附件 2:

粤港电子签名证书互认证书策略

版本序号：1.0

工信部的对象标识符为：2.16.156.339.1.1.1.2.1（自然人）/ 2.16.156.339.1.1.2.2.1（法人）

香港资科办的对象标识符为：2.16.344.8.2.2008.810.2.2012.1.0（繁简体版本使用同一对象标识符）

生效日期：2012 年 8 月 10 日

粤港电子签名证书互认证书策略

版本序号：1.0

目录

工信部的对象标识符为: 2.16.156.339.1.1.1.2.1 (自然人) / 2.16.156.339.1.1.2.2.1 (法人)
香港资科办的对象标识符为: 2.16.344.8.2.2008.810.2.2012.1.0 (繁简体版本使用同一对象标识符)

一、适用证书范围

（一）本证书策略是核准由依据《中华人民共和国电子签名法》获得电子认证服务许可并在广东省注册登记的第三方电子认证服务机构或依据香港特别行政区《电子交易条例》成立的认可核证机关（以下统称为电子认证服务机构）签发的电子签名证书或认可数码证书（以下统称电子签名证书）能否应用于粤港跨境电子交易的重要依据。

（二）本证书策略主要适用于粤港跨境电子交易使用的个人电子签名证书和组织机构电子签名证书（以下简称为“个人证书”和“组织机构证书”，或统称为“证书”）。本证书策略亦适用于签发上述证书的电子认证服务机构本身的证书（以下简称为“电子认证服务机构本身的证书”）。

（三）本证书策略在规范签发上述证书的电子认证服务机构行为基础上，对规范证书持有人（以下简称为“订户”）、证书依赖方（以下简称为“依赖方”）等参与方行为亦提出明确要求。

二、规范范围

本证书策略对电子认证服务机构有关证书的服务和管理提出以下规范性要求：

* 信息发布；
* 身份标识与鉴别；
* 证书生命周期操作要求；
* 认证机构设施、管理和操作控制；
* 认证系统技术安全控制；
* 证书和证书吊銷列表的描述；
* 合规性；
* 赔偿限额、赔偿安排和法律解决；
* 信息保密。

三、总体责任

（一）电子认证服务机构（包括其注册机构）须[1]承担以下责任，包括但不限于：

* 制定符合本证书策略要求的电子认证业务规则，依据本证书策略的要求及相关电子认证业务规则的条款，提供认证服务和相关的基础设施；

[1] 在本证书策略中，“须”和“应”也是表示“必须”的意思。

* 电子认证服务机构须建立和执行符合相关规定的安全机制，保证私钥得到安全的存放和保护；

* 所有和认证业务相关的活动须符合本地法律法规和主管部门的规定。

（二）电子认证服务机构须对证书订户承担以下责任，包括但不限于：

* 证书中没有电子认证服务机构所知的或源于电子认证服务机构的错误陈述；

* 生成证书时，不因电子认证服务机构的失误而导致证书中的信息与电子认证服务机构所收到的信息不一致；

* 签发给订户的证书符合本证书策略及相关电子认证业务规则的要求；

* 将按本证书策略及相关电子认证业务规则的规定，及时吊销证书；

* 将向订户通报任何已知的、将在根本上影响证书有效性和可靠性的事件。

（三）电子认证服务机构须对依赖方（按照本证书策略及相关电子认证业务规则合理地依赖签名（该签名可通过证书中所含的公钥验证）的人）承担以下责任，包括但不限于：

* 除未经验证的订户信息外，证书中或证书指向的所有信息都是准确的；

* 完全遵照本证书策略及相关电子认证业务规则的规定签发证书；

* 通过公开发布证书，向所有合理依赖证书中信息的依赖方证明：发证机构已向订户签发了证书，并且订户已按照本证书策略及相关电子认证业务规则的规定接受了该证书。

四、信息发布

（一）信息库

1、电子认证服务机构建立和维护一个或多个可公开查询的在线信息库，用于发布：

* 证书策略、电子认证业务规则及相关披露文档等信息；

* 证书和证书状态查询（包括但不限于证书目录信息、证书状态信息、证书吊销列表）等信息；

* 可公开的订户协议和必须公开的依赖方协议的最新版本；

* 本地主管部门指明必须发布的其他信息。

2、电子认证服务机构应在电子认证业务规则中清楚指出证书状态信息的发布方式。证书状态可以通过电子认证服务机构网站发布证书吊销列表，也可以通过 LDAP 目录服务器、OCSP 服务器作为证书吊销列表的有效补充。

3、电子认证服务机构须根据 RFC3647 标准（或相关更新版本）制定电子认证业务规则的内容范

围。若有不适用于该电子认证服务机构或某类型、类别或种类的证书范围时，电子认证服务机构须在电子认证业务规则中清楚指出不适用的范围及其原因。

4、电子认证服务机构须通过信息库发布信息让证书的依赖方清楚知道，在依赖方信赖电子认证服务机构签发的证书时，必须对证书的使用承担以下的主要责任，包括但不限于：

* 依赖方已经熟悉本证书策略及相关电子认证业务规则的条款，了解证书的使用目的和可提供的保证，依赖方在信任证书前，须同意依赖方协议中的条款，并根据使用的环境和条件判断该证书是否可信任；

* 如果依赖方需要电子认证服务机构提供额外的保障，即电子认证业务规则中有关条款所提供的额外保障，依赖方应在确认可以获得这些保障之后，自行决定是否信任相应的证书；

* 依赖方对证书进行合理的检查和审核，包括检查电子认证服务机构公布的最新的证书吊销列表，确认该证书没有被挂起或吊销；检查证书信任路径中所有出现过的证书的可靠性；检查证书的有效期；检查其它能够影响证书有效性的信息；

