德班 – GAC 与 SSAC 会议
2013 年 7 月 16 日（星期二）– 09:00 - 10:00
ICANN – 南非，德班

主席 DRYDEN： 各位早上好。请大家就座。

今天早上，GAC 和安全与稳定咨询委员会在这里开展交流，向大家介绍一些重要议题。

SSAC 的活动涉及多个方面，因此我们要充分利用今天早上与 SSAC 这个短暂的会面机会，多多交流。

事不宜迟，现在就由安全与稳定咨询委员会主席 Patrik Faltstrom 发表讲话。

那么，Patrik，请发言。

PATRIK FALTSTROM： 非常感谢，Heather。也感谢所有 GAC 成员，让我们有这个机会可以跟大家见面交流。

我是 ICANN 安全与稳定咨询委员会主席，坐在我左边的这位是副主席 Jim Galvin。

SSAC 成立于 2001 年，并于 2002 开始运行。我们作为一个咨询委员会，与大家所属的政府咨询委员会一样。

SSAC 的章程包括：负责针对互联网名称和地址分配系统的安全性和完整性向 ICANN 社群和董事会提供有关问题的建议。

目前我们有 39 位成员，由 ICANN 董事会任命，任期三年。

由于时间限制，而且大家已经从我们这里拿到了一些资料，我就介绍到这里，下面，如果大家对 GAC 以及我们的运营有任何问题，欢迎大家直接提问。

我没有看到有人提问，那我们就到这里。下面我们讲解内部名称证书咨询。

这是我们的文件编号 57。我们编写文件的过程包括：成立工作小组。由各个工作组分工准备文件材料。

首先在工作组内部达成一致意见，然后在整个 SSAC 统一编写文件，并发布文件。

SSAC 成员可以自行回避参与文件讨论，也可以申请添加反对意见到文件。这种情况发生过几次，但是一般情况下，SSAC 能够对文件达成共识。

这是其中一份我们达成了共识的文件。

这次咨询确定了为确保安全通讯负责颁发证书的证书颁发机构，特别是针对网站和其他协议，如果广泛使用该惯例，会对安全网络通信的隐私和完整性造成重大风险。此 CA 惯例会对新 gTLD 计划产生影响。

在此报告中，我们建议 ICANN 立即采取措施以缓解此类风险。

此报告于 2013 年 1 月初定稿。

请看下一张幻灯片。

我们将这份报告交给 ICANN，ICANN 采取了 SSAC 的建议，立即采取行动缓解这一风险。但是仍然存在一些风险，还需要采取更多措施才能解决。

请看下一张幻灯片。

哎呀，好吧。返回上一张。

简单来讲，本报告讲的是证书颁发机构有一个惯例，会为 DNS 中不存在的域名颁发证书。本报告介绍了在新 gTLD 过程中，如果将证书颁发给根区域中尚不存在的域名后会得到授权。

从技术方面来讲会发生这样的情况，你为一个域名取得了一个证书，然后该域名得到授权并覆盖一项服务，确保到服务的连接安全，但是并没有对这项服务颁发证书。

今天来参加本次会议的很多 SSAC 工作人员会很乐意跟大家讨论这个问题。

ICANN 启用的缓解策略包括与 CA 浏览器论坛交流和协作，证书颁发机构与浏览器供应商正是通过该组织提出相应策略，采取行动和更改惯例将风险降到最低。

先到这里。谢谢。

大家有问题吗？

主席 DRYDEN： 非常感谢，Patrik。

我先来问一个问题，我看到意大利代表也准备发言。

我要向你提的问题是，因为我们正处在新 gTLD 计划过程中，或者说接近计划的尾声，这个问题会对当前的计划或者已经做出的申请有什么影响？

PATRIK FALTSTROM： 经过调查公共网络上存在的证书，我们在这份报告中确认，现在确实存在为新 gTLD 系统中申请的域名颁发了证书的情况。

我们在这份报告中也稍微谈到了需要进一步调查相关影响，但是也提出了一些缓解措施，包括 CA 浏览器论坛同意的一些策略，其中有：停止此惯例并撤销 CA 证书，正如我们在 SSAC 中讨论的，这样可以大大降低风险。但是对于现有的，已经申请的域名，仍然可能有证书。

