ZH

ICANN73 | 筹备周 — DNS 和域名安全的知识共享和实例规范 (KINDNS) 最新动态
大西洋标准时间 2022 年 2 月 23 日星期三 — 11:00 至 12:00

阿迪尔 • 阿科普罗根

(ADIEL AKPLOGAN)： 我们将向大家简要介绍 KNDNS，这基本上就是一个推广域名系统 (DNS) 最佳实践的项目。我们今天会提供同声传译服务，所以请大家使用。发言者请尽量放慢语速，口齿清晰，以方便译员翻译。

请在问答窗格中提问，这样我们就能看到。我想如果你想发言，也可以举手，他们将让你发言。史蒂夫 (Steven)，请翻到下一张幻灯片。

我们的演示将分为两部分。首先我会给你们做个介绍，之后我会请出 [菲利普 • 雷诺 (Philip Regnauld)]，他是我们这个项目的专家，将给你们介绍一下这个项目的实质进展情况。

在 ICANN72 期间我们已经开会介绍了 KINDNS，并且稍微解释了我们要做什么，所以我会直接从 KINDNS 的相关活动开始讲。它是一个以 DNS 和 [域名] 安全著称的知识共享协会。简而言之，它是关于共享最佳实践以及能够与社群和 DNS 运营商合作，自愿将他们的意见添加到最佳实践当中，同时也帮助我们在 ICANN 的所有人在全球推广这些最佳实践，确保我们像平常一样协同工作，尽可能地保障 DNS 的安全。请播放下一张幻灯片。

你们有的人可能已经熟悉了《路由安全相互协议规范》(MANRS)，这是一个保障在线路由安全的项目。KINDNS 和它稍微有点关系，所以我们可以说，如果我们有良好的 MANRS 和 KINDNS，那么我们就将在安全方面更进一步，保障互联网对所有人的安全。

在这里我们想要实现的就是，制定简化的可操作或易于遵守的最佳实践，以确保他们运营 DNS 的方式是安全的。在这里我们要强调 DNS 运营，因为这个项目将是关于 DNS 运营本身的纯技术的最佳实践。通常，围绕 DNS 有各种各样的服务，有许多应用程序运行，而该项目试图更有针对性地聚焦 DNS 运营的技术方面。

如果你熟悉 DNS，你很可能听说过 DNS [听不清]，它确定了所有和 DNS 有关的最佳实践 [听不清]，数量非常庞大，超过 2000 页讲的都是 DNS。我们要做的就是，从中提取出最重要的最佳实践，要求运营 DNS 任何部分的任何运营商都应该遵守，以保障 DNS 安全。请播放下一张幻灯片。

这个项目被 [划分] 成了几个组成部分。第一个部分是确定并记录最关键的 DNS 运营安全规范。这是在菲利普 • 雷诺的帮助下完成的，我前面提到过他，从某种程度上说还有社群，因为我们有一个电子邮件清单，在那里我们经常分享这项工作的最新进展，通知规范的内容，并征求社群的反馈意见。

然后，在这些最佳实践的基础上，我们将推出一个专门的门户网站来发布这些最佳实践，提供如何实施它们的指南，也为社群提供一个地方来评估一般或有用的信息，同时也让那些支持这个项目、致力于实施这些最佳实践的运营商可以加入进来，帮助我们推广这些最佳实践，正如我前面提到的那样。

因此所有内容都将 [听不清] 发布在一个专门的网站上，域名为 KINDNS.org。做完这些之后，我们将再次开始和所有人合作，确定一些有助于我们了解该项目对 DNS 安全影响的指标，确定其中一些

可以长期衡量的关键指标，了解它们是如何往正确或错误的方向上发展，并相应地进行调整。这将是我们运行项目之后下一阶段的工作。

通常，当我们在 ICANN 环境中介绍它的时候，常常会得到的一个反馈是：这是否会涉及到 DNS 的供应功能？也就是注册管理机构、注册服务机构和注册人的最佳实践。

简单的回答就是，一开始不会，因为就像我说的，它关注和针对的是 DNS 的核心功能。但是在它的另一个阶段，有可能。我们将研究如何将其中一些最佳实践映射到供应系统，也就是注册管理机构和注册服务机构最佳实践，并把它添加到项目中。但是它已经 [听不清]，但第一阶段将主要关注运营。请播放下一张幻灯片。

