马拉喀什 — ICANN 董事会和 SSAC 联合会议
欧洲西部时间 2016 年 3 月 8 日星期二 — 14:00 至 15:00
ICANN55 | 摩洛哥马拉喀什

拉姆 • 莫罕 (Ram Mohan)： 欢迎出席本次会议。本次会议由 ICANN 董事会和安全与稳定咨询委员会联合召开。在各位面前的有很多是安全与稳定咨询委员会的成员，还有几位董事会成员，当然还有其他同事会陆续加入我们。下面我要交给 —

我是拉姆 • 莫罕。我是 SSAC 在董事会的联络人。下面我要把麦克风交给帕特里克，请你做开场发言。

帕特里克 • 弗斯特朗姆 (Patrik Faltstrom)： 非常感谢拉姆。我是帕特里克 • 弗斯特朗姆。我是 ICANN 安全与稳定咨询委员会的主席。

首先我要感谢 ICANN 董事会参加本次会议。董事会与 SSAC 之间已经有好几年没有进行过真正有组织的互动，我想现在，经过了前面几次会议，不管是讨论的质量，讨论的价值，还是我们之间的互动都大大增加。

我想说这一点非常好。

下面请允许我介绍这里的另一位同事，在我左边的是 SSAC 的副主席吉姆 • 加尔文 (Jim Galvin)，在会议桌两边还坐着几位 SSAC 成员。

注：下文是通过音频文件转换而成的文本文档。尽管文本记录稿基本准确，但某些情况下会因音频不清或语法修正而导致部分文本缺漏或有误。本文本的发布旨在作为原音频文件的补充资料，不得视其为权威记录。

目前在 SSAC 共有 30 名成员。向出席本次会议的其他同事介绍一下，我们是一个咨询委员会，我们的章程受 ICANN 章程制约，探讨的是我们在互联网中所使用的标识符的安全性和稳定性。

拉姆 • 莫罕： 谢谢帕特里克。我想在议程上有一些问题和话题是 SSAC 要提给董事会的，还有一些是董事会要提给 SSAC 的。

要不我们先从董事会对 SSAC 的问题开始，然后 —

董事会对 SSAC 提出了两个问题。

第一，在 ICANN，多样性被认为是一个挑战。你们咨询委员会在加强各方面的多样性上做得怎么样？ICANN 可以做些什么来支持你们？

帕特里克 • 弗斯特朗姆： 非常感谢。

在 SSAC，我们非常严肃地对待多样性问题。另一方面，在评估 SSAC 新成员时，我们主要关注技术上的多样性。

对任何一个全球性的志愿组织而言，多样性都很重要，而且是一个有益的、重要的目标，SSAC 也不例外。

我们 — 正如我昨天在开幕式上表达的那样 — 我们对这方面非常注意，比如地理多样性。因为 SSAC 的每一个决定都是通过

电子邮件做出的，所以面对面会议对 SSAC 达成任何（决定）的重要性不大 — 成员们不是非要参加面对面会议才能加入决策流程，这一点我们认为很重要。

至于 ICANN 可以帮助我们做什么，在 SSAC，我们尽量与 ICANN 已经在组织的各种外展项目发生联系。比如，我们密切关注英才计划。

我们有一些 SSAC 成员直接来自英才计划，我们一直在关注英才计划中的学员，以便能够从中发掘新的 SSAC 成员。

此外我们也开展 DNSSEC 研讨会，其中既有一般介绍性研讨会，也有面向更专业的技术人员的研讨会。我们感谢 ICANN 持续给予我们支持，使我们能够拥有这些外展项目。

在发掘 SSAC 潜在新领导层和参与人方面，以及其他一些方面，我们也能获得了一定帮助，可以说是延续我们在外展方面的合作。

即便如此，SSAC 毕竟只有 30 人，所以仅凭一己之力我们无法完成上述任何一件事情。我们非常依赖于 ICANN 已经在做的工作。谢谢。

拉姆 • 莫罕： 董事会成员有什么看法吗？阿莎？

阿莎 • 合美嘉妮 (Asha Hemrajani)：

我是阿莎 • 合美嘉妮。

帕特里克，非常感谢你提到 DNS 研讨会。我真的要表扬一下这个研讨会。我认为你们组织的这个研讨会非常好。我个人从中学到了很多，并且这一次在马拉喀什举办的研讨会上，我还看到你们迎来了一支规模庞大的来自非洲社群的代表团。从他们一些人当中，我也得到了非常正面的反馈。所以我非常赞赏它。谢谢。

拉姆 • 莫罕：

董事会还有其他意见吗？

好的。下面我们进入屏幕上的第二个问题，帕特里克。

你们对问责制 CCWG 的最终报告有什么反馈？

帕特里克 • 弗斯特朗姆：

我们完全认可问责制 CCWG 的第 1 阶段最终报告，没有任何意见，所以对此也没有太多要说的。

不过，在我们早前的文件中给出了许多意见，它们更多地是和实际实施阶段有关。

所以，我们没有留下只言片语并不表示我们睡着了，而是要等到整个 ICANN 重组之后再提。我们将非常密切地关注此事。谢谢。

拉姆 • 莫罕： 谢谢。请放前一张幻灯片，这里有很多问题。这些问题全都来自我所认为的技术领域，还有一些技术性的回复和问题。

关于技术方面，还有什么其他话题应该补充的？我看到了琼尼。

琼尼 • 索尼能 (Jonne Soininen)： 是。大家好。我是 IETF 在 ICANN 董事会的联络人琼尼 • 索尼能，也是董事会 IDN 工作组的成员。

我们董事会 IDN 工作组还有一个问题，这个问题不在原来的清单上，它和 IDN 和二级字符串有关 — 这个请求来自 ccNSO 中的工作组，当它创建时，这个工作组以及像 GAC 和 SSAC 这样的团体将会参与进来，我们想知道的是：SSAC 对这项工作的参与计划或当前的参与情况是什么样的？

