神户 — 社群合作会议：非公开注册数据访问 TSG
2019 年 3 月 11 日（星期一）— 13:30 至 15:00 JST
ICANN64 | 日本神户

拉姆 • 莫罕

(RAM MOHAN)： 大家好。我们的非公开注册数据访问技术研究组会议马上就要开始了。谢谢。

大家下午好。我是拉姆 • 莫罕，是非公开注册数据访问技术研究组（也称 TSG-RD）协调人。本次会议大约会持续 90 分钟。

在本次会议中，我们预计在本次 90 分钟的会议中会用 45 分钟时间实际讨论我们实施的流程，向大家演示技术模型草案，了解你们的反馈和意见。

我们希望这将是一场互动会议。这不仅仅是会议。我们昨天与 EPDP 的人员会面了，今天晚些时候和明天我们还打算与其他几个工作组会面，向他们介绍我们已经完成的工作。

下面，我来说说本次会议的议程。我们计划在本次会议中讨论这些主题。希望我们能有足够的时间来讨论你们提出的任何问题。我们的会务人员也会查看远程参与者提出的意见，所以我们也能处理这些意见。

下面，我首先来简单介绍一下技术研究组。请跃然 (Göran) 为我们介绍背景信息，介绍我们是如何开始的，介绍我们是谁。

马跃然 (GÖRAN MARBY)： 谢谢，拉姆 (Ram)。在开始之前，我首先想感谢小组成员在过去三个月开展的辛勤工作。从外部来看，我始终感到很欣慰和幸运，能有志愿者来做这些工作。

为什么会成立这个小组？首先，我们通过潜在的技术解决方案讨论一些在法律上有意义的事情。所以我要重复一些事情，这些事情你们之前可能已经听我说过 200 次了。

GDPR 非常具体地规定了数据控制人、数据处理人的职责。根据 GDPR，接收数据、拥有数据并做出有关数据的决策的人是数据负责人。

对我们而言，数据负责人就是签约方。ICANN 组织作为法人实体，并不拥有数据库。我知道你们会对此感到惊讶。

因此，就这一点而言，很久以前我们很明显很难通过一种媒介制定出任何形式的统一接入模型，因为签约方作为个人拥有法律责任。

这就是说，即使我们拥有与之相关的政策 — 我看到史蒂夫 • 克罗克 (Steve Crocker) 先生到了。我要指出的是，史蒂夫 • 克罗克过去三个月一直在为我工作。史蒂夫 (Steve) 你好！

史蒂夫 • 克罗克： 你好！

马跃然： 这样说感觉真好。抱歉。这只是一种假设，假设签约方要做出个人决策。

我们首先会考虑不同的解决方案，如何减少签约方在 WHOIS 方面的法律责任。我不知道你们是否还记得，在巴塞罗那，我收到了一封所有签约方联名寄来的信，他们在信中说，“你为什么不不出去看看是否有任何可能的解决方案来减少他们的法律责任，以创建统一接入模型？”

因为如果我们不改变 DPA 对法律的当前解释，或者提出一些[改变策略的东西]，那么真的很难创建统一接入模型，因为我们不能超越法律强制实施 ICANN 组织制定的规则。法律始终驱动着 ICANN。

所以，我们开始这项讨论的背景是我们也在欧洲委员会内部进行了有关不同备选方案的讨论，在讨论中我们首先考虑了 ICANN 组织是否能合法地成为询问问题的地方。我们创建了一种基于 RDAP 的想法，即你带着问题来到 ICANN 组织，然后问题根据 GDPR 原则以安全的方式被传输至签约方。唯一能回答问题的人是签约方，再由签约方将答案返回至 ICANN。

这从表面来看非常容易，但是我们也意识到，我们需要真正的技术知识才能创建模型。不是让 ICANN 组织内部的我们坐在这里创建模型，我做出了一个明智的决定，让拉姆召集一组具备高水平技术的人来考量这个问题。

现在的问题是，在此次演讲之后会出现怎样的情况？首先，我期望收到大家对于他们所处理的解决方案的意见。

在这之后，我们将要做些什么，因为这是主要系统中的一个部分，这就是一种交换点。就此而言，必须有人认可谁可以提出问题。[听不清]一般术语，称为认证机构。

这里有若干个认证机构。例如 Europol 就是其中的一个。我知道这个社群中还有部分成员正在研究以不同的方式构建认证机构。很早以前我就提议将 WIPO 作为一个潜在的认证机构。

我的想法是连接认证机构，这些机构会验证谁是请求者、谁通过这个[机制]验证问题、谁在询问问题，然后将问题传输至签约方。

我们开展这项工作的方式就是将这些方面共同连接起来。我们的目的是向数据保护机构询问一个简单的问题：这是否会减少签约方的法律责任？

如果答案是肯定的 — 这里我们使用了“指导”一词，如果任何 DPA 会听取这一点，那么以欧洲视角来看指导实际上具有法律约束力，即当 DPA 给出一个问题的书面答案时，这可以作为其决策过程的一部分。所以它更强大。就是这个词。那就是我所认为的。如果没有处于合法背景中，有些事数据保护机构就不能说。

所以，由此得出的想法是，如果发生这种情况，这事实上为 ICANN 社群提供了为统一接入模型制定政策的机会。谁应该访问这个模型，我们对隐私和信息访问有什么看法？

这样做的目的不是接管 ICANN 内部的政策工作，而是能够向 ICANN 社群告知统一接入模型的法律可能性，或者我们也可以用其他名称来指代它。

我想提醒大家的是，如果你访问数据保护机构的网页，他们会说，“我们不是咨询公司，你们必须自己做自己的工作。”从任何数据保护机构获取法律指导，这是我们需要努力完成的事情，特别是与欧洲委员会一道来完成。

我们是为数不多的在上一次 — 我们称之为 [Calzone] 流程中实际获得指导的人之一。由于要进行记录，我不能在 ICANN 内部更多地指出任何项目的名称。

所以这也是一个存在问题的[听不清]。当我们探究临时规范时，我们实际上得到了 DPA 的法律指导。记住法律指导中说了些什么。其中说，[我们有]权利，我们可以收集数据。没有具体说明[哪些数据]，但说了我们可以收集数据。

指导中还说，他们接受我们使用一种覆盖模型，其中一些信息是公开的，一些信息是非公开的。这对我们来说是非常强有力和非常重要的指导。如果没有这些指导，我认为 DPA [听不清]的工作会更困难。

我们现在面临的情况是，我们没有获得关于第二阶段的法律建议，这就是我们在尽力解决的问题。欢迎大家提问。

没有？我突然感到很孤独。

女性发言人（姓名不详）：我有一个问题。减少后的责任是否足够？许多公司将会投入资金。这是否足以说他们的责任可能会减少？对于 DPIA 明确不接受哪些内容，我们不能得到更精确的回答吗？

马跃然：是的，我希望是这样。那取决于 DPA。GDPR 很有意思。我是一名监管者，事实上，GDPR 在技术上很有意思。我觉得我的幽默感很差，所以我曾经把它称为[母亲般的]法律，因为当我十几岁的时候，我的母亲曾经说过，如果我表现得好，我就可以出去。然后我出去了并且表现得好，但是显然，她对表现好的看法与我并不相同。

当有人告诉她我表现得不好时，我就会遇到麻烦。这事实上就是法律。法律说了，你应该做你认为是正确的事情。只要你能够解释你的行为，那就好。但是如果你不能，我们就会跟在你后面追究你的责任。

