

## 拟就有关「认可核证机关业务守则」进行检讨 所收集的意见而作出的回应建议

### 目的

本文件阐述拟就有关「认可核证机关业务守则」(下文简称「业务守则」)进行检讨的咨询所收集的意见而作出的回应建议。

### 背景

2. 认可核证机关业务守则咨询委员会(下文简称「咨询委员会」)于二零零三年一月举行的第八次会议上,决定由资讯科技署对业务守则进行检讨。

3. 在二零零三年三月至四月,我们向委员传阅 ACCOP 文件第 4/2003 号,请委员就检讨业务守则的咨询安排建议发表意见。其后,我们在二零零三年六月至七月向下列对象展开了咨询:

- (a) 咨询委员会各委员及(透过委员)其所附属的机构(参考: ACCOP 文件第 6/2003 号及 7/2003 号);
- (b) 各认可核证机关;以及
- (c) 与核证机构的服务和进行稳妥电子交易有关的其他六个机构。

4. 在咨询期间,我们邀请咨询对象就业务守则的修订建议及业务守则任何其他方面发表意见。

### 接获的意见

5. 在咨询期内，我们接获以下八位人士 / 机构提交的意见：

- (a) 郑利明博士
- (b) 网际威信(香港)有限公司
- (c) 香港货品编码协会
- (d) 香港国际仲裁中心
- (e) 香港邮政
- (f) Information Systems Audit and Control Association
- (g) 个人资料私隐专员
- (h) 专业资讯保安协会

#### **拟作出的回应**

6. 我们经仔细研究和考虑上述人士 / 机构提交的意见后，已制订拟作出的回应建议，详情列具于本文的附件。

#### **征询意见**

7. 欢迎各委员就附件所载的回应建议提出意见。

8. 我们会参考委员的意见对业务守则展开修订。

**资讯科技署**

**二零零三年十二月**

**对「认可核证机关业务守则」进行的检讨  
接获的意见及拟作出的回应**

条	意见撮要	拟作出的回应
3.6	修订建议没有明确提述修订是以《个人资料(私稳)条例》为依据。较可取的做法是明确界定“个人资料”一词，并指明该定义是以《个人资料(私稳)条例》内的定义为依据。	我们会按照意见在「认可核证机关业务守则」(下文简称「业务守则」)中提供“个人资料”一词的清晰定义。
3.8	(a) <u>有关修订建议的第(ii)点</u> 有关规定交代不清。此项关乎资料要公布至什么程度和数量，才能满足建议的规定。	我们会在第 3.8 条提供进一步的阐释，说明认可核证机关所公布的事实，应可让有关各方清楚辨认在认可核证机关发出的证书当中，那些类别是根据《电子交易条例》(第 553 章)(下文简称「条例」)获认可的证书，而那些类别不是根据条例获认可的证书。
	(b) <u>有关修订建议的第(ii)点</u> “储存库”一词有特定含义。基本上是指用来储存已发出证书的详细资料的目录。因此，从纯技术角度而言，要求核证机关在储存库内公布此等事实，并不切实可行。取而代之，署长可要求使用独立的储存库，分别储存已获认可和未获认可的证书。	根据业务守则附录第 10 条，储存库可以不同的标准建立，例如对目录适用的轻量式目录接达规约(LADP)、对网页适用的超文本标示语言(HTML)等。因此，认可核证机关可以在其储存库以适当的方式公布有关事实。  我们同意建议，宜使用独立的储存库分别储存已根据条例获得认可和未获得认可的证书。

条	意见撮要	拟作出的回应
4.12	(a) 建议没有指明呈报重大变更应采用的格式类别，可能会影响重新评核和作出决定的时间。	现时认可核证机关通知资讯科技署署长(下文简称「署长」)拟就认可核证机关的运作作出的重大变更时，可自行选择使用什么格式作出陈述。这种安排迄今一直行之有效。因此，我们认为无须限定呈报方式的规格。我们虽容许认可核证机关弹性选用呈报重大变动的格式，我们仍会尽快处理认可核证机关的报告。
	(b) 可有任何加快处理较次要变更的建议？	当我们收到认可核证机关拟就运作作出变更的报告时，我们会评估拟作出的变更会否对认可核证机关的稳当程度构成重大影响。我们只会就重大变更与认可核证机关进行跟进。
	(c) <i>有关修订建议的第(ii)点</i> 有意见认为署长应考虑制定上诉或复核机制，以处理认可核证机关对署长的裁决不表赞同的情况（关于拟就认可核证机关的运作作出的重大变更是否符合条例及业务守则的规定）。	如认可核证机关就其运作作出署长认为有违条例或业务守则的重大变更，署长可根据条例第 23 或 24 条撤销或暂时吊销对该核证机关作出的认可。按照条例第 28 条，认可核证机关可就署长的决定向工商及科技局局长提出上诉。条例已设有提出上诉的机制。
5.9.2	业务守则并无对操作人员的个人背景作出规定。这一点可能会对核证机关构成潜在保安风险。有意见认为可以以一套类似警方现时甄别保安持牌公司所采用的程序作为准则。	现时已有措施处理认可核证机关人员的背景所涉及的风险。根据条例第 21(4) 条，署长在考虑申请认可的核证机关是否适合获发认可时，须考虑的事项包括申请人及负责人员是否适当人选。按照条例第 21(5) 条就适当人选所定的准则，署长会向警务处处长查询有关的负责人员可有任何刑事记录。署长还会向破产管理署署长查核有关的负责人员是否有任何破产记录。署长在考虑核证机关的负责人员是否适当人选