* 依赖方在电子认证业务规则中的其他合理责任；

* 依赖方须承担因未履行以上责任所产生的法律责任。

5、电子认证服务机构在电子认证业务规则及其它相关文档中须清楚指出其信息库的位置和查询方式，以便能让有关人士查询并获取所需信息，尤其是证书订户和依赖方对电子认证业务规则、证书及证书状态的查询。

6、电子认证服务机构须采取有效安全的措施防止信息库受到未经授权的增加、删除、修改等，且在运行及管理信息库时，不得进行任何对依赖信息库（包括证书和其他信息）的人士造成不合理风险的活动。

7、电子认证服务机构须在其与本证书策略相关的电子认证业务规则中声明，在遵守本地法律监管要求和本证书策略的基础上，任何由于电子认证服务机构或相关证书的不足或疏忽所引起的责任和索偿，电子认证服务机构、订户和依赖方对两地政府和电子认证服务主管部门免责。

（二）电子认证服务机构信息发布

8、电子认证服务机构在其信息库中须公布以下证书信息，包括但不限于：

* 电子认证服务机构本身的证书，其中包含与电子认证服务机构用作签发证书的私钥所对应的公钥；

* 电子认证服务机构本身或其主管部门对电子认证服务机构本身的证书进行挂起、吊销或不获续期的通知；

* 任何对电子认证服务机构发出的证书的可靠性或服务能力造成重大及不利影响的事件。

（三）发布时间或频率

9、电子认证服务机构须及时发布及更新信息库中有关披露文档和文档的修订信息，包括但不限于：

* 证书策略；
* 电子认证业务规则；
* 使用电子认证服务机构有关证书服务所需要的相关文档；
* 电子认证服务机构上述文档以往发布、修订信息的披露记录。

10、电子认证服务机构签发的证书和相关信息，必须在生效后及时发布，以供下载、查询和使用。

11、电子认证服务机构应发布证书（包括电子认证服务机构本身的证书）挂起或吊销的信息（包括证书吊销列表和任何其他有关挂起或吊销的信息）。

* 当证书被挂起或吊销时，电子认证服务机构应及时发布有关信息；
* 当证书被挂起或吊销时,电子认证服务机构应及时发布有关的证书吊销列表；
* 电子认证服务机构应至少每 24 小时发布一次证书有关的证书吊销列表；
* 当电子认证服务机构本身的证书被挂起或吊销时，电子认证服务机构应及时发布有关信息；
* 当电子认证服务机构本身的证书被挂起或吊销时,电子认证服务机构应及时发布有关的证书吊销列表；
* 电子认证服务机构应至少每年签发一次电子认证服务机构本身证书有关的证书吊销列表；
* 电子认证服务机构应在合理时间内发布证书吊销列表，并在其相关的电子认证业务规则中清楚指出其证书吊销列表的发布时间。

12、电子认证服务机构不应在其信息库中载有已确认为不正确或不可靠的信息。

五、身份标识与鉴别

（一）证书上的身份命名

电子认证服务机构应在其签发的证书保证:

1、证书在主体名称 (subject name)中包含一个 X.501 甄别名(Distinguished Name (DN))，且按照 X.500 的解释作为不同命名的规则。

2、订户的命名一定要有意义，应具有通常能够被理解的语义，可以明确确定证书主体中的个人或者组织机构的身份，能够把名称与唯一一个确定的实体（个人或者组织机构）联系起来。当出现相同的名称时，电子认证服务机构应有明确制度决定申请者的优先使用顺序。证书不允许使用匿名或假名。个人证书的证书主体应以个人身份命名；组织机构证书的证书主体应以组织机构身份命名。

3、电子认证服务机构应要求证书申请者确保不会使用任何侵犯知识产权的名称。电子认证服务机构应要求证书申请者当其申请的证书内容包含商标信息时，应提交有关的商标注册文件，例如由政府机构发出的合法性证明文件。

（二）初次申请证书时的身份鉴别

4、组织机构身份的鉴别：

当任何组织机构（政府机构、企事业单位或其它社会组织等）提出证书申请时，电子认证服务机构应当先对其身份进行严格的鉴别，包括但不限于：

* 由独立、权威的第三方提供的资料证明该组织确实存在，例如由政府机构发出的合法性证明，或由其它被认可的权威组织提供的证明资料；

* 通过有效方式确认组织机构申请资料的真实性，确保申请已得到该组织机构充分的授权并能提供其它必须验证的信息；

* 申请的组织机构证书包括个人身份名义时，电子认证服务机构应要求该组织机构核实确认个人身份的真实性，并要求提交有关材料进行审核；

* 申请的组织机构证书由授权代表申请时，电子认证服务机构应要求授权代表提交该组织机构充分授权的书面证明文件（如授权书），审核确认授权代表得到该组织机构的明确授权；

* 以面对面的审核方式确认授权代表身份时,通过法定的身份证明文件（包括但不限于身份证、护照或者其它相身份证明资料），确认授权代表的真实身份；

* 在合理情况下使用认为必须的其它额外鉴别方式和资料。

5、个人身份的鉴别：

当个人提出证书申请时，电子认证服务机构应先对其身份进行严格的鉴别：

* 以面对面的审核方式确认个人身份时,通过法定的身份证明文件（包括但不限于身份证、护照或者其它身份证明资料），确认个人的真实身份，且其身份必须与所申请的证书主体相对应；