帕特里克 • 弗斯特朗姆： 首先介绍一个背景，SSAC 是通过达成共识做出决定的。而且正如我之前说的，我们通过完成一份声明表达共识，这份声明是在 48 小时，或者更多的时候是一周内，在召开完最后一次电话会议后通过电子邮件达成一致的。这就是我们提出自己立场的方式。那意味着对 SSAC 而言这非常困难，或者说，实际上 SSAC 无法参与到任何像这样的工作当中。

SSAC 能够做的就是回应某一些问题。我们可以审核文件本身。一般来说，我们可以向研究诸如此类事项的工作小组提出

意见、说明或建议。最后，我们可以指定我们认为技术娴熟，可以加入的个人。

另一方面，这并不表示他们以任何方式、模式或形式代表 SSAC 发言，无论这些人是不是 SSAC 成员。

这是第一个部分。

第二，关于 ccTLD 和 IDN，我们在 SSAC 刚刚成立了一个工作小组来研究通用 IDN 问题，特别是，从我们的角度来看，有没有问题 — 研究国际化域名以及像商标信息交换中心、标签生成专家组、ccTLD 快速通道等类似问题的不同流程之间是否缺乏调和。

所以问题是，比如说标签生成专家组的工作成果也应该直接作为 ccTLD 快速通道的指示，反之亦然，那么是否有风险 — 比如说，你可以获取一个带有某些无法在 ccTLD 快速通道中获得的字符的新 gTLD，或者反之亦然，但如果有差异，那会不会对安全性和稳定性有影响。我们不知道。

所以我们要研究它。我们将会研究它。而且统一域名编码 (Unicode) 的版本不同也是影响标签生成专家组的一个因素。

关于 ccTLD 以及这个流程的实际问题，我想重要的是不但要研究技术问题，还要研究 ccTLD 的实际流程本身。因为人们当然会问自己，ICANN 是否真的可以对某个 ccTLD 或者实际申请某个字符串的国家或地区说不。

琼尼 • 索尼能： 这个问题也许可以不考虑，但问题是 — 你们 — 因为工作组很可能也需要安全方面的帮助。你们是否计划用自己的方法 — 包括，比如，指定专人跟进这项工作 — 来关注这方面？

我们关心 — 或者说感兴趣的另一件事就是，你们了解这项工作并且对此进行了跟进，那么你们是否需要做出反应。

帕特里克 • 弗斯特朗姆： 昨天晚上 7:34 我收到了联络人拉姆的问题。

在本次董事会会议之后，我们会召开一个 SSAC 会议，届时将会讨论是否要向这个小组委派一名人员。我无法回答这个问题。

但是我们将会讨论它。

关于我们在工作小组中所做的工作，以及相关工作成果是否会对他人有所帮助，每次我们与某个小组会面时我都会说，我们 SSAC 真的非常希望得到他们的意见，但我们还是没有得到足够的意见。

在这里我们确实收到了意见，而且我们确实有一个工作小组在研究这个话题，所以我可以肯定我们将提出能带来切实帮助的成果。

琼尼 • 索尼能： 这是一个很好的回答，非常感谢。

拉姆 • 莫罕： 谢谢。

帕特里克，让我们继续讨论议程的下一部分，也就是来自 SSAC 的问题，他们提出的话题。

第 1 个问题，阿莎是董事会方面的指导人。

帕特里克 • 弗斯特朗姆： 非常感谢。

SSAC 在 2013 年撰写了第 63 号文件，我们写这份文件的原因是，在 2010 年，ICANN 对根区签名，一段时间后，在一份名为“实践声明”的文件中，有信息表明届时将会有一个密钥定期轮替流程，而且这个流程将会在必要时或者五年后启动。

所以在 2013 年，由于 SSAC 看到这方面没有什么动静，所以我们撰写了 SAC63，鼓励 ICANN 开始研究与密钥定期轮替有关的问题，因为这个过程需要花一些时间，而且就像 IANA 移交一样，不管是计划的制定还是实施都要花时间。

我们在建议中指出，我们认为实际上，在我们看来，我们认为它理应得到更高重视。

关于 SAC63 中的建议，为何我们直到现在才开始讨论这个话题的真正原因，在一定程度上是因为，实际上，我们作为一个咨询委员会，以及 ICANN 员工和参与其中的每一个人，都没

有真正将功课做到位，没有很好地跟踪这类意见，所以者可以说是 —

所以延迟是这里存在的一个问题，我们其实并不知道这个意见在哪里。但这是一个单独的问题，在此我们不做讨论。

后来到了 2015 年，我们看到一些工作正在进行，但不是很多，于是我们开始密切注意这个为期五年的工作，以 SAC73 的形式发送了一封信函。在信中我们再一次指出在这方面必须做一定工作，我们希望得到多一点注意，希望工作向前推进。

在上一次在都柏林的会议上，我们也向 ICANN 董事会提到此事。

所以，从我们的角度来看，我们依然，也是一如既往地认为启动这个定期轮替流程非常重要。

当然，我们知道，域签名密钥，也是目前正在使用的两种密钥之一，可能需要根区管理人 — 目前是威瑞信公司 (Verisign) — 进行更改，不管是扩大还是其他什么方式。

我们也知道有一个设计团队一直在编制相关报告，有几位 SSAC 成员也加入了这个报告编制团队。SSAC 收到了报告内容的简报。顺便说一下，今天早上还发布了一份报告。所以现在，每个人都可以读到其中的内容。

