人选担任获信任职位（例如产生认可核证机关密码匙）的程序，及界定该等职位的责任。一般来说，该等程序的规定会指明将执行的工作、执行每项工作的所需人数及职级，及将会推行的管制措施如双重管制、识别以至认证有关人士等。

获信任职位的例子包括：

- 核证机关行政主管——负责监察所有证书的发出、认可核证机关的运作及收集及备存纪录。基本来说，核证机关行政主管应确保该机关的核证机关功能按照其核证作业准则内的规定执行；
- 密码匙复原代理人——与备存密码匙复原资料或系统有关的特定功能的负责人员；及
- 其他获信任职位——认可核证机关可在核证机关行政主管的监督下界定其他角色。该等角色须按照核证作业准则内的有关条文执行特定功能。在适当的情况下，所有对系统完整性有潜在影响的运作须实行区分职责的措施。

6.3 人事保安管制措施

认可核证机关须阐述有关该机关人员的聘用、监察、评估、培训及终止雇用的管制措施。可予说明的具体事项包括：

- 聘用程序，包括对招聘担任获信任职位及其他执行敏感程度较低的职位的人士进行的背景审查和保安查核程序；
- 培训规定及程序，包括任何再培训期限及再培训程序；
- 不同角色之间职务轮换的频密程度及次序；
- 工作表现评核架构，及对擅自行动、不适当使用权力及擅自使用认可核证机关系统的人员采取的纪律处分和终止雇用的程序；
- 对合约人员的管制措施，包括合约内的规定，例如：合约人员须就其行动所引致的损失作出弥偿，以及监察合约人员的工作表现等；及
- 为有关人员提供的文件，例如：使用者手册、操作程序等，以支援该等人员执行职务。

7 技术保安管制措施

认可核证机关须界定该机关制订的技术保安措施，该等措施特别用于保护其密码匙及启动数据（例如：个人识别密码、密码等）。此外，该机关可阐述其打算对储存库或登记人等采取的任何规定或限制，以确保其密码匙及关键的保安参数得到适当的保护。稳妥的密码匙管理对维持稳当系统甚为重要。它确保所有私人密码匙及启动数据受到保护，并且只有获授权人才可使用。此外，认可核证机关须阐述该机关所采用的其他技术保安管制措施，以支援密码匙及证书管理的运作。

认可核证机关所执行的管制措施必须与其他人士的管制措施，例如任何以外发形式执行的功能（如注册功能、储存库等）以及登记人所执行的管制措施分开，以清楚识别有关方面的责任。

可予说明的具体管制范围包括：

- 配对密码匙的产生、安装，及配对密码匙管理工作的其他方面，包括：
  - 产生公开及私人配对密码匙的责任；
  - 把私人密码匙稳妥地交付证书申请人（如该配对密码匙是由认可核证机关为申请人而产生的）；
  - 把申请人的公开密码匙稳妥地交付发出证书的人（如该配对密码匙是由申请人产生的）；
  - 把认可核证机关的公开密码匙稳妥地交付登记人；
  - 所采用的密码匙大小（可供使用的技术须予以考虑）；
  - 有关公开密码匙参数的产生及品质检查的管制措施；
  - 所使用的密码模组类型及品质的规定；及
  - 密码匙的使用及目的(根据《X.509 公开密码匙基础建设证书结构》（第三版）及《证书撤销清单结构》（第二版）(X.509 PKI Certificate Profile version 3 and CRL Profile version 2)的标准在密码匙使用旗标上作出标示)。
- 私人密码匙的保护，例如：
  - 密码匙产生模组的规定标准(如有的话)，例如符合《ISO 15782-1/ FIPS 140-1 密码模组的保安规定》（ISO 15782-1/ FIPS 140-1 Security Requirements for Cryptographic Modules）的某个水平的标准；
  - 对私人密码匙使用多人管制的措施；
  - 把私人密码匙备份，包括备份的形式及备份系统的有关保安管制措施；