主席 DRYDEN： 好。谢谢 Patrik。有请意大利代表发言。

意大利代表： 我的问题与主席提的问题一样，所以感谢你的回答。

主席 DRYDEN： 好。请英国代表。

英国代表： 非常感谢，Patrik，谢谢你告诉我们这个问题。我是说，这个问题看起来相当重要。但是，我不太清楚解决这个问题的最佳方案是什

么。如果你已经提到过，可能是我没听清楚。如果是我没跟上，请你原谅。

但是，遇到这种情况后，你是不是需要暂停一些特定的申请，同时研究出解决方案，防止系统出现不稳定性因素？这是最佳解决方案吗？可能出现这个问题的情形是什么样的，我想申请人会想知道这个问题。

谢谢。

PATRIK FALTSTROM：

在我们看来，SSAC 提出的建议是撤销已有的证书会对申请有效，例如，实际验证这些撤销列表，将已经颁发的证书作废。这是一种缓解方法。

当然，还有另一种方法，停止颁发这些证书，这是另一个策略。结合这两种方法可以将网络上产生的这些证书的风险降到最低。

等待或搜索这些证书是没有用的，因为这些证书中有很多只是在企业内部使用，在网络上根本看不到。通过搜索的方式只能找到其中很小的一部分，甚至找不到，没有人知道具体有多少。你只能找到暴露在公共网络上的那些证书，有时候是因为本地配置错误，因为企业配置错误才暴露出来。

因此，从 SSAC 的角度来讲，我们在报告中指出，这说明当前的信托证书系统确实存在问题。这个问题类似于，例如，大家可能听说过的 DigiNotar 事件，以及证书颁发机构存在安全漏洞的其他事件。因此，当今互联网使用的受信任证书颁发机构列表机制并不稳定。

当今互联网所定义的信任分配是通过这种方式完成：例如，域名系统以及 DNSSEC，然后以更加现代化的技术 DANE 使用，每个域名真正使用的证书信息是存储在 DNS 上，由 DNSSEC 签发。

因此，我们在报告中指出的真正解决方案是，开始使用 DANE 和 DNSSEC，继承 DNSSEC 层次结构和 DNSSEC 的信任，使用它确定要信任的证书信息，而非使用受信任方列表，因为列表更新非常慢，而且你可能延迟更新，在这个延迟期间，可能存在漏洞和攻击因素。

主席 DRYDEN： 感谢你的回答，Patrik。

对于这个内容，大家还有什么意见或问题吗？

英国代表。

英国代表： 谢谢。我再补充问一点。

企业的内部服务器造成此冲突的规模大吗？我是想问，有上百家公司吗？或者上千家？

这会对企业造成影响，有没有一种方法可以纠正这个问题。这是我的理解。

PATRIK FALTSTROM： 这个问题有两个不同的答案。首先，根据实际描述，我必须承认这一点，因为我们在 1 月到 3 月间发布了这份报告，很抱歉我不记得

具体时间。所以我要参考一下报告，以便保持我的陈述与报告一致。

但是结果，我们发布这份报告正是因为我们发现使用的范围比较大，这样说可以吗？

我们得出的结论是，这些方法可以非常好地解决问题。因为使用的技术存在固有问题，导致我们无法更好地解决问题。在实际操作中会存在问题，因此我说，延迟使用 TLD 也没有用。

如果没有经过细想，你可能会问另一个问题，稍微不同的问题，如果公司或企业以任何方式使用今天在互联网上还不存在，但稍后会被授权的域名，会怎样？

好。

SSAC 已经在研究这个问题，我们也向董事会提出了解决方案，要求研究名称冲突问题。

所以，你可以阅读内部名称证书报告，将它作为名称冲突问题的一个示例。

例如，如果授权的域名正在某个企业中使用，会怎样？是的，因为各种技术原因这会造成一些影响，例如搜索路径和其他事件。

但是根据董事会的研究要求和一份更早的 SSAC 报告，ICANN 已于 2010 年秋发布了 SAC 45，着手研究域名空间冲突问题，了解域名空间冲突问题实际的严重性，或者存在哪些风险。