我们关注了某些类别。如果你运行 DNS，那么你是在一个环境下运行的，其中还有其他组成部分会对 DNS 的总体稳健性和安全运营产生影响。

就像我原来说的，我们不会纠正每一件事，而是会关注 DNS 的组成部分，也就是在不同环境下运行的权威服务器，也就是顶级域 (TLD)，或者运行关键区，也可以是二级域的人。总的来说就是二级域名经理。所以我们在关键区中有 TLD，例如 [.seal.uk] 或者任何 NIC.TLD，它们对这些 TLD 的运营很关键，所以我们将会把它们加入到第一个类别中。而第二个类别是，让注册人管理二级域名的所有人。

接着我们还有递归服务器解析器运营商。在这个类别下，我们还将处理三个子类别：私有（封闭）解析器、共享私有解析器和公共解析器。

所以我们将要推广的最佳实践将围绕这五个类别的解析展开。但是除此之外，我们也将提供有关如何 [听不清] 运营环境的指南，在服务、系统和网络方面，并且还涉及到一些会影响某个方面安全的隐私考虑。

在现阶段，如果任何运营商想要加入 KINDNS 并与这个项目合作，将会只对照我提到的两个主要类别再次对其进行评估 — 或者自我评估，也就是定义为权威服务器运营或解析器运营。

当然，我们将会公布实施指南、具体做法、检查清单和配置流程等等。这里有一个问题，我们将会提供关于哪个软件的指南。我们将会使用最流行的一个，但是当然，如果我们对它的呈现让人们理解这个概念，那么他们就很容易在运营中将这些概念应用到任何其他软件上。请播放下一张幻灯片。

从这里开始，我要请菲利普给我们介绍这些不同类别当中的不同元素。菲利普？

菲利普 • 雷诺： 好的。感谢阿迪尔的介绍。这是一个非常有趣的项目，我希望我们能够获得社群对我们提出并确定的各种最佳实践的反馈。

我们的划分方法，对这些 DNS 运营商的分类方法，决定遵循…起初我们觉得可能要按顶级域和二级域之类来划分。但是后来发现这有点不简单，反而更加复杂。

所以我们决定首先确定这是权威域名运营商，还是提供递归解析器服务的 DNS 服务器运营商。

所以，从权威服务器开始，我们所做的就是按层级性查看互联网上的区类型，当然，层级越高，DNS 就越重要，显然，根最重要，也许也最 — 不是最脆弱，抱歉 — 而是最容易成为破坏的目标，如果发生安全事故，它更有可能被选中。

所以，TLD 有一个重要的地方。但是我们也看到其他可能有重要运营的域。例如，在很多国家的域名服务器中，有一点很常见，例如我现在居住的丹麦 (DK)，DK 域的域名服务器被放在一个名叫 nic.dk 的子域中。可以说，这些二级域很可能和它们的域名服务器所在的 TLD 一样重要。

因此，我们决定按这样划分类别。我们称它们为关键区。显然顶级域，除了用于提供某种服务的所有辅助或所谓的支持区外，都托管了域名服务器或存在类似的依赖条件。

另一个我们决定包含在关键区中的元素并不和 DNS 本身的运营直接相关，但是如果我们从 ccTLD 的角度来看，某些区文件或 DNS 域名关系到非常关键的领域，例如医疗、电子政务、市民服务、身份识别系统，它们也许比其他域名更重要，但是在这种情况下，我举个例子。在丹麦，我们有一个国家身份系统，我注意到，如果 myid.dk 关闭，那么很多人就没法登录。你可能会想，那怎么会影

响 DNS。好吧，这将受一个自我评估模型驱动，这里我们要做的其实不一定是规定哪些区关键，哪些非关键。它更多的是一个框架，让人们确定：我运行的是关键区吗？或者让组织确定：我们提供的是关键服务吗？因此，指南是什么？我们应该遵循哪些最佳实践以保护这些服务？