条	意见撮要	拟作出的回应
		<p>时，会继续采取此等措施。</p> <p>此外，根据业务守则第 5.9.1(b)(i)条，认可核证机关须透过多种机制发展和备存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及程序对其员工的背景进行保安审核。在独立评估人对认可核证机关进行的评估中(于申请认可或每年评估时)，会评估有关认可核证机关是否符合业务守则（包括业务守则第 5.9.1(b)(i)条）的规定。</p>
5.10.8	<p>证书撤销清单是公布撤销证书详情的公认方法，而且已有适用于证书撤销清单的国际标准。因此，没有加入“公布撤销资讯的任何其他方式”的必要，尤其是考虑到核证机关有责任采用业界的技术及开放的标准。</p>	<p>加入“公布撤销资讯的其他方式”的建议，是为了顾及一些特定类型的电子证书。此等证书在公布证书撤销资讯方面，尚未有通用的业界作业实务。一旦有了在这方面广为接受的业界作业实务，认可核证机关便应遵照业务守则第 14.1 条的规定，在适当情况下采用这些通用业界作业实务，作为促进互通性的开放及共通的界面。上述的通用业界作业实务可以是惯用的证书撤销清单，又或者一些其他新的业界标准。</p>
5.11	<p>(a) 有意见认为如登记人选择使用自己的系统来产生配对密码匙，认可核证机关的责任是建议登记人使用稳当系统以产生密码匙。</p>	<p>为针对证书申请人使用自己的系统产生配对密码匙的情况，我们会修订第 5.11 条，明文规定认可核证机关须要求申请人使用稳当系统以产生申请人的配对密码匙。认可核证机关须要向申请人提供指引，并须采取合理可行的步骤，以确定申请人已遵从指引使用稳当系统以产生申请人的配对密码匙。如认可核证机关认为申请人未能遵从指引的规定，或在任何其他方面没有使用稳当系统以产生配对密码匙，认可核</p>

条	意见撮要	拟作出的回应
		<p>证机关应拒绝接受申请人的配对密码匙。</p> <p>至于认可核证机关为本身及证书申请人所产生的密码匙，认可核证机关须使用稳当系统。</p>
	(b) 从遵从的角度而言，认可核证机关很难(甚至不可能)确保登记人将会使用稳当系统。	请参阅上文(a)项的回应建议。
	(c) 如登记人使用自己的密码匙产生系统，核证机关应就产生密码匙的程序的稳妥性，提供合理的指引和建议。此外，如核证机关认为有必要，应考虑产生密码匙的系统是否稳当。核证机关应保留拒绝接受由被认为不稳妥的系统所产生的密码匙的权利。	请参阅上文(a)项的回应建议。
6.4	(a) 谘询文件建议把核实证书的内容改为核实证书申请人的个人资料。有意见认为原本的安排较为可取，因为申请人除可核实其个人资料外，亦应有机会核实证书上的其他资料，例如有效期、密码匙的使用等。	除证书申请人提供的资料外，证书上的其他资料(例如有效期、密码匙的使用、签署及加密算法识别编号、认可核证机关的签署等)都是由认可核证机关建立。确保此等资料准确应该是认可核证机关的责任，而非倚靠证书申请人对此等资料作出核实。在认可核证机关建立的资料当中，有些属技术性质，一般证书申请人未必容易明白这些资料。因此，我们认为业务守则只需要求认可核证机关为证书申请人提供机会，核实已置于或将置于证书上的申请人资料。