* 在合理情况下使用认为必须的其它额外鉴别方式和资料。

6、电子认证服务机构须在与某类型、类别或种类的证书对应的电子认证业务规则内清楚指出所采用的组织或个人身份鉴别方法（包括是否采用面对面的审核方式等）。

7、当证书上存在未经明确的、可靠验证的订户信息时，电子认证服务机构须在电子认证业务规则及证书上清楚指出未经验证的信息或信息类别。

（三）证书吊销请求時的身份鉴别

8、电子认证服务机构须对证书吊销请求进行合理的鉴别，包括但不限于以下程序：

* 当订户申请吊销时，电子认证服务机构应要求订户提交与证书申请时相同的身份资料或利用原证书提交合法有效的电子签名的吊销申请，并对订户进行身份鉴别。申请者由于条件限制无法进行现场身份鉴别时，电子认证服务机构或其注册机构应通过合理的方式，例如通过电话、邮递、其他第三方的证明等，对申请者的身份予以鉴别验证。当司法机关依法提出证书吊销时，电子认证服务机构或其注册机构可直接以司法机关书面的吊销请求文件作为鉴别依据，不再进行其他方式的鉴别；

* 考虑到一般情况下，申请者的身份鉴别需要一定时间，不能即时吊销证书，因此容许电子认证服务机构在合理情况下，可挂起证书，但仍应及时进行申请者的身份鉴别程序或处理司法机关书面的吊销请求。

六、证书生命周期操作要求

（一）证书申请

1、电子认证服务机构（包括其注册机构）可接受下列证书申请：

* 任何组织机构（政府机构、企事业单位或其它社会组织等）；

* 任何组织机构（政府机构、企事业单位或其它社会组织等）的授权代表；

* 个人申请者本人。

组织机构、授权代表和个人申请者的身份必须符合本策略的身份鉴别要求。

2、电子认证服务机构须要求所有证书申请者应在证书申请的过程中，

* 清楚了解及同意订户协议的内容，特别是关于责任和担保的内容；

* 根据申请的证书类型提供真实、可靠、完整的身份资料；

* 承担任何因提供虚假、伪造信息所产生的法律责任。

（二）证书申请处理

3、接受或拒绝证书申请:

电子认证服务机构在下列情况下，不应批准下述证书申请：

* 申请未能完全满足本证书策略关于订户信息的标识和鉴别的规定；

* 申请者未能提供必需的身份证明材料或其他必须提供的支持文件；

* 申请者未能接受订户协议的内容和要求，特别是关于义务和担保的内容。

4、电子认证服务机构须保留足以识别申请者身份的文档记录。

5、证书申请的处理期限：

电子认证服务机构必须在电子认证服务规则中明确规定处理时间，并且在承诺的处理时间内完成证书申请。

（三）证书签发

6、电子认证服务机构接受申请者的证书申请后，基于对其证书申请文件进行审核和对申请人的身份进行鉴别的结果，进行证书签发。

7、电子认证服务机构在安全的环境下通过系统为订户制作订户证书（包括密钥对）、以及将证书以安全的方式交给订户等过程，均须保证私钥不受干扰。电子认证服务机构不应接受订户提供的私钥，也不应接受订户的密钥更新请求。

8、电子认证服务机构一旦签发证书，即向任何合理依赖该证书的人或任何合理依赖该证书的公钥所能核实的电子签名的人士保证：

电子认证服务机构已按照相关法律法规、本证书策略和证书相关的电子认证业务规则签发该证书。

9、电子认证服务机构应将已经签发的证书及其他有关的信息发布到可以被公开查询的信息库中。

10、电子认证服务机构及其注册机构均须记录所有与发出证书有关的交易事项，包括日期和时间。

11、电子认证服务机构签发证书后，电子认证服务机构应及时通知订户，并提供获得证书的方式，以确保订户能通过合理方式获得证书。

（四）接受证书

12、电子认证服务机构应在订户协议和电子认证业务规则中清楚说明构成订户接受证书的行为（例如订户接受了包含有证书的介质），并要求订户清楚知道和确认这些构成接受证书的行为。

（五）证书更新

13、电子认证服务机构签发的每张证书须包含有效期，当证书到期时，订户须获得一张更新的证书以继续使用该证书。

14、电子认证服务机构处理证书续期时须确保提出证书续期请求的人是被更新证书所标识的订户。

15、电子认证服务机构及其注册机构均须记录与证书续期有关的所有交易事项，包括日期和时间。

（六）证书变更

16、当证书包含的信息（除公钥外）发生变化时，订户须重新办理证书。电子认证服务机构应不予接受对已发出的证书的内容作出变更的申请。

（七）证书吊销和挂起

17、如电子认证服务机构有合理理由相信其发出的证书已经不可靠，则无论订户同意与否，电子认证服务机构应挂起该证书。电子认证服务机构须在一段合理时间内完成有关证书可靠性的调查，以及决定是恢复该证书的有效性或是吊销该证书。如电子认证服务机构在考虑所有可取得的信息后，认为应即时吊销其发出的证书的，则无论订户同意与否，电子认证服务机构须吊销该证书。电子认证服务机构须在其电子认证业务规则中说明，若未能联络订户时应采取的行动。