主席 DRYDEN： 谢谢。

接下来有请马来西亚代表和荷兰代表提问。

马来西亚代表： 你好，谢谢。好的。我来自马来西亚。

我有一个问题。也许我提的问题你已经做出了解答，但是我想请你稍微解释一下证书颁发机构的这个问题会对最终用户产生哪些影响。这对我们很有帮助。

谢谢。

PATRIK FALTSTROM： 证书问题对最终用户的影响，可能发生的最糟糕的情况是，例如，最终用户通过网络浏览器连接网站。你看到挂锁成锁定状态，你相信自己具有信任的通信，但是实际上连接到的网站并不是你想要的网站，而是另一个网站。这是可能发生的最糟糕的情况。

也是因为此，我们在 SSAC 中说仍然存在一些风险，但是这还是缓解了很多风险，因为还有很多其他攻击机制可能欺骗最终用户，让他们相信自己的通信是安全的。如果要回答你的问题，我得说，与其他因素相比，我们没有评估这一风险。

主席 DRYDEN： 谢谢。有请荷兰代表发言。

荷兰代表： 好的，Patrik，谢谢你的演讲。

我有一个问题。你期望 GAC 做什么？我认为你已经，SSAC 已经指出了问题所在，并且已经采取了一些行动。而且你还说，ICANN 会进行进一步的沟通。你期望 GAC 做什么？

PATRIK FALTSTROM： 对于 GAC，我没有什么具体的目标，但是我对包括 GAC 在内的整个 ICANN 社群确实抱有期望。

名称空间冲突问题非常严重。这一点已经在许多文件中指出过。大家看看我们在 SSAC 中所做的努力，包括 2010 年 11 月 15 日的 SAC 45 以及 2013 年 3 月 15 日的 SAC 57，即这份内部名称证书文件，以及其他文件的内容。

虽然目前 ICANN 发表了一份研究，调查名称冲突的实际风险。据我所知，这份研究已接近尾声，并提交给 ICANN。我们与 ICANN 的其他群体一样，都在等待了解报告的结果，以及根据报告得出的结论。董事会已经明确要求 SSAC 对得出的任何结论发表意见，对相关文件提出修改建议。

我个人希望能有一个公众意见征询，例如，针对发现的结果和/或得出的结论。因此，我希望所有人，包括 GAC 能够留心，并在必要时对此发表意见。

而且已经明确要求 SSAC 关注此问题，确保从技术安全和稳定性方面考虑，研究和结论以及所有方面都以健康的方式进行，这就是我们的使命。

主席 DRYDEN： 谢谢。

下面请斯里兰卡代表发言。

斯里兰卡代表： 谢谢主席。

早上好。我是来自斯里兰卡的 Jayantha Fernando，我是 GAC 代表。首先，我要感谢 Patrik 和 SSAC 团队在这方面做出的所有出色工作。我只想简单评价一下，并有一个建议。

虽然我们是 DNSSEC 签署的第一批国家代码之一，在这种环境下运行时，我们发现了其他域系统中有很多银行和组织。在这种环境下，我们也需要构建 CA 环境。

我们现在的情况是，他们希望寻求更大的合作。你的惯例陈述中，有没有一种方法可以适合发展中国家环境的 CA 运行？可能 GAC 可以提供一个环境或平台，通过它，可以在开始运行时或在发展中国家环境中，将信息传播到 CA。这只是一种看法，你对此有什么建议吗？

谢谢。

PATRIK FALTSTROM： 就像我之前说过的，在 SSAC 中，我们在内部名称证书报告中指出，如果我们继续按照之前的方式使用证书，即列出受信任的 CA，我们并没有为证书问题找到一个 100% 的解决方案。