所以，你有很大的空间可以自行进行解释。这为法律带来了一个问题，这是因为各个签约方事实上不得不自行做出判断。

ICANN 通过我们的合同作为一个法律实体，在向签约方强制执行合同方面存在一个很大的问题。

鲁本斯 • 库尔 (RUBENS KUHL)：

我是鲁本斯 • 库尔，来自 nic.br。我有一个意见和一个建议。意见是，虽然其中一项动机是减少责任，但是这个模型可能会减少解决统一接入模型方面的运营成本。因此，可能存在消极和积极的激励因素。

我的建议是，ICANN 不要尝试强制使用此模型。任何被迫的东西通常会产生抵触情绪，人们会问“这是为什么？为什么要这样，为什么要那样？”但是如果是可供选择的，但在 gTLD 空间中具有强大的覆盖范围，那么它可能比强制实施的内容更强大，这正是因为这些不是强制实施的。这只是一个建议。

马跃然：

[听不清]第二件事是，我们已经在 ICANN 的合同中规定了，当本地法律取代我们的合同义务时，我们可以豁免合同义务。你可能会说，这是一个非常大的豁免。事实上，它实际上始于 28 个成员国和欧洲经济区国家等等。

ICANN 没有也不应持这样一种态度 — 如果本地法律与我们的合同义务产生任何冲突，我们不能强制执行我们的合同。我在

说的这点 — 昨天我听到有人说这只是一个梦想。是的，但是有时候我们也在说，我们会尝试做到。

我保证百分之百能做到了吗？没有，我没有做出这样的保证。但是我认为非常重要的一点是，调查减少签约方法律责任的可能性。当然，如果他们接受 — 因为这将成为他们接受的事情，因为这也是根据法律进行的事情 — DPA 的建议在法律上必须是强大的，他们可以确信有人为他们做出这个决定。所以很难[听不清]。

但是另一方面，ICANN 作为一个机构可以进行相当自愿的安排。我们与签约方签订的合同是基于社群通过自下而上的政策制定流程制定的政策。所以在某种程度上，我们采用的是共识模型，共识意味着你接受。不过我了解你的意思。但是我们不是政府。

女性发言人（姓名不详）：我有几个问题。抱歉，我没有参加 EPDP，所以我不确切知道这些问题是否已经得到了解决。但我想知道两件事。GDPR 让最终用户更多地承担有关其数据的责任。能否请你告诉我，如果一位最终用户，一位网站所有者希望访客在新模型下看到他的信息，是否会有提示信息指出，信息是公开的或者信息必须保密？这是第一个问题。

第二，我昨天听到注册服务机构的人对一位请求消费者访问权限以核实网站真实性的女士说，由于注册服务机构不能区别个

人和公司，因此他们根本不会进行这种区分。首先，这是真的吗，新系统中不会在个人和公司之间进行区分吗？

马跃然： 你询问的是关于政策的问题，在 PDP 中有许多这样的问题。所以这是一个政策问题，我和会议桌旁的其他人都没有参与政策制定。

我设定了非常严格的界限，因为我认为这些问题应该属于[最终的政策工作和政策]。技术解决方案具有一个具体的目标，这就是看看我们是否能够减少签约方的法律责任。

我接受这样一个事实 — 这使你的问题非常明智 — 立法者，DPA 可能对现有的 PDP 产生意见，这可能会产生影响。但是我们还没有答案。

这项法律还比较新，几乎没有法庭案例来[听不清]什么是隐私数据。对于你的第一个问题，就是如果你愿意你是否完全可以自行选择，我事实上并不知道这个问题的答案。

本尼迪克特 • 阿迪斯 (BENEDICT ADDIS)： 大家好。我是本尼迪克特 • 阿迪斯，我也在参与 EPDP。所以，我的发言完全从 EPDP 的角度出发，而不是从技术小组成员的角度出发，我可以告诉你们，我们针对由注册域名持有人

自行选择是否发布他们的详细信息进行了大量的讨论。这个问题还在考量当中。

答案可能是肯定的，这是有可能的。但是在目前还不是这样。这已经深深扎根在人们的思想中了。对于你的第二个关于法人-自然人之间区别的问题，因为许多原因，很难回答这个问题。看起来这属于乍一看似乎相对容易做的事情，但是如果将它拆分开来就会发现它具有很大的复杂性。例如，某些组织根据本地法律有权在其国家/地区享有隐私权。你可以想象一个堕胎诊所可能有权享有隐私权。

因此，关于该问题存在不规则的复杂程度，这意味着我们在 EPDP 中没有对此问题说“是”或“否”，但我们已将该决定推迟到第二阶段。感谢你提出了非常好的问题。

拉姆 • 莫罕： 谢谢本尼迪克特，谢谢跃然，谢谢大家提出的问题。如果大家还有更多关于政策事项和其他事项的问题，欢迎大家向我们提出，我们将把问题传递到各个小组，他们可能会采取相关的方法来解决这些问题。

让我 — 跃然。

马跃然： 我要到那边去听。

拉姆 • 莫罕： 你知道该怎么做。谢谢。

马跃然： 谢谢。

拉姆 • 莫罕： 好的。我们来谈谈我们已经做了哪些工作，以及我们是如何开始的。跃然给大家介绍了如何开始工作的背景。TSG（技术研究组）的目的是探讨技术解决方案，对具有建立在 RDAP 上的合法利益的第三方进行身份验证，向其授权并提供访问非公开注册数据的权限。这是目的。

现在，这里有关于 TSG 的章程。所有这些都发布在章程中。如果你访问你面前的屏幕上显示的网站，你将能够访问所有信息。

现在，我们非常清楚，正如跃然刚刚提到的，由于我们已经尝试在这里增加尽可能多的信息，TSG 将不会就政策问题做出任何决定或提出任何建议。例如，关于谁获得访问权限，甚至什么是访问权限，是否应该将其称为访问权限，在什么情况下哪些数据字段应该提供访问权限，什么是合法利益等的问题。这里存在着一大堆问题，我们很高兴存在这些问题，但它们大部分都不在我们的职权范围内。我们一直非常明确地专注于事物的技术方面。

谁是 TSG 的成员？如我们所说，跃然是发起人。去年 10 月，他让我组建一个小组。我花了一点时间来做出决定，你们可以看到这里有一些照片，但是最重要的是，你们可以看到技术研究组中几乎所有的人都在我们前面。我认为只有来自 Facebook 的默里 (Murray) 不在这里。但是技术研究组中的其他人员都在这里，在你们前面。

我们非常幸运的是，TSG 志愿者的工作得到了绝对一流的 ICANN 组织团队的大力支持，你们可以在这里看到其中的几个志愿者。这位是艾丽莎 (Elisa)，这位是黛安娜 (Diana)，这位是约翰 • 克莱恩 (John Crain)，这位是古斯塔夫 (Gustavo)。这位是弗朗西斯科 • 阿瑞亚斯 (Francisco Arias)，他没有参加今天这场会议。伊薇特 (Yvette) 和埃里卡 (Erika) 也对我们一直在做的工作提供了极大的帮助。

在一开始，我就非常清楚我们获得实际成果的方式是，让 TSG 采用以共识驱动的方式开展工作，我们必须在我们的流程中迭代，我们的关注点必须是技术。这就是我们开展工作采用的主要参与模型。

事实上，我们将过程连接起来制定模型、制定解决方案的方式是：我们首先从定义关键问题和考虑因素着手。然后，我们确定了主要假设。接下来，我们确定了使用案例和用户旅程，然后我们定义了系统要求，包括功能、操作、管理等所有这些系

统要求。我们制作了一份功能要求映射图，构建了一些行动者模型，确定了实施注意事项。

当我们完成了所有这些事情的时候，我们就可以在上个月召开面对面会议了，并且我们可以在会议上提出拟议解决方案。我们拥有的是一个非常迭代的流程，我们面前提出了若干个模型，我们能够检查这些模型，逐一查看各个模型是好是坏，并最终提出一项拟议解决方案，我们称之为技术模型。