条	意见撮要	拟作出的回应
	(b) 为与《个人资料(私隐)条例》第 DPP2(1)条的规定一致，可能有需要考虑增加一项规定，要求“认可核证机关应采取一切合理可行的步骤，以确保证书所载个人资料的准确性”。	我们会修订第 6.4 条，指明认可核证机关应为证书申请人提供合理机会，核实已纳入或将纳入证书内的“申请人资料”。此外，认可核证机关须采取一切合理可行的步骤，确保已纳入或将纳入证书的资料的准确性。  “申请人资料”指由证书申请人提供并已为或将为认可核证机关纳入证书内的资料。视乎证书的类别，申请人资料可能包含一如《个人资料(私隐)条例》(第 486 章)第 2 条所界定的个人资料。
	(c) 证书的内容不只包括个人资料，例如伺服器证书会载有网站划一资源定位(URL)，而机构证书则载有机构名称。因此，此项的适用范围不应只局限于“个人资料”。	请参阅上文(b)项的回应建议。
8.2	(a) 就索偿总额作出的总投保额，是否应按已发出的证书的总数为比例，而不是如为(咨询文件的)附件二第 4 页 (a) 项或 (b) 项所述定为赔偿限额的 10 倍？	在世界各地的核证机关行业的作业实务里，都很少要求核证机关按已发出的证书的数目为比例来购买保险。我们研究过其他地区(包括澳洲、新加坡、英国、美国若干州等)的有关规管制度，发现类似的规定绝无仅有。因此，我们无意在业务守则中采纳这种方针。
	(b) 订定投保额为这些数额的理据为何？	我们在二零零一年二月公布现行的保险规定前，曾参考其他地区(即新加坡、马来西亚、美国若干州等地区)的有关规管规定。我们界定

条	意见撮要	拟作出的回应
		的保险规定是与国际上通用的作业实务看齐的。
	(c) <u>有关修订建议的第(i)点</u> 修订应进一步澄清，指明投保期间内就索偿总额作出的总投保额，是根据证书的数目计算、按证书的类型 / 类别数目计算、或是以整体方式计算。	我们的修订建议已述明在任何单一的投保期内厘定索偿总额的准则。此准则与证书的数目或证书的类型 / 类别 / 种类数目无关。请参阅上文(a)及(b)项的回应建议。
	(d) <u>有关修订建议的第(ii)点</u> 请说明建议中下述句子的含义：「此外，认可核证机关及保险人均须同意香港特别行政区各级法院对保险单范围内发生的任何申索或问题具非专有审判权。」	这是一条非专有审判权条文。非专有审判权条文并不会限制申索人选择诉讼的场所（即法院和仲裁中心），只要诉讼在便于审理的诉讼场所进行，便构成表面证据成立的个案。在这种情况下，如申索人向香港特别行政区的法院提出要求，香港特别行政区的法院会根据有关保险单就索偿作出一般的裁决，但如所选的诉讼场所位于海外，则会拒绝就索偿作出裁决。
	(e) <u>有关修订建议的第(ii)点</u> 修订建议栏中指“香港特别行政区各级法院...具非专有审判权”，与备注栏中“受本地法律规管”一语，在字义上可有抵触？	备注栏中的说明旨在强调，如申索人要求香港特别行政区的法院根据有关保险单就索偿作出裁决，香港特别行政区的法院过常会就索偿作出裁决。
	(f) <u>有关修订建议的第(ii)点</u> 投保额有可能是在团体层面上购买的，所以就国际性的核证机关的情况而言，虽然在香港的	这项修订建议的目的，是要确保认可核证机关所购买的投保额乃购自认可承保人，受到香港特别行政区法律的规管，并受香港特别行政区各级法院的非专有审判权所规管，以进一