但是，一条可行的途径是使用像 DANE 这样的机制，这样可以在 DNSSEC 和证书之间建立技术连接。

一条途径，我个人认为，因为我们还没有在整个 SSAC 中讨论过这一点，您国家的域名持有者可以从当地 CA 处获得 CA，然后采用该 CA 的指纹或哈希，在 DNS 中采用 DANE 技术进行存储，注册 DNSSEC，以此方式告诉互联网上的其他人连接到该网站，查找域名，从这里，在 DNSSEC 和 DNS，客户端 2，有该网站的任何人都会在 DNS 中查找并通过 DNSSEC 验证是否使用了正确的证书。

因此信任关系是来自 DNSSEC，实际上是将指纹存储在 DNSSEC 签名的记录中，而非是因为 CA 受到信任。因为现在我发现，不仅是在发展中国家，而且在许多国家或地区，包括瑞典，有时候都会遇到这样的问题。因为如今，CA 必须终止这些受信任的 CA 列表，例如操作系统中的内部浏览器。对于 CA 来讲，有时候这会非常困难，因为他们希望将精力集中在销售证书上面，希望保证安全运行。他们希望集中精力做这些，而不是这些浏览器和受信任的列表。谢谢。因此，是的，我确实认为这可以帮助开始执行 CA 和创新以及确保环境安全。

主席 DRYDEN： 感谢你的发言。GAC 对这个问题还有其他疑问或意见吗？伊朗代表，请讲。

伊朗代表： 谢谢你，主席女士。感谢今天为我们做出的演讲和清晰的解答。

我有一个简单的问题。你如何确保受证书中所规定条款约束下域名的功能，有没有可能不遵守这些条款？如果回答是有，你如何监控这种行为，并确保妥善执行和遵守条款。谢谢。

PATRIK FALTSTROM：

我只能从 DNS 角度进行回答。正如我之前提到的，CA 浏览器论坛已经就 CA 当局和 CA 证书颁发机构最佳实践达成一致意见。我不知道 CA 浏览器论坛采用什么政策或审核方式达成了此协议。所以你需要跟他们谈论这一点。对于 DNS，证书本身包含证书覆盖的域名。现在，证书中的域名可以包含任何域名，说明证书以及证书和域名所有者之间的关联在于证书颁发机构的验证操作。政策上也是这么规定的。因此，审核就在于证书颁发机构按照这条政策进行验证。

所以我们提到了一项新技术 DANE。因为 DANE 允许证书所有者在特定域名下的 DNS 中提供指纹，一个证书校验和，并通过 DNSSEC 签名。

例如，如果我作为一个证书所有者执行了这些操作，而你连接到我的网站，首先，你使用我的域名。通过 DNSSEC 验证返回的 DNS 记录是正确的。然后查看 DNS 记录，找到我在 DNS 中放的证书指纹。检查该指纹的 DNSSEC 签名，确定指纹正确。借此确定域名，以及它的证书。然后检查，取得证书。

这件事比较复杂。关键是，你检查证书内的域名，确定该域名就是你要查找的域名，并且通过 DNSSEC 验证了这个域名。如果域名是对的，你就能知道这个证书确实是为你通过 DNSSEC 连接的域名颁发的，这说明，在 DNSSEC 的帮助下，最终用户有额外的能力可以

验证证书颁发机构的行为正确。所以说这一点很重要。因为现在，证书颁发机构可以为任何域名颁发域名。当然，并非随意颁发，因为有审核和自我控制。但是我们工程人员希望有额外的技术手段来确保这些。

主席 DRYDEN： 伊朗代表有补充吗？

伊朗代表： 是的，补充一点。如果两个域名不一致，你要怎么做？会采取什么操作？谢谢。

PATRIK FALTSTROM： 现在，通过 DNSSEC，如果 DNSSEC 签名回复没有验证，客户的计算机不会得到回复。所以，现在你在使用浏览器时，通常会显示这个屏幕。噢，这个域名不安全。您要继续吗？是/否？每个人都会单击是。好。如果采用新技术，根本不会显示这个屏幕。这样，最终用户得到了保护。但是，在某些情况下，最终用户也会收到此类信息，或者应用程序取得了足够的信息，能够告知最终用户他们将进入不安全的通信，当然，我们也知道，有时候实际上你宁愿可以通信，因为就算你知道它不安全，但是通信本身确实非常重要。