这份报告包含一个时间表，我们认为现在重要的是立即开展一项调查，看看这个时间表能否实现，如果不能的话，应该怎么办。

至于 SSAC 的真正建议和看法，我们认为 — 总结起来就是，既然签名实际上正在进行，而且 — 抱歉，是密钥定期轮替要尽快启动，不管那意味着什么。

而且，要启动密钥定期轮替流程，很重要的一点是要有某种升级流程，这样如果发生崩溃，当出现某些征兆时，这些征兆是否正确，是否应该回退，就已提前决定。

正常单纯的运营实际上并非一蹴而就的。你必须提前做好这些准备。但是所有这一切，在一定程度上，或多或少都纳入到了设计团队今天已经发布的计划中。

所以这就是我们一直在讨论的事情，而且阿莎和我本人讨论了很长一段时间，在 SSAC — 让我这么说吧 — 我们对过去几天与 ICANN 员工、ICANN 董事会以及相关所有人员展开的所有讨论都非常满意，我想利用这个机会感谢每一个人，感谢你们提供这些非常有益的、非常有建设性的讨论。谢谢。

拉姆 • 莫罕： 阿莎？

阿莎 • 合美嘉妮： 好的。谢谢拉姆。首先，感谢帕特里克分享对定期轮替系统的关切，这个问题你在都柏林也曾提出来过。

首先，我们感谢大家为 KSK 定期轮替所做的准备工作，以及 SSAC 为 SAC63 和 73 所做的工作。为了让那些可能不了解 SAC63 是什么的人有所了解，我解释一下，它是 SSAC 关于根区中 DNSSEC 密钥定期轮替的一份咨询报告。

我们注意到，正如你所说的，SAC63 发表于 2013 年，ICANN 的第一份详细回复在 2014 年发出，其中指出这个问题需要更好的沟通和一轮更紧凑的反馈。

我知道工作人员采取了一些措施来改进和简化沟通渠道。

现在，随着新的董事会意见登记流程刚刚开始，董事会正把精力集中在及时、全面地回复 SSAC 的建议上。我怎么强调它都不为过。事实上，是要及时、全面地回复来自任何 SO 或 AC 的建议。

董事会意见登记处，或者帕特里克，我们昨天在讨论中称之为 BAR，它将实现对意见的更有效跟踪，并且应该可以确保提供这轮更紧凑的反馈。

所以在都柏林的时候，如果你们还记得的话，当时史蒂夫 (Steve) 提名了梅丽莎 (Melissa) 主管或者进入 BAR 工作，以及 — 噢，这里有一只小鸟。你好。

[笑声]

阿莎 • 合美嘉妮： — 还提名了戴维 (David) 进入 BAR 工作。据我了解，关于 BAR 有过一些沟通，我希望通过沟通将完成这轮反馈，并尽快为你们运行。

但是我要代表董事会说一句，我们将继续对这项工作以及 SSAC 向我们提出的其他重要的安全性和稳定性问题履行监督职责。所以谢谢你们。

下面 — 我要问问其他董事会成员还有没有什么要补充的。

好的，布鲁斯，请讲。

布鲁斯•托金 (Bruce Tonkin)： 谢谢阿莎。我是来自董事会的布鲁斯 • 托金。有一点可能需要提醒一下，因为我知道有时候大家会以为董事会成员没来到现场。这里前两排大部分都是董事会成员。所以我们有一个庞大的董事会，而且大部分董事会成员都到了这里。

关于这个话题，我确实是第一次听说它的时间问题。我想这始终会是一个挑战。比如，不管你什么时候试图让密钥轮替，总是会打破一些东西。那实际上也是关键所在。我想，实际上这项工作可能宜早不宜迟。如果我们再等两到三年，基础会越来越固化，将来如果出现了问题，很可能会造成更大的影响。

我主张继续推进根区密钥定期轮替的规划工作。也许将来真正启动的时候，曾经面临的一些挑战可能会烟消云散，因为今年有太多工作在同时进行。

但是我认为我们应该继续推进所有准备工作。特别是考虑到沟通策略方面，我认为这是一定要做好的一项真正关键的工作，我们要能对人们解释它意味着什么，这样当发生崩溃时，人们就知道崩溃的原因是什么，也知道他们可以做出纠正。所以，对，我主张继续推进。

帕特里克 • 弗斯特朗姆： 谢谢。在邀请其他 SSAC 成员发言之前，我说明一下，这些基本上也是我们在 SSAC 所说的。另一方面，我还要补充强调一点。首先，设计团队的报告确实包括一个时间表，当然，很多人都知道，在设计团队制定报告的同时，在运营社群以及其他团体中也在制定自己的计划。

所以从 SSAC 的角度我要强调的唯一一点就是，ICANN 不能只是孤立地决定自己的时间表。关键还要协调，以便也能够发现这里的潜在问题。

所以即使 ICANN 因为某种原因而决定等待，但仍要采取一些行动，因为其他团体可能为已经公布的材料设定了他们的时间表。所以“干等着”实际上是行不通的。

还有人 — 抱歉。应该说“干等着，什么也不做”实际上是行不通的。还必须从报告发布当天开始，就持续跟踪事情的进展。

哦，拉姆也说了其中的一些日期。所以有关这份报告，下面我要交给杰夫，他实际上是设计团队的一员，可以谈谈这方面的情况。

杰夫 • 休斯顿 (Geoff Huston)：

谢谢帕特里克。我是杰夫 • 休斯顿，也来自 SSAC。我有幸成为 KSK 设计团队的一员，所以对报告，当然还有这些日期都很熟悉。

我们都很清楚一个事实，那就是密钥得到了应有的尊重和关照，实际上它们只在年内的某些时期，也就是所谓的“密钥签名仪式”期间才会开放和使用。我们认为应该结合对这些密钥签名仪式的现有时间安排，来考虑密钥的作用。这个流程预计将在今年 4 月 1 号开始。对于到十二月底之前的剩下的七个月，我们将利用这段时间真正生成新密钥，以便在密钥签名仪式中使用，并分发到第二个中心；换句话说，就是进行必要的密钥准备工作，同时不会变更区域自身的任何运营部分。