我们参与的下一个部分是 — 在我们开展所有这些工作的时候，在我们提出技术模型、逐一查看行动者模型、考量实施注意事项和要求的时候，我们遇到了几个事情，这些显然是在整个空间中的考虑因素，但同样清楚的是，我们所做的这些考虑和这些观察并不是我们作为技术研究组实际采取行动的事情。

但是我们所做的是，作为一个完整性问题，并且作为一个非常好的管理权问题，我们正在记录这些观察意见和这些考虑因素，这将成为我们发布的最终文件中的部分内容，所有这些都旨在让社群中的其他部分而不是让技术研究组本身据此开展工作。

在这之后，下一步就是请社群提供反馈了。这就是我们向大家寻求反馈的其中一场会议，在这之后，本周晚些时候技术研究组就会在神户召开面对面会议，审核我们在这里收到的反馈，考量我们是否需要对提出的模型进行任何变更或其他修改。

然后，我们将用几周时间 — 另外三周或四周时间，进一步迭代我们正在做的工作。我们的目的是在 4 月中旬完成我们的工作，在 4 月底发布我们的最终工作成果，将其交给你们和社群以及跃然，最终我们就能够进行章程第 13 项了。

早些时候我谈到了流程，如果你们看看我们所做的工作就可以发现，我们做的第一件事是考虑什么是关键问题、有哪些考量因素。

如果你们返回到 ICANN.org/TSG 页面，你们就会找到章程，在章程中你们会找到列出的主要类别以及各个类别下的问题。这些各个不同的类别大约包括 17 或 18 个问题。这有助于理顺我们的思路，让我们明确我们应该学习什么，我们应该针对这些领域做些什么。

在我们开始开展工作的时候，我们首先明确的事情是，我们必须非常清楚我们做了哪些假设，因为如果我们没有定义这些假设，我们的一些核心工作就会夭折，就不会完成。

根据这一流程，我们首先做的事情之一就是列出关键假设。我们在流程中进行迭代的同时完善了这些假设，我们是在 11 月开始的，最初有七八项假设，在我们经历这一流程的过程中还提出了许多其他假设。这是个很好的信号。这表示我们认识到了更多问题。

现在，我想指出的一件事是，当你看到我们在谈论假设时，无论是在文档还是在幻灯片中，你应该认识到的是，我们自己并

没有断言这些是要做的正确的事情。事实上你看到我们所做的只是记录这些是断言，或者这些是假设，是在空间中做出或存在的，并且我们工作的基础是基于这些假设都为真。

现在，显然，如果某些假设不为真或者需要发展或者其他，这就可能对模型本身造成一些连锁反应，我当然希望处在你们的位置，坐在观众席上，倾听下一个工作组的发言，了解他们接下来会做什么，看看技术解决方案会得到怎样的改进。

因此，所有这些工作的一个重要方面是确认断言，我们的职权范围专注于技术方面。如果你们看到我们在这里做出的假设，如果你们看看政策部分或者觉得你不得不质疑这些假设是否会得到维持，我们在这里提供了一些声明。

请将问题提供给我们，但请认识到，我们无法就这些假设是否合适提供任何权威答案。我们想要知道的是，对于我们正在做出的这些假设，无论我们是否遗漏了一些假设，第一项或第二项，我们所做的假设是否实际上是完全错误的，从而可能会削弱技术模型的有效性。

因此，这些将作为一个框架，史蒂夫，我把麦克风传给你，请你为我们介绍一下有关这些假设的幻灯片。

史蒂夫 • 克罗克： 谢谢，拉姆。这里的图片是通过 ICANN 网关协调的非公共 gTLD 数据查询的基本概念图，该网关利用并访问应用于特定查询以及身份验证和授权过程的凭据。

这里有 12 项假设。我在这张幻灯片的括号中提到了其中 6 项假设，在下一张幻灯片中，我将向大家展示全部 12 项假设。基本模型是，RDAP 是将要采用的机制，因此端口 43 访问将被弃用，只有通过此协调访问才能访问 gTLD 非公共数据，来自未经证实的来源的查询将根据该政策进行处理，由 ICANN 负责监督与所有这些相关的凭据保护和有效性。

这张幻灯片列出了所有 12 项假设。上方所列的假设与我们刚刚介绍的是一样的，下方所列的假设是有效处理使模型具体化的过程中出现的演变、修改和相关问题的各种假设。所以必须有一个处理数据集和规则变化的流程，它必须与正常的 RDAP 使用相匹配，并演变为现有的 RDAP 实践。这必须是一项试点，必须反映政策选择以及实施实际性。

这必然是一个非常简洁、紧凑的演示文稿。阅读报告可以了解其余的详细信息。交给你了，拉姆。

拉姆 • 莫罕： 谢谢史蒂夫。介绍这些假设之后，如果我们可以转到下一张幻灯片，那么我们就可以定义一堆用例。先前我与你们讨论了我们遵循的流程。用例是我们所做工作的下一部分。安迪 (Andy)，请你来为我们介绍这一部分，好吗？

安迪 • 纽顿

(ANDY NEWTON)： 好的。我们经历过的用例 — 这又是迭代的，所以我们回过头来对这些进行了改进，但是我们想谈谈授权用户，他们需要访问这些信息。我认为执法机构是我们反复谈到的行动者，但是还有其他行动者，比如安全研究人员、知识产权律师，与此类似的人员。他们需要访问他们的多项查询，或者他们甚至需要进行单次的一次性使用查询。

我们还说过在线获得授权的用户，他们需要尽快获得授权，我们还有第三个用例，我们说有些用户需要能够访问与他们相关的数据。我们甚至需要支持经过身份验证的用户可能无权查看数据的用例。

最后，我们讨论了作为数据主体的用户以及他们如何访问数据。所以从那里开始，我们提出了除此之外的一些系统要求。这也是可以迭代的。首先，我们从考虑系统的不同构成部分开始，然后我们稍微扩展了一下。但总的来说，我们说过这必须基于互联网标准，必须支持 Ipv6，需要是分布式或能够支持分布式模型，我们需要使用安全协议，例如 TLS 和其他适当的安全协议，它们可以适用于我们在此指定的系统。

我们立即提出的一件事是，我们讨论了为那些需要快速请求或一次性请求的人创建一个门户网站。所以我们要求由 ICANN 运营基于浏览器的门户网站。

我们讨论了身份验证和授权确定。我们将这两个问题分开来看。我们希望在可能的情况下根据 ICANN 政策将其授权给合格的代理商。然后我们讨论了如何实际执行此操作，并且我们具有由 ICANN 运营的 RDAP 网关的概念，该网关查询签约方及其 RDAP 服务器。我们说过，它必须支持多个经过身份验证的请求者及其身份和不同的政策。

它必须能够处理对各种数据元素的细粒度访问，它必须支持将请求者的属性传递给签约方，当你收到未经授权的请求时，它必须知道在哪里重定向该请求。此外，我们还需要能够支持自动化。

然后这里是由签约方运营的 RDAP 服务器，他们基本上需要响应来自 ICANN RDAP 网关的请求。

我再谈谈一些更一般的系统要求，我们制定有关于记录和审计的要求，我们希望记录这些查询。我们需要一定程度的数据保留能力，我们需要有一种方法来协调来自所有这些方面的查询，以便我们可以进行审计并处理系统滥用问题。

整个系统范围要求的另一个方面是，我们查看了性能和服务水平协议，我们说必须签订针对所有子系统的服务水平协议，因为如果没有，你就永远不会知道系统的哪个部分在发生故障。对于正在发生的事情，必须有某种程度的保证。