18、电子认证服务机构须提供热线电话或其他方式，以供订户向电子认证服务机构报告有关影响其证书或私钥的事件，例如密钥遗失或密钥资料外泄等。

19、电子认证服务机构收到吊销请求后，须验证申请者的身份、权限和吊销理由的正当性，确认无误后方可进行吊销。电子认证服务机构须在其电子认证业务规则明确自接到吊销请求到完成吊销的时限，任何挂起证书的处理不得超过合理的时限。电子认证服务机构须在有关的电子认证业务规则中清楚指出有关时限，并应力求不超过一个工作日。所有非经订户提出的吊销请求，必须通过严格的内部程序并经由指定管理人员审批。当电子认证服务机构挂起或吊销所发出的证书时，须在合理时间内通知该证书的订户。

20、电子认证服务机构必须严格控制由于证书制作过程中的失误（例如证书下载错误、密钥对不匹配）而导致证书吊销。

21、证书被吊销后，电子认证服务机构应在 24 小时内发布吊销信息，包括使用证书吊销列表和其他已公开的证书状态查询渠道（如适用）。电子认证服务机构应在电子认证业务规则中明确具体的吊销信息更新时间。

22、当电子认证服务机构的密钥（包括本身或子电子认证服务机构的密钥）的安全被损害或者怀疑遭受损害时，电子认证服务机构应在合理的时间内采用适当的方式及时通知订户和依赖方。

23、电子认证服务机构必须对证书吊销过程进行适当的记录。

24、电子认证服务机构本身的证书吊销请求，必须经过相关监管部门确定后才可以进行。

（八）密钥对和证书的使用

25、电子认证服务机构须要求所有订户必须在签订订户协议和确认接受证书后，才能使用证书对应的私钥，并要求订户确认一旦接受电子认证服务机构签发的证书，订户即须承当如下责任：

* 订户私钥的使用应符合证书中“密钥用途”（KeyUsage）的要求；

* 订户私钥和证书的使用应符合订户协议的要求；

* 订户在使用证书的公钥所对应的私钥进行电子签名时，即保证是以订户的名义进行电子签名，并且在生成电子签名时，应已确保该证书没有过期或被吊销(若证书已到期或被吊销，订户应停止使用私钥)；

* 订户应保持对其私钥的控制，并采取合理的措施来防止私钥的遗失、泄露、被篡改或未经授权被使用；

* 订户不允许将证书用于非法活动；

* 订户应承担订户协议中的其他责任。

（九）证书状态服务

26、电子认证服务机构必须力求证书状态服务维持 7*24 小时不间断可用，尽量减少服务中断时间。电子认证服务机构须在其电子认证业务规则中列出证书状态服务不间断可用和服务中断时间的安排。证书状态服务如需中断（在安排下或不可预知或非电子认证服务机构能控制的情况下），电子认证服务机构必须尽量减少服务中断时间。电子认证服务机构应确保可预先安排的证书状态服务中断时间每星期不得超过两小时。电子认证服务机构应按本地监管要求，就服务中断事项通知有关各方。

（十）终止证书服务/订购的结束

27、电子认证服务机构须向订户和依赖方（包括在电子认证业务规则中）说明什么情形下代表该订户的证书服务已经终止或订购结束，包括但不限于下列情况：

* 在证书有效期内，证书被电子认证服务机构吊销；

* 在证书到期前提出终止服务的申请，并获电子认证服务机构接受；

* 证书有效期满，没有进行证书更新或密钥更新。

28、电子认证服务机构应明确有关证书订购结束的规定，制定证书订购结束的具体实施流程，并妥善保存记录。

（十一）密钥托管与恢复

29、电子认证服务机构应在其电子认证业务规则中，明确密钥托管和恢复服务的具体实施流程。

30、电子认证服务机构本身的密钥不能被托管，订户的签名密钥也不能被托管。

七、认证机构设施、管理和操作控制

（一）物理安全和环境控制

1、电子认证服务机构须采取有效的物理安全控制措施：

* 识别及界定安全区域（例如有效区分公共区、服务区、管理区、核心区、屏蔽区等），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；

* 制定电子认证服务机构职员及访客进入该范围的正规程序，并设立适当的安全控制措施（包括进入保安范围的监察机制）；

* 须对影响储存物理安全设备的地方加以特别保护；

* 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；

* 具备机房环境监控系统，对基础设施设备、机房环境状况、安防系统状况进行 7*24 小时实时监测，监测记录保存时间应满足故障诊断、事后审计的需要；电子认证服务机构须在其电子认证业务规则中指明监控记录的保存时间，并至少保留 3 个月；

* 门禁系统应有进出时间记录和超时报警提示，电子认证服务机构须定期对记录进行整理归档；电子认证服务机构须在其电子认证业务规则中明确进出时间记录的保存时间，并至少保留 3 个月；

* 确保只有授权人员才能操作电子认证服务机构的物理设备，并应针对不同安全级别的物理设备采取不同程度的访问控制措施，包括但不限于：

  ① 授权人员须使用授权的口令登录物理设备；

  ② 授权人员进入敏感区域时应有两个因子以上的认证机制，其中一个因子应是生物特征认证；

  ③ 确保设备访问日志不被篡改并进行定期检查；

  ④ 需要至少两个具有操作权限的人员来操作密码模块或者计算机系统；

  ⑤ 对高安全级别的物理设备进行 24 小时自动监视或者人工监视。

2、电子认证服务机构及其注册机构的物理安全设施须配置主、备电力供应系统，以确保持续不间断的电力供应。同时，也须有空调系统来控制温度和湿度。

3、电子认证服务机构及其注册机构应通过采取预防措施、采用相应的设备配置、制定相应的处理程序来保护物理设施的安全，尤其应防止水灾或者漏水对系统造成损害及其它不利后果。火灾防护措施应当符合本地消防管理部门的要求。机房应设置火灾自动报警系统和自动灭火系统，电子认证服务机构须在其电子认证业务规则中指明有否设置两种火灾探测器以检测温度和烟雾，火灾报警系统应与灭火系统联动。