区域变更将在正常安排的区域管理运营时间开始。第一次变更将在 2017 年 1 月 1 日进行。届时将宣布新的密钥，我们相信这一事件将不具有破坏性。

下一次变更将在三个月之后进行，届时将从旧密钥转换到新密钥。我们相信，从潜在破坏性来看，那几乎是最具破坏性的事件。

如果有旧的解析器未能跟踪到这一转变，将会发现 DNS 出现故障。我们非常清楚，我们不知道这一人群会有多大。我们希望把它想象成很小，但我们无法真正了解到底有多小。

假设前两个事件完成后没有影响，也不需要后退，那么再过三个月后将进行下一步。

第三个事件发生在年中，那就是撤销旧密钥，这样在该旧密钥中就没有残留信用。

我要指出一点，所有这些尽管听起来技术性很强 — 可能也确实是如此 — 但在这当中有一个统观全局的文件，那就是实践声明，作为一个证明，里面详细说明了 ICANN 是如何照管这一批数据的。

全世界应该信任这批数据的唯一原因就是，ICANN 将向公众单方面承诺，它会以某种方式管理密钥。事实上，我相信董事会应该阅读并始终全面考虑这份实践声明文件，因为这是全世界信任你们，信任处于 DNS 系统安全核心的密钥信息管理的原因之一。

所以，当在实践声明中做出这些承诺时，我们当然会拥护你们，因为这些承诺是代表 ICANN 全体做出的。而且董事会要

承担一定责任，确保这份文件充分传达，同时也要负责遵守这份实践声明。所以，作为你们董事会所肩负责任的一个关键部分，我当然会向你们推荐它。这样，ICANN 员工就能真正理解技术层面的要求，并认识到实践声明是一份意义重大的文件。谢谢。

帕特里克 • 弗斯特朗姆： 阿莎，请讲。

阿莎 • 合美嘉妮： 谢谢帕特里克。谢谢杰夫。这确实是非常有用的信息。我只想请 ICANN 员工或者戴维谈谈时间表的问题，并回应一下帕特里克之前提出的问题，或者应该说是关切。谢谢。

戴维 • 康纳德 (David Conrad)： 当然。我们了解，设计团队的建议中显然包含时间表。我们员工所面临的挑战是，你们可能也知道，眼下有几项工作同时在进行。特别是负责密钥管理的人员刚好也是 IANA 的工作人员。在移交过程中，他们要处理流程变更，修改必要的脚本用于生成密钥签名材料，以便在各次密钥签名仪式上审核，然而他们的精力是有限的。

因此，我们目前所面临的挑战本质上是资源有限的问题。而且我想，我们所面临的风险就是，延迟 KSK 轮替的时间越长，可能受到影响的用户群就越大。

不过与此同时，我们延迟密钥轮替的时间越长，将会用于实施 DNS 的软件就越有可能以更合理的方式支持密钥定期轮替，减少遭遇崩溃的可能性。

这些软件既包括 DNS 软件，也包括路由软件和过滤软件，我们预计这些软件最有可能出现问题，因为左右两边的数据包规模大大减小。

所以目前，我们正努力评估在可用资源有限的情况下，最佳的行动路线是什么。眼下，我们还没有对何时发起密钥定期轮替流程达成具体的决定。

但我们已着手开启制定沟通计划的流程。我们聘请了 Adelman 来帮助我们制定这一计划。我们一直在制定实际运营规划，这些规划将会和威瑞信公司一起完成。如果 NTIA 给出的期限允许，实施规划将会把设计团队的建议用作参考。

除了实施规划外，还有测试计划 — 我们需要制定它，以便将崩溃的风险最小化，撤出计划 — 应对发现崩溃比预期更严重，致使我们不得不后退的情况，以及沟通计划，我们都期望能够在不久的将来完成。我没有确切的日期和时间，因为那需要我们进一步掌握实际的实施要求后才能确定。希望这个解释能够回答你的问题。

阿莎 • 合美嘉妮： 是的，谢谢戴维。

拉姆 • 莫罕： 有没有其他 — 拉斯？

拉斯 • 芒迪 (Russ Mundy)： 谢谢。也谢谢你，戴维。我是拉斯 • 芒迪。关于风险和风险平衡，我想再说两句。每一个活动都有一系列特定的风险，有时往往不容易预见到。在根区密钥定期轮替的情况下，等待的时间越长，风险就不断变换升级。

目前，似乎我们等待的时间越长，DNSSEC 的使用频率就越高，开始解决算法轮替的压力就越大，而这甚至比根区密钥定期轮替更加复杂。

所以当我们想要或需要进行算法轮替时，在我看来，如果我们在进行算法轮替之前，至少已合理进行了密钥定期轮替的实践，就可以简化步骤，那样会好得多。

虽然我们现在知道大部分大型验证解析器是什么，但不是全部知道。然而等待的时间越长，数量就会越庞大，问题也会变得更难，特别是当新的验证者开始寻找新算法来取代当前算法时。

戴维 • 康纳德： 我是戴维 • 康纳德。我不知道。

对密钥定期轮替的相关风险进行评估实际上极其困难。例如，仅仅一个月前，几周前，就在一个许多软件包中使用的库里发现了一个缺陷。而在这个缺陷的咨询建议 — 或者也许是观察意见中说到，如果过滤响应大小，就不会受到这个缺陷影响。

过滤响应长度意味着，如果人们这么做的话，那么密钥定期轮替不管什么时候进行，对所有做此配置的解析器而言都会有非常高的失败率。

随着时间推移，我不知道现在轮替的风险更大，还是以后轮替的风险更大，但我可以看到两种观点都有人支持。在我看来，目前那真的不是问题。

我们目前所面临的问题，我认为就是缺乏可以为这个问题投入的资源。正如我所说的，参与国际化级别 IANA 移交的人员也是参与密钥管理的人员。IANA 内部有多个处理移交的项目正在进行。