当然，我们也纳入了像金融和银行网站这样的域名，它们可以被视为对一个经济体或一个国家的运行很关键。

所以我不认为它是随意判断，而是我们决定像这样构建它。从脆弱性以及对选区、经济体、国家的影响角度，如果这些域名关闭会怎么样，显然 ccTLD 本身是最关键的？请播放下一张幻灯片。

我们还有其他域名。当然就是在顶级域之下的所有其他域名。它们也很重要。它们将提供各种各样的服务和网站，以及电子政务和电子商务，还有我们在互联网上所熟知的一切事物。这些也必须受到负责任的管理。

这不是因为他们是二等公民或怎么样，但是我们要遵守的最佳实践限制可能会更少，原因是我们想让这个运营鼓励人们开始采用 KINDNS，开始实施这些最佳实践，而不是因为其复杂性而打退堂鼓。所以，如果你运行的是二级域，你可能不会给他人带来太大影响，因为你不进行授权，但是仍然有…你可能会遭遇网络攻击。你可能会遭遇系统故障。你会做尽职调查吗？你会运行可以让你缓解或者至少从这些事故中恢复的最佳实践吗？

在这方面真正有影响的不是域有多重要。每个人都应该这么做，因为一个配置错误或者被劫持的域将会以这样或那样的方式遭到破坏。下一张幻灯片，说到…对。

递归 DNS 运营商。那是这个生态系统的另一半，对吧？我们有权威运营商，还有递归 DNS 运营商，这里我们就必须考虑我们拥有的是哪种递归解析器。

简单来说，它们要么是公共的，要么是私有的。更仔细来看，私有解析器是完全的公司网络，完全封闭，外界不可访问，VPN 类型的访问，并且通常是在私有地址空间，它们将是一些公司和组织，比如医疗机构、银行以及大多数企业都会像这样构建。但是从某种程度上说，可能还有家庭网络和住宅网络。

更开放一点的有共享私有解析器，这可能是一个很有意思的名称，但是我们试图找到一些…我不想具体指明必要的 ISP 或者任何类型的提供商。我们称之为共享私有，是因为它们对一组客户或者一组机构而言是私有的。我把它想象成一个大学网络。它们无法从外部访问，但是可能仍然在法律上不同的实体之间共享。例如，多个客户共享一个 ISP 的解析器，或者可能是一个共同技术管理下的组织同盟。

这些将属于另一个类别，在那之后我们还有公共解析器。公共解析器我们很快就能了解。想象一下，也许是来自 Google 的 8888 或者 Quad9 以及这种类型的服务，但是在那之间，实际上是封闭的 DNS 服务，我们有商业 DNS 过滤，它们可能以某种形式开放，也可能不开放，但是…抱歉，我会试着讲慢一点。

对于公共解析器，我们有前面提到的 Google 等类似服务，还有半开放的 — 或者你们怎么称呼它？带有商业成分的开放解析器，签订了合适的协议或合同，你们将以清理或被动 DNS 服务的形式从这些特定解析器运营商那里获得附加服务，期间将会分析你们的 DNS 流量，以了解你们是否有主机被恶意软件破坏或感染。

这类运营商通常是公共的，但他们有某种访问控制机制，也许要支付一些费用或者签订某个合同，这样你们就可以使用他们的服务，并受益于 — 你们怎么称呼来着？受益于他们将提供的增值服务。

所以这就是不同的类别，在上面的部分中，我们确定了访问是如何局限于这些解析器的。它可以是 IP 地址访问，也可以是证书或者 VPN。这并不重要。这里真正重要的是，我们要将其中每个运营商归到一个类别中，然后看看 KINDNS，说“好吧，这适用于我们。最佳实践是什么？”

而且从某种程度上说，可能是对最终用户和组织的最佳实践。例如一个企业想要查找说“嘿，我在连接我的 ISP。我正使用他们的解析器来将我的 DNS 查询转发到互联网上。”他们应该遵循哪些最佳实践，他们有没有坚持？他们是否真正遵守了这个计划？