- 私人密码匙存档，包括存档密码匙的形式及存档系统的有关保安管制措施；

- 对私人密码匙启动、使用及停止启动的管制措施，包括密码匙数据输入所需的人数、私人密码匙的形式、启动机制、已启动的密码匙的生效期等；

- 有关销毁密码匙的管制措施，例如：交出权标、销毁权标或重写密码匙；

- 公开密码匙存档；及

- 公开及私人密码匙的使用期间。

- 启动数据的管制措施，扼要列出启动数据生命周期(即由产生、分派至存档及销毁的过程)的管制措施。管制措施的考虑因素应与上文阐述的产生配对密码匙及保护私人密码匙的考虑因素相似；

- 电脑保安管制措施，扼要列出为防止及侦测认可核证机关系统的擅自接达、修改或资料泄漏所采取的保安措施。适当的电脑保安级别架构可予参考，例如《ISO 15408：1999 资讯科技保安评估通则》(ISO 15408：1999 Common Criteria for Information Technology Security Evaluation (CC))；

- 系统发展生命周期管制措施，扼要列出认可核证机关对系统发展生命周期所采取的管制措施，涵盖为初次配置的认可核证机关设备而采购或发展的软件及硬件的机制和程序，以防止擅自改动的情况；

- 网络保安管制措施，扼要列出保护认可核证机关设备所有连接情况的管制措施，例如：适当配置及维持的防火墙，或相等的接达管制装置，及监察尝试擅自接达的情况并防止遭受恶意的攻击；及

- 密码模组工程管制措施，扼要列出密码模组的具体管制规定。在制订管制措施时，可参考适合的标准，例如《ISO 15782-1/FIPS 140-1 密码模组的保安规定》(ISO 15782-1/FIPS 140-1 Security Requirements for Cryptographic Modules)。

8 证书及证书撤销清单的结构

认可核证机关须指明核证机关采用的证书格式、证书撤销清单的格式及公布证书撤销资讯的任何其他方式的格式（如适用），包括结构、版本及所使用的伸延的资讯。认可核证机关一般会根据《ITU X.509》(第三版)（ITU X.509 v3）的证书格式发出及管理公开密码匙证书，并根据《ITU X.509》(第二版)（ITU X.509 v2）的证书撤销清单格式产生及公布证书撤销清单。

认可核证机关须尽可能采用获广泛接受的标准，以促进使用证书的应用系统之间的互通性。因此，在证书及证书撤销清单方面，极力建议使用符合《RFC 3280 互联网 X.509 公开密码匙基础建设证书及证书撤销清单结构》(RFC 3280 Internet X.509 PKI Certificate and CRL Profiles)（或互联网工程专责小组其后公布的任何更新版本）的标准，及避免使用关键的伸延。

8.1 证书结构

认可核证机关须提供与证书结构的具体规格有关的资讯，涵盖范围可载列如下：

- 所支援的版本编号；
- 证书所使用的伸延，特别是已有内容的伸延及其关键性；
- 加密算法的物件识别项目;
- 所使用的名称形式；
- 命名限制；
- 证书政策的物件识别项目；
- 政策限制伸延的使用；
- 政策识别字段的语法及语义；及
- 主要的证书政策伸延的语义处理。

8.2 证书撤销清单的结构

认可核证机关须提供与证书撤销清单有关的资讯，并可提述适合的标准，涵盖范围包括：

- 证书撤销清单所支援的版本编号；及
- 证书撤销清单所采用的资料伸延及其关键性的详情。

如认可核证机关采用其他方式公布有关证书撤销的资讯，该机关须提供关于该公布方式的资讯，以便其他人士得以接达有关证书撤销的资讯。

9 规格的管理

认可核证机关须阐述如何备存核证作业准则。

9.1 规格的变更程序

认可核证机关须阐述对核证作业准则作出任何变更的程序，包括根据本业务守则载列的规定把有关的变更通知总监、登记人及倚据人士的机制。认可核证机关须尽快在该机关的储存库内公布及提醒对核证作业准则作出的变更。此外，该机关可指明无须给予事先通知的变更的类型。