此外在 IANA 内部还有多个旨在改善基础架构的项目，以便能更加灵活地开展像定期更换密钥和管理密钥签名仪式这样的工作。

因此，虽然我完全同意风险问题事关重大，但是在我看来，在此之上还有一些与密钥管理运作有关的因素要优先处理。

我就讲到这里，下面有请克里斯。

帕特里克 • 弗斯特朗姆： 克里斯请讲。

克里斯 • 狄思潘 (Chris Disspain)： 大家下午好。我是克里斯 • 狄思潘。在正式发言之前我要先讲两点。第一，我的发言可能非常不成熟；第二，我对技术一窍不通。

我认为，从实践的角度来看，不管什么时候进行真正的密钥定期轮替，制定一个计划都没有害处。这样当准备好定期更换密钥时，就有现成的计划，届时就可以进行风险评估。

所以我想对于戴维而言，问题是：你是不是说目前没有足够的精力来制定这个计划，所以即使我们决定启动时也无法至少有一个现成的定期轮替计划？

戴维 • 康纳德： 不是，抱歉。实际上我们现在正在开展计划制定工作。所以不仅仅是一个计划，而是一系列计划。实际上我们现在就处在制定这些计划的过程当中。

我们等了设计团队一段时间。等到他们完成报告，我想大概是在去年的十一月份。我的团队内部资源有限，导致了延迟，所以造成设计团队的最终计划看起来像是花了很长时间才完成，对此我很抱歉。但是，正如我所说的，它今天已经发布。而且这是一份参考文件，需要纳入到我们目前多项计划的制定当中。

帕特里克 • 弗斯特朗姆： 非常感谢。

有请格雷格。

格雷格 • 亚伦 (Greg Aaron)： 克里斯，我是格雷格。实际上这项工作的规划由两部分组成。一个是纯粹的技术规划，由戴维和他的团队负责，还有一个是外展和沟通规划部分，因为我们要打破一些固有的东西。

所以 SSAC 在这份计划中建议，我们必须提前解决这个问题，并与相关社群讨论，以便他们了解接下来会发生什么并有时间为它做准备。

戴维 • 康纳德： 说明一下，就像我之前提到的，我们聘请了 Adelman 来帮助我们制定外展计划。

拉姆 • 莫罕： 谢谢你，戴维。

下面我要确认一下是否还有其他同事要发言，之后我们将完成这一项的讨论。我看到丹尼在等候发言。还有其他人吗？丹尼。

丹尼 • 麦弗逊 (Danny McPherson)：

我是丹尼 • 麦弗逊，来自 SSAC。我只想说一点，这里还有一个相关事项，那就是有人认为，要能够将大小至少为 1,024 位的 ZSK 密钥链接纳入到一个由威瑞信公司管理的 2,048 位的根区签名密钥中。

在这方面已经与 ICANN 沟通并协调了一个计划，而且威瑞信公司肯定已经准备好推行这个计划。我们认为，这些时间表不一定要和今天提出来、预计将在年底完成的 KSK 计划重叠。

即便如此，还是有一些技术上的相关事项应当考虑。但是我认为，一般来说，作为 SSAC 成员，对这些活动的考虑、意见和维护对基础架构的安全性和稳定性至关重要。作为移交计划的一部分，正如 NTIA 在 3 月 14 号所说的，安全性和稳定性是基本原则，这些活动不能破坏基础架构的安全性和稳定性。

所以我相信这极为重要。杰夫刚才表达的观点极为重要。

我要指出的另外一点，也是我希望将来尽量避免的是，很多与域名冲突问题相关的基本元素，比如基础架构的仪器检测、与基础架构相关方的广泛外联，以及可能会受到失败影响的各方等，等同于 DNSSEC 密钥定期轮替功能所需要的基本元素。这项工作无论如何都要做到位。而且我认为，从 ICANN 和社群在这方面所做的工作来看，我们确实取得了突飞猛进的进展。

但是当然，我们需要研究后续的准备工作，以及与基础架构相关方的沟通。我认为，对于需要做什么这个问题很好理解。但

是我不知道其他很多外部活动的价值在哪里。我想，SSAC 和社群非常清楚需要做什么。那仅仅是开始实施的问题，而且我也意识到这部分很棘手。

戴维 • 康纳德： 我想要说明的是，我强烈同意丹尼所说的，用仪器检测基础架构。如果我们现在就进行这一检测，将对我们理解密钥定期轮替的潜在影响大有帮助。遗憾的是，我们没有进行。

拉姆 • 莫罕： 谢谢你，戴维。

帕特里克请发言。

帕特里克 • 弗斯特朗姆： 好的，非常感谢。我认为这是一个非常好的讨论。同时我想，过去几天没有参与过讨论的人现在也能理解，我为什么会如此感激帮助推进这项工作的每一个人。

所以从 SSAC 的角度来看，你们也听到了，在这份已发布的报告中，第一个日期是 4 月 1 号。从 SSAC 的角度来看，在 4 月 1 号以前决定在 4 月 1 号当天要做什么，或者此前要做哪些准备工作，这一点十分重要。所以我对你们以及董事会有一个问题。你们有没有抽时间考虑一下，你们要怎么协助推进这项工作，以及我们在 SSAC 可以怎么协助推进这项工作。

当然，我理解这主要是我们和戴维之间的事情。但是，另一方面，我们也听到杰夫说了，它涉及到我们所有人。所以，从现在起到 4 月 1 号之前，我们可以一起做哪些工作？

拉姆 • 莫罕： 布鲁斯？

布鲁斯•托金： 谢谢帕特里克。我想你已经引起了我们的注意。在之前的两分钟，董事会交换了数千条讯息。

所以我想现在你已经引起了我们的注意，现在是我们要负责和 CEO 做一些工作。事实上，在 4 月 1 号我们将迎来一位新的 CEO。或者抱歉，新（听不清）。

[笑声]