4、电子认证服务机构及其注册机构须严格保护备份系统数据及其它任何敏感信息的存储介质，避免这些介质受到水灾、火灾、电磁以及因其它环境要素造成的损坏，并且须建立严格的保护手段以防止对这些介质被未经授权的使用、访问或者披露。

5、电子认证服务机构及其注册机构须建立严格的废物处理流程，特别是包含隐私或者敏感信息的纸张、电子介质及其他任何废弃物，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。

6、电子认证服务机构及其注册机构须建立关键系统和数据（包括审计数据在内的任何敏感信息）的备份制度，对于关键系统和数据应采取异地备份手段以确保其处于安全的设施内。

7、凡电子认证服务机构依靠第三方提供服务以保障物理安全及环境控制的，该类服务须在该电子认证服务机构与第三方供应商订立的正式服务协议内清楚说明。

8、电子认证服务机构的设施应受到保护，并避免受到自然灾害影响。

9、电子认证服务机构应符合本地法律法规、监管条例、技术标准相关的其他适用要求（例如国家机房建设标准、消防条例等）。

（二）过程控制

10、电子认证服务机构应只容许被认定为可信的人员，才可在可信岗位上进行工作。可信岗位上的人员是指能够访问、进入或者控制证书或者密钥操作的角色，可能会对以下几个方面产生重要影响的人员，包括但不限于：

* 证书申请中的信息验证和确认；
* 对证书申请、吊销进行批准、拒绝或者其他操作；
* 证书签发和吊销；
* 对严格控制访问的信息库进行访问；
* 处理订户信息或请求。

11、电子认证服务机构及其注册机构须建立、维护和执行严格的控制流程，根据工作要求和工作安排采取职责分离措施，建立互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。须进行职责分离的角色，包括但不限于下列人员：

* 从事证书申请信息验证的人员；
* 负责证书申请、吊销、更新和信息注册等服务请求的批准、拒绝或其他操作的人员；
* 负责证书签发、吊销等工作或者能够访问受限区域、敏感信息的人员；
* 处理订户信息的人员；
* 生成、签发和销毁电子认证服务机构系统证书的人员；
* 系统上线或者下线的人员；
* 掌握重要口令的人员；

* 密钥及密码设备管理、操作人员。

关键的控制须通过物理和逻辑的分割来实施，其中系统设备的逻辑和物理访问等敏感操作应至少有 2 名可信人员参与。在电子认证服务机构的硬件密钥设备的生命周期（从设备开始运作到逻辑/物理销毁）过程中，对该设备的访问应至少有 3 名可信人员共同参与。另外，一旦一个系统设备的密码模块被激活，进一步的逻辑或物理访问必须实施职责分割。掌握系统设备的物理权限的人员不能再持有系统设备的秘密分割，反之亦然。

（三）人员安全

12、电子认证服务机构须制定有效的人员安全控制规定，并在有需要时更新。

13、对于所有将要在可信岗位上工作的人员，电子认证服务机构必须进行严格的身份识别和考核，确保其能够满足所从事的工作职责的要求，应：

* 根据实际需要确定不同的角色，划分权限，设定不同角色的资历和背景要求，并确保人员符合相应要求；
* 对人员进行安全审查（包括但不限于对被调查人的身份进行当面核查、要求被调查人提供有效身份证件）；
* 根据工作性质和职位权限的情况，赋予在可信岗位上工作的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（包括但不限于用于身份识别的系统操作卡、门禁卡、登录口令、操作证书、作业帐号等安全令牌），以完整地记录该人员所有敏感的操作行为；
* 在员工合同内加入与安全相关的条款。

14、电子认证服务机构须确保其所有人员（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。培训的内容可包括但不限于：

* 适当的技术培训；
* 规章制度和程序；
* 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。

15、电子认证服务机构须制定适当的控制措施以考察人员的表现，例如：

* 定期进行的工作绩效考核；
* 正规的纪律程序（其中包括如何处置未获授权的行为）；
* 正规的终止服务程序。

（四）事件纪录程序/审计流程

16、电子认证服务机构须备存足够的事件纪录存档，包括保留与该电子认证服务机构发出及管理的证书的有关文件，并须定期（不少于每个月一次）检查事件纪录，就任何异常情况采取适当行动。

17、电子认证服务机构须备存纪录所有主要事件，包括但不限于：

* 对用于产生密钥的资料及设备的访问；
* 密钥及证书的产生、发出、分派、储存、备份、挂起、吊销、撤回、存档、销毁及其他有关事项；
* 安全事件，包括但不限于密钥资料泄露、网络入侵等；
* 密码设备的采购、安装、使用、解除运作及弃用；
* 计算机设施的开发和运维记录。

18、电子认证服务机构应保存原始审计日志至少两个月，并定期检查审计日志，以便发现重要的安全事件和管理问题，对发现的事件或问题应采取相应的措施，并对调查或审计行为进行记录备案。电子认证服务机构应当采取严格的物理和逻辑访问控制措施，防止所有的审计日志和记录被未经授权的浏览、修改、读取、删除等。电子认证服务机构应当建立和执行可靠的审计日志备份制度，定期进行备份（至少两个月备份一次），并在其电子认证业务规则中对备份周期进行明确规定。