最后，我们研究了信息安全要求，并且基本上说需要对要求进行评估，然后需要有一种方法来接受审计并向请求审计信息的

人提供相关信息。最后，如果存在违规行为，则需要有报告这些违规行为的途径。

最后，我们研究了组织控制，我们说这需要由业务连续性管理计划来管理，我们需要确保当前使用的所有加密存储技术都是需要使用的当前最佳实践。这些就是我要说的了。斯科特 (Scott)，你想介绍一下模型本身吗？

斯科特 • 赫伦贝克 (SCOTT HOLLENBECK)：

好的。谢谢你，安迪。正如幻灯片的标题所示，我们作为提案提出的模型基于两个基于标准的协议，即 OAuth 2.0 和 OpenID Connect。

在我介绍这张充满技术信息的幻灯片之前，我想向大家展示一张图片。这个类似于数据流的图表，它是史蒂夫向你们展示的图表的演变，更详细地介绍了行动者之间的互动以及各个数据元素之间的流动。

如果你熟悉单点登录服务就会知道，从概念上讲，这就是与访问网络资源有关的事情，你根据提示使用 Twitter 凭据或 Gmail 地址或 Facebook ID 登录，你们已经了解了这个模型。显然这里有更多细节，但数据流非常相似。

现在让我们快速回顾一下，然后我们再回到这一点上来。好了，这些单点登录系统要开始工作就需要满足几个先决条件。

首先，这些额外服务提供商必须是存在的。必须有一些流程使这些提供商存在，显然必须进行软件开发工作才能使这些服务设立并运行。

请求者，这个术语是我们从 EPDP 借用的，用于指称请求数据的人，请求者必须具有由身份供应商签发给他们的凭证。这些身份供应商是这些新的行动者之一。他们在签发这些凭证时的部分职责是将身份属性与凭证关联起来。

这个特定解决方案的一个好处是，它可以使用支持 OpenID 和 Oauth 的 Google、Microsoft 和 Yahoo 等公司提供的服务立即可用。但是事实证明，这些提供商对 RDAP 一无所知，因此他们还没有关联这些额外的凭证。他们暂时还没有这样做。

一旦满足了先决条件，当请求者使用某种形式的客户端应用程序向访问服务发送 RDAP 请求时，整个流程就会启动。访问服务收到此请求，并且因为访问服务不知道谁在请求，所以它向客户端发送重定向，与名为身份供应商的对象进行交互。

人们将看到的下一件事是由实体提供商运营的某种网站，他们在该网站上根据提示提供自己的凭证。这可以是用户名和密码，或者如果身份供应商和客户端提前协商，它也可能支持使用客户端证书。

为了便于讨论，对凭证进行了确认和验证。然后，客户端或人们将看到的下一件事是请求选择各种身份位，我们谈论的这些

属性，并提供他们的同意，同意与底层依赖方或实体共享此信息，由访问服务控制对此受保护信息的访问。

因此请求者做出响应，填写所有这些表单，按下提交按钮，身份供应商向客户端返回名为授权代码的东西，然后发送另一个重定向，一个 http 重定向到这个称为访问服务的东西，由它启动创建 RDAP 查询的流程。

访问服务获取此授权代码并使用它从身份供应商处提取称为“令牌”的不透明数据块。令牌返回至客户端。现在，这些令牌包含有关与请求者关联的身份的信息以及用于确定授权的一些状态信息。

客户端拥有令牌，然后他们将带有此令牌信息的 RDAP 查询发送至 ICANN 的 RDAP 网关。当网关收到此信息时，它便开始处理实际的 RDAP 查询。

网关接收查询和令牌，然后将两个信息位发送给第三方授权者进行验证。授权者处理这些输入信息，确保身份信息有效，并且查询与属性匹配良好，然后将验证结果返回至网关。这通常是“是的，准备好了”或者“不，那个人没有获得他们所请求内容的授权。”

因此，假设我们已获得授权，网关将向相应的签约方 RDAP 服务器发送 RDAP 查询，根据适当的情况，这些服务器可以是注册管理机构也可以是注册服务机构，提取所有非公开数据，网

关处理并过滤这些响应以形成完整的 RDAP 响应，响应返回至客户端，然后客户端向请求者显示结果。

这是我们的摘要表格图片。一些基本数据流。传递下去吧。

拉姆 • 莫罕： 谢谢。斯科特，如果你能用一点时间分别指出身份验证提供商和授权服务的话，我觉得会有帮助，我们是故意将这两者分开指定的。昨天我们收到了一些问题，询问我们是否打算将这两者绑定到一起，它们是否可以分发等等。所以我认为把这个问题讲得详细点会有所帮助。

此外，我们在审议过程中还讨论了我们对身份供应商的看法以及该角色的作用。

斯科特 • 赫伦贝克： 当然可以，拉姆，没问题。是的，所以那些熟悉 WHOIS 目前如何运作的人 — 我认为这个会议室里几乎所有人都对此熟悉 — 将会认出这个模型中的至少两个行动者。客户端和注册管理机构/注册服务机构 RDAP 服务器。

当你必须做出有关身份、身份验证和访问控制的决策时，该模型的运作效果不太好。在此情况下，引入了这些基于标准的服务。Open ID Connect 和 OAuth 2.0 旨在为我们提供正确识别客户端，对其进行身份验证以及根据其身份关联的属性制定访问控制决策所需的工具。

但这意味着我们需要在此矩阵中添加一些额外的参与者，第一个就是这个 ICANN RDAP 访问服务。在我们自己的小组中，我们称之为代理。因此，如果你熟悉代理的工作原理，你当然可以用同样的方式来考虑它。它就相当于经纪人。它接收查询，然后决定谁需要参与进来以及如何适当地传递查询。

但是，当服务获得查询时，它必须做的第一件事就是需要知道它正在与谁通话，并且它通过此身份验证提供商和此授权服务来了解这点。

现在，协议的工作方式，这些服务可以由一个有时被描述为身份供应商的实体来执行，或者可以将这些功能拆分开来由不同的行动者分别执行。我们描述的模型支持两种运作方式，最终，它可能是一个政策问题，确切地确定如何执行这种拆分以及哪个行动者执行哪个功能。

但是正如你们在这里看到的交互，身份验证提供商从 RDAP 服务处接收查询。它事实上是在与客户端交互。这就是我先前描述过的基于网络的接口。客户端在此提供其凭证。身份验证提供商签发凭证，所以它们能够执行身份验证功能，RDAP 服务永远不必接触这个信息。它只是从身份验证提供商处获得有关客户端是否已完全识别和进行身份验证的证明。

然后，这会将我们带入授权服务。一旦 RDAP 访问服务知道它正在与适当识别和验证的人打交道，就需要确定该请求者是否具有适当的访问级别以查看他们要求的内容。如我之前所说，

从传统来看这是 OAuth 中的一个功能，它由身份供应商执行，但它允许我们将该功能拆分为第三方服务。我们在模型中描述了这种可能性，它的工作方式是发送查询，根据一些尚未确定的政策进行比较，并向服务返回一个拇指向上/向下的响应类型，然后在建立和查询签约方 RDAP 服务器方面相应地采取行动。我说得够详细了，拉姆？

拉姆 • 莫罕： 是的，非常好。谢谢斯科特。还有另外一件事，有一个关于这个 ICANN RDAP 访问服务的问题，在我们的模型中这是否意味着来自各种来源的数据，ICANN 是否会在我们的模型中获得该数据的副本。所以，解决这个问题也很好。

斯科特 • 赫伦贝克： 好的。此模型中的数据与权威来源保持一致。我需要描述一下权威意味着什么，因为我知道详尽 WHOIS 政策就是说注册管理机构是数据的“权威”。