但是，届时在任的 CEO 实际上将会是阿克兰 (Akram)，谢谢。

所以我猜这只是一个一般性观察。我听到戴维讲到工作孰先孰后的问题。众所周知，大量社群都忙于研究如何重组 ICANN。但是与此同时，我们的根本任务其实是保障标识符系统的安全性和稳定性。我们必须践行这一点。所以，你们知道，这确实是我们优先级最高的工作之一。我可以向你保证，明天我们将会和 ICANN 员工商量此事，并有望很快回到 SSAC 告知时间安排的具体情况。

帕特里克 • 弗斯特朗姆： 非常感谢。就像我说的，如果有 — 我们 — 因为我们 — 呃，让我重新组织一下语言。我希望你们理解，我们指出 4 月 1 号这个日期其实是向你们表示，我们已经做好从现在到那时之前埋头苦干的准备。

拉姆 • 莫罕： 谢谢帕特里克。我想，到这里，第一个重要话题的讨论可以圆满结束。下面我们转到第二个话题。

帕特里克 • 弗斯特朗姆： 本，请发言。

本 • 巴特勒 (Ben Butler)： 好的，我是本 • 巴特勒。我们想要借此机会讨论一下 ICANN 最近引入关键绩效指标也就是 KPI 的工作。在公共评议期或者最近开启的一个评议期内，我们在 SAC77 文件中提交了意见。为了节省时间，在这里，我们从这份文件提出的看法中总结了一些讨论要点。我想，在最高层面，我们最主要的意见就是：提出 KPI 所采用的方式方法有点儿落后。提出的衡量指标似乎是建立在一些很容易收集到的数据基础上，并且试图从这些指标中推导出某种意义。然而，要真正指示域名空间的健康程度，更有意义的做法是思考我们真正需要确定的是什么，然后思考哪些指标可以让我们真正达到这个目标。

比如，我们最近发布了一份文件，我想是 SAC74，其中我们探讨了注册人数据保护和凭证管理生命周期。而且有一个推荐 KPI 是说，你可以使用注册服务机构报告的违规数作为消费者对域名空间信任度的指标。这个信息很容易获得，因为注册服务机构总会报告一定数量的违规事件。但那其实不能说明消费者的信任度如何。虽然可能还有其他资源能够作为更好的指标，但是显然，如果我们要真正探究域名空间中的关键绩效指标有哪些，就必须从注册服务机构社群、注册管理机构等方面获取一些目前无法收集或没有共享的数据。

格雷格 • 亚伦在评议期中提出的几条意见我们也可以考虑，但是同样地，它们主要也是围绕我们研究 KPI 的方式很落后这个中心观点阐述的。我们希望，或许可以鼓励 ICANN 后退一步，从更全面的视角来研究这个问题。

拉姆 • 莫罕： 史蒂夫。

史蒂夫 • 克罗克 (Steve Crocker)： 谢谢。基本上我非常赞同使用一个投诉指标，因为对投诉的衡量有一个独特之处。人们在两种情况下会停止投诉。一种情况是，他们感到满意；另一种是，他们不再认为投诉会带来帮助。我不确定 — 你知道，我认为，我们必须避免仅仅以它作为衡量指标。

拉姆 • 莫罕： 你要回应吗，本？

本 • 巴特勒： 我只是想抛砖引玉而已。抱歉。

格雷格 • 亚伦： 我是格雷格 • 亚伦。在推荐的指标中，有一些是围绕对 ICANN 投诉的指标。有的时候，它们可能是有用的。还有的时候，这些投诉并不能衡量人们认为它们可以用来衡量的对象。比如，由于获取违规信的流程原因，发送到注册服务机构和注册管理机构的违规信数量其实并不能告诉我们遵守合同的机构有多少。WHOIS 是另外一个将投诉数量用作指标，衡量准确度和人们对准确度的满意度的例子。我们说过 — 或者有人说过，我们实际上有一个 WHOIS 准确度衡量计划。让我们使用这个计划中的指标。这个计划实际上会告诉我们一些事实和数据，让我们了解到自己做得怎么样。

所以我们要利用这个机会来进行一些教育，特别是一些安全性和稳定性相关问题以及如何有效衡量它们，它们会告诉我们有关 ICANN 和整个生态系统表现如何的一切信息。

拉姆 • 莫罕： 谢谢。接下来是谢林。下面依次是谢林、埃里卡和赛勒斯。谢林。

谢林 • 查拉比 (Cherine Chalaby)： 我对你的观点很感兴趣，因为我想要确保我们都理解它。所以，你们用“落后”这个词是说，我们在收集数据，然后决定怎么处理这个数据，而不是识别你希望这些数据反映的问题，然后进一步收集数据来证实它或否定它；你说的是这个意思吗？

本 • 巴特勒： 基本上是。而且这样的方式有时会造成你们想法和实际说法的不一致。

谢林 • 查拉比： 这很有意思 — 我不知道阿克兰或赛勒斯在不在这里 — 对此有什么看法。好的。那是一个很好的 — 好，谢谢你的观察。

拉姆 • 莫罕： 埃里卡。

埃里卡 • 曼 (Erika Mann)： 好。我想问的问题和谢林的差不多。实际上我读了你写的文件，你引用了格雷格 • 亚伦的观点。你还说可以使用其他指标，因为那样可能会更清楚。你说格雷格观察到，一些推荐的 KPI 是围绕目前可用的数据来设计，这样收集起来将经济高效，但那不代表这些数据总是适用于指定的用途。在某些情况下，ICANN 可能需要挖掘新的数据来源。