主席 DRYDEN： 感谢你补充的问题，也感谢 Patrik 的答复。好的。GAC 同事还有其他问题吗？

PATRIK FALTSTROM： 就到这里吗？

主席 DRYDEN： 是的。我们手上有一些报告，说明了 SSAC 负责的内部名称证书和名称冲突问题。我认为 GAC 应该另外抽时间阅读这些报告。如果 GAC 还有其他问题，SSAC 也会予以作答。

PATRIK FALTSTROM： 现在，跟我在参加其他会议时一样，我想要告诉大家，在 SSAC 的 39 位成员当中，几乎有 20 位出席了德班会议。他们都很乐意与大家交谈。所以，大家不用只向我提问。对于其中的某些主题，他们实际上是 SSAC 在这方面的问题专家，比我掌握更多的详细情况。如果你有问题需要弄明白，可以找他们中的任何人。因为这就是我们的目标，我认为我们应该利用这些面对面的会议机会，通过高密度的沟通，听取报告，与 SSAC 成员交流，与他们讨论，向他们提问，真正了解这些建议。是。这是个好主意。今天来开会的 SSAC 成员可以站起来吗？

这些就是我们的 SSAC 成员。

主席 DRYDEN： 一群优秀的工作人员。好。

感谢你。我看到澳大利亚代表要提问。好。有请澳大利亚代表。

澳大利亚代表： 谢谢主席。谢谢 Patrik。这是一次非常有趣的讨论。我们还剩下几分钟时间，但是我们还有些问题没有提到。有一份 SSAC 报告是关

于无点域。我在会议中听到很多人在讨论无点域。我阅读了这份报告，SSAC 的观点非常明确。这里强烈推荐不使用无点域。

但是我认为，SSAC 在发表这份报告以后，应该采取了一些后续工作并做出了一些考虑。我希望你能告诉我们无点域的进展情况。

PATRIK FALTSTROM： 感谢你提的问题，Peter。

首先，申请人指导手册中说明，除非申请人能证明他们能够安全使用，否则不允许使用无点域，我们在 SSAC 中是称它为无点域。

SSAC 进行了调查，并强力建议默认情况下，绝对应该这样授权，即不应允许使用无点域。

在 ICANN 工作人员公众意见征询期间，根据我们的报告，有些供应商做出了一些回复，说如果使用无点域，许许多多最终用户的本地环境将会被破坏。

所以，供应商基本承认他们的无点域申请得出具体结论，例如，当使用无点域时，客户使用的域名甚至不会作为 DNS 查询。因为申请会将无点域字符串解释为其他内容，而非域名。例如，如果你在浏览器中输入一个不带点的单词，浏览器会执行单词搜索。对吗？这就是区别。

所以，在此以后，董事会要求 ICANN 工作人员发布一份报告，说明它对企业和经济的影响。并就此开展了一些谈话。今年春季，ICANN 工作人员针对无点域发布了一份调查，如果我没有说错，这

份调查已经完成，只是没有对外公布。我也不知道这份调查的结果如何。

在启动这份调查的同时，互联网架构理事会还根据互联网上针对各项协议（包括电子邮件）使用的标准撰写了一份文档。互联网架构理事会也强烈建议不要使用无点域。强烈反对无点域的文件数量在不断增加。而且，大家可以注意到申请人指导手册从一开始也反对使用它。所以，所有这些讨论并非是要请求变更。更像是在说明申请人指导手册的正确性。

主席 DRYDEN： 感谢你的发言。阿根廷代表请发言。

阿根廷代表： 谢谢主席。Patrik，谢谢你的演讲。也要对大家做出的所有工作表示祝贺。我要向 SSAC 提一个问题。SSAC 成员采用的是什么样的任命方式？我看了名单，只有一位成员来自拉丁美洲。我们的 GAC 代表可以做些什么来提高这个团体的多样性？如果这个团体需要更加多样化，而且我看很少有女性，我们需要做些什么。谢谢。