然后你就可以联系到你的提供商或 ISP 或你的 IT 部门。对于这些解析器最佳实践，我们有没有遵循 KINDNS？我们有没有按这里描述的方式保护用户的隐私？下一张。

对私有解析器的建议。对于权威解析器，我们其实尚未涵盖许多建议，但目前这不太重要。让我们聚焦私有方面。

私有解析器，正如我们提到的，位于私有网络上。它们有时是受信任的竞争域的一部分，像活动目录之类。所以你们可以在很多 Windows 环境中找到它们。

当我们聚焦它们时，我们所做的就是，我们主要聚焦网络安全，并确定对透明度的需求，这就意味着，某些建议可能在其他地方也有用，例如 DoH 或 DoT，很多这些网络对启用这些服务仍然是不确定的，但它们依然可以从使用 DoH 或 DoT 中获益，并将他们的请求转发到一个启用了加密的上游解析器，这样你至少能防止查询在网络外被窃听。所以对于每个运营商来说，这是一个稍微不同的场景。

接下来是服务的可用性和弹性。就像阿迪尔说的，有一些最佳实践将涵盖良好的旧系统管理最佳实践，因此我们目前不会研究它们，但相关详细信息将放到网站和计划中，这样在系统强化和适当的系统管理方面至少可以有一些信息参考。

这里非常突出的是，我们看到了 DNSSEC 验证。我忘记提到它了。对于权威服务器，当然，我们预期将向权威区运营商推广一个主要最佳实践，就是 DNSSEC 签名。这里在解析器方面，我们将鼓励 — 或者更确切地说是要求解析器进行 DNSSEC 验证。

幸运的是，很多软件已经这么做了，但是我们将强调它，并规定，现在你必须进行 DNSSEC 验证。再次说明，很多软件可能已经这么做了。下一张。

共享私有解析器，我们说过，是 ISP 类型。它们是 ISP 或类似提供商。他们将有和很多私有解析器类似的要求，但是他们的客户范畴不一样，因为他们的客户可能是移动、有线、光纤、住宅等混合类型。他们会有某种访问控制。

由于这些解析器在许多不同客户之间共享，因此也会有隐私问题。还存在像缓存窥探之类的问题，目前我们不做探讨。但是你要确定的是，当你提供 DNS 服务时，是以保护隐私的方式进行，因此在这里我们提出的一个建议是，在你的解析器服务上启用 DoH 或 DoT 或者两者都启用，这样你的客户就能更放心地向你转发查询，他们可以这么做。这也让他们感到可以使用你的服务，而不必因为延迟而另觅他处进行解析。他们可以通过提供 DoH 和 DoT 使用你的网络。他们可以使用你的系统，并且他们知道，他们已经与作为 ISP 的你建立了业务关系。那么你就应当提供 DoH 和 DoT。那只在隐私方面有意义。这当然会和现有的传统加密 DNS 并存，后者也将存在一段时间。

DNS 服务的可用性和弹性。在这方面我们也提出了一些建议。这些建议很快就会放到维基页面和网站上，它们也是良好的系统实践，卫生、强化。还有 DNSSEC 验证。目前可以预期，任何运行 ISP 解析器的人都要进行 DNSSEC 验证。下一张。

对于公共解析器运营商，我们谈的主要是大型开放运营商，像 Google 等等。当然，他们有自己的做事方式，但是我可以肯定他们当中有很多人已经实施了其中许多最佳实践，我们 [听不清] 现在其中之一就是 DNSSEC 验证。幸运的是，一些大型运营商都采用了 DNSSEC 验证以及隐私考量，DoT、DoH。所有大型运营商都提供

DoT、DoH 或两者，所以你可以将你的查询转发到比如说 Quad9 或 Cloudflare 的 1111，并使用他们的 DoT 或 DoH 服务。

我们提到的另一点是限定名称最小化，我忘记对其他人说了，限定名称最小化是为了避免不必要地向根泄露完全合格域名。通过启用它，可以确保只显露部分域名，因为不管我们想不想，域名都会显露。它们会透露有关我们的用户及其习惯以及他们所查看内容的信息。这不一定是为了公共使用。