目前，我同意你的观点。这始终是一个问题。如果你想要分析数据，就需要了解你实际上想要分析的是什么，这样才能提出对的问题，然后才有可能获取一些不能随时获取的数据。那么究竟缺少了什么？我仔细阅读了这份文件，但是我希望从中看到的，我想也是对我们大家都有所帮助的，是对问题类型的一个简单概括 — 你实际上想要获取哪些类型的数据？也许我漏掉了一些要点，但是如果你能给出一个更简单的版本将会很有帮助。

拉姆 • 莫罕： 本。

本 • 巴特勒： 谢谢。文件中指出了一些具体的例子，比如我之前提到的违规通知。根据 2013 年的 RAA，注册服务机构必须报告违规情况，但那仅仅是在要求的范围内。在 SAC74 中，我们的建议是，必须对违规报告再次进行分析。作为一个社群，如果我们不仅能够获取违规数量，还能了解违规类型，有多少用户受到影响，是否与凭证管理有关，那将会很有用。你知道，我们可以在不让注册服务机构或注册管理机构难堪的前提下了解这些讯息，而且信息越详细，实际上就能更好地指示域名空间的健康程度。这就是其中一个例子，表明采用这种方法可能需要取得我们当前无法获取的新数据。

拉姆 • 莫罕： 谢谢，本。帕特里克，你要就数据方面插两句。

帕特里克 • 弗斯特朗姆： 是。当我们说其他数据或不可用数据的时候，并不是说数据的总量增加了。有可能是收集到的很多数据都是不需要的。所以你们需要进行这个评估，来收集真正需要的数据，不要更多。

我看到马克和赛勒斯想要发言。马克，请你先讲。

马克 • 塞登 (Mark Seiden)： 我们当中撰写凭证文件 SAC74 中注册人保护问题的成员认为要遵守一个根本原则，那就是当人们的凭证遭到泄露时，应该设法让他们了解到这一情况，而且在美国，常见的做法就是向这类人发送违规通知。虽然 ICANN 拥有注册服务机构违规报告的数据，但不会详细公布这些数据。所以我个人认为，应该收集并公布这些数据，以便保护注册人。

拉姆 • 莫罕： 赛勒斯，你是最后一个发言人，请注意时间。本次会议还剩下大约 9 分钟。所以在赛勒斯就这个话题发完言后，我们将转到第三项，也就是一个信息简报。

赛勒斯 • 那马兹

(Cyrus Namazi)： 谢谢，拉姆。我是赛勒斯 • 那马兹，来自 ICANN GDD。也许由我来解释一下这个计划是什么，会对在座各位有所帮助，也有助于我们达成一致意见。有的人可能不了解。

这是一个计划当中的一项举措，旨在构建一个公告板用于分析和跟踪 gTLD 市场的健康度和多样性。这是它背后的主要目标。为此，在员工方面，我们撰写了一份文件。在这份文件中，我们加入了一系列人们提议的想法和标准。在这里我要强调“提议”这个词。因为我们实际上询问了社群、专家、你们 SSAC 方面以及其他人，让大家一起帮助解答我们应该跟踪什么这个问题，告诉我们比如说衡量域名市场健康程度意味着什么，以及我们需要收集数据来得到哪些衡量指标和标尺。其中有的数据，就像你说的，是可用的，有的是现成的，还有的不可用。去年年底我们发布了这份文件征询公众意见。

我们所收到回复的深度和广度，坦白说，完全出乎我的意料。人们的热情十分高涨。我们收到了 30 多条公众意见，当然，其中一条来自 SSAC。里面提供了非常有用的信息。

在我们的文件提案中，任何内容都不是板上钉钉的。它们仅仅是提议，是为了激发讨论。而且我很高兴它其实帮助我们达到了这个目的。

实际上，SSAC 的意见非常有帮助。所以从一月底以来，当公共评议期结束后，ICANN 员工就采纳了每一个人的意见。我们已

将它们纳入到文件中，很快就会再次发布，以供公众审阅。提出这项计划后，现在共有 30 名志愿者自愿组成一个咨询委员会与员工合作，定义 gTLD 市场健康的含义，然后就像你说的，回过头来看看我们需要衡量、跟踪什么，我们需要收集什么类型的数据。

我其实非常乐观，也非常感谢社群为此投入的精力，因为它的知识基础和视野必须由你们这些在各自领域的专家来决定。请放心，实际上没有什么内容是 ICANN 员工预先就确定下来的。它需要由你们来完成。这是一个反复沟通的过程，所以将会持续改进和微调，直到进入下一阶段。但是我希望它有所帮助。

拉姆 • 莫罕： 帕特里克。

帕特里克 • 弗斯特朗姆： 非常感谢。下面是最后一个话题，向 ICANN 董事会通报一项我们刚刚开始的工作。吉姆。

吉姆 • 加尔文 (Jim Galvin)： 谢谢帕特里克，我是吉姆 • 加尔文，现任 SSAC 副主席。在本例中，我是 SSAC 内部这个工作小组的联合主席。和我一起担任联合主席的是坐在我左边的莱曼 • 查宾先生 (Lyman Chapin)。我相信你们还有一张幻灯片，上面有一个图表。请切换到那一张幻灯片。

大多数董事会成员都还记得，我们在上一次 ICANN 会议上进行了一个简报，着重向董事会指出了一个我们认为具有一定重要意义的问题。所以以下就是我们对这个域名空间相关话题的信息更新。基本上，我们的目标就是要让你们了解并提醒你们 — 我们认为这个话题很重要。

这里我们绘制了一个图表，也是我们目前讨论的基础，我们认为它反映了这个问题空间。我只花几分钟来提取这个图表的一些要点，我们希望能够以此来解释我们正在处理并与工作小组一起研究的整个问题空间。

从这个图表中，要理解三件事。第一，这仅仅是对现存的所有潜在 TLD 字符串的部分子集的一个快照。比如，IETF 有一个特殊用途域名的注册管理机构，申请人指导手册有自己的保留 TLD 名称列表，对吧？这是一个根区中 TLD 名称的列表，其中每一个都代表某些 TLD 名称列表的子集。