我们在这里采取略微不同的观点，权威意味着它是与数据主体有关系的实体。因此，这是一个出处问题，是数据最紧密地收集或产生的地方。

因此，这是你在此处看到注册管理机构和注册服务机构职能之间存在拆分和分隔的原因之一。注册服务机构将保留他们具有权威的数据。ICANN RDAP 服务不会保留数据的副本。数据通

过服务传输，因此可以对数据进行处理，但除了通过访问日志记录之外没有其他记录。数据本身不会被复制，不会被保留，不会进行缓存。它是短暂存在的，就目前而言就是这样。

拉姆 • 莫罕： 非常感谢。我知道你一直在试着推动我的进度。但我还想在这个问题上再说一点，因为这是我们共同开展的工作的核心。斯科特，另一个提出的问题是，ICANN RDAP 访问服务，这个提出的问题出现在我们的模型中，那就是我们是否想象这些都是集中的？我们是否想象它只是通过一个网站，或者我们是否有其他自动化机制？这是第一个问题。第二个问题，如果你的身份未得到验证，甚至不是寻求公共数据或受限数据的经授权的请求，并且这个数据不是 gTLD，那么我们的计划是怎样的，我们对此有什么想法？引导程序，重定向，也可能有一些价值。

斯科特 • 赫伦贝克： 好的。RDAP 访问服务，我们将其设想为网络界面，但它拥有两个面。如安迪所说，我们需要在线自动访问，但也需要异步访问，这意味着你会遇到不一定拥有凭证的人，但他们实际上可能有合法目的来请求信息。因此，对客户端可能会有一些支持，可能会填写一个表单，对该表单进行审核和处理，并以其他方式返回响应。

但是作为网络服务，这项 RDAP 访问服务可以按照通常执行网络服务的任何方式来执行。不一定是一台服务器。它当然可以分布在各个地方，以处理负载平衡之类的事情。这真的是支持 http 服务的最佳实践问题。

身份验证提供商和授权服务功能可以集中在一起，但也可以分开。我们在这里所讲的模型中，这些功能不是集中在一起的，而是适当分开的。让与请求者有关系的实体来执行这些功能是很有道理的，因为他们知道请求者是谁。例如，他们能够签发这些凭证，并根据预先存在的关系做出适当的身份验证决策。

然后就公共数据而言，你会看到我们在这里有一件事是，我们预计签约方将拥有公共数据的公共接口，以便客户端能够直接向注册管理机构和注册服务机构发送查询。他们将得到的是任何确定成为公共数据的政策。我说清楚了吗？

拉姆 • 莫罕： 是的。

斯科特 • 赫伦贝克： 好的。谢谢。

男性发言人（姓名不详）：在我们的文档中，我们实际上涵盖了由身份供应商和授权确定者组成的不同组合，我们称之为行动者模型。我们拥有文件中实际定义的一组组合。我认为有四组。

另一件事是返回到未经身份验证的用户或未授权用户，总体而言，我们所希望的是 ICANN RDAP 网关在收到其中一个请求时，能更多地以标准 RDAP 引导服务器来采取行动，以便它可以执行转至 IANA 引导程序文件中列出的源的 HTTP 级别的重定向。

我们提出这点希望的其中一个原因不仅是从 ICANN gTLD 角度来看，而是因为 RDAP 还用于其他环境，例如 RIR 和 ccTLD 空间。

拉姆 • 莫罕：谢谢。谢谢，斯科特。接下来我要请嘉文 (Gavin) 来为我们介绍一下注意事项部分。

嘉文 • 布朗 (GAVIN BROWN)：谢谢，拉姆。好的，拉姆在一开始就提到了这点，我只是再重复一下：在我们进行审议和讨论时，我们发现了一些我们认为在开始工作之前没有完全具体化的事情。我们也觉得这些事情超出了我们的职权范围，因为我们密切地关注着技术解决方案，对参与政策不太感兴趣。

我来简单地讲一些事项。你们可以看到这里有几张幻灯片。我们将逐一查看这些幻灯片。

我们已经简单地讨论了数据保留。正如之前所说，我们没有设想访问网关具有或者保存注册数据，用术语来讲，它是一个反向代理，但它不是缓存反向代理。它不会存储任何东西，只是传递从签约方服务器获得的东西。

但是某些数据元素会得到存储。例如，会得到存储的主要数据是日志。我们认识到，这些日志可能具有与之相关的一些风险和价值，并且在政策方面，将数据保留规则应用于这些日志的做法是适当的，应该这样执行。

显然，系统需要具备各种各样的要素以便能够确保 — 我们将在下一张关于透明度的幻灯片中进行一些讨论。能够审计系统以确保事情正常进行，这一点是非常重要的。因此，日志记录是可审计性的关键部分，但是首先需要降低披露的风险，因为某人提交请求的事实本身就是有价值的信息，因此采取适当的政策来降低披露这类信息的风险是非常合适的做法。

之前还提到了服务水平协议。显然，会有一些依赖方。我们描述的模型具有多个可能相互独立的实体，每个实体都依赖彼此的服务，以履行其在系统中的职责。显然，最终，存在着系统的最终用户，请求者也依赖于系统来满足他们的需求并实现他们请求访问的合法目的。

我们已经确定，应该定义并落实一系列服务水平协议，以保证系统的可用性和稳定性。

我们还建议 ICANN 组织应该提供有关履行这些服务水平协议的透明度，例如，提供状态页面，请求者可以在该页面上看到系统的状态。

我们认为，ICANN 应该审核承担运行此类系统的责任的潜在影响，尤其是考虑到其作为协调方的角色，这个列表中的第 3 项和第 4 项可以一起看待。

这里显然存在法律风险，也有运营风险，风险可能很大。根据有关系统如何部署的政策决策处于何种水平，还有许多其他风险需要考虑。显然，还有我们已经提出的信息安全风险。

我们必须要向 ICANN 组织和 ICANN 社群指出这些风险，以及需要开展某些审核和评估，以尝试解决这些风险。

我们认为，有必要指出有关减少签约方责任的问题。我们是一群极客，我们不是律师，所以我们无法回答我们所提议的系统是否会减少责任这个问题。所以我们觉得有必要鼓励签约方提出自己的看法，我可以肯定他们会提出的。

刚刚简单地讲述了一下透明度。我们的确认为，如果 ICANN 选择运行这样一个系统，这是确保系统中的信任的关键要素，应该积极地在系统运行方式和使用方式方面做到透明。显然，我们并不是说应该发布或披露具体请求，但是有关系统使用方式的统计信息在确保对系统完整性给予信任方面是一个关键数据点，所以我们建议为了社群的利益定期发布透明度报告。

最后，我们还认识到任何类型的授权流程都会产生这样的结果，即请求者可能不同意结果，因此应该落实投诉处理机制，以便能够收到、相应地升级有关流程或系统问题的投诉，并通过投诉处理流程进行纠正，这也可能包括根据 GDPR 第七条和其他类似法律删除请求，在这些情况下，请求者可能前往 ICANN 并要求删除关于他们的数据。拉姆。

拉姆 • 莫罕： 谢谢嘉文。如果方便的话，请你帮我点到上一张幻灯片吧。很好。谢谢。这实际上或多或少地总结了我们为今天的会议准备的评论。我们现在正在走上正轨。我们希望从现在一直到本周三甚至在星期三之后都能收集到社群意见，我们真的很想收到你们的意见。我们的目的是反思这些意见并将其纳入到技术模型中。我们计划在 4 月中旬再召开几场电话会议和面对面会议，以便最终敲定我们的工作，我们希望能在 4 月 23 日发布最终技术模型。在完成这项工作之后，这个小组将解散，我们将完成我们的任务。