对于封闭公共解析器也是如此，这些解析器提供支付服务或以某个协议或访问控制为基础，它们也需要提供 DoT/DoH，很多可能已经是这么做的。

如今限定名称最小化几乎总是启用的，作为一项标准实践，但是现在我们把它作为一项要求提出来。显然也有 DNSSEC 验证。下一张。

我想我要讲的就是这些。

阿迪尔 • 阿科普罗根： 我可以从这里开始。谢谢！菲利普向大家大致介绍了不同的最佳实践将会如何构建。再次说明，请记住，我们的目标是简化，并专注于最重要的一个方面，我们只想提供数量有限的最佳实践供实施，不超过我们总共 7:10 的目标，让人们能够心中有数，而不是感到更加困惑。

下面稍微回顾一下，所有这些内容在推出时将会如何呈现并构建。正如我前面所提到的，它将托管在一个专门的网站上，主要由 ICANN 支持和赞助，感兴趣的人可以以不同的方式加入这个项目，并获得他们所需要的信息。

我们将召开一个会议，探讨菲利普提到的不同类别。在支持和参与方面，想要加入并支持项目的运营商可以注册为赞助商、成员、域名运营商或者项目大使。

接着我们会有一个工具会议，运营商可以进行自我评估。我们还在讨论和研究这些自我评估工具将会是什么样子。我们希望它非常轻松、简单、直接，因为它不是强制性的。这是一个自愿参与的项目，由人们自行参加，并承诺实施这些最佳实践。

这个自我评估工具也主要基于人们对实施其中一些最佳实践的自我承诺，例如提前回答这些问题。

我们将有一个公告板。我们将开发一个公告板，其中会给我们提供一些信息。正如我前面所提到的，这样我们也能够跟踪我们选择的一些指标，以便了解它对整体情况的影响。接着我们还有关于如何实施最佳实践的指南，或者提供关于任何最佳实践或考量的更多细节和信息。

例如，如果你们仔细查看菲利普提到的关于强化核心或系统安全等等的幻灯片，所有这些将不会成为核心最佳实践，但是会在比如说指南中进行突出显示，人们可以前往查看。但它们不属于我们的核心内容。之后我们将会有博客、活动以及所有其他相关的事情。

所以在我们朝着这方面努力，总结、确定最关键最佳实践的同时，我们也已经开始制定其中一些指南。最近我们在我们的 [首席技术官办公室 (OCTO)] 文件中发布了一份 DNSSEC 签名指导手册。这类文件也将在 KINDNS 中参考，很快还将发布更多指南。请播放下一张幻灯片。

现在我们有一个签约方帮助我们设计和开发新网站，看起来可能像这样，但是我们还处在非常早期的阶段，还在 [帮助] 他们确定最终布局和最终设计。但是基本上，这将会是这个项目取得的下一个成果。下一张。

由于各种各样的原因，我们必须稍微调整我们自上次介绍以来的时间线，我们现在的目标是在 2022 年第一季度结束之前推出，也就是大约 3 月底之前。

也许我们不会推出网站的全部功能，但我们将推出大部分关键功能，这样我们就能开始运行它，开始铺开，开始观察运营商对此的反应。

在这个过程中，我们将向社群提供最新信息，包括在电子邮件清单上。如果你们感兴趣，我建议你们加入电子邮件清单。它是开放的。任何人都可以加入，向我们提供反馈，在讨论中建言献策。

与此同时，我们还建立了一个维基页面，我们会在那里公布我们当前工作的大部分内容，作为一个临时存储库。这些内容在 [添加] 后将会移动到正式网站上。

我想这就是最后一张幻灯片了。是的。谢谢大家的关注。我们愿意听取你们的任何问题、意见和建议。这也是本次会议的目的。谢谢。

金嘉 • 科瓦兹克 (KINGA KOWALCZYK)： 我们在问答窗口中有一个问题。阿迪尔，要我读出来吗？

阿迪尔 • 阿科普罗根： 好的。

金嘉 • 科瓦兹克： 这个问题来自西瓦苏布拉玛尼安 (Sivasubramanian)。“KINDNS 会不会也制定一个共同承诺，承诺不把用户绑定在一个解析器上，而是维持多个冗余解析器，任何人都可使用？一个 [粗略]、不准确、有点牵强的场景是 [听不清] 大学阻止学生使用外部解析器，或者市长坚持市内的所有人都不得使用另一个城市的解析器。除了共享最佳实践外，有没有这个和其他相关共同承诺？”