19、电子认证服务机构应按照本证书策略的要求，对所有审计日志的记录进行归档。归档后原记录应保存至少 5 年，或根据本地相关的法律法规要求，以较高的期限为准。

（五）记录归档

20、电子认证服务机构除纪录事件的规定外，还须对其他所有的重要记录进行归档保存，重要记录包括但不限于：

* 证书系统建设和升级文档；
* 证书和证书吊销列表；
* 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；
* 审计记录；
* 证书策略、电子认证业务规则文档；
* 员工资料，包括但不限于背景调查、录用、培训等资料；
* 各类外部、内部评估文档。

21、不同归档记录的保留期限可能是不同的，电子认证服务机构须根据法律法规的要求、业务

需要和运营服务的实际情况，制订不同归档记录的保留期限，但自证书期满或吊销之日起，各种归档记录应至少保存五年。

22、电子认证服务机构必须保留归档记录的准确时间信息，包含记录产生的日期和时间。

23、电子认证服务机构须采取适当的物理和逻辑访问控制措施，保证只有获授权的可信人员才能访问所有归档的记录。电子认证服务机构应将受保护的归档记录保存在可靠的系统或者场所内，以防止受保护的归档记录被进行未经授权的浏览、修改、删除等非法操作。电子认证服务机构应保证归档记录在保留期内可以被有效的访问，并只有获授权的可信角色人员能够访问归档记录。归档时，电子认证服务机构应对归档记录的一致性进行验证。归档期间，电子认证服务机构必须验证所有被访问的记录（通过适当的技术或方法）的一致性。

24、电子认证服务机构应定期对系统生成的电子归档记录进行备份，并对备份文件实行异地存放。若没对书面的归档资料进行备份，电子认证服务机构须采取严格的措施保证其安全性。

（六）事故处理、紧急应变、灾难恢复及业务持续

25、电子认证服务机构须为包括所有关键运营范围内可能发生的重大事故，制定事故处理、紧急应变、灾难恢复和业务持续运作的程序和应对措施以保证应有的服务水平（包括证书状态查询服务应参照本证书策略第六章“证书生命周期操作要求”第九点“证书状态服务”的要求；其他证书核心服务如证书挂起服务、证书吊销服务等，应指明中断时间），并适时进行维护及更新。可能发生的重大事故包括但不限于：

* 计算机资源、软件、数据出现损坏或重大故障的事件（包括影响外部访问信息库的事件）；
* 注册机构因事故终止服务；
* 电子认证服务机构或其子电子认证服务机构私钥出现损毁、遗失、泄露、被破解、被篡改，或者有被第三者窃用的怀疑时。

26、电子认证服务机构应定期对灾难恢复和业务持续运作的应对措施进行演练，并对演练程序和结果进行记录。应对措施中所包括的有关主要人员均须参与演练。

八、认证系统技术安全控制

（一）密钥对生成和安装

1、电子认证服务机构须制定和采取有关生成密钥对的操作控制措施，包括但不限于：

* 用以确保产生密钥对设备完整无误的程序；
* 用以确保密钥对是由获授权人员在受到严密控制的方式下生成的程序。

2、当电子认证服务机构为订户生成密钥对后，电子认证服务机构应通过安全的途径、以防篡改封装的方式将私钥分发给订户。用于存储证书（包括私钥）的介质技术应符合《粤港两地电子签名

证书互认技术标准列表和采用措施》内的规定(附件 1.2），电子认证服务机构须在电子认证业务规则中指明存储订户证书私钥的介质技术。分发订户私钥和激活私钥的数据应采用不同的途径发给订户，电子认证服务机构应对每次私钥分发进行记录。

3、电子认证服务机必须在符合本地安全、本地监管要求和本策略要求的硬件设备条件下生成用于签发证书和证书状态信息的密钥对。

（二）电子认证服务机构密钥变更

4、电子认证服务机构应适时更新其本身的证书和密钥对，保证其本身的证书链和密钥对可顺利过渡，力求减少对订户和依赖方的影响。

5、电子认证服务机构更替其密钥对时，电子认证服务机构必须保证整个证书链的顺利过渡。

（三）私钥保护和密码模块工程控制

6、电子认证服务机构应保证产生密钥的密码模块的安全标准符合《粤港两地电子签名证书互认技术标准列表和采用措施》内的规定（附件 1.2)。

7、电子认证服务机构须在其与某类型、类别或种类的证书对应的电子认证业务规则中清楚指出所采用的所有相关密码算法技术标准。

8、电子认证服务机构须就产生密钥的工具的采购、接收、安装、验收测试、调试、使用、维修、保养及弃用等制定有效的程序及控制措施，包括但不限于：

* 制定有效程序，以确保密码模块的完整性；
* 制定有效程序，以确保产生密钥的工具由获授权的人员在适当的督导下操作，防止工具遭擅自改动；设立控制机制，以确保密码模块不会在不能侦测的情况下被擅自改动；
* 制定有效程序，以确保使用密码模块产生的密钥的强度，是符合电子认证服务机构及订户使用密钥的目的所需的适合强度，也符合《粤港两地电子签名证书互认技术标准列表和采用措施》（附件 1.2）内关于电子签名有关密码算法的规定；
* 制定有效的程序及控制措施，以确保在不同密码模块之间传输密钥时，不会发生私钥丢失、失窃、泄露、被篡改或者未经授权的被使用；
* 电子认证服务机构的私钥需要在密码模块中以加密方式保存。