PATRIK FALTSTROM： 感谢你提的这个问题。我们有一个工作组叫做成员资格审查委员会，由副主席 Jim Galvin 负责。我们采用接收提名的方式操作，所以大家可以自我提名，或提名其他人。然后对提名人进行面试。具体说来，成员资格审查委员使用一个列有 MTU 评估标准处理的技能或各种问题清单。而且是的，性别和地理多样性也是其中的条件。但是也还存在其他标准。例如，具备各种技能，所有我们需要的技

能集合，对 SSAC 来说非常重要。例如，这样才能研究各种报告。例如，需要有人具备非常深厚的 DNS 专业知识。我们不需要很多。但是我们确实需要，例如，最近任命的两个人来自执法体系，也有女性。

所以，我们确实有一个内部流程。对于地理和性别多样化的要求，我个人感到非常失望。我们能做些什么？跟其他的许多情况一样，鼓励和欢迎大家来申请成为 SSAC 成员。

主席 DRYDEN： 谢谢 Patrik。还有几个代表要发言。然后我想结束这次会议。新加坡代表请讲。

新加坡代表： 谢谢主席。谢谢 Patrik，谢谢你们团体所做的贡献。我有一个一般性的问题。我们知道，本行业中有几个利益相关团体在监控着互联网的安全性。例如，反网络钓鱼工作小组 APWG 和 PhishTank。这些工作组列出了网络钓鱼网站的清单。我们可以定期查看这份清单，了解我们是否有一些域名被列为网络钓鱼网站。我想知道的是，SSAC 是否与所有这些行业专家组有工作上的联系？如果你们要寻求指导，会怎么做？我们会联系 SSAC 或 APWG 吗？

PATRIK FALTSTROM： 谢谢。答案很简单。没有，我们与其他任何团体都没有联系或正式关系。我们有的 SSAC 成员同时也是 APWG 成员。所以，SSAC 会与 APWG 及类似团体共享大量的信息。

主席 DRYDEN： 谢谢。下面请俄罗斯代表发言，然后是英国代表。

俄罗斯代表： 谢谢主席。

Patrik，对于你的建议，对于 SSAC 关于无点域的建议，我有一个问题。这个要求应该强制执行，还是仅作为软性建议，因为你知道这只能应用到新 gTLD，因为新 gTLD 目前在实际惯例中还没有此类限制？谢谢。

PATRIK FALTSTROM： 大家都知道，就像你提出的，TLD 中的地址记录是在 zone APEX，在互联网上确实存在。我上一次查看时，就在几分钟前，互联网仍在工作。所以，显然这不会给互联网带来致命影响。也就是说，在非常特殊的条件下，你可以在 zone APEX 中使用地址记录，不会带来次级后果，我认为这说明每个人都知道，特别是从技术的角度来讲，没有必要在互联网中完全禁用它。但是，它的风险是如此之高，因此必须鼓励不要使用它。

俄罗斯代表： Patrik，我要声明。这更多的是关于游戏规则。从技术角度看，很明显是这样。对我来说，这个问题非常明显。但是它涉及的是规则。因为，如果 ICANN 对一些注册机构提出了要求，但是不对其他注册机构采取特定要求，这会导致问题。

PATRIK FALTSTROM： 是的。但是现在，我们要讨论的是 SSAC 范围以外的事项，涉及合同安排，以及如何处理合同双方以及其他方。SSAC 的工作并不涉及这些。

主席 DRYDEN： 谢谢。

那么，英国代表，你还有问题吗？我们现在要对这次会话做个总结。你要求发言。对吗？

英国代表： 是的。

主席 DRYDEN： 请你简单一点讲，好吗？

英国代表： 还有一个方面我们没有提及。这可能属于刑事剥削，你在总结中提到。你是否希望 GAC 向董事会建议“停止它”？

PATRIK FALTSTROM： 你说的“它”是指什么？

英国代表： 对于不带点域名的做法，你认为这是新申请人需要的吗？

PATRIK FALTSTROM： 我不介意得到 GAC 的支持，例如，对于 SSAC 建议。

主席 DRYDEN： 谢谢。非常简洁的回复。好。非常感谢 SSAC 来这里为我们做简报。通过这些意见交流，我们确实受益颇多。GAC 成员，现在是 30 分钟的休息时间。谢谢大家。

[音频结束]