9.2 公布及通知程序

认可核证机关须阐述在所有登记人及倚据人士知悉的储存库公布所有有关资讯的程序，而该储存库可以是一个网站。认可核证机关必须指出该储存库的位置及其他的资讯来源。

10 互通性

为促进互通性，认可核证机关须采用获广泛接受的技术标准及管理措施。为方便应用系统使用其证书及服务，认可核证机关须在适当的情况下指明其所采用的标准及作业实务，以及已选定的选项及界面规格的详情。认可核证机关须公布的详情包括但不限于其储存库采用的标准（例如：对目录的轻量式目录接达规约（LADP）或兼容规约、网页的超文本标示语言（HTML）等），及具体的证书结构（例如 X.509）、证书伸延等。

附录 2 — 就核证机关的评估而指明的《电子交易条例》及本业务守则的条文

1 为施行《电子交易条例》（第 553 章）（“条例”）第 20(3)(b)(i)、27(5A)(b)(i)及 43(1)(a)(i)条而指明的条例及本业务守则的条文

1.1 条例的下列条文属于获总监认可为合资格人士所作评估的范围：

(a) 第 VII 部 — 总监对核证机关及证书的认可：
第 21(4)(a)、(b)、(c)及(f)条。

(b) 第 X 部 — 关于认可核证机关的一般条文：
第 36、37、39、40、42(1)及(2)、44 及 45(1)条。

(c) 第 XI 部 — 关于保密、披露及罪行的条文：
第 46、47 及 48 条。

1.2 本业务守则的下列条文属于获总监认可为合资格人士所作评估的范围：

(a) 认可核证机关的一般责任：
第 3.1 至 3.6 各段及第 3.8 段。

(b) 核证作业准则：
第 4.1 至 4.13 各段。

(c) 稳当系统：
第 5.1 至 5.3 各段、5.6 至 5.17 各段及 5.19 至 5.21 各段。

(d) 证书及认可证书：
第 6.1 至 6.23 各段。

(e) 登记人身分的核实：
第 7.1 及 7.2 段。

(f) 倚据限额以及为法律责任投保：
第 8.1 至 8.4 各段。

(g) 储存库：
第 9.1 至 9.5 各段。

(h) 披露资讯：
第 10.1 至 10.6 各段。

(i) 终止服务：
第 11.1 至 11.5 各段。

(j) 对遵守条例及本业务守则的评估：
第 12.1 段。

(k) 声明遵守条例及本业务守则的规定：
第 13.1 段。

(l) 标准及技术的采用：
第 14.1 段。

(m) 互通性：
第 15.1 及 15.2 段。

(n) 附录 1：
本业务守则附录 1 所有段落。

2 为施行条例第 20(3)(c)(i)、27(5A)(c)(i)及 43(1)(b)(i)条而指明的条例及本业务守则的条文

2.1 条例的下列条文须以核证机关一名负责人员作出法定声明的方式处理：

(a) 第 VII 部 — 总监对核证机关及证书的认可：
第 21(4)(e)条。

2.2 本业务守则的下列条文须以核证机关一名负责人员作出法定声明的方式处理：

(a) 认可核证机关的一般责任：
第 3.7 及 3.9 段。

(b) 稳当系统：
第 5.18 段。

(c) 披露资讯：
第 10.7 至 10.9 各段。

(d) 消费者的保障：
第 16.1 段。

3 为施行条例第 43A(1)(c)(i)及(d)(i)条而指明的条例及本业务守则的条文

3.1 视乎认可核证机关将会或已经对其系统、运作、管制措施及程序作出的重大变更的具体情况而定，总监会在他根据条例第43A(1)条可向认可核证机关发出的通知中，为施行条例第43A(1)(c)(i)及(d)(i)条而指明条例及本业务守则的相关条文。