9、电子认证服务机构应对任何用于存储密钥的存储介质（如智能卡）的预备、启动、使用、分派及终止使用制定有效的程序及控制措施。

10、电子认证服务机构的私钥操作应采用多人控制（M 选 N 多人控制（M>N>1））的策略，使用“秘密分割”技术，将使用和操作电子认证服务机构私钥时所需的激活数据分成若干部分，由获管理层授权的可信人员持有，并在对私钥进行操作时，共同完成生成和分割程序。电子认证服务机构须以安全的方式分开保存机构本身的私钥及其激活数据。

11、电子认证服务机构必须以安全的方式对电子认证服务机构私钥进行备份，并根据备份灾难恢复操作需要，以安全的设备和方式保管私钥备份。

12、电子认证服务机构私钥生命期结束后，电子认证服务机构应遵从本证书策略关于归档的规定，采取安全保密方法进行保存。归档期限结束后，电子认证服务机构对机构私钥的销毁应符合本证书策略关于私钥销毁的规定。

13、电子认证服务机构须制定能够确保安全销毁密钥对及任何有关设施的控制措施，包括采取足以确保销毁私钥的所有备份的程序（确保私钥在销毁后再不能被复原或重组），以及吊销对应的证书的程序。

（四）密钥对管理的其他方面

14、电子认证服务机构须对本机构所有的公钥进行归档。

15、电子认证服务机构应遵守以下证书操作周期和密钥对使用期限的要求，包括但不限于：

* 证书操作周期应于过期或被吊销后终止；
* 订户密钥对的使用周期与证书的操作周期应是相同的；仅在签名验证时，证书操作周期结束后密钥对的公钥还可以继续使用；
* 电子认证服务机构所签发的证书的操作周期应不得超过电子认证服务机构密钥对的使用周期；
* 用于身份鉴别的证书，其密钥对只可以在证书有效期内使用；仅在签名验证时，证书操作周期结束后密钥对的公钥还可以继续使用；
* 订户证书有效期应指明最长不得超过 5 年。电子认证服务机构本身的证书应指明最长的有效期不得超过 50 年。

16、电子认证服务机构必须保证所有生成和安装激活数据的程序是安全可靠的，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非经授权的披露。

（五）计算机和网络安全控制

17、电子认证服务机构应制定全面、完善的安全管理策略和制度，通过严格的安全控制手段，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。

18、电子认证服务机构应建立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。

19、电子认证服务机构应采用多级防火墙、入侵检测、安全审计、病毒防范系统等措施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，尽可能降低来自网络的风险。

20、电子认证服务机构处理废旧设备时，必须清除影响认证业务安全性的信息存储并加以确认。

21、电子认证服务机构应按照《粤港两地电子签名证书互认办法》要求，定期聘请独立第三方机构进行包括计算机和网络安全在内的整体评估。

（六）系统开发控制

22、电子认证服务机构须制定系统开发、升级和维护工作的程序，采取有效的控制措施，并适时作出修改或更新。这些程序及措施的内容应包括但不限于：

* 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；
* 将生产及开发的环境分隔开的有效程序；
* 将操作、运维、开发人员的职责得以区分的有效程序；
* 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；
* 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）；
* 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；
* 对采购设备及服务进行妥善管理的有效程序。

（七）时间戳

23、电子认证服务机构应保证各种系统日志、操作日志有准确的时间标识。

九、证书和证书吊销列表的描述

1、电子认证服务机构应保证证书所采用的技术和证书结构符合《粤港两地电子签名证书互认办法》和《粤港两地电子签名证书互认技术标准列表和采用措施》（附件 1.2）内的规定。电子认证服机构采用具体技术方案时应考虑证书跨境使用所需的互联互通需求。

2、电子认证服务机构应根据《ITU X.509》（第三版）（ITU X.509 v3）的证书格式发出及管理公钥证书，并根据《ITU X.509》（第二版）（ITU X.509 v2）的证书吊销列表格式产生及公布证书吊销列表。

3、电子认证服务机构须在与某类型、类别或种类的证书对应的电子认证业务规则中清楚说明所采用的证书结构（包括证书扩展项）及所包含的技术标准（例如包括采用何种数字符代码）。

4、如电子认证服务机构采用 OCSP 技术作为证书吊销列表的补充，以方便证书订户和依赖方及时查询证书状态信息，电子认证服务机构须在其电子认证业务规则中具体说明操作方式、所提供的信息及使用的技术标准。

十、合规性

1、电子认证服务机构须建立和执行有效的内部审查程序，以确保其遵守所有适用的法律法规、本证书策略、对应的电子认证业务规则及其相关的内部规章制度。

2、电子认证服务机构须按照《粤港两地电子签名证书互认办法》的要求以本证书策略为依据每年聘请独立第三方机构进行执行审查。

3、对执行审查报告中提出的例外情况、不足之处或建议，电子认证服务机构须作出回应，并适时提交包括改善和预防措施的整改计划书。

十一、赔偿限额、赔偿安排和法律解决

1、电子认证服务机构在向订户发出某类型、类别或种类的证书时，须在与该类型、类别或种类证书对应的有关电子认证业务规则中指明该证书的赔偿限额，同时指明依据限额对使用该证书所代表的涵义和重要性。