关于这个图表，要理解的第二件事是，每一个子集都有自己的入选标准。在某些情况下，这个标准定义得非常清楚，所以我们可以考虑根区中的 TLD 标签。我认为，在很大程度上我们都认同这一点，那就是，对于哪些名称能够进入根区、哪些不能有一个非常清楚的定义。尽管要考虑到一些特例，但大多数都得到了非常清楚的定义。

关于这个图表，要理解的第三件事是，有一些规则用来确定某个字符串能否移进或移出其中任何一个子集。在这里，有一些

案例表明这些规则得到了清楚的定义，比如根区中的 TLD 标签以及一些其他列表，而且在其他一些列表中，还有着更为宽松的定义。

有一点需要谨记，就是我在第一点中所说的，这仅仅是一个快照。所以还有一点要考虑到，那就是 — 这不一定是所有可能可以作为有效 TLD 字符串的标签列表。可能还有其他组织、其他场合、其他机构有他们自己的清单，基于他们自己的原因用于他们自己的目的，这一点也必须谨记。

这给我们提出了三个主要问题，这三个问题奠定了我们讨论的基础。我们也想让你们了解这些问题，这样你们就可以花一些时间来思考。如果你们想要更详细了解，当然可以和我们当中的任何一个人交谈，他们都可以提供信息，方便你们讨论这个话题。

第一个问题是，其中任何一个子集的加入规则是如何定义的？由于这些列表的来源各不相同，这些不同来源将对哪些可以加入他们的列表、哪些不能有自己的意见。而且还要理解一点，那就是，其中一些列表的加入规则定义要优于其他。

第二个问题是，将某个字符串移进或移出某个子集的规则是什么？同样，在某些情况下，对于能否加入其中以及是获得还是撤销加入资格，可能有清楚的定义，也可能没有。谨记这些事项十分重要。

最后一个问题既是最重要的问题，也是我们相信这个议题具有某种意义的原因，特别是在 ICANN 社群中，也是我们最希望向你们强调，以便你们谨记于心的问题。那就是，任何两个或多个子集的交集意味着什么？某个名称或某个字符串出现在其中一个列表上，而不在另一个列表上意味着什么？如果某个字符串同时出现在其中两个列表上又意味着什么？以及，比如，请看这里的方框，你们看到有至少三个方框没有任何交叉，那又会怎么样。这其实是一个传统的维恩图，如果你们愿意这么说的话。所以（这是）根区中的 TLD 标签。你们有一个名称列表，特殊用途域名，比如像 .ONION。在申请人指导手册中，你们有一个保留 TLD 标签列表，例如 ICANN。这事实上就是没有交集或交集为空的情况。那里什么都没有。你们希望是这种情况，可能在所有这些情况下都是这样，对吧？但是，这个意思有没有得到清楚的理解，有没有文件记录？创建并管理自身列表的各个机构有没有互相交流和沟通，是否了解他们必须尊重彼此的列表这个事实？

这就是这部分的最后一个问题，以上仅仅是向大家做一个信息更新。我们主要希望借助这幅图表，向你们做一个非常清晰务实的解释，告诉你们这个问题空间是什么、我们为什么认为它很重要。谢谢。

拉姆 • 莫罕： 史蒂夫。

史蒂夫 • 克罗克： 谢谢，吉姆。你的介绍非常有用，非常清楚。一段时间以来，我一直在跟踪有关这方面的信息交流。特殊用途名称似乎出自于一个传统，不一定是在 IETF 自身当中，但也相距不远。首先我们将构建并使用它，然后让人们讨论我们是否要注册它。

而为了展开关于如何协调这些事项的讨论，意味着有一份协议或隐含协议，规定应该做一些协调。但是我注意到，至少有部分社群非常反对我们来协调一切这个理念，他们认为我们想要做什么就去做，不要被任何规则束缚。

也许我说得有点儿绕口，但是你明白我的意思。

拉姆 • 莫罕： 谢谢，史蒂夫。

吉姆，请讲。

吉姆 • 加尔文： 哦。好。我回应一下。我认为对此的应对就是要考虑图表底部的那些不受约束的名称，也就是：home、corp 和 mail。

我的意思是，的确，从某种程度上说，这些机构可以独立存在，而且当然可以有自己的保留名称，自己的保留列表。但是我们大家都记得，域名冲突这个问题从几年前就开始出现，至今仍然存在。

你们所面临的问题是，即便不同的机构可以有自己的列表，但这些名称的使用会蔓延到其他环境中，这就是为什么有必要进行协调的原因。你们要么协调，要么就必须处理其中的一些技术问题。实际上就是这一点导致了这个问题的产生，或者说使更多人看到了这个问题。谢谢。

拉姆 • 莫罕： 谢谢，吉姆。我认为，对董事会而言，要了解几个讯息。

一是要关注这个空间。这个事务很重要。

第二，我想代表董事会，对你们一直关注这个空间，帮助解释各种差异，并说明跟踪这些差异的重要性，表示由衷的感激。

董事会将通过多种方式，向你们 SSAC 成员寻求帮助，请求你们提供对当前问题和后续工作步骤的指导。

因此我要感谢 SSAC 过来与我们会面，感谢你们所做的一切。最后请你讲两句，帕特里克。

帕特里克 • 弗斯特朗姆： 好。我也要感谢 ICANN 董事会召开本次会议。就像我在会议开始时说的，我们非常期待在每一届 ICANN 会议上与董事会召开这些会议，并且当然，也期望未来继续与你们合作，期待下一届 ICANN 会议的到来。谢谢。

拉姆 • 莫罕： 谢谢。现在我宣布休会。

史蒂夫 • 克罗克： 谢谢。

[掌声]

[会议记录结束]