阿迪尔 • 阿科普罗根： 谢谢！非常有趣的场景。这个问题和本次会议的注册人部分也就是用户部分有关。在很大程度上和政策有关，因为当某人要求他们的客户、他们的用户、他们的社群、他们的居民使用某个运营商或某个服务时，这属于政策决定。而政策方面从某种角度上说其实不涵盖在内，因为我们对这类事情的控制微乎其微。

从注册人的角度，就运营业务而言，当然你可以在你的设置中设置多个解析器，这基本上是网络管理的最佳实践，服务供应的最佳实践，或者 DNS 服务的弹性和冗余性方面的最佳实践。但是我们没有具体关注这方面，因为它更多的是注册人和 ISP 最佳实践，不是 DNS 运营本身的核心所在。

金嘉 • 科瓦兹克： 我们没有收到其他问题。大家如果想提问的话，请举手，我们将打开你的麦克风并让你发言，或者也可以在问答窗口中输入问题，我将把它读出来。

阿迪尔 • 阿科普罗根： 这里有一个方面，我想听取参会者的意见。菲利普提到了。我想那是在关于公共解析器的幻灯片上，我们强调了隐私考量，这方面我们内部进行了大量讨论。

众所周知，DoH 和 DoT 起初非常具有争议，一开始引发了一些担忧，但是越来越多的解析器运营商实施它，而且总体上对隐私而言也是一个良好实践。

问题是，有多少隐私考量应当成为 KINDNS 的一部分？如果你看了去年之前的最佳实践文件，就会发现它们大都…隐私考量没有得到足够的强调。但是过去几年，隐私已成为在线用户的一个非常重要的考虑因素。

所以我们基本认为，KINDNS 中应该考虑隐私。限定名称最小化是全面的，从解析器的角度来说都与它有关，它是直接的，涵盖大部分软件，所以我认为在这方面没有争议。我没看到任何争议。

但是对于 DoT 或 DoH，有时会有人提出质疑。“噢，你们要涉及这方面吗？你们要说它是最佳实践，还是不是最佳实践？”在电子邮件清单上，直到现在对这两者一直都没有确凿的证据 [听不清]，特别是 DoT，但是我想听听大家对隐私的想法，从隐私考量的角度谈谈 DoT 和 DoH。有人举手了。乌尔里希 (Ulrich) 举手了。能不能打开他的麦克风让他发言？

乌尔里希 • 维塞尔 (ULRICH WISSER)：大家好。我是乌尔里希。对。谢谢阿迪尔让我在这里发言。我想说，我认为…DoT 解决了部分隐私考量问题，因为显然它不允许人们 [听不清] 聆听你的请求，但是你仍然要对你的运营商充满信任。那显然只能通过 Oblivious DNS 解决，但是我认为 Oblivious DNS 现在还完全没有准备好成为最佳实践。

阿迪尔 • 阿科普罗根：我同意。

乌尔里希 • 维塞尔：但是我想有一件事也许应该提一下，DoT 解决了部分隐私问题，但远远没有解决所有问题。

阿迪尔 • 阿科普罗根： 谢谢。这是从运营商的角度出发的一个很好的反馈。你提到了一些很重要同时也很有趣的事情。在解析器用户和提供商之间已经以某种方式存在的信任关系。例如在 ISP 的背景下，显然有一份服务协议。这里有一些限制，可能会从某种程度上带来隐私考量，或者如果你 [听不清] 有一项政策让你使用公司的解析器，那么隐私方面就有所淡化，因为不管怎么说，你使用的是公司网络，所以你必须遵守特定的政策。