2、电子认证服务机构须安排采购适当的保险或作出符合监管部门要求其他方式的赔偿安排（例如赔偿保证存款金），以确保该机构有足够能力承担因发出或使用证书而引起的或与此有关的潜在法律责任。为证书采购保险的电子认证服务机构应在其信息库中发布有关保险的保险号或其他存在证据。当本地主管部门或独立第三方机构在审查中提出要求时，电子认证服务机构应立即提交该保险号或上述保险的存在证据。

3、电子认证服务机构应承诺分别在订户协议及其电子认证业务规则中明确规定对订户和依赖方的赔偿。

4、无论证书订户、依赖方等实体在何地居住以及在何处使用证书，本证书策略的执行、解释和程序有效性均适用于签发该证书的当地法律。电子认证服务机构须明确注明就本证书策略或电子认证业务规则所涉及的任何争议可处理该争议的法庭。

十二、信息保密

电子认证服务机构必须对保密信息（包括但不限于须保密的业务信息和个人隐私信息）承担相应的保护责任，清楚界定受保护范围，并通过有效的管理制度和技术手段对其进行保护。

十三、附则

1、本证书策略适用于根据《粤港两地电子签名证书互认办法》参与粤港两地电子证书互认机制的电子认证服务机构。

2、本证书策略由“粤港电子签名证书互认工作組” 依据《粤港两地电子签名证书互认办法》进行修订。

3、本证书策略自《粤港两地电子签名证书互认办法》发布日起实施和生效。

附件 1.1：互认策略主要名词术语的两地对照表

名词术语	内地习惯用法	香港习惯用法	名词解释*
电子签名证书	电子签名证书 (electronic signature certificate)	数码证书 (digital certificate)	以电子形式发出的证书，其所储存的数据可用以核实证书拥有人的身份。证书通常包含的资讯包括用户的公开密码匙、姓名及电子邮件地址。
电子签名	电子签名	数码签署 (digital signature)	指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。
证书策略	证书策略	证书政策 (certificate policy)	一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。
电子认证服务机构	电子认证服务机构	核证机关 (certification authority)	指向个人或组织发出证书的机构。
电子认证业务规则	电子认证业务规则	核证作业准则 (certification practice statement)	关于电子认证服务机构在签发、管理、吊销或更新证书过程中所采纳的业务实践的声明。
注册机构	注册机构	登记机关 (registration authority)	代表电子认证服务机构承担某些任务的实体，但并不签发证书。
私钥	私钥	私人密码匙 (private key)	指对密钥配中用作产生电子签名的密钥。
公钥	公钥	公开密码匙 (public key)	指配对密钥中用作验证电子签名的密钥。

名词术语	内地习惯用法	香港习惯用法	名词解释*
主体名称	主体名称	主体名称（subject name）	指证书持有者名字的信息。
甄别名	甄别名	甄别名（distinguished name）	指证书里唯一标识证书用户的身份的信息。
订户	订户	登记人（subscriber）	泛指被颁发一个证书的证书主体。
依赖方	依赖方	依赖方（relying party）	证书的接收者，依赖于该证书和（或）该证书所验证的电子签名。
吊销证书	吊销证书	撤销证书（certificate revocation）	指电子认证服务机构终止证书的有效性。
挂起证书	挂起证书	暂时吊销证书（certificate suspension）	指电子认证服务机构令证书暂时失效。
证书吊销列表	证书吊销列表	证书撤销清单（certificate revocation list）	指由电子认证服务机构公布的列表，列载其发出却已被吊销或挂起的证书。
赔偿限额	赔偿限额	倚据限额（reliance limit）	指就证书的倚据而指明的金钱限额。
证书口令	证书口令	证书密码（certificate password）	指订户使用证书时所输入的字符串。
工作绩效考核	工作绩效考核	工作表现评核（performance assessment）	对电子认证服务机构工作人员在执行职务时的工作表现所作的系统化评审过程。

- 释义仅作参考用途，所有名称的定义应以两地各自的法律法规、惯常定义或证书相关协议内容等所使用的定义为准。

附件 1.2：《粤港两地电子签名证书互认技术标准列表和采用措施》

相关技术范围	两地互认证书采用有关基本标准
证书格式	ITU X.509 V3 或 符合《GB/T 20518-2006 信息安全技术公钥基础设施　数字证书格式》
证书吊销列表	ITU X.509 V2
信息库	HTML, LDAP, HTTP
电子签名有关密码算法	第一类： • RSA, SHA-1 （未来将过渡至 SHA-2） • 证书和电子认证服务机构本身的证书：RSA 2048 位 或 第二类： • SM2、SM3
密码模块的安全标准	按本地监管部门批准的标准
数字证书介质技术	PKCS#11 兼容装置 或 符合国家密码管理局《智能 IC 卡及智能密码钥匙密码应用接口规范》

电子签名证书应载明的内容（根据《粤港两地电子签名证书互认办法》）	
1、证书签发机构名称； 2、证书持有人名称； 3、证书序列号； 4、证书有效期； 5、证书持有人的签名验证数据； 6、证书签发机构的签名； 7、证书策略对象标识符； 8、规定的其他内容。	
鼓励（或要求）采用、跨境证书使用便利化的措施	
电子认证业务规则	鼓励电子格式化（XML）和 PDF 文档格式，双语言（中、英语）； **要求有中文 PDF 文档格式并以此为准**。
符合互认条件的证书“信任列表”（监管范围）	鼓励 HTML/PDF（人读）和 XML（机读）置放于安全网站上或其他合适的渠道； **要求有 HTML/PDF（人读）文档格式置放于安全网站上或其他合适的渠道，并以此为准**。