条	意见撮要	拟作出的回应
	<p>业务可能会依据香港法律寻求认可，但集团可能在国际层面上安排投保额。因此，有意见认为署长不宜在这方面施加具体限制。此外，管辖的法律和司法裁判权的问题涉及商业决定。大家都知道有些商业合约是在某国订立，但却受别国的司法裁判权所规管。故此，建议的修订非属必要。</p>	<p>步保障认可核证机关的本地用户的利益。我们认为修订建议是适当的。</p>
11.5(e)	<p>除非把资料转移给保管人是为了维持有关认可核证机关原先提供的服务，否则若未经有关人士的订明同意，以任何方式使用资料作任何其他用途均可能违反《个人资料(私隐)条例》第 DPP3 条的规定。为此，此 11.5(e)条应清楚注明资料转移给保管人的特定用途。</p>	<p>我们会按照意见修订第 11.5(e)条。</p>
12.4	<p>有意见认为其他国际认可的专业资讯保安资格，亦应获接纳为核准准则（即指获核准为具备资格进行评估的人士）。这些资格包括认可资讯系统保安人员资格 (CISSP) 及认可资讯系统审计师资格 (CISA)。根据经修订的《立法会(修订)条例草案》，身为专业资讯保安协会 (Professional Information Security Association) 正式会员并持有认可资讯系统保安人员资格四年或以上的人士，均为合格的</p>	<p>我们欢迎任何人士或组织，就有关根据条例作为合格替核证机关拟备评估报告的人提出意见，以供署长考虑。有关合格人士及其所属的专业组织的条件，已详载于业务守则第 12 条。</p> <p>如专业资讯保安协会 (PISA) 或其他专业协会希望其会员可以担任合格的评估人，我们欢迎各协会向我们呈递有关资料，以证明各协会及其会员符合业务守则第 12 条所列的要</p>

条	意见撮要	拟作出的回应
	选民。因此，宜作出类似的安排。	求。我们收到有关资料后会立即予以考虑。
<b>业务守则附录</b>		
2.2.4	有意见认为修订并无必要。一般来说，核证机关与倚据证书人士没有合约关系。另外须考虑的一个要点，是核证作业准则属公开资料，登记人或非登记人均可下载。无需特别就倚据证书人士作出提述，以避免核证机关与倚据证书人士之间存有任何稳含的义务 / 法律责任。	我们认为修订建议是适当的。一如第 2.2.4 条第三句所述，一般来说，认可核证机关会在核证作业准则最少列出一个电话号码、邮递地址和电邮地址，供登记人和倚据证书人士与该机关联络。我们建议对第一句作出的修订与第二句的含意贯彻一致，即认可核证机关应为登记人和倚据证书人士提供联络点。
3.4.2	与其让认可核证机关制订解决争议程序的条文，有意见认为不如由资讯科技署(下文简称「本署」)制定有关条文供认可核证机关依循。这个做法可以确立条文的一致性和可预测性，而更重要的是这个做法可保障消费者的利益。	让认可核证机关自行制定解决争议程序，是与核证机关业界的国际作业实务一致的。我们研究过世界上其他一些地区(包括新加坡、马来西亚、英国等地)的有关规管制度，并无发现制定供当地核证机关依循的解决争议程序。因此，我们认为没有需要由本署制定解决争议程序以供认可核证机关依循。
4.1.7	有意见认为修订并无必要，原文已能满足需求。须知在某些情况下，证书是被用作识别伺服器，这一点是很重要的。在这些情况下，证书上的名称可能并非申请人的名称。原文已说明有关的规定，所以修订主要是多余的。	我们认为有需要作出修订建议，以便更清晰地阐明证书上所示登记人的名称应与将获发该证书的申请人的名称相同的规定。  为涵盖申请人名称以外的其他资讯(例如伺服器系统的识别项目)，我们会扩大第 4.1.7 条的规定范围，包括例如认可核

条	意见撮要	拟作出的回应
		证机关采取特定措施,以核实除申请人名称以外的其他已载或将载于证书上的申请人资料,认可核证机关须在核证作业准则内阐释该等特定措施。
5.3	与就业务守则第 6.4 条所提出的意见相同。	请参阅上文第 6.4 条的回应建议。
5.4.3	(a) <u>有关修订建议的第(i)点</u> 有意见认为修订并无必要。修订必然会禁止认可核证机关采用第三方所提供,涵盖由认可及非认可核证机关发出并已被撤销的证书的验证服务。	修订建议旨在令认可核证机关所备存的证书撤销清单与业务守则第 2 条所载的定义一致,并无意对任何“第三方提供的验证服务”作出提述。因此,我们认为修订建议是适当的。
	(b) <u>有关修订建议的第(ii)点</u> 谘询文件建议以“可能提供...的理由”取代“提供...的理由”。所持理据是核证机关未必知道撤销证书的原因。有意见表示对此理据有所保留。核证机关撤销证书须有理可循,并应把理由公布周知。核证机关运作的透明度,是建立公众对其信任和信心的其中一个关键所在。	我们的修订建议与核证机关市场的国际作业实务一致。我们曾向世界上其他一些地区的多个核证机关进行调查(即新加坡、马来西亚、澳洲、英国等)。大多数受调查的核证机关都不公布撤销由其发出的证书的理由。因此,我们认为修订建议是适当的。  况且,不论是否有公布撤销的理由,在证书撤销清单公布的资料当中,最重要的一项是指出某证书已被撤销和再不可信赖。