下面是提问时间。我看到那里有位男士想要提问。如果大家有其他问题，请排队。两边都有麦克风，我会尽力协调。这位先生，请讲。

鲁本斯 • 库尔： 我想知道小组是否考虑了这样一种情景，ICANN 仅使用 OAuth 和 OpenID 发布令牌，然后客户端直接询问签约方？因为这样

做会避免数据在 ICANN 系统中[流动]。这可以避免大多数 SLA 问题。即使它不是缓存代理，受损代理仍然会导致数据泄露。

所以可以不将数据流集中在一起，但没有选择这样做。请问原因是什么？

安迪 • 纽顿： 是的，我们的确讨论过这个问题。我们没有沿着这条道路前进的原因是，你必须采用向所有签约方分配政策的机制，并且遵循和不断更新该政策给签约方增加了很大的负担。我们认为，如果 ICANN.org 是进行所有政策过滤的地方，那么事情将会变得更容易。这就是为什么我们采用这种模型的原因，这是一种简化的模型，将访问[听不清]直接转到签约方。

在 SLA 方面，我并不认为 — 我不知道小组中是否有其他人 — 它实际上改变了任何 SLA。

鲁本斯 • 库尔： 即使 ICANN 采用集中式政策引擎，数据流也可能不集中。因此，没有必要让一个决定影响另一个。

安迪 • 纽顿： 我理解你的意思，但是就 SLA 而言，ICANN 仍然会有一个 SLA，用于管理 ICANN 正在运行的任何服务。因此，我认为 SLA 的问题不会随着任何一种系统而改变。

嘉文 • 布朗： 我认为，将 ICANN 作为单一访问点也可以解决我们收到的或者我们从执法机构那里听到的一些问题，即不希望将太多关于他们的请求的信息传递给签约方。也许本尼迪克特或者史蒂夫可以谈谈这一点。但我确实认为，当我们进行这次讨论时，我的主要和中心观点是，执法机构已经提出了强烈反馈，尽管他们没有对透明度提出问题，但是有一个关切 — 他们是一个特定的执法机构或执法机构的特定官员，他们正在提出请求并且注册服务机构知道这是他们提出的请求，这是他们关注的问题。

本尼迪克特 • 阿迪斯： 我会稍微谨慎一点，对参与 EPDP 第二阶段的人说，这是我们现在正在为你们提出的一个考虑因素，因为在请求的假名之间存在可调整性，在这种情况下所有请求都停留于 ICANN，ICANN 负责进行记录而不是更多地披露，会减少向签约方的披露，这是一项政策讨论，执法机构将需要与签约方针对请求的匿名或请求的假名与签约方知晓谁在查询的能力进行讨论，且签约方知晓查询者可能会使其承担相应的责任。但是如果这是一个肯定的回答，那就超出我们的职权范围了。

拉姆 • 莫罕： 谢谢。

本尼迪克特 • 阿迪斯： 还有一项福利，这就是，从透明度角度来看，拥有一项集中式服务可允许你记录和编制透明度报告，我认为我们都可以同意是一件好事。

拉姆 • 莫罕： 谢谢。左边的那位男士。

克劳斯 • 斯托尔 (KLAUS STOLL)： 非常感谢。我是克劳斯 • 斯托尔，来自[听不清]小组。我要提出一条简短的意见和建议。在第六点透明度的考量中，你提到了学术研究，因为许多人将对此非常感兴趣，超出了统计数据。提出这一点很好。谢谢。

拉姆 • 莫罕： 非常感谢。我们会把这点记下来，并在我们的讨论中对此进行反思。

维托里奥 • 贝尔托拉 (VITTORIO BERTOLA)： 大家好。我是维托里奥 • 贝尔托拉，来自[听不清]。我的问题与之前提出的问题非常类似。我想试着指出你们为什么希望[在中间]实施这种集中式系统，特别是无论其是否是一种技术性选择，所以你得出了一些技术性决策，这在技术意义上会更

好，或者其是否是一种政策选择，因为在技术方面，如果我必须建立类似的东西，我认为分散式系统会更好地通过很多方式将[听不清]分散并传输，这样签约方就可以验证它们，我们可以对此进行讨论。如果你们愿意，我甚至可以提出一些提案。

但是另一方面，当提出问题时，我听到的两个原因是政策原因，比如我们希望记录有关透明度的一切，或者执法机构希望我们扮演代理的角色，以便签约方不会看到他们想要查询的东西。但是这些是政策决策。

在你的演讲中，你说过，你无法说明这些在政策或签约方的责任方面是否会更好。我有点理解不清的是，你们是否在尝试通过最佳技术解决方案解决技术问题，或者你们是否制定了一些政策要求使这个集中式系统成为必要，在此情况下，这些要求是什么，可以对这些要求进行讨论吗？

嘉文 • 布朗： 我同意你的看法，在一些回答中，你可以说其中混合了一些政策。但我们的确拥有合理的技术原因，这就是降低系统的技术和操作复杂性。

分发政策并让签约方必须不断更新政策并了解政策内容以及如何理解，但是这样做会是一项巨大的技术任务，我们所做事情的原因之一就是要尽量降低系统技术复杂性。

另一方面，我之前没有提到这点 — 我们在文件中提出了 — 通过我们定义这点的方法，签约方至需要使用双边 TLS 就可以了解谁可以信任，然而，如果我们使用客户端直接向签约方提供的令牌进行访问控制，则会提高签约方必须处理的问题的标准。

拉姆 • 莫罕： 谢谢。这位先生，请讲。

亚历克斯 • 迪肯 (ALEX DEACON)： 谢谢。我有一个问题，这个问题与鲁本 (Ruben) 的问题有关，它具体涉及系统要求 4E 和 4F，其中涉及将属性和标识符信息传递给签约方。在我看来，它清楚地表明这是政策。我认为你们在这里讨论的是政策和技术之间的分离。

但我想知道的是，是否已经决定我们将要使用主动模型二，我认为这是正确的决定，并且该模型将 ICANN 描述为唯一的授权者，我不清楚我们是否需要将这些数据发送给签约方。你是否可以给我提供一些关于为什么要提出这些要求的一些背景 — 我不是说它们好或者不好或者不同意它们，只是想知道为什么这些要求最后[听不清]的思考过程。

安迪 • 纽顿： 是的。问得好。要求是系统必须能够做到这一点，拥有请求者的这些身份和属性，并且如果这是政策所要求的，必须能够支持将其传递给签约方。

这不是真正的政策。这是我们要传达的信息。这有关于系统的一个特性，如果政策说应该强制执行或者应该落实，那么系统就无法支持这点。

亚历克斯 • 迪肯： 明白了，如果政策决定所有一切都发生在这个 ICANN 代理中，那么就不必设置这些属性。系统会支持它，但我们不会使用它。

安迪 • 纽顿： 对，我们需要能够支持它，这就是为什么我们制定四个不同的行动者模型。我们不确定哪个模型是正确的，或者是否会有更多模型。但这就是我们按照我们的方式做出安排的原因。

亚历克斯 • 迪肯： 好的。谢谢。

拉姆 • 莫罕： 谢谢。

尼尔 • 麦克弗森
(NEAL MCPHERSON)： 大家好。我是尼尔 • 麦克弗森，来自 1&1 Ionos。我有一个关于历史数据的问题。我认为史蒂夫提到过，整个过程不一定要实时发生，会有一些用例，需要出去获取主张或者获取信息，这需要很长时间。那么，是否有时间戳或类似的东西，你必须根据今天或昨天或首次收到主张的时间在此时间戳之前提供数据？另外，在请求方面，我们收到的大量请求都是基于谁是域名所有者[听不清]。