但是当你处在野生环境，处在开放环境中时，也许隐私就变得更加关键，这就是为什么我们想要在涵盖公共和开放解析器的类别中更加强调隐私考量，在这里任何人都可以决定使用任何解析器，于是我们更关注隐私以及他们对解析器签名的内容。

在解析器方面，或者当然还有 [听不清] 方面、KINDNS 以及我们探索的最佳实践方面，其他人还有什么要分享的吗？

好的。如果没有其他问题或意见的话，那也就是说我们…我解读到我们处在正确的方向。我要感谢各位加入电子邮件清单，以及到目前为止对项目提供的意见。我想还有一个问题。哦，问答窗口中有一个问题。我漏掉了。你能读一下吗？

金嘉 • 科瓦兹克： 好的。衡量是不是 KINDNS 设计的一部分，有没有某种形式的衡量，可以让社群评估各个解析器维护的解析器数据，以及比较的方法？这种衡量是不是 KINDNS 设计的一部分？

阿迪尔 • 阿科普罗根： 好的，我前面说过，我们会确定一些指标，以便大致了解这会如何影响 DNS 运营的安全方面。这些指标是什么，目前还没有明确的定义。我们也可能会分享其他 ICANN 项目的一些指标，比如 [标识符合技术健康指标 (ITHI)] 或者其他已有的项目指标。

但是在这个问题中，提到了评估解析器数据。我不知道这里说的是哪种数据，以及在具体情况下的相关性。

通常从我们的角度来说，当我们衡量这类数据时，我们会试着从我们的角度衡量我们能够衡量的部分，而不会试着访问并非由我们控制的私人数据。而且我们可能会根据最佳实践衡量这些数据，并且只和我们 [听不清] 中的最佳实践有关，也许可以说，通过衡量那些启用了 DoT 或 DoH 或限定名称最小化的解析器，了解过去一个月、一年左右有隐私考量 [听不清] 的解析器数量。这是一个我们可以直接衡量的方式。

但是我不知道你说的评估解析器数据是什么意思，因为当你开始说到评估解析器数据的时候，这给了我一个完全不一样的视角。我们将衡量我们可以公开看到的部分，但是只和我们先前 [遵守] 的最佳实践有关。

另外我们也想让尽可能多的解析器加入这个项目，并承诺遵守这些最佳实践。如果在这个过程中，我们能够以某种方式与其中一些解析器运营商合作，来对他们的观察进行一些深度衡量和深度研究，那么当然也可以加入到项目中。

但是我要重申，我们将使它尽量直接，这样我们所呈现的内容就不会带来或造成任何争议，不管是给用户，还是给将要 [听不清] 项目结果的人。

好的。电子邮件清单是开放的。请随意加入，我们可以继续这里的一些讨论。在那里你可以提出其他考量或问题，或者也可以直接在 OCTO 联系我们。如果你有直接问题，也可以直接发送电子邮件到 OCTO@ICANN.org。

我看到戴思瑞 (Desiree) 提了一个问题。谢谢，戴思瑞。好的。就像我说过的，这里有一个沟通和外展部分，也倍受关注。当然我们和整个社群合作。这就是为什么我们有一个大使计划，隐藏在某个角落，通过它我们将与社群合作进行推广。但是在我们宣布启动项目后，ICANN 也将投入一些资源来宣传和推广这个项目。当然，项目的成功或许非常依赖推广，还有我们如何使它易于被社群理解和使用。

感谢大家参加本次会议。我们只剩下九分钟。我看到没有其他问题了，但是非常希望能够在线下见到大家，在电子邮件清单上和大家一起讨论。金嘉，我们还有其他要说的吗？没有的话，就交回给你。

金嘉 • 科瓦兹克： 没有了，我们回答了所有问题。谢谢大家。幻灯片可能会在几天后发布在 ICANN73 网站上。谢谢！

阿迪尔 • 阿科普罗根： 谢谢金嘉。谢谢，史蒂夫。也谢谢菲利普。大家再见。

菲利普 • 雷诺： 谢谢！

[会议记录结束]