拉姆 • 莫罕： 请你离麦克风近些，可以吗？我听到了用例，听到了历史数据，我正在填补空白，我宁愿不这样做。

尼尔 • 麦克弗森： 好的。是的，现在好些了。在时间戳方面，这个过程可能超出[范围]，它可能需要很长时间。根据不实时发生的流程，你必须提供 WHOIS 数据或 RDAP 数据的什么时间戳？另外，我说过，我们获得了大量关于历史数据的请求。这是如何影响这个过程的，请求者说，我需要六个月前的数据，谁是域名所有者？

安迪 • 纽顿： 我在 ARIN 工作，我们拥有名叫 WHOWAS 的事物，意思基本上就是“为我提供六个月前的注册数据”或者其他。我们讨论过

批量 WHOIS、WHOWAS 服务等内容，我们将它们排除在范围之外，至少目前是这样，因为这基本上会进一步加大我们对哪些工作属于我们职权范围的不确定性。

但是我们的确讨论过这些事情，我们说过，不，让我们暂时把它们放在一边吧。这样能否回答你的问题？

尼尔 • 麦克弗森： [谢谢。是的。]

拉姆 • 莫罕： 下一个问题。

格里高利 • 莫尼耶 (GREGORY MOUNIER)： 大家好，我是来自 Europol 的格里高利 • 莫尼耶，我想询问的问题与这个有关，这是关于刑事侦查员一直在使用的另一个特性，他们 80% 的调查都会使用这个特性，这就是反向搜索。我向对此不熟悉的人简单介绍一下，这就是能够交叉引用或者识别使用一种特定类型的信息注册的所有域名。可以是注册人的地址或姓名。

我在你们的报告中读到，从技术上讲，这可以开发，但是由于一些我尚不了解的原因，TSG 还没有说要开发它。所以我的第

一个问题是，什么让你决定将其纳入研究范围？不将其纳入研究范围的原因是什么？谢谢。

安迪 • 纽顿： 好的，不将其纳入的基本原因是反向搜索目前不属于 RDAP 的组成部分。IETF 中有一个草案，两周之后在布拉格讨论反向搜索问题时将讨论这个草案，而这从来都不是基础 RDAP 开头的组成部分。

除了草案的内容以及其将如何得到支持以外，还有关于你如何从空间中的所有签约方获取数据的问题。本尼迪克特，你想说些什么吗？是的，这就是不将其纳入的原因。

格里高利 • 莫尼耶： 如果在最后，政策说，是的，你可以这样做，而在技术[方面]，我们会说，哦，我们由于某种原因没有处理它，我认为这将是一个非常大的遗憾。如果在这个过程的最后，我们可以在技术上实际做到这一点，这将会很好。

拉姆 • 莫罕： 谢谢。我们马上就会联系你，请不要离开麦克风。现在是 2:46。当地时间 2011 年 3 月 11 日下午 2:46，日本本州岛西北海岸的太平洋发生了 9.1 级地震。

这场被称为“东日本大地震”的地震引发了大规模的海啸，海浪高达 40 米，并在内陆行进了 10 公里。

这是日本有史以来最强烈的地震，也是世界上第四大地震。

估计有 20,000 人失踪，近 500,000 人被迫撤离。为了纪念东日本大地震造成的死亡者和影响，我们现在将进行片刻默哀。

谢谢。安迪，你要回复后续问题吗？

安迪 • 纽顿： 抱歉，我忘记了。后续问题是什么？

格里高利 • 莫尼耶： 这不是后续问题，这更多的是一项声明，指出如果政策表示可能，但从技术上无法实现，这将是一大遗憾。

安迪 • 纽顿： 希望 RDAP 中的未来功能可以运用于此。是的。这可能是一个政策问题。可能会有更多技术问题需要解决，但是如果社群真的决定需要，这会是将来值得支持的一件事。

拉姆 • 莫罕： 谢谢。

塞维琳 • 沃特布雷

(SÉVERINE WATERBLEY)： 大家好。大家下午好。我是塞维琳 • 沃特布雷，来自比利时。我是 GAC 成员。如果我理解正确的话，ICANN 将成为 GDPR 意义上的处理器，授权服务将是处理器[的]处理器。预计注册管理机构和服务之间是否存在合同关系，以便为我们提供授权或认证？谢谢。

拉姆 • 莫罕： 我认为这是一个非常好的问题，我并不认为我们有资格为你提供与此相关的回答。我们将要做的是确保这没有被遗漏，我们将记录它，我们将确保将其传递给 ICANN 组织的人员，因为我们没有在它的法律等方面投入大量的时间和精力。

本尼迪克特 • 阿迪斯： [EPDP 需要对此进行一定程度的讨论。]我以我在 EPDP 的身份发言，人们针对 ICANN 和签约方内部的法律协议的确切性质进行了大量的讨论。我知道 ICANN 法务部针对这个问题发表了意见。我认为 EPDP，特别是第二阶段非常便利，40 分钟后这个会议室将会有一场讨论会。

蒂姆 • 陈 (TIM CHEN)： 好的。谢谢。我是来自 DomainTools 的蒂姆 • 陈。首先，感谢你们所完成的工作。我认为在政策制定的同时考虑完成这项工

作的技术现实是一项很好的服务，所以[就像所有]志愿者一样，我为你们开展的工作鼓掌。感谢你们。

我快速地提两个技术问题。一个是，前面关于注意事项的幻灯片下方有一个备注，其中提到 — 我认为这个术语是多用途查询。我只是对这个术语的意思感到好奇。在前面[— 拉姆，这可能是你的章节]或者在紧接这个的后面。是一个很长的列表，大概有 13 项。纠正这里，多用途请求。抱歉。

能请你解释一下这个术语的意思吗，在幻灯片的下方？

拉姆 • 莫罕： 好的。这是在我们工作的早期阶段。我们所考虑的是，数据请求可能会采取多种形式进行。一种形式可能是，它是获得授权仅访问一次数据元素数据的一方，而在其他情况下，授权的持续时间可能更加持久，但是，这种持久是针对某一类请求或者只能访问一定数量的数据元素而言的。

所以，在我们审议的这一部分中，我们不清楚我们应该将模型限制为它必须只针对每个数据元素处理一次请求，针对每个对象处理一次请求，或者以持久方式或以短暂方式进行处理。这就是与多用途请求问题相关的说明。

蒂姆 • 陈： 好的。谢谢。如果可以的话，我想提出第二个问题。在你昨天与签约方进行的会议中提到了引导服务，然后今天也提到了这

个名词。[我不是技术人员]，我试图在 RFC 中查找了几分钟这个方面的信息，但是我认为我们澄清了一个最大的问题，那就是没有在一定程度上传达到 — 我认为昨天这个术语就已经传达到了签约方。这不是提供反向服务。它就像是引导服务的基础点，旨在找出权威来源。但是返回到关于引导服务的简短意见上来 — 可能是斯科特说过 — 是否存在[某种应用程序]，使该服务将处理 gTLD 域名数据之外的信息请求？如果有，是否详细说明一下？

斯科特 • 赫伦贝克： 好的。从理论上说，这是有可能的。我知道我们曾经开玩笑地谈论过，如果 internic.net 这些天再次执行了一些有用的服务，那不是很好吗，对吗？不，事实上，对于最终随着时间的推移这将如何演变，这是政策协调和实施方面的问题。但是从理论上说，答案是肯定的，这是完全有可能的。

蒂姆 • 陈： 谢谢。

安迪 • 纽顿： 我想补充一下。很可能有人会编写 RDAP 客户端，他们不希望自己进行引导过程。他们可能已经用 [Kerl] 和 Bash 或类似的东西做到了这一点，他们只是将会选择一个引导源，这可能是

ICANN。在此情况下，如果 ICANN 扮演使用 IANA 文件的典型引导服务器的角色，那就太好了。

拉姆 • 莫罕： 谢谢。好的，有请。

女性发言人（姓名不详）：只是讲一点我的观察意见。我认为，被排除在这个模型和 EPDP 之外的唯一一方是最终用户。我知道你有一个用例中提到，你可以检查你自己的数据，但是这个模型，我感觉最终用户就是矿井中的金丝雀，我们总是被牺牲的一方。我就是一名最终用户，我不属于任何组织，这真是不幸。我觉得这是我们必须为之奋斗的事情，但我们总是被排除在外，我们总是得到最糟糕的对待，所有各方都会找到机制，通过限制、通过法律手段或者通过授权，获得他们想要的数据，但我们是唯一被排除在外的一方。

这真是不幸。我觉得这是我们必须为之奋斗的事情，这只是开始。谢谢。

拉姆 • 莫罕： 谢谢你的意见。这是一个我们应该考虑的特殊问题，因为在我们所有讨论中 — 如果你返回去看看，听过录音，查看文字记录，你就会发现我们花费了大量的时间，从提出请求的最终用户角度考量这个问题。虽然归根结底，我们有五个用例，但实

际上有很多关于最终用户的讨论，实际上是安迪所谈论的原则，保持简单并尽量不提供多项服务，让最终用户在多个地方获取信息。这直接专注于确保将用户旅程和用户体验作为首要考虑事务。

至少从我的角度来看，感觉我们一直都在考虑最终用户。但是在整体流程中，我同意，我们所有人都必须考虑最终用户的需求和要求。还有其他问题吗？史蒂夫，你举手了吗？

史蒂夫 • 克罗克： 是的。我想深入探讨一下你的问题。这里的实际问题是什么？据推测，注册人可以进入注册服务机构的帐户，查找所有信息并进行验证。他们拥有直接访问权限。

所以我真的很困惑，我们在这里讨论的问题是什么，这对于支持最终用户而言是有意义的。

拉姆 • 莫罕： 本尼迪克特刚刚帮助了我，他说也许你所说的是数据主体而不是实际的最终用户。

女性发言人（姓名不详）： 是的。完全正确。

拉姆 • 莫罕： 这是我们已经谈论过的用例五。

女性发言人（姓名不详）：我能补充一点吗？在那之前我并不知道 WHOIS。现在我知道了 WHOIS 的存在，我会予以使用。我想要使用它。来自 GAC 的法国女士说，她试图推动消费者获取公司的信息，这是一件事。这对我们来说很重要。

我认为解决方案实际上对我们来说，如果我们是其中心，那就是将 WHOIS 的使用作为我们的保护而不是消除它。是的。

本尼迪克特 • 阿迪斯：在我们最初对术语产生困惑之后 — 我将不以技术小组成员的身份发言，而是再次以 EPDP 成员的身份发言，我觉得你提出了非常绝妙的观点。看到这样一个系统成为男孩俱乐部，针对经过[监管]考验的少数人时，我感到很难过。

我认为这个模型的好处是，它确实具有灵活性，如果社群决定以针对普通互联网用户的方式使用这个词语的话，我们要再次使用它来弄清他们是在与谁交互。这是一项你与社群互动时必须遵守的政策。

女性发言人（姓名不详）：是的。对。我将会为此奋斗。

本尼迪克特 • 阿迪斯：谢谢。

拉姆 • 莫罕： 谢谢。最后一个问题留给你了。

男性发言人（姓名不详）： 谢谢。我很快。这与我之前针对报告第 4.1 节用户旅程发表的意见有点相关。报告描述的用户旅程我不太熟悉，很长时间以来我一直使用 WHOIS RDS，特别是第二个要点。我已经读了几次了，我认为应该对用户旅程进行一些改进，以便将其真正置于 WHOIS 用户、RDS 用户或者我们之后提出来的用户环境中，并清楚地阐明我们讨论的是什么用户，他们要经历什么旅程，真正站在将要使用服务查询 RDS 数据的人的立场来看待问题。

拉姆 • 莫罕： 谢谢。这是一个很好的反馈。谢谢。我们的会议马上就要结束了。我想做的是将麦克风传递给技术研究组的各位成员，看看在我们结束会议之前你们是否还有其他任何想要说的话。斯科特，从你开始吧。

斯科特 • 赫伦贝克： 好的。谢谢你们。请记住，这是一场协商会议。我们把问题提出来了。我们认为这样做是有用的，但我们也在寻求你们的意见。请将你们的意见发送给我们，我们希望倾听你们的想法。

拉姆 • 莫罕： 安迪？

安迪 • 纽顿： 我想回应一下斯科特刚才所说的。我们期待你的意见，请将它们提交过来，我们将对其进行讨论。谢谢。

拉姆 • 莫罕： 本尼迪克特？

本尼迪克特 • 阿迪斯： 真是一个团队。谢谢各位，谢谢大家前来听取我们的看法。

拉姆 • 莫罕： 霍赫 (Jorge)？

霍赫 • 卡诺 (JORGE CANO)： 我想说，谢谢你们的意见。真的非常感谢。

拉姆 • 莫罕： 乔迪 (Jody)？

乔迪 • 科克 (JODY KOLKER)： 我没有要补充的了。[那很好。]

拉姆 • 莫罕： 嘉文。

嘉文 • 布朗： 我有一件事想说，这是基于先前关于将注册数据用作消费者保护从而实现消费者保护的意见。我认为关于 RDAP 的一个令人惊奇的事情是，当它通过 RDAP 而不是通过端口 43 WHOIS 提供时，注册数据会变得多么容易获取。如果你使用 JavaScript 编写网站应用程序或者你为手机编写移动应用程序，除非你使用某种代理服务器，并且你必须坚持永远为你的用户运行，否则几乎无法访问端口 43 数据。RDAP 在网络上运行，数据以 JSON 格式提供。任何程序员都知道什么是 JSON。

我认为采用 — 而且从 TSG 正在做的事情来看这有点迂回的意思，但被采用时实际说的是 RDAP。我认为它有可能为希望获得对他们正在使用的任何标识符的信任的消费者带来很多好处，因为它将便于更容易地向最终用户提供有关 RDAP 提供的那些域名和其他资源的关键信息。我能想象出浏览器扩展之类的事物，你可以点击地址栏中的一个小图标，浏览器可以从注册管理机构或注册服务机构 RDAP 服务本地加载这些数据并在浏览器中显示，而不必经过不灵活的端口 43 系统。你可以使用 — 网络框架的好处使我们能够拥有缓存和安全性等功能，从而在该系统中为你提供极大的完整性。

拉姆 • 莫罕： 谢谢嘉文。托莫弗米 (Tomofumi)。

托莫弗米 • 欧库伯 (TOMOFUMI OKUBO)： 非常感谢大家能以积极的状态坚持到会议结束。我非常期待 —

男性发言人（姓名不详）：并不是每个人都这样。

拉姆 • 莫罕： 史蒂夫。

史蒂夫 • 克罗克： 我没有异议。谢谢。黛安娜？伊莱扎 (Eliza)，古斯塔夫 (Gustavo)？约翰 (John)。

约翰 • 克莱恩： 我只说一点，我非常感谢这个团队。作为工程师，我们总是讨厌不得不构建没有要求的系统，这正是这个团队必须要做的。而且我认为他们做得非常出色，这些人和你们所有人一样都是志愿者，他们需要开展许多繁重的工作来构建我们希望的东西 — 我使用的术语是“跨政策的系统”。这不是一个非常好的术语，但它具有足够的灵活性，能够在未来几年的打击中得以幸存，并在很短的时间内完成很多繁重的任务。你们的工作做得非常好。

拉姆 • 莫罕： 谢谢。本次会议到此结束。感谢在座各位的参与。谢谢。

[会